

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

[iDRAC6 の概要](#)

[iDRAC6 を始めるにあたって](#)
[iDRAC6 の基本インストール](#)
[ウェブインタフェースを使用した iDRAC6 の設定](#)
[iDRAC6 の詳細設定](#)
[iDRAC6 ユーザーの追加と設定](#)
[Microsoft Active Directory での iDRAC6 の使用](#)
[スマートカード認証の設定](#)
[GUI コンソールリダイレクトの使用](#)
[仮想メディアの設定と使用法](#)
[WS-MAN インタフェースの使用](#)
[iDRAC6 SM-CLP コマンドラインインタフェースの使用](#)
[VMCLI を使ってオペレーティングシステムを導入する](#)

[Intelligent Platform Management Interface \(IPMI\) の設定](#)

[iDRAC6 設定ユーティリティの使用](#)
[監視と警告管理](#)
[管理下システムの回復とトラブルシューティング](#)
[iDRAC6 のリカバリとトラブルシューティング](#)
[センサー](#)
[電源モニタおよび電源管理](#)
[セキュリティ機能の設定](#)
[RACADM サブコマンドの概要](#)
[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)
[サポートされている RACADM インタフェース](#)
[用語集](#)

メモおよび注意



メモ: メモは、コンピュータを使いやすくするための重要な情報を説明しています。



注意: 注意は、手順に従わない場合は、ハードウェアの損傷やデータの損失の可能性があることを示しています。

本書の内容は予告なく変更されることがあります。
© 2009 すべての著作権は Dell Inc. にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

この文書中に使用されている商標 (Dell, DELL ログ, Dell OpenManage, および PowerEdge) は Dell Inc. の商標です。また、Microsoft, Windows, Windows Server, Windows Vista および Active Directory は Microsoft 社の米国および他の国における商標または登録商標です。Red Hat および Linux は、Red Hat, Inc. の米国および他の国における登録商標です。SUSE は、Novell, Inc. の登録商標です。Intel and Pentium は、米国およびその他の国における Intel Corporation の登録商標です。UNIX は、米国およびその他の国における The Open Group Inc. の登録商標です。VMware は、米国およびその他の国における VMware, Inc. の登録商標または商標です。

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、OpenLDAP の公開ライセンスによって許可されている限度内でのみ許可されます。このライセンスのコピーは、配布の最上位ディレクトリにある「ライセンス」ファイルまたは www.OpenLDAP.org/license.html から入手できます。OpenLDAP は OpenLDAP Foundation の登録商標です。個々のファイルや提供パッケージは、他社が著作権を所有している場合があり、その他の制約を受ける可能性があります。この製品はミシガン大学 LDAP v3.3 配布から派生しています。この製品には、公共ソースから派生した材料も含まれています。OpenLDAP に関する情報は www.openldap.org/ から入手できます。Portions Copyright 1998-2004 Kurt D. Zellenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、OpenLDAP の公開ライセンスによって許可されている限度内でのみ許可されます。Portions Copyright 1999-2003 Howard Y. H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Halvard B. Furuseth. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、この通知が保持された形式でのみ許可されます。事前の書面による許可なくこの著作権所有者をこのソフトウェアから派生した製品を推薦または促進するために使用することはできません。このソフトウェアは「そのまま」の形で、明示または黙示を問わず一切の保証なく提供されます。Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、この通知を保持し、アン・アーバー所在のミシガン大学のへのしかるべき功績を認めた上でのみ許可されます。事前の書面による許可なくこの大学をこのソフトウェアから派生した製品を推薦または促進するために使用することはできません。このソフトウェアは「そのまま」の形で、明示または黙示を問わず一切の保証なく提供されます。商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。Dell Inc. は、Dell 以外の商標や社名に対する所有権を一切否認します。

2009 年 3 月 リビジョン A00

[目次ページに戻る](#)

RACADM サブコマンドの概要

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [help](#)
- [config](#)
- [getconfig](#)
- [getssninfo](#)
- [getsysinfo](#)
- [getractime](#)
- [setniccfg](#)
- [getniccfg](#)
- [getsvctag](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [getraclog](#)
- [crraclog](#)
- [getsel](#)
- [crrsel](#)
- [gettracelog](#)
- [sslcsrgen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [testemail](#)
- [testtrap](#)

本項では、RACADM コマンドラインインタフェースで使用できるサブコマンドについて説明します。

help

[表 A-1](#) に、help コマンドについて説明します。

表 A-1 Help コマンド

コマンド	定義
help	racadm で使用できるすべてのサブコマンドをリストにし、それぞれの短い説明を表示します。

概要

```
racadm help
```

```
racadm help <サブコマンド>
```

説明

help サブコマンドは racadm コマンドで使用できるサブコマンドすべてをリストにし、各サブコマンドにつき一行ずつの説明を表示します。help の後にサブコマンドを入力して、そのサブコマンドの構文を表示することもできます。

出力

racadm help コマンドはすべてのサブコマンドのリストを表示します。

racadm help <サブコマンド> コマンドは、指定したコマンドだけの情報を表示します。

対応インタフェース

- ローカル RACADM

config

[表 A-2](#) に、config および getconfig サブコマンドについて説明します。

表 A-2 config/getconfig

コマンド	定義
------	----

サブコマンド	定義
config	iDRAC を設定します。
getconfig	iDRAC 設定データを取得します。

概要

```
racadm config [-c|-p] -f <ファイル名>
```

```
racadm config -g <グループ名> -o <オブジェクト名> [-i <索引>] <値>
```

対応インタフェース

- 1 ローカル RACADM

説明

config サブコマンドを使用すると、iDRAC 設定パラメータを個別に設定、または設定ファイルの一部として一括設定できます。データが異なる場合は、その iDRAC オブジェクトは新しい値で書き込まれます。

入力

表 A-3 に、config サブコマンド オプションについて説明します。

表 A-3 config サブコマンドオプションと説明

オプション	説明
-f	-f <ファイル名> オプションを使用すると、config は <ファイル名> で指定したファイルの内容を読み取り、iDRAC を設定します。ファイルの内容は「設定ファイルの構文」で指定した形式のデータでなければなりません。
-p	パスワードオプション -p は、設定が完了した後、config ファイル -f <ファイル名> に含まれているパスワードエントリを削除するように config に指示します。
-g	-g <グループ名> (グループオプション) は、-o オプションと一緒に使用する必要があります。<グループ名> は、設定するオブジェクトを含むグループを指定します。
-o	-o <オブジェクト名> <値> (オブジェクト) オプションは、-g オプションと一緒に使用する必要があります。このオプションは、文字列 <値> で書き込まれるオブジェクト名を指定します。
-i	-i <索引> (索引) オプションは、索引付きのグループのみに有効で、固有のグループを指定できます。この場合、索引は「名前付き」の値ではなく、索引値で指定されます。
-c	-c (チェック) オプションは、config サブコマンドと一緒に使用し、.cfg ファイルを解析して構文エラーを見つけることができます。エラーが検出されたら、その行番号とエラーの短い説明が表示されます。iDRAC には書き込まれません。このオプションはチェックのみです。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

- 1 無効な構文、グループ名、オブジェクト名、索引、またはその他の無効なデータベースメンバ
- 1 RACADM CLI エラー

このサブコマンドは、.cfg ファイル内にあるオブジェクトの総数のうちいくつかの設定オブジェクトが書き込まれたかを示す数値を返します。


例

```
1 racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.110
```

cfgNicIpAddress 設定パラメータ(オブジェクト)の値を 10.35.10.110 に設定します。この IP アドレスオブジェクトは cfgLanNetworking グループにあります。

```
1 racadm config -f myrac.cfg
```

iDRAC を設定または再設定します。getconfig コマンドで myrac.cfg ファイルを作成することもできます。myrac.cfg ファイルは、構文解析ルールに従って手動で編集することもできます。

 **メモ:** myrac.cfg ファイルにはパスワードは含まれていません。ファイルにパスワードを含めるには、手動で入力する必要があります。設定中にパスワードを myrac.cfg ファイルから削除する場合は、-p オプションを使用します。

getconfig

getconfig サブコマンドを使うと、個別の iDRAC 設定パラメータを取得、またはすべての iDRAC 設定グループを取得して 1 つのファイルに保存できます。

入力

表 A-4 に、getconfig サブコマンド オプションについて説明します。


 **メモ:** ファイルを指定しないで -f オプションを使用すると、ファイルの内容が端末画面に出力されます。

表 A-4 getconfig サブコマンドオプション

オプション	説明
-f	-f <ファイル名> オプションを getconfig に追加すると、iDRAC 設定のすべてが設定ファイルに書き込まれます。このファイルは config サブコマンドを使用した一括設定操作に使用できます。 メモ: -f オプションでは cfglpmiPet と cfglpmiPef グループ用のエントリは作成されません。cfglpmiPet グループをファイルに取り込むためのトラップ先を少なくとも 1 つ設定する必要があります。
-g	-g <グループ名> (グループ) オプションを使用すると、単一グループの設定を表示できます。グループ名 は、racadm.cfg ファイルで使用されているグループの名前です。グループが索引付きグループの場合は、-i オプションを使用してください。
-h	-h (ヘルプ) オプションは、使用可能な設定グループすべてを表示します。このオプションは、正確なグループ名を覚えていない場合に便利です。
-i	-i <索引> (インデックス) オプションは、索引付きのグループのみに有効で、固有のグループを指定できます。-i <索引> を指定しなければ、グループに 1 の値が想定されます。これは複数のエントリを含んだテーブルです。この場合、索引は「名前付き」の値ではなく、索引値で指定されます。
-o	-o <オブジェクト名> (オブジェクト) オプションは、クエリで使用するオブジェクト名を指定します。このオプションは、-g オプションと一緒に使用できます。
-u	-u <ユーザー名> (ユーザー名) オプションを使うと、指定したユーザーの設定を表示できます。<ユーザー名> オプションはユーザーのログイン名です。
-v	-v (詳細) オプションはその他の詳細とプロパティを表示し、-g オプションと一緒に使用します。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

- 1 無効な構文、グループ名、オブジェクト名、索引、またはその他の無効なデータベースメンバ
- 1 RACADM CLI 転送エラー

エラーが発生しなければ、指定した設定の内容が表示されます。

例

```
1 racadm getconfig -g cfgLanNetworking
cfgLanNetworking グループ内の設定プロパティ(オブジェクト)をすべて表示します。
1 racadm getconfig -f myfile.cfg
iDRAC のグループ設定オブジェクトすべてを myrac.cfg に保存します。
1 racadm getconfig -h
iDRAC で使用可能な設定グループのリストを表示します。
1 racadm getconfig -u root
root という名前のユーザーの設定プロパティを表示します。
1 racadm getconfig -g cfgUserAdmin -i 2 -v
索引 2 のユーザーグループインスタンスとプロパティ値の詳細情報を表示します。
```

概要

```
racadm getconfig -f <ファイル名>
racadm getconfig -g <グループ名> [-i <索引>]
racadm getconfig -u <ユーザー名>
racadm getconfig -h
```

対応インタフェース

- 1 ローカル RACADM

getssninfo

[表 A-5](#) に、getssninfo サブコマンドについて説明します。

表 A-5 getssninfo サブコマンド

サブコマンド	定義
getssninfo	Session Manager のセッションテーブルから、1 つまたは複数の現在アクティブまたは保留中のセッションの情報を取得します。

概要

```
racadm getssninfo [-A] [-u <ユーザー名> | *]
```

説明

getssninfo コマンドは、iDRAC に接続しているユーザーのリストを返します。概要情報では次の情報が表示されます。

- 1 ユーザー名
- 1 IP アドレス(該当する場合)
- 1 セッションの種類(例:SSH、telnet)
- 1 使用コンソール(例:仮想メディア、仮想 KVM)

対応インタフェース

- 1 ローカル RACADM

入力

[表 A-6](#) に、getssninfo サブコマンドオプションについて説明します。

表 A-6 getssninfo サブコマンドオプション

オプション	説明
-A	-A オプションを指定するとデータヘッダは印刷されません。
-u	-u <ユーザー名> ユーザー名オプションは、そのユーザー名の詳細セッション記録のみを印刷出力します。ユーザー名としてアスタリスク(*)を入力すると、すべてのユーザーが一覧表示されます。このオプションを指定すると、概要情報は印刷されません。

例

```
1 racadm getssninfo
```

[表 A-7](#) に racadm getssninfo コマンドの出力例を示します。

表 A-7 getssninfo サブコマンド出力例

ユーザー	IP アドレス	Type	Consoles
root	192.168.0.10	Telnet	Virtual KVM

```
l racadm getssninfo -A
"root" 143.166.174.19 "Telnet" "NONE"

l racadm getssninfo -A -u *
"root" "143.166.174.19" "Telnet" "NONE"

l "bob" "143.166.174.19" "GUI" "NONE"
```

getsysinfo

[表 A-8](#) に、racadm getsysinfo サブコマンドについて説明します。

表 A-8 getsysinfo

コマンド	定義
getsysinfo	iDRAC 情報、システム情報、ウォッチドッグステータス情報を表示します。

概要

```
racadm getsysinfo [-d] [-s] [-w] [-A]
```

説明

getsysinfo サブコマンドは、iDRAC、管理下サーバー、ウォッチドッグ設定に関連する情報を表示します。

対応インタフェース

- ローカル RACADM

入力

[表 A-9](#) に、getsysinfo サブコマンドオプションについて説明します。

表 A-9 getsysinfo サブコマンドオプション

オプション	説明
-d	iDRAC 情報を表示します。
-s	システム情報を表示します。
-w	ウォッチドッグ情報を表示します。
-A	ヘッダ / ラベルを印刷しません。

出力

getsysinfo サブコマンドは、iDRAC、管理下サーバー、ウォッチドッグ設定に関連する情報を表示します。

出力例

```
RAC Information:
RAC Date/Time           = Wed Aug 22 20:01:33 2007
Firmware Version       = 0.32
Firmware Build         = 13661
Last Firmware Update   = Mon Aug 20 08:09:36 2007

Hardware Version       = NA
Current IP Address     = 192.168.0.120
Current IP Gateway     = 192.168.0.1
Current IP Netmask     = 255.255.255.0
```

```
DHCP Enabled           = 1
MAC Address            = 00:14:22:18:cd:f9
Current DNS Server 1   = 10.32.60.4
Current DNS Server 2   = 10.32.60.5
DNS Servers from DHCP = 1
Register DNS RAC Name = 1
DNS RAC Name           = iDRAC-783932693338
Current DNS Domain     = us.dell.com
```

```
System Information:
System Model           = PowerEdge M600
System BIOS Version    = 0.2.1
BMC Firmware Version  = 0.32
Service Tag           = 48192
Host Name              = dell-x92i38xc2n
OS Name                =
Power Status           = OFF
```

```
Watchdog Information:
Recovery Action        = None
Present countdown value = 0 seconds
Initial countdown value = 0 seconds
```

例

```
l racadm getsysinfo -A -s

"System Information:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"

l racadm getsysinfo -w -s

System Information:
System Model           = PowerEdge M600
System BIOS Version    = 0.2.1
BMC Firmware Version  = 0.32
Service Tag           = 48192
Host Name              = dell-x92i38xc2n
OS Name                =
Power Status           = ON

Watchdog Information:
Recovery Action        = None
Present countdown value = 0 seconds
Initial countdown value = 0 seconds
```

制限

getsysinfo 出力の **ホスト名** フィールドと **OS 名** フィールドには、管理下サーバーに Dell OpenManage がインストールされている場合にのみ正確な情報が表示されます。管理下サーバーに OpenManage がインストールされていない場合は、これらのフィールドには空白または不正確な情報が表示されます。

getractime

表 A-10 に、getractime サブコマンドについて説明します。

表 A-10 getractime

サブコマンド	定義
getractime	リモートアクセスコントローラから現在の時刻を表示します。

概要

```
racadm getractime [-d]
```

説明

オプションを何も指定しないと、getractime サブコマンドは時刻を一般的な形式で表示します。

-d オプションを指定すると、getractime は時刻を `yyyymmddhhmmss.mmmmmms` 形式で表示します。これは UNIX `date` コマンドで返されるのと同じ形式です。

出力

getractable サブコマンドは出力を 1 行で表示します。

出力例

```
racadm getractable
Thu Dec 8 20:15:26 2005
racadm getractable -d
20071208201542.000000
```

対応インタフェース

- 1 ローカル RACADM
-

setniccfg

[表 A-11](#) に、setniccfg サブコマンドについて説明します。

表 A-11 setniccfg

サブコマンド	定義
setniccfg	コントローラの IP 設定を指定します。

概要

```
racadm setniccfg -d
racadm setniccfg -s [<IP アドレス> <ネットマスク> <ゲートウェイ>]
racadm setniccfg -o [<IP アドレス> <ネットマスク> <ゲートウェイ>]
```

説明

setniccfg サブコマンドは、iDRAC の IPアドレスを設定します。

- 1 -d オプションは NIC の DHCP を有効にします(デフォルトは DHCP 有効)。
- 1 -s オプションは静的 IP 設定を有効にします。IP アドレス、ネットマスク、ゲートウェイを指定できます。指定しなければ、既存の静的な設定が使用されます。<IP アドレス>、<ネットマスク>および<ゲートウェイ> は、文字列をドットで区切って入力する必要があります。

```
racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1
```

- 1 -o オプションは、NIC を完全に無効にします。<IPアドレス>、<ネットマスク>、<ゲートウェイ> は文字列をドットで区切って入力する必要があります。

```
racadm setniccfg -o 192.168.0.120 255.255.255.0 192.168.0.1
```

出力

setniccfg サブコマンドは操作に失敗した場合にエラーメッセージを表示します。成功した場合は、成功したことを知らせるメッセージが表示されます。

対応インタフェース

- 1 ローカル RACADM
-

getniccfg

[表 A-12](#) に `getniccfg` サブコマンドについて説明します。

表 A-12 getniccfg

サブコマンド	定義
<code>getniccfg</code>	iDRAC の現在の IP 設定を表示します。

概要

```
racadm getniccfg
```

説明

`getniccfg` サブコマンドは、現在の NIC 設定を表示します。

出力例

`getniccfg` サブコマンドは操作に失敗した場合にエラーメッセージを表示します。成功した場合は、出力が次の形式で表示されます。

```
NIC Enabled      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
Gateway          = 192.168.0.1
```

対応インターフェース

- 1 ローカル RACADM
-

getsvctag

[表 A-13](#) に `getsvctag` サブコマンドについて説明します。

表 A-13 getsvctag

サブコマンド	定義
<code>getsvctag</code>	サービスタグを表示します。

概要

```
racadm getsvctag
```

説明

`getsvctag` サブコマンドはホストシステムのサービスタグを表示します。

例

コマンドプロンプトで `getsvctag` と入力します。出力は次のように表示されます。

```
Y76TP0G
```

成功すると 0、エラーの場合はゼロ以外の値を返します。

対応インターフェース


- 1 ローカル RACADM
-

racreset

[表 A-14](#) racreset サブコマンドについて説明します。

表 A-14 racreset

サブコマンド	定義
racreset	IDRAC をリセットします。

 **注意:** racreset サブコマンドを発行すると、iDRAC が使用可能な状態に戻るまでに最大 1 分間かかることがあります。

概要

```
racadm racreset
```

説明

racreset サブコマンドは iDRAC にリセットを発行します。リセットイベントは iDRAC ログに書き込まれます。

例

- 1 racadm racreset
iDRAC のソフトリセットのシーケンスを開始します。

対応インターフェース

- 1 ローカル RACADM
-

racresetcfg

[表 A-15](#) は、racresetcfg サブコマンドについて説明しています。

表 A-15 racresetcfg

サブコマンド	定義
racresetcfg	RAC 設定全体を工場出荷時のデフォルト値に戻します。

概要

```
racadm racresetcfg
```

対応インターフェース

- 1 ローカル RACADM

説明

racresetcfg コマンドは、データベースプロパティのすべてのユーザー設定エントリを削除します。データベースには、iDRAC を元のデフォルト設定に戻すデフォルトのプロパティがすべてのエントリにあります。

- **注意:** このコマンドは現在の iDRAC の設定を削除し、元のデフォルト設定に戻します。リセット後、デフォルトの名前およびパスワードはそれぞれ、root と calvin になり、IP アドレスは 192.168.0.120 にシャーシ内のサーバーのスロット番号を加えた値になります。

serveraction

表 A-16 に、serveraction サブコマンドについて説明します。

表 A-16 serveraction

サブコマンド	定義
serveraction	管理下サーバーのリセットまたは電源の投入 / 切断 / 入れ直しを実行します。

概要

racadm serveraction <動作>

説明

serveraction サブコマンドを使うと、ホストシステムの電源管理を行うことができます。表 A-17 で、serveraction 電源管理オプションについて説明します。

表 A-17 serveraction サブコマンドオプション

文字列	定義
<動作> >	動作を指定します。<動作> の文字列のオプションを次に示します。 <ul style="list-style-type: none">1 powerdown - 管理下サーバーの電源を切ります。1 powerup - 管理下サーバーの電源を入れます。1 powercycle - 管理下サーバーの電源の入れ直しを行います。この動作は、システムのフロントパネルの電源ボタンを押すことでシステムの電源を切ってから入れ直すのと同様です。1 powerstatus - サーバーの現在の電源ステータス(オンまたは オフ)を表示します。1 hardreset - 管理下サーバーのリセット(再起動)を実行します。

出力

serveraction サブコマンドは、要求された動作が実行できなかった場合はエラーメッセージを表示し、要求された動作が正常に完了した場合は成功したことを知らせるメッセージを表示します。

対応インターフェース

- 1 ローカル RACADM

getraclog

表 A-18 で、racadm getraclog コマンドについて説明します。

表 A-18 getraclog

コマンド	定義
getraclog -i	iDRAC ログ内のエントリ数を表示します。
getraclog	iDRAC のログエントリを表示します。


概要

```
racadm getraclog -i
```

```
racadm getraclog [-A] [-o] [-c count] [-s start-record] [-m]
```

説明

getraclog -i コマンドは、iDRAC ログ内のエントリ数を表示します。

 **メモ:** オプションを何も指定しないと、ログ全体が表示されます。

以下のオプションを使うと、getraclog コマンドでエントリを読み込むことができます。

表 A-19 getraclog サブコマンドオプション

オプション	説明
-A	ヘッダーやラベルなしで出力を表示します。
-c	返されるエントリの最大数を表示します。
-m	一度に 1 画面ずつの情報を表示して、ユーザーに続行するように指示します (UNIX の more コマンドに類似)。
-o	出力を 1 行で表示します。
-s	表示を開始するレコードを指定します。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは、1 月 1 日の午前零時に開始し、管理下サーバー起動時まで増分されます。管理下サーバーの起動後、タイムスタンプには管理下サーバーのシステム時間が使用されます。

出力例

```
Record:      1
Date/Time:   Dec 8 08:10:11
Source:      login[433]
Description: root login from 143.166.157.103
```

対応インターフェース

- 1 ローカル RACADM

clrraclog

概要

```
racadm clrraclog
```

説明

clrraclog サブコマンドは、iDRAC のログから既存のレコードをすべて削除します。新しいレコードが 1 つ作成され、ログがクリアされたときの日時が記録されます。

getsel

表 A-20 に、getsel コマンドについて説明します。

表 A-20 getsel

--	--

コマンド	定義
getsel -i	システムイベントログ内のエントリ数を表示します。
getsel	SEL エントリを表示します。

概要

```
racadm getsel -i
```

```
racadm getsel [-E] [-R] [-A] [-o] [-c count] [-s count] [-m]
```

説明

getsel -i コマンドは SEL 内のエントリ数を表示します。

以下の getsel オプション(-i オプションなし)はエントリの読み込みに使います。


 **メモ:** 引数を何も指定しないと、ログ全体が表示されます。

表 A-21 getsel サブコマンドオプション

オプション	説明
-A	表示ヘッダーやラベルなしの出力を指定します。
-c	返されるエントリの最大数を表示します。
-o	出力を 1 行で表示します。
-s	表示を開始するレコードを指定します。
-E	16 バイトの SEL の生データを、16 進数の値のシーケンスとして各行の終わりに付加します。
-R	生データのみが印刷されます。
-m	一度に 1 画面ずつの情報を表示して、ユーザーに続行するように指示します (UNIX の more コマンドに類似)。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、重要度、説明が表示されます。

次に、例を示します。

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

対応インタフェース

- 1 ローカル RACADM

clrsel

概要

```
racadm clrsel
```

説明

clrsel コマンドは、システムイベントログ(SEL)から既存のレコードをすべて削除します。

対応インタフェース

gettracelog

[表 A-22](#) に、gettracelog サブコマンドについて説明します。

表 A-22 gettracelog

コマンド	定義
gettracelog -i	iDRAC トレースログ 内のエントリ数を表示します。
gettracelog	iDRAC トレースログ を表示します。

概要

```
racadm gettracelog -i
```

```
racadm gettracelog [-A] [-o] [-c count] [-s startrecord] [-m]
```

説明

gettracelog(-i オプションなし)コマンドはエントリを読み込みます。以下の gettracelog エントリを使ってエントリを読み込みます。

表 A-23 gettracelog サブコマンドオプション

オプション	説明
-i	iDRAC トレースログ 内のエントリ数を表示します。
-m	一度に 1 画面ずつの情報を表示して、ユーザーに続行するように指示します (UNIX の more コマンドに類似)。
-o	出力を 1 行で表示します。
-c	表示するレコード数を指定します。
-s	表示を開始するレコードを指定します。
-A	ヘッダーやラベルを表示しません。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは、1 月 1 日の午前零時に開始し、管理下システム起動時まで増加します。管理下システムの起動後、タイムスタンプには管理下システムのシステム時間が使用されます。

次に、例を示します。

```
Record:      1

Date/Time:  Dec 8 08:21:30

Source:  ssnmgrd[175]

Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

対応インターフェース

sslcsgen

[表 A-24](#) に、sslcsgen サブコマンドについて説明します。

表 A-24 sslcsgen

コマンド	定義
sslcsgen	

サブコマンド	説明
sslcsrgen	RAC から SSL 証明書署名要求 (CSR) を生成してダウンロードします。

概要

```
racadm sslcsrgen [-g] [-f <ファイル名>]
```

```
racadm sslcsrgen -s
```

説明


sslcsrgen サブコマンドを使って、CSR を生成し、クライアントのローカルファイルシステムにファイルをダウンロードできます。CSR は、RAC 上での SSL トランザクションに使用できるカスタム SSL 証明書の作成に使用できます。

オプション

[表 A-25](#) に、**sslcsrgen** サブコマンドオプションについて説明します。

表 A-25 sslcsrgen サブコマンドオプション


オプション	説明
-g	新しい CSR を生成します。
-s	CSR 生成プロセスのステータスを返します (生成進行中、アクティブ、なし)。
-f	CSR をダウンロードする先の場所の <ファイル名> を指定します。

 **メモ:** -f オプションを指定しないと、ファイル名はデフォルトで現在のディレクトリ内の **sslcsr** になります。

オプションを何も指定しないと、生成された CSR はデフォルトでローカルファイルシステムに **sslcsr** としてダウンロードされます。-g オプションは -s オプションと一緒に使用できず、-f オプションは -g オプションと一緒にしか使用できません。

sslcsrgen -s サブコマンドは次のいずれかのステータスコードを返します。

- 1 CSR は正常に生成されました。
- 1 CSR はありません。
- 1 CSR の生成の進行中です。

 **メモ:** CSR を生成するには、その前に CSR フィールドを RACADM [cfgRacSecurity](#) グループで設定する必要があります。例: `racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany`

例

```
racadm sslcsrgen -s
```

または

```
racadm sslcsrgen -g -f c:\Ycsr\Ycsrtest.txt
```

対応インタフェース

- 1 ローカル RACADM

sslcertupload

[表 A-26](#) に、**sslcertupload** サブコマンドについて説明します。

表 A-26 sslcertupload

サブコマンド	説明
sslcertupload	カスタム SSL サーバー証明書または CA 証明書をクライアントから iDRAC にアップロードします。

概要

```
racadm sslcertupload -t <種類> [-f <ファイル名>]
```

オプション

表 A-27 に、sslcertupload サブコマンドオプションについて説明します。

表 A-27 sslcertupload サブコマンドオプション

オプション	説明
-t	アップロードする証明書の種類が CA 証明書かサーバー証明書を指定します。 1 = サーバー証明書 2 = CA 証明書
-f	アップロードする証明書のファイル名を指定します。ファイルを指定しないと、現在のディレクトリ内の sslcert ファイルが選択されます。

sslcertupload コマンドはアップロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

例

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

対応インタフェース

- 1 ローカル RACADM

sslcertdownload

表 A-28 に、sslcertdownload サブコマンドについて説明します。

表 A-28 sslcertdownload

サブコマンド	説明
sslcertdownload	SSL 証明書を RAC からクライアントのファイルシステムにダウンロードします。

概要

```
racadm sslcertdownload -t <種類> [-f <ファイル名>]
```

オプション

表 A-29 に、sslcertdownload サブコマンドオプションについて説明します。

表 A-29 sslcertdownload サブコマンドオプション

オプション	説明
-t	ダウンロードする証明書の種類が Microsoft® Active Directory® 証明書かサーバー証明書を指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-f	ダウンロードする証明書のファイル名を指定します。-f オプションまたはファイル名が指定されていないと、現在のディレクトリ内の sslcert ファイルが選択されます。

sslicertdownload コマンドはダウンロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

例

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

対応インタフェース

- 1 ローカル RACADM
-

sslicertview

表 A-30 に、sslicertview サブコマンドについて説明します。

表 A-30 sslicertview

サブコマンド	説明
sslicertview	iDRAC に存在する SSL サーバー証明書または CA 証明書を表示します。

概要

```
racadm sslcertview -t <種類> [-A]
```

オプション

表 A-31 に、sslicertview サブコマンドオプションについて説明します。

表 A-31 sslicertview サブコマンドオプション

オプション	説明
-t	表示する証明書の種類が Microsoft Active Directory 証明書かサーバー証明書かを指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-A	ヘッダー / ラベルを印刷しません。

出力例

```
racadm sslcertview -t 1

Serial Number          : 00

Subject Information:
Country Code (CC)     : US
State (S)              : Texas
Locality (L)          : Round Rock
Organization (O)       : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)      : iDRAC default certificate

Issuer Information:
Country Code (CC)     : US
State (S)              : Texas
Locality (L)          : Round Rock
Organization (O)       : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)      : iDRAC default certificate

Valid From             : Jul 8 16:21:56 2005 GMT
Valid To               : Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A
```

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT

対応インタフェース

- 1 ローカル RACADM

testemail

[表 A-32](#) に、testemail サブコマンドについて説明します。

表 A-32 testemail の設定

サブコマンド	説明
testemail	iDRAC の電子メール警告機能をテストします。

概要

racadm testemail -i <索引>

説明

iDRAC から指定の宛先へテスト電子メールを送信します。

testemail コマンドを実行する前に、RACADM [cfgEmailAlert](#) グループ内の指定された索引が有効で正しく設定されていることを確認してください。 [表 A-33](#) に、[cfgEmailAlert](#) グループのコマンド例を示します。

表 A-33 testemail の設定

動作	コマンド
警告を有効にします。	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
宛先の電子メールアドレスを設定します。	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com
宛先の電子メールアドレスに送信するカスタムメッセージを設定します。	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "これはテストです"
SNMP の IP アドレスが正しく設定されていることを確認します。	racadm config -g cfgRemoteHosts -o cfgRhostsSmtptServerIpAddr -i 192.168.0.152
現在の電子メール警告設定を表示します。	racadm getconfig -g cfgEmailAlert -i <索引> ここで、<索引> は 1~4 の数値です。

オプション

[表 A-34](#) に、testemail サブコマンドオプションについて説明します。

表 A-34 testemail サブコマンドオプション

オプション	説明
-i	テストする電子メール警告の索引を指定します。

出力

なし

対応インターフェース

1 ローカル RACADM

testtrap

[表 A-35](#) に、testtrap サブコマンドについて説明します。

表 A-35 testtrap

サブコマンド	説明
testtrap	iDRAC の SNMP トラップ警告機能をテストします。

概要

racadm testtrap -i <索引>

説明

testtrap サブコマンドは、iDRAC からネットワーク上の指定した宛先トラップリスナにテストトラップを送信して、iDRAC の SNMP トラップ警告機能をテストします。

testtrap サブコマンドを実行する前に、RACADM [cfgIpmiPet](#) グループ内の指定した索引が正しく設定されていることを確認してください。

[表 A-36](#) に、[cfgIpmiPet](#)グループに関するコマンドを示します。

表 A-36 cfg 電子メール警告コマンド

動作	コマンド
警告を有効にします。	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
宛先の電子メールの IP アドレスを設定します。	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
現在のテストトラップ設定を表示します。	racadm getconfig -g cfgIpmiPet -i <索引> ここで、<索引> は 1~4 の数値です。

入力

[表 A-37](#) に、testtrap サブコマンドオプションについて説明します。

表 A-37 testtrap サブコマンドオプション

オプション	説明
-i	テストに使うトラップ設定の索引を指定します。有効な値は 1~4 です。

対応インターフェース

1 ローカル RACADM

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC プロパティデータベースのグループとオブジェクトの定義

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [表示可能文字](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgStandardSchema](#)
- [cfgIpmiSol](#)
- [cfgIpmiLan](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)

iDRAC プロパティデータベースには iDRAC の設定情報が格納されています。データは関連オブジェクト別に整理され、オブジェクトはオブジェクトグループ別に整理されています。本項には、プロパティデータベースでサポートされているグループとオブジェクトの ID のリストが掲載されています。

RACADM ユーティリティでこれらのグループとオブジェクト ID を使って iDRAC を設定します。以下の各項で、それぞれのオブジェクトについて説明し、オブジェクトが読み取り可能か、書き込み可能か、またはその両方が可能であることを示します。

文字列の値は、特に記載のない限り、表示可能な ASCII 文字のみとします。

表示可能文字

表示可能文字には以下の文字セットが含まれます。

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#\$%^&*()_+={}|~:;'<>,./?

idRacInfo

このグループにはクエリされる iDRAC の特定の情報を提供するための表示パラメータが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

idRacProductInfo (読み取り専用)

有効値

最大 63 文字の ASCII 文字列。

デフォルト

iDRAC (Integrated Dell Remote Access Controller)

説明

製品を識別するテキスト文字列。

idRacDescriptionInfo (読み取り専用)

有効値

最大 255 文字の ASCII 文字列。

デフォルト

このシステムコンポーネントは Dell PowerEdge サーバー用のリモート管理機能一式をすべて提供します。

説明

RAC のタイプを説明するテキスト。

idRacVersionInfo (読み取り専用)

有効値

最大 63 文字の ASCII 文字列。

デフォルト

1.0

説明

現在の製品ファームウェアバージョンを示す文字列。

idRacBuildInfo (読み取り専用)

有効値

最大 16 文字の ASCII 文字列。

デフォルト

現在の RAC ファームウェアビルドバージョン。例: 05.12.06

説明

現在の製品ビルドバージョンを示す文字列。

idRacName (読み取り専用)

有効値

最大 15 文字の ASCII 文字列。

デフォルト

iDRAC

説明

このコントローラを識別するためにユーザーが割り当てた名前。

idRacType (読み取り専用)

デフォルト

8

説明

リモートアクセスコントローラのタイプを iDRAC として識別します。

cfgLanNetworking

このグループには iDRAC NIC を設定するためのパラメータが格納されています。

このグループでは 1 つのインスタンスが使用できます。このグループのすべてのオブジェクトで iDRAC NIC がリセットされる必要があり、このため接続が一時的に途絶える場合があります。iDRAC NIC IP アドレス設定を変更するオブジェクトによってすべてのアクティブなユーザーセッションが閉じられるので、ユーザーはアップデートされた IP アドレス設定を使って再接続する必要があります。

cfgDNSDomainNameFromDHCP (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0


説明

iDRAC DNS ドメイン名をネットワークの DHCP サーバーから割り当てる必要があることを指定します。

cfgDNSDomainName (読み取り / 書き込み)

有効値

最大 254 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。文字は英数字、「-」 および「.」に制限されています。

 **メモ:** Microsoft® Active Directory® は、64 バイト以下の完全修飾ドメイン名 (FQDN) しかサポートしていません。

デフォルト

...


説明

DNS ドメイン名。このパラメータは、cfgDNSDomainNameFromDHCP が 0 (FALSE) に設定されているときにのみ有効です。

cfgDNSRacName (読み取り / 書き込み)

有効値

最大 63 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。

 **メモ:** 一部の DNS サーバーは 31 文字以内の名前しか登録しません。

デフォルト

rac-サービスタグ

説明

デフォルトの RAC 名 rac-サービスタグ が表示されます。このパラメータは、cfgDNSRegisterRac が 1 (TRUE) に設定されているときにのみ有効です。

cfgDNSRegisterRac (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバーに iDRAC 名を登録します。

cfgTrapsSnmpFromDHCP (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバーの IP アドレスをネットワーク上の DHCP サーバーから割り当てることを指定します。


cfgDNSServer1 (読み取り / 書き込み)

有効値

有効な IP アドレスを表す文字列。例: 192.168.0.20

説明

DNS サーバー 1 の IP アドレスを指定します。このプロパティは、`cfgDNSServersFromDHCP` が 0 (FALSE) に設定されている場合にのみ有効です。

 **メモ:** アドレスのスワップ中、`cfgDNSServer1` と `cfgDNSServer2` を同一値に設定することができます。

cfgDNSServer2 (読み取り / 書き込み)

有効値


有効な IP アドレスを表す文字列。例: 192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 2 の IP アドレスを取得します。このパラメータは、`cfgDNSServersFromDHCP` が 0 (FALSE) に設定されているときにのみ有効です。

 **メモ:** アドレスのスワップ中、`cfgDNSServer1` と `cfgDNSServer2` を同一値に設定することができます。

cfgNicEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)


デフォルト

0

説明

iDRAC ネットワークインタフェースコントローラを有効または無効にします。NIC を無効にすると、iDRAC へのリモートネットワークインタフェースにアクセスできず、ローカル RACADM インタフェースでしか iDRAC を使用できなくなります。

cfgNicIpAddress (読み取り / 書き込み)

 **メモ:** このパラメータは、`cfgNicUseDhcp` パラメータが 0 (FALSE) に設定されているときにのみ設定できます。

有効値

有効な IP アドレスを表す文字列。例: 192.168.0.20

デフォルト


192.168.0.n

n は 120 にサーバーのスロット番号を加えた値です。

説明

RAC に割り当てる静的 IP アドレスを指定します。このプロパティは、`cfgNicUseDhcp` が 0 (FALSE) に設定されている場合にのみ有効です。

cfgNicNetmask（読み取り / 書き込み）

 **メモ:** このパラメータは、`cfgNicUseDhcp` パラメータが 0 (FALSE) に設定されているときにのみ設定できます。

有効値

有効なサブネットマスクを表す文字列。例: 255.255.255.0


デフォルト

255.255.255.0

説明

iDRAC の IP アドレスの静的割り当てに使用されるサブネットマスク。このプロパティは、`cfgNicUseDhcp` が 0 (FALSE) に設定されている場合にのみ有効です。

cfgNicGateway（読み取り / 書き込み）

 **メモ:** このパラメータは、`cfgNicUseDhcp` パラメータが 0 (FALSE) に設定されているときにのみ設定できます。

有効値

有効なゲートウェイ IP アドレスを表す文字列。例: 192.168.0.1

デフォルト

192.168.0.1

説明

RAC IP アドレスの静的割り当てに使うゲートウェイ IP アドレス。このプロパティは、`cfgNicUseDhcp` が 0 (FALSE) に設定されている場合にのみ有効です。

cfgNicUseDhcp（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC の IP アドレスの割り当てに DHCP を使用するかどうかを指定します。このプロパティを 1 (TRUE) に設定すると、iDRAC の IP アドレス、サブネットマスク、ゲートウェイがネットワーク上の DHCP サーバーから割り当てられます。このプロパティを 0 (FALSE) に設定すると、静的 IP アドレス、サブネットマスク、ゲートウェイは `cfgNicIpAddress`、`cfgNicNetmask`、`cfgNicGateway` プロパティから割り当てられます。

cfgNicMacAddress（読み取り専用）

有効値

RAC NIC MAC アドレスを表す文字列。

デフォルト

iDRAC NIC の現在の MAC アドレス。例: 00:12:67:52:51:A3

説明

iDRAC NIC の MAC アドレス。

cfgUserAdmin

このグループは、使用可能なリモートインタフェース経由での RAC へのアクセスが許可されているユーザーについての設定情報を提供します。

最大 16 のユーザーグループのインスタンスを使用できます。各インスタンスは各ユーザーの設定を表します。

cfgUserAdminIpmiLanPrivilege (読み取り / 書き込み)

有効値

- 2 (ユーザー)
- 3 (オペレータ)
- 4 (Administrator: システム管理者)
- 15 (アクセスなし)

デフォルト

- 4 (ユーザー 2)
- 15 (その他すべて)

説明

IPMI LAN チャンネル上での最大権限。

cfgUserAdminPrivilege (読み取り / 書き込み)

有効値

0x00000000~0x000001ff

デフォルト

0x00000000

説明

このプロパティは、ユーザーのロール (役割) ベースの権限を指定します。値は、権限の値を自由に組み合わせることのできるビットマスクとして表します。表 B-1 に、組み合わせてビットマスクを作成できるユーザー権限ビット値について説明します。

表 B-1 ユーザー権限を表すビットマスク

ユーザー権限	権限ビットマスク
iDRAC へのログイン	0x0000001
iDRAC の設定	0x0000002
ユーザーの設定	0x0000004
ログのクリア	0x0000008
サーバーコントロールコマンドの実行	0x0000010
コンソールリダイレクトへのアクセス	0x0000020
仮想メディアへのアクセス	0x0000040
テスト警告	0x0000080
デバッグコマンドの実行	0x0000100

例

表 B-2 に、1 つまたは複数の権限を持つユーザーを表す権限ビットマスクの例を示します。

表 B-2 ユーザー権限ビットマスクの例

ユーザー権限	権限ビットマスク
ユーザーは iDRAC にアクセスできません。	0x00000000
ユーザーは iDRAC にログインして iDRAC とサーバーの設定情報を表示することのみできます。	0x00000001
ユーザーは iDRAC にログインして設定を変更できます。	0x00000001 + 0x00000002 = 0x00000003
ユーザーは RAC にログインして、仮想メディアにアクセスし、コンソールリダイレクトにアクセスできます。	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (読み取り / 書き込み)

有効値


文字列。最大 16 文字。

デフォルト

...

説明

この索引のユーザーの名前。索引に何も入っていない場合は、文字列をこの名前フィールドに書き込むとユーザー索引が作成されます。二重引用符 (") の文字列を書き込むと、その索引のユーザーが削除されます。この名前は変更できません。名前を削除してから再作成する必要があります。文字列に / (フォワードスラッシュ)、¥ (バックスラッシュ)、. (ピリオド)、@ (アット記号) および引用符を含めることはできません。

 **メモ:** このプロパティ値は、ユーザー名で固有の値でなくてはなりません。

cfgUserAdminPassword (書き込み専用)

有効値

最大 20 文字の ASCII 文字列。

デフォルト

...

説明

このユーザーのパスワード。ユーザーパスワードは暗号化され、プロパティに書き込んだ後は参照や表示ができなくなります。

cfgUserAdminEnable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

ユーザーを個別に有効または無効にします。

cfgUserAdminSolEnable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

シリアルオーバー LAN (SOL) ユーザーアクセスを有効または無効にします。

cfgEmailAlert

このグループには、RAC 電子メール警告機能を設定するためのパラメータが入っています。

以下の各項では、このグループの各オブジェクトについて説明します。このグループは 4 つのインスタンスまで使用できます。

cfgEmailAlertIndex (読み取り専用)

有効値

1~4

デフォルト

このパラメータは既存のインスタンスに基づいて設定されます。

説明

警告インスタンスの固有の索引。

cfgEmailAlertEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

電子メール警告の送信先の電子メールアドレスを指定します。例: user1@company.com

cfgEmailAlertAddress

有効値

電子メールアドレス形式、最大 64 文字の ASCII 文字。

デフォルト

""

説明

警告元の電子メールアドレス。

cfgEmailAlertCustomMsg

有効値

文字列。最大 32 文字。

デフォルト

""

説明

警告と一緒に送信するカスタムメッセージを指定します。

cfgSessionManagement

このグループには、iDRAC に接続できるセッション数を設定するパラメータが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgSsnMgtConsRedirMaxSessions（読み取り / 書き込み）

有効値

1~2

デフォルト

2

説明

iDRAC で許可されるコンソールリダイレクトセッションの最大数を指定します。

cfgSsnMgtWebserverTimeout（読み取り / 書き込み）

有効値

60~1920

デフォルト

300

説明

ウェブサーバーのタイムアウトを定義します。このプロパティでは、接続がアイドル（ユーザー入力なし）な状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、セッションはキャンセルされます。この設定を変更しても現在のセッションには影響はありません（新しい設定を有効にするには、ログアウトしてからログインし直す必要があります）。

時間切れになったウェブサーバーのセッションは、現在のセッションからログアウトします。

cfgSsnMgtSshIdleTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60~1920

デフォルト

300

説明

セキュアシェル（SSH）のアイドルタイムアウトを定義します。このプロパティでは、接続がアイドル（ユーザー入力なし）な状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、セッションはキャンセルされます。この設定を変更しても現在のセッションには影響はありません（新しい設定を有効にするには、ログアウトしてからログインし直す必要があります）。

時間切れになったセキュアシェル（SSH）セッションでは、Enter キーを押した後にのみ、次のエラーメッセージが表示されます。

警告：セッションは有効でなくなりました。タイムアウトしたようです。

メッセージが表示された後、セキュアシェルセッションを生成したシェルに戻ります。

cfgSsnMgtTelnetIdleTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60～1920

デフォルト

300

説明

Telnet のアイドルタイムアウトを定義します。このプロパティでは、接続がアイドル（ユーザー入力なし）な状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、セッションはキャンセルされます。この設定を変更しても、現在のセッションには影響しません（新しい設定を有効にするには、ログアウトしてログインする必要があります）。

時間切れになった Telnet セッションでは、Enter キーを押した後にのみ、次のエラーメッセージが表示されます。

警告：セッションは有効でなくなりました。タイムアウトしたようです。

メッセージが表示された後、Telnet セッションを生成したシェルに戻ります。

cfgSerial

このグループには、iDRAC サービスの設定パラメータが含まれます。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgSerialSshEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC のセキュアシェル（SSH）インタフェースを有効または無効にします。

cfgSerialTelnetEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC の Telnet コンソールインタフェースを有効または無効にします。

cfgRacTuning

このグループは、有効なポートやセキュリティポート制限など、iDRAC の各種設定プロパティの指定に使用します。

cfgRacTuneHttpPort (読み取り / 書き込み)

有効値

10~65535

デフォルト

80

説明

RAC との HTTP ネットワーク通信に使うポート番号を指定します。

cfgRacTuneHttpsPort (読み取り / 書き込み)

有効値

10~65535

デフォルト

443

説明

iDRAC との HTTPS ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneIpRangeEnable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC の IP アドレス範囲の検証機能を有効または無効にします。

cfgRacTuneIpRangeAddr

有効値

IP アドレス形式の文字列。例: 192.168.0.44

デフォルト

192.168.1.1

説明

範囲マスクプロパティ (cfgRacTuneIpRangeMask) 1 で決定される IP アドレスビットパターンの可能な位置を指定します。

cfgRacTuneIpRangeMask

有効値

左寄せビットを使用した標準的な IP マスク値

デフォルト

255.255.255.0

説明

IP アドレス形式の文字列。例: 255.255.255.0

cfgRacTuneIpBlkEnable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の IP アドレスブロック機能を有効または無効にします。

cfgRacTuneIpBlkFailCount

有効値

2~16

デフォルト

5

説明

ウィンドウ（cfgRacTuneIpBlkFailWindow）内で何回ログインに失敗したら、この IP アドレスからのログイン試行が拒否されるかを指定します。

cfgRacTuneIpBlkFailWindow

有効値

10~65535

デフォルト

60

説明

ログインの失敗を数える時間枠を秒で定義します。ログイン試行がこの制限時間に達すると、失敗回数カウントはゼロにリセットされます。

cfgRacTuneIpBlkPenaltyTime

有効値

10~65535

デフォルト

300

説明

失敗回数が制限値を超えた IP アドレスからのセッション要求を拒否する時間枠を秒で定義します。

cfgRacTuneSshPort（読み取り / 書き込み）

有効値

1~65535

デフォルト

22

説明

iDRAC の SSH インタフェースに使用するポート番号を指定します。

cfgRacTuneTelnetPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

23

説明

iDRAC の Telnet インタフェースに使用するポート番号を指定します。

cfgRacTuneConRedirEncryptEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

コンソールリダイレクトのセッションでビデオを暗号化します。

cfgRacTuneConRedirPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

5900

説明

iDRAC のコンソールリダイレクト時にキーボードとマウスのトラフィックに使用するポートを指定します。

cfgRacTuneConRedirVideoPort (読み取り / 書き込み)

有効値


1～65535

デフォルト

5901

説明

iDRAC のコンソールリダイレクト時にビデオのトラフィックに使用するポートを指定します。

 **メモ:** このオブジェクトは、アクティブになる前に iDRAC をリセットする必要があります。

cfgRacTuneAsrEnable (読み取り / 書き込み)

有効値

0 (FALSE)


1 (TRUE)

デフォルト

0

説明

iDRAC の前回クラッシュ画面キャプチャ機能を有効または無効にします。

 **メモ:** このオブジェクトは、アクティブになる前に iDRAC をリセットする必要があります。

cfgRacTuneWebserverEnable (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

iDRAC ウェブサーバーを有効または無効にします。このプロパティを無効にすると、クライアントのウェブブラウザを使用して iDRAC にアクセスできなくなります。このプロパティは Telnet/SSH またはローカル RACADM インタフェースには影響しません。

cfgRacTuneLocalServerVideo (読み取り / 書き込み)

有効値

1 (有効)

0 (無効)

デフォルト

1

説明

ローカルサーバービデオを有効（スイッチオン）または無効（スイッチオフ）にします。

cfgRacTuneLocalConfigDisable（読み取り/書き込み）

有効値

0（有効）

1（無効）

デフォルト

0

説明

iDRAC 設定データへの書き込みアクセスを無効にします。デフォルトでは、アクセスは有効になっています。



メモ: アクセスは、ローカル RACADM または iDRAC ウェブインタフェースを使って無効にできますが、一度無効にしたアクセスを再度有効にするには、iDRAC ウェブインタフェースを使用する必要があります。

ifcRacManagedNodeOs

このグループには、管理下サーバーのオペレーティングシステムを記述するプロパティが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

ifcRacMnOsHostname（読み取り / 書き込み）

有効値

文字列。最大 255 文字。

デフォルト

""

説明

管理下サーバーのホスト名。

ifcRacMnOsOsName（読み取り / 書き込み）

有効値

文字列。最大 255 文字。

デフォルト

""

説明

管理下サーバーのオペレーティングシステム名。

cfgRacSecurity

このグループは、iDRAC SSL 証明書署名要求 (CSR) 機能に関連するオプションを設定するために使用します。このグループのプロパティは、iDRAC から CSR を生成する前に設定する必要があります。

証明書署名要求の生成の詳細については、RACADM [sslcsrgen](#) サブコマンドを参照してください。

cfgSecCsrCommonName (読み取り / 書き込み)

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 共通名 (コモンネーム: CN) を指定します。

cfgSecCsrOrganizationName (読み取り / 書き込み)

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 組織名 (O) を指定します。

cfgSecCsrOrganizationUnit (読み取り / 書き込み)

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 部門名 (OU) を指定します。

cfgSecCsrLocalityName (読み取り / 書き込み)

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 地域 (L) を指定します。

cfgSecCsrStateName (読み取り / 書き込み)

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 都道府県名 (S) を指定します。

cfgSecCsrCountryCode (読み取り / 書き込み)

有効値

文字列。最大 2 文字。

デフォルト

""

説明

CSR 国番号 (CC) を指定します。

cfgSecCsrEmailAddr（読み取り / 書き込み）

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR の電子メールアドレスを指定します。

cfgSecCsrKeySize（読み取り / 書き込み）

有効値

1024

2048

4096

デフォルト

1024

説明

CSR の SSL 非対称キーサイズを指定します。

cfgRacVirtual

このグループには iDRAC 仮想メディア機能を設定するためのパラメータが含まれています。このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgVirMediaAttached（読み取り / 書き込み）

有効値

1 (TRUE)


0 (FALSE)

デフォルト

1

説明

このオブジェクトは、USB バスを介して仮想デバイスをシステムに接続するために使用されます。デバイスを接続すると、サーバーは、システムに接続された有効な USB 大容量記憶装置を認識します。これは、ローカル USB CD-ROM/ フロッピードライブをシステムの USB ポートに接続する場合と同じです。デバイスが接続されると、iDRAC の ウェブインタフェースまたは CLI を使用してこれらの仮想デバイスにリモート接続できるようになります。このオブジェクトを 0 に設定すると、デバイスは USB バスから切断されます。

 **メモ:** 変更を有効にするには、システムを再起動する必要があります。

cfgVirAtapiSrvPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

3668

説明

暗号化された仮想メディアと iDRAC との接続に使用するポート番号を指定します。

cfgVirAtapiSrvPortSsl (読み取り / 書き込み)

有効値

未使用のポート番号 0~65535 (10 進数)。

デフォルト

3670

説明

SSL 仮想メディアの接続に使用するポートを設定します。

cfgVirMediaBootOnce (読み取り / 書き込み)

有効値

1 (有効)

0 (無効)

デフォルト

0

説明

iDRAC の仮想メディアのブートワンス機能を有効または無効にします。ホストサーバーの再起動時にこのプロパティが有効であれば、デバイスに適切なメディアが取り付けられている場合に、仮想メディアデバイスから再起動が試行されます。

cfgFloppyEmulation (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

0 に設定されている場合、仮想フロッピードライブは Windows オペレーティングシステムにより、リムーバブルディスクとして認識されます。Windows オペレーティングシステムは列挙中に C: 以降のドライブ文字を割り当てます。1 に設定されている場合、仮想フロッピードライブは Windows オペレーティングシステムにより、フロッピードライブとして認識されます。Windows オペレーティングシステムは A: または B: のドライブ文字を割り当てます。

cfgActiveDirectory

このグループには iDRAC Active Directory 機能を設定するためのパラメータが格納されています。

cfgAD RacDomain (読み取り / 書き込み)

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

...

説明

DRAC が置かれている Active Directory ドメイン。

cfgAD RacName (読み取り / 書き込み)

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

...

説明

Active Directory フォレストに記録された iDRAC 名。

cfgAD Enable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)


デフォルト

0

説明

iDRAC で Active Directory によるユーザー認証を有効または無効にします。このプロパティを無効にすると、ユーザーログインにローカルの iDRAC 認証が使用されます。

cfgADAuthTimeout (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、iDRAC の設定権限が必要です。

有効値

15~300

デフォルト

120

説明

Active Directory 認証要求の完了がタイムアウトになるまでの時間を秒で指定します。

cfgADRootDomain (読み取り / 書き込み)

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

""

説明

ドメインフォレストのルートドメイン。

cfgADSpecifyServerEnable (読み取り / 書き込み)

有効値

1 または 0 (TRUE または FALSE)

デフォルト

0

説明

1 (True) を選択すると、LDAP または グローバルカタログサーバーを指定できます。0 (False) を選択すると、これを指定できません。

cfgADDomainController (読み取り / 書き込み)

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN)

デフォルト

デフォルト値なし

説明

iDRAC は指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADGlobalCatalog (読み取り / 書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN)

デフォルト

デフォルト値なし

説明

iDDRAC は指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADType (読み取り / 書き込み)

有効値

1 = 拡張スキーマで Active Directory を有効にします。

2 = 標準スキーマで Active Directory を有効にします。

デフォルト

1 = 拡張スキーマ

説明

Active Directory と併用するスキーマタイプを指定します。

cfgStandardSchema

このグループには Active Directory 標準スキーマ設定を行うためのパラメータが格納されています。

cfgSSADRoleGroupIndex (読み取り専用)

有効値

1～5 の整数。

説明

Active Directory で記録したロール（役割）グループの索引。

cfgSSADRoleGroupName（読み取り / 書き込み）

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

（空白）

説明

Active Directory フォレストで記録したロール（役割）グループの名前。

cfgSSADRoleGroupDomain（読み取り / 書き込み）

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

（空白）

説明

ロール（役割）グループが置かれている Active Directory ドメイン。

cfgSSADRoleGroupPrivilege（読み取り / 書き込み）

有効値

0x00000000～0x000001ff

デフォルト

（空白）

説明

[表 B-3](#) のビットマスク番号を使って、ロール（役割）グループのロール（役割）ベースの権限を設定します。

表 B-3 ロール（役割）グループの権限のビットマスク

ロールグループの権限	ビットマスク
iDRAC へのログイン	0x00000001
iDRAC の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100

cfgIpmiSol

このグループは、システムのシリアルオーバー LAN (SOL) 機能の設定に使用されます。

cfgIpmiSolEnable (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

SOL を有効または無効にします。

cfgIpmiSolBaudRate (読み取り / 書き込み)

有効値

19200、57600、115200

デフォルト

115200

説明

シリアルオーバー LAN 通信のボーレート。

cfgIpmiSolMinPrivilege (読み取り / 書き込み)

有効値

- 2 (ユーザー)
- 3 (オペレータ)
- 4 (Administrator: システム管理者)

デフォルト

4

説明

SOL アクセスに必要な最小権限レベルを指定します。

cfgIpmiSolAccumulateInterval (読み取り / 書き込み)

有効値

1~255

デフォルト

10

説明

SOL 文字データパケットの一部を送信する前に通常 iDRAC が待機する時間を指定します。この値は 1 を基準に 5 ms 間隔で増分されます。

cfgIpmiSolSendThreshold (読み取り / 書き込み)

有効値

1~255

デフォルト

255

説明

SOL しきい値の限界値。SOL データパケット送信前にバッファする最大バイト数を指定します。

cfgIpmiLan

このグループは、システムの IPMI オーバー LAN 機能の設定に使用されます。

cfgIpmiLanEnable (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

デフォルト

0

説明

IPMI オーバー LAN インタフェースを有効または無効にします。

cfgIpmiLanPrivLimit (読み取り / 書き込み)

有効値

2 (ユーザー)

3 (オペレータ)

4 (Administrator: システム管理者)

デフォルト

4

説明

IPMI オーバー LAN アクセスに許可される最大権限レベルを指定します。

cfgIpmiLanAlertEnable (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

デフォルト

0

説明

グローバル電子メール警告を有効または無効にします。このプロパティは個々の電子メール警告の有効 / 無効プロパティすべてに優先されます。

cfgIpmiEncryptionKey (読み取り / 書き込み)

有効値

空白文字を含まない 0~20 文字の16 進数文字列。

デフォルト

00000000000000000000

説明

IPMI 暗号化キー。

cfgIpmiPetCommunityName (読み取り / 書き込み)

有効値

最大 18 文字の文字列。

デフォルト

public

説明

トラップの SNMP コミュニティ名。

cfgIpmiPef

このグループは、管理下サーバーで使用可能なプラットフォームイベントフィルタの設定に使用されます。

イベントフィルタは、管理下サーバーで重大なイベントが発生したときにトリガされる処置に関するポリシーを制御するために使用できます。

cfgIpmiPefName (読み取り専用)

有効値

文字列。最大 255 文字。

デフォルト

索引フィルタの名前。

説明

プラットフォームイベントフィルタの名前を指定します。

cfgIpmiPefIndex (読み取り専用)

有効値

1～17

デフォルト

プラットフォームイベントフィルタオブジェクトの索引値。

説明

特定のプラットフォームイベントフィルタの索引を指定します。

cfgIpmiPefAction（読み取り / 書き込み）

有効値

- 0 (なし)
- 1 (電源を切る)
- 2 (リセット)
- 3 (電源を入れ直す)

デフォルト

0

説明

警告がトリガされたときに管理下サーバーで実行される処置を指定します。

cfgIpmiPefEnable（読み取り / 書き込み）

有効値

- 0 (FALSE)
- 1 (TRUE)

デフォルト

1

説明

特定のプラットフォームイベントフィルタを有効または無効にします。

cfgIpmiPet

このグループは、管理下サーバーのプラットフォームイベントトラップの設定に使用します。

cfgIpmiPetIndex（読み取り / 書き込み）

有効値

1~4

デフォルト

適切な索引値。

説明

トラップに対応する索引の固有の識別子。

cfgIpmiPetAlertDestIpAddr (読み取り / 書き込み)

有効値

有効な IP アドレスを表す文字列。例: 192.168.0.67

デフォルト

0.0.0.0

説明

ネットワーク上でのトラップレシーバの送信先 IP アドレスを指定します。トラップレシーバは、管理下サーバーでイベントがトリガされたときに SNMP トラップを受信します。

cfgIpmiPetAlertEnable (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

個々のトラップを有効または無効にします。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC SMCLP プロパティデータベース

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [/system1/sp1/account<1-16>](#)
- [/system1/sp1/enetport1/*](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse_ndpt1](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse_ndpt1/remotesap1](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse_ndpt1/remotesap2](#)
- [/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1](#)
- [/system1/sp1/group<1-5>](#)
- [/system1/sp1/oem Dell_ adservice1](#)
- [/system1/sp1/oem Dell_ racsecurity1](#)
- [/system1/sp1/oem Dell_ ssl1](#)
- [/system1/sp1/oem Dell_ vm service1](#)
- [/system1/sp1/oem Dell_ vm service1/tcpendpt1](#)

/system1/sp1/account<1-16>

このターゲットは、使用可能なリモートインタフェース経由での RAC へのアクセスが許可されているローカルユーザーについての設定情報を提供します。最大 16 のユーザーグループのインスタンスを使用できます。<1-16> のインスタンスはそれぞれ、個々のローカルユーザーの設定を表します。

userid(読み取り専用)

有効値

1-16

デフォルト

アクセスするアカウントインスタンスによります。

説明

インスタンス ID またはローカルユーザー ID を指定します。

username(読み取り / 書き込み)

有効値


文字列 最大 16 文字

デフォルト

""

説明

このアカウントのローカルユーザー名を含むテキスト文字列。スラッシュ(/)、ピリオド(.)、アット記号(@)、引用符(")を文字列に含めることはできません。アカウントを削除すると、ユーザーが削除されます (アカウント <1-16> を削除します)。

 **メモ:** このプロパティ値は、ユーザー名において固有の値でなくてはなりません。

oem Dell_ ipmilanprivileges(読み取り / 書き込み)

有効値

2(ユーザー)

3(オペレーター)

4(Administrator: システム管理者)

15(アクセスなし)

デフォルト

4 (ユーザー 2)

15 (その他すべて)

説明

IPMI LAN チャンネル上での最大権限。

password(書き込み専用)

有効値

4~20 文字のテキスト文字列。

デフォルト

""

説明

このローカルユーザーのパスワードを保持します。ユーザーパスワードは暗号化され、プロパティに書き込んだ後は参照や表示ができなくなります。

enabledstate(読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

個々のユーザーを有効または無効にします。

solenabled(読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

シリアルオーバー LAN (SOL) ユーザーアクセスを有効または無効にします。

oemhell_extendedprivileges(読み取り / 書き込み)

有効値

0x00000000~0x000001ff

デフォルト

0x00000000

説明

このプロパティは、ユーザーのロール(役割)ベースの権限を指定します。値は、権限の値を自由に組み合わせることのできるビットマスクとして表します。[表 C-1](#) に、組み合わせてビットマスクを作成できるユーザー権限ビット値について説明します。

表 C-1 ユーザー権限に応じたビットマスク

ユーザー権限	権限ビットマスク
iDRAC へのログイン	0x00000001
iDRAC の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100

例

[表 C-2](#)に、1 つまたは複数の権限を持つユーザーの権限ビットマスクの例を示します。

表 C-2 ユーザー権限ビットマスクの例

ユーザー権限	権限ビットマスク
ユーザーは iDRAC にアクセスできません。	0x00000000
ユーザーは iDRAC にログインして iDRAC とサーバーの設定情報を表示することのみできます。	0x00000001
ユーザーは iDRAC にログインして設定を変更できます。	0x00000001 + 0x00000002 = 0x00000003
ユーザーは RAC にログインして、仮想メディアにアクセスし、コンソールリダイレクトにアクセスできます。	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

/system1/sp1/enetport1/*

このグループには iDRAC NIC を設定するためのパラメータが格納されています。このグループでは 1 つのインスタンスが使用できます。このグループのすべてのオブジェクトで iDRAC NIC がリセットされる必要があり、このため接続が一時的に途絶える場合があります。iDRAC NIC IP アドレス設定を変更するオブジェクトによってすべてのアクティブなユーザーセッションが閉じられるので、ユーザーはアップデートされた IP アドレス設定を使って再接続する必要があります。

macaddress(読み取り専用)

有効値

RAC NIC MAC アドレスを表す文字列

デフォルト

iDRAC NIC の現在の MAC アドレス。例:00:12:67:52:51:A3

説明

iDRAC NIC の MAC アドレスを保持します。

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdellicenable(読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

iDRAC ネットワークインタフェースコントローラを有効または無効にします。NIC が無効な場合は、iDRAC へのリモートネットワークインタフェースにアクセスできなくなり、iDRAC のレンダリングはローカル RACADM インタフェースを通してのみ可能になります。

ipaddress(読み取り / 書き込み)

有効値

有効な IP アドレスを表す文字列。例:192.168.0.20

デフォルト

192.168.0.n(n は 120 以上のサーバスロット番号)

説明

RAC に割り当てる静的 IP アドレスを指定します。このプロパティは、oemdellicusedhcp が 0(無効)に設定されている場合にのみ有効です。

subnetmask(読み取り / 書き込み)

有効値

有効なサブネットマスクを表す文字列。例:255.255.255.0

デフォルト

255.255.255.0

説明

iDRAC の IP アドレスの静的割り当てに使用されるサブネットマスク。このプロパティは、oem Dell_UsedHCP が 0 (無効) に設定されている場合にのみ有効です。

oem Dell_UsedHCP (読み取り / 書き込み)

有効値

0 (無効)

1 (有効)

デフォルト

0

説明

iDRAC の IP アドレスの割り当てに DHCP を使用するかどうかを指定します。このプロパティを 1 (有効) に設定すると、iDRAC の IP アドレス、サブネットマスク、ゲートウェイがネットワーク上の DHCP サーバーから割り当てられます。このプロパティが 0 (無効) に設定されている場合は、静的 IP アドレス、サブネットマスク、およびゲートウェイは、ユーザーが手動で挿入した値を取得します。

Committed (読み取り / 書き込み)

有効値

0 (コミット保留)

1 (コミット)

デフォルト

1

説明

ユーザーが現在のセッションを終了しないで IP アドレスやサブネットマスクを変更できるようにします。プロパティが 1 (コミット) に設定されている場合は、IP アドレスとサブネットマスクは有効です。IP アドレスまたはサブネットマスクのいずれかが変更されると、自動的にこのプロパティが 0 (コミット保留) に変更されます。ネットワーク設定を有効にするには、プロパティを 1 に戻す必要があります。

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1

oem Dell_DomainNameFromDHCP (読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

iDRAC DNS ドメイン名をネットワークの DHCP サーバーから割り当てる必要があることを指定します。

oemdelI_dnsdomainname(読み取り / 書き込み)

有効値

最大 254 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。

デフォルト

""

説明

DNS ドメイン名を保持します。このパラメータは、oemdelI_domainnamefromdhcp が 0(無効)に設定されている場合にのみ有効です。

oemdelI_dnsregisterrac(読み取り / 書き込み)

有効値

0(未登録)

1(登録済み)

デフォルト

0


説明

DNS サーバーに iDRAC 名を登録します。

oemdelI_dnsracname(読み取り / 書き込み)

有効値

最大 63 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。

 **メモ:** 一部の DNS サーバーは 31 文字以内の名前しか登録しません。

デフォルト

rac-サービスタグ

説明

RAC 名 (デフォルトでは RAC サービスタグ) が表示されます。このパラメータは、oemdelldnsregisterrac が 1 (登録済み) に設定されているときにのみ有効です。

oemdelldnsregisterrac (読み取り / 書き込み)

有効値

0 (無効)

1 (有効)

デフォルト

0

説明

DNS サーバーの IP アドレスをネットワーク上の DHCP サーバーから割り当てることを指定します。

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1/remotesap1

dnserveraddress (読み取り / 書き込み)

有効値

有効な IP アドレスを表す文字列。例: 192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 1 の IP アドレスを指定します。このプロパティは、oemdelldnsregisterrac が 0 (無効) に設定されている場合にのみ有効です。

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1/remotesap2

dnserveraddress (読み取り / 書き込み)

有効値

有効な IP アドレスを表す文字列。例: 192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 2 の IP アドレスを指定します。このプロパティは、oemdel_l_serversfromdhcp が 0 (無効) に設定されている場合にのみ有効です。

/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1

defaultgatewayaddress (読み取り / 書き込み)

有効値

有効なゲートウェイ IP アドレスを表す文字列。例: 192.168.0.1

デフォルト

192.168.0.1

説明

RAC IP アドレスの静的割り当てに使うゲートウェイ IP アドレス。このプロパティは、oemdel_l_usedhcp が 0 (無効) に設定されている場合にのみ有効です。

/system1/sp1/group<1-5>

これらのグループは、Active Directory 標準スキーマ設定を行うためのパラメータを含んでいます。

oemdel_l_groupname (読み取り / 書き込み)

有効値

空白スペースを含まない最大 254 文字の印刷可能テキスト文字列。

デフォルト

...

説明

Active Directory フォレストで記録したロール (役割) グループの名前を保持します。

oemdel_l_groupdomain (読み取り / 書き込み)

有効値

空白スペースを含まない最大 254 文字の印刷可能テキスト文字列。

デフォルト

...

説明

ロール(役割)グループが置かれている Active Directory ドメインを保持します。

oemdel_l_groupprivilege(読み取り / 書き込み)

有効値

0x00000000~0x000001ff

デフォルト

""

説明

Table B-3 のビットマスク番号を使って、ロール(役割)グループのロール(役割)ベースの権限を設定します。

表 C-3 ロール(役割)グループの権限のビットマスク

ロール(役割)グループ	権限ビットマスク
iDRAC へのログイン	0x00000001
iDRAC の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100

/system1/sp1/oemdel_l_adservice1

このグループには iDRAC Active Directory 機能を設定するためのパラメータが格納されています。

enabledstate(読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

iDRAC で Active Directory によるユーザー認証を有効または無効にします。このプロパティを無効にすると、ユーザーログインにローカルの iDRAC 認証のみが使用されます。

oemdel_l_adracname(読み取り / 書き込み)

有効値

空白スペースを含まない最大 254 文字の印刷可能テキスト文字列。

デフォルト

""

説明

Active Directory フォレストに記録された iDRAC 名。

oemdel_l_adracdomain(読み取り / 書き込み)**有効値**

空白スペースを含まない最大 254 文字の印刷可能テキスト文字列。

デフォルト

""

説明

iDRAC が置かれている Active Directory ドメイン。

oemdel_l_adrootdomain(読み取り / 書き込み)**有効値**

空白スペースを含まない最大 254 文字の印刷可能テキスト文字列。

デフォルト

""

説明

ドメインフォレストのルートドメイン。

oemdel_l_timeout(読み取り / 書き込み)**有効値**

15~300

デフォルト

120

説明

Active Directory 認証要求の完了がタイムアウトになるまでの時間を秒で指定します。

oemdelI_schematype(読み取り / 書き込み)

有効値

1(拡張スキーマ)

2(標準スキーマ)

デフォルト

1

説明

Active Directory と併用するスキーマタイプを指定します。

oemdelI_adspecifyserverenable(読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

ユーザーが LDAP または Global Catalog(グローバルカタログ) サーバーを指定できるようにします。

oemdelI_addomaincontroller(読み取り / 書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名(FQDN)。

デフォルト

...

説明

iDRAC が LDAP サーバーでユーザー名を探すために使用する、ユーザー指定の値。

oemdelI_adglobalcatalog(読み取り / 書き込み)

有効値

有効な IP アドレスまたは FQDN。

デフォルト

デフォルト値なし

説明

iDRAC が Global Catalog (グローバルカタログ) サーバーでユーザー名を探すために使用する、ユーザー指定の値。

/system1/sp1/oemdel_lracsecurity1

このグループは、iDRAC SSL 証明書署名要求 (CSR) 機能に関連するオプションを設定するために使用します。このグループのすべてのプロパティは、iDRAC から CSR を生成する前に設定する必要があります。

commonname (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

""

説明

CSR 共通名 (コモンネーム: CN) を指定します。

organizationname (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

""

説明

CSR 組織名を指定します。

oemdel_lracorganizationunit (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

""

説明

CSR 部門名を指定します。

oemdellocalityname(読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

""

説明

CSR 地域を指定します。

oemdelstate(読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

""

説明

CSR 都道府県名を指定します。

oemdelcountrycode(読み取り / 書き込み)

有効値

最大 2 文字の文字列。

デフォルト

""

説明

CSR 国番号を指定します。

oemdel_emailaddress(読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

""

説明

CSR の電子メールアドレスを指定します。

oemdel_keysize(読み取り / 書き込み)

有効値

1024

2048

4096

デフォルト

1024

説明

CSR の非対称キーサイズを指定します。

/system1/sp1/oemdel_ssl1

証明書署名要求(CSR)の生成と証明書の表示に必要なパラメータを含みます。

generate(読み取り / 書き込み)

有効値

0(生成しない)

1(生成)

デフォルト

0

説明

1 に設定されている場合は、CSR を生成します。CSR を生成する前に、oemdel_racsecurity1 ターゲットのプロパティを設定します。

oem Dell_status (読み取り専用)

有効値

CSR not found (CSR が見つかりません)

CSR generated (CSR が生成されました)

デフォルト

CSR not found (CSR が見つかりません)

説明

現在のセッションで前に発行された generate コマンドがある場合は、そのステータスを表示します。

oem Dell_certtype (読み取り / 書き込み)

有効値

SSL

AD

CSR

デフォルト

SSL

説明

表示する証明書のタイプを指定し (AD または SSL)、generate プロパティを使って CSR を生成します。

/system1/sp1/oem Dell_vm service1

このグループには iDRAC 仮想メディア機能を設定するためのパラメータが含まれています。

enabledstate (読み取り / 書き込み)

有効値

VMEDIA_DETACH

VMEDIA_ATTACH

VMEDIA_AUTO_ATTACH

デフォルト

VMEDIA_ATTACH

説明

USB バス経由で仮想デバイスをシステムに接続するために使用され、システムに接続された有効な USB 大容量記憶装置をサーバーが認識できるようにします。これは、ローカル USB CD-ROM/ フロッピードライブをシステムの USB ポートに接続する場合と同じです。デバイスが接続されると、iDRAC の ウェブインタフェースまたは CLI を使用してこれらの仮想デバイスにリモート接続できるようになります。このプロパティを 0 に設定すると、デバイスは USB バスから切断されます。

oemdel1_singleboot(読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

iDRAC の仮想メディアのブートワンス機能を有効または無効にします。ホストサーバーの再起動時にプロパティが有効な場合は、サーバーは仮想メディアデバイスから起動しようと試みます。

oemdel1_floppyemulation(読み取り / 書き込み)

有効値

0(無効)

1(有効)

デフォルト

0

説明

0 に設定されている場合、仮想フロッピードライブは Windows オペレーティングシステムにより、リムーバブルディスクとして認識されます。Windows オペレーティングシステムは列挙中に C:以降のドライブ文字を割り当てます。1 に設定されている場合、仮想フロッピードライブは Windows オペレーティングシステムにより、フロッピードライブとして認識されます。Windows オペレーティングシステムは A: または B: のドライブ文字を割り当てます。

/system1/sp1/oemdel1_vmervice1/tcpendpt1

portnumber(読み取り / 書き込み)

有効値

1~65535

デフォルト

3668

説明

暗号化された仮想メディアと iDRAC との接続に使用するポート番号を指定します。

oem Dell_sslenabled(読み取り専用)

有効値

FALSE

デフォルト

FALSE

説明

ポートで SSL が無効になっていることを示します。

portnumber(読み取り / 書き込み)

有効値

1~65535

デフォルト

3670

説明

暗号化された仮想メディアと iDRAC との接続に使用するポート番号を指定します。

oem Dell_sslenabled(読み取り専用)

有効値

TRUE

デフォルト

TRUE

説明

ポートで SSL が有効になっていることを示します。

[目次ページに戻る](#)

[目次ページに戻る](#)

RACADM と SM-CLP との対応付け

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

表 D-1 に、RACADM グループとオブジェクト、および SM-CLP MAP 上での対応する SM-CLP の場所 (存在する場合) を示します。

表 D-1 RACADM グループ / オブジェクトと SM-CLP との対応付け

RACADM グループ / オブジェクト	SM-CLP	説明
idRacInfo		
idRacName		最大 15 文字の ASCII 文字列。デフォルト:iDRAC
idRacProductInfo		最大 63 文字の ASCII 文字列。デフォルト: Integrated Dell Remote Access Controller
idRacDescriptionInfo		最大 255 文字の ASCII 文字列。デフォルト:このシステムコンポーネントは Dell PowerEdge サーバーのリモート管理機能一式をすべて提供しています。
idRacVersionInfo		最大 63 文字の ASCII 文字列。デフォルト:1
idRacBuildInfo		最大 16 文字の ASCII 文字列。
idRacType		デフォルト:8
cfgActiveDirectory	/system1/sp1/ oemdel_adservice1	
cfgADEnable	enablestate	無効にするには 0、有効にするには 1。デフォルト:0
cfgADRacName	oemdel_adracname	最大 254 文字の文字列。
cfgADRacDomain	oemdel_adracdomain	最大 254 文字の文字列。
cfgADRootDomain	oemdel_adrootdomain	最大 254 文字の文字列。
cfgADAuthTimeout	oemdel_timeout	15 ~ 300 秒。デフォルト:120
cfgADType	oemdel_schematype	標準スキーマは 1、拡張スキーマは 2。デフォルト:1
cfgADSpecifyServerEnable	oemdel_adspecifyserverenable	有効になっている場合、LDAP またはグローバルカタログサーバーを指定します。 無効にするには 0、有効にするには 1。デフォルト:0
cfgADDomainController	oemdel_addomaincontroller	LDAP 検索に使用するドメインコントローラの DNS 名または IP アドレス。
cfgADGlobalCatalog	oemdel_adglobalcatalog	LDAP 検索に使用するグローバルカタログサーバーの DNS 名または IP アドレス。
cfgStandardSchema		
cfgSSADRoleGroupIndex	/system1/sp1/group1 ~ /system1/sp1/group5	RACADM - グループ索引 ID(1-5)。 SM-CLP - アドレスバスで選択。
cfgSSADRoleGroupName	oemdel_groupname	最大 254 文字の文字列。
cfgSSADRoleGroupDomain	oemdel_groupdomain	最大 254 文字の文字列。
cfgSSADRoleGroupPrivilege	oemdel_groupprivilege	0x00000000 ~ 0x000001ff のビットマスク値。
cfgLanNetworking	/system1/sp1/enetport1	
cfgNicMacAddress	macaddress	インタフェースの MAC アドレス。編集不可。
	/system1/sp1/enetport1/ lanendpt1/ipendpt1	
cfgNicEnable	oemdel_nicenable	NIC を無効にするには 0、NIC を有効にするには 1。デフォルト:0
cfgNicUseDHCP	oemdel_usedhcp	静的ネットワークアドレスを設定するには 0、DHCP を使用するには 1。デフォルト:0
cfgNicIpAddress	ipaddress	iDRAC の IP アドレス。デフォルト:192.168.0.120 + サーバーのスロット番号。
cfgNicNetmask	subnetmask	iDRAC ネットワークのサブネットマスク。デフォルト:255.255.255.0
	committed	グループ値が変更されると、committed は 0 に設定され、新しい値は保存されていないことを示します。新しい設定を保存するには値を 1 に設定します。デフォルト:1
	/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	

cfgDNSDomainName	oemdelldnsdomainname	最大 250 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。
cfgDNSDomainNameFromDHCP	oemdelldomainnamefromdhcp	DHCP からドメイン名を取得するには 1 に設定します。デフォルト:0
cfgDNSRacName	oemdelldnsracname	最大 63 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。デフォルト: iDRAC- + Dell サービスタグ
cfgDNSRegisterRac	oemdelldnsregisterrac	DNS の iDRAC 名を登録するには 1 に設定します。デフォルト:0
cfgDNSServersFromDHCP	oemdelldnsserversfromdhcp	DHCP から DNS サーバーのアドレスを取得するには 1 に設定します。デフォルト:0
	/system1/sp1/enetport1/lanendpt1 /ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	DNS サーバーの IP アドレスを表す文字列。
	/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1/remotesap2	
cfgDNSServer2	dnsserveraddresses2	DNS サーバーの IP アドレスを表す文字列。
	/system1/sp1/enetport1/lanendpt1/ ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	デフォルトゲートウェイの IP アドレスを表す文字列。デフォルト:192.168.0.1
cfgRacVirtual	/system1/sp1/oemdelldvmservice1	
cfgFloppyEmulation	oemdelldfloppyemulation	フロッピーディスクのエミュレーションを有効にするには 1 に設定します。デフォルト: 0
cfgVirMediaAttached	enabledstate	メディアを接続するには、(RACADM)/VMEDIA_ATTACH (SM-CLP) を 1 に設定します。デフォルト:1 (RACADM)/VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdelldsingleboot	選択したメディアから次回の起動を実行するには 1 に設定します。デフォルト:0
	/system1/sp1/oemdelldvmservice1/ tcpendpt1	
	oemdelldsslenabled	最初の仮想メディアデバイスに対して SSL が有効な場合は 1 に、そうでない場合は 0 に設定します。編集不可。
cfgVirAtapiSvrPort	portnumber	最初の仮想メディアデバイスに使用するポート。デフォルト:3668
	/system1/sp1/oemdelldvmservice1/ tcpendpt2	
	oemdelldsslenabled	2 つ目の仮想メディアデバイスに対して SSL が有効な場合は 1 に、そうでない場合は 0 に設定します。編集不可。
cfgVirAtapiSvrPortSsl	portnumber	2 つ目の仮想メディアデバイスに使用するポート。デフォルト:3670
cfgUserAdmin	/system1/sp1/account1 ~ /system1/sp1/account16	
cfgUserAdminEnable	enabledstate	ユーザーを有効にするには 1 に設定します。デフォルト:0
cfgUserAdminIndex	userid	ユーザー索引、1 ~ 16。
cfgUserAdminIpmilanPrivilege	oemdelldipmilanprivileges	2(ユーザー)、3(オペレータ)、4 (Administrator: システム管理者)、15(アクセスなし)。デフォルト:4
cfgUserAdminPassword	パスワード	最大 20 文字の ASCII 文字列。
cfgUserAdminPrivilege	oemdelldextendedprivileges	0x00000000 ~ 0x000001ff のビットマスク値。デフォルト:0x00000000
cfgUserAdminSolEnable	solenabled	シリアルオーバー LAN を使用可能にするには 1 に設定します。デフォルト:0
cfgUserAdminUserName	username	最大 16 文字の文字列。
cfgEmailAlert		
cfgEmailAlertAddress		電子メール送信先アドレス、最大 64 文字。
cfgEmailAlertCustomMsg		電子メールで送信するメッセージ、最大 32 文字。
cfgEmailAlertEnable		電子メール警告を有効にするには 1 に設定します。デフォルト:0
cfgEmailAlertIndex		電子メール警告インスタンスの索引。1 ~ 4 の番号。
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		許可されている同時コンソールリダイレクトセッションの数(1 または 2)。デフォルト:2
cfgSsnMgtSshIdleTimeout		SSH セッションがタイムアウトするまでのアイドル時間(秒)。0(タイムアウトを無効にする)、また

cfglpmiPef		
cfglpmiPefAction		イベントが検知された場合取る処置。0(なし)、1(電源を切る)、2(リセット)、3(電源を入れ直す)。デフォルト:0
cfglpmiPefEnable		プラットフォームイベントフィルタを有効にするには 1 に設定します。デフォルト:0
cfglpmiPefIndex		プラットフォームイベントフィルタの索引番号。 (1 ~ 17)
cfglpmiPefName		プラットフォームイベント名、最大 254 文字の文字列。編集不可。
cfglpmiPet		
cfglpmiPetAlertDestIpAddr		プラットフォームイベントトラップシーバの IP アドレス。デフォルト:0.0.0.0
cfglpmiPetAlertEnable		プラットフォームイベントトラップを有効にするには 1 に設定します。デフォルト:1
cfglpmiPetIndex		プラットフォームイベントトラップの索引番号(1 ~ 4)。

表 D-2 RACADM サブコマンドと SM-CLP の比較

RACADM サブコマンド	SM-CLP	説明
sslcsrgen -g	set /system1/sp1/oemdel_ssl1 oemdel_certtype=CSR set /system1/sp1/oemdel_ssl1 generate=1 dump -destination <iDRAC 証明書署名要求 TFTP URI> /system1/sp1/oemdel_ssl1	SSL 証明書署名要求 (CSR) を生成してダウンロードします。
sslcsrgen -s	show /system1/sp1/oemdel_ssl1 oemdel_status	CSR 生成プロセスのステータスを表示します。
sslcertupload -t 1	set /system1/sp1/oemdel_ssl1 oemdel_certtype=SSL load -source <iDRAC サーバー証明書 TFTP-URI> /system1/sp1/oemdel_ssl1	iDRAC サーバー証明書を iDRAC にアップロードします。
sslcertupload -t 2	set /system1/sp1/oemdel_ssl1 oemdel_certtype=AD load -source <ActiveDirectory 証明書 TFTP URI> /system1/sp1/oemdel_ssl1	iDRAC に Active Directory 証明書をアップロードします。
sslcertdownload -t 1	set /system1/sp1/oemdel_ssl1 oemdel_certtype=SSL load -source <iDRAC サーバー証明書 TFTP-URI> /system1/sp1/oemdel_ssl1	iDRAC から iDRAC サーバー証明書をダウンロードします。
sslcertdownload -t 2	set /system1/sp1/oemdel_ssl1 oemdel_certtype=AD load -source <ActiveDirectory 証明書 TFTP URI> /system1/sp1/oemdel_ssl1	iDRAC から Active Directory 証明書をダウンロードします。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC の概要

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2 ユーザーガイド

- [iDRAC の管理機能](#)
- [iDRAC のセキュリティ機能](#)
- [対応プラットフォーム](#)
- [対応オペレーティングシステム](#)
- [対応ウェブブラウザ](#)
- [対応リモートアクセス接続](#)
- [iDRAC のポート](#)
- [その他のマニュアル](#)

Integrated Dell™ Remote Access Controller (iDRAC) はシステム管理ハードウェアおよびソフトウェアのソリューションで、Dell PowerEdge™ システムのリモート管理機能、クラッシュしたシステムのリカバリ機能、電源制御機能などを提供します。

iDRAC は、リモート監視 / 制御システムに、システムオンチップの内蔵マイクロプロセッサを採用しています。iDRAC は、管理下 PowerEdge サーバーとシステム基板上で共存します。サーバーオペレーティングシステムはアプリケーションの実行に関係し、iDRAC はサーバー環境およびオペレーティングシステム外の状態の監視と管理に関係します。

警告やエラーが発生したときに、電子メールまたは 簡易ネットワーク管理プロトコル (SNMP) のトラップ警告を送信するように iDRAC を設定できます。システムクラッシュの原因を診断する際の助けとして、iDRAC はシステムクラッシュを検出すると、イベントデータをログに記録し、画面イメージをキャプチャできます。

管理下サーバーは、モジュール電源、冷却ファン、Chassis Management Controller (CMC) と共に Dell M1000-e システムエンクロージャ (シャーシ) に設置されています。CMC は、シャーシに搭載されているすべてのコンポーネントの監視と管理を行います。冗長 CMC を追加すると、Primary (一時) CMC に障害が発生した場合にホットフェールオーバーを提供することもできます。シャーシは、LCD ディスプレイ、ローカルコンソール接続、およびウェブインタフェースを介して iDRAC へのアクセスを提供します。

iDRAC へのネットワーク接続はすべて、CMC ネットワークインタフェース (「GB1」というラベルの CMC RJ45 接続ポート) を経由します。CMC は、サーバー上の iDRAC へのトラフィックを専用の内部ネットワークにルーティングします。この専用の管理ネットワークは、サーバーのデータバス外で、オペレーティングシステムの制御域外、つまり 帯域外 (アウトバンド) にあります。管理下サーバーの帯域内 (インバンド) ネットワークインタフェースへは、シャーシに搭載されている I/O モジュール (IOM) からアクセスします。

iDRAC ネットワークインタフェースは、デフォルトでは無効になっています。これを設定しなければ、iDRAC にアクセスできません。iDRAC をネットワーク上で有効にして設定すると、iDRAC ウェブインタフェース、Telnet、SSH や、Intelligent Platform Management Interface (IPMI) などの対応するネットワーク管理プロトコルを使用して、割り当てられた IP アドレスにアクセスできるようになります。

iDRAC の管理機能

iDRAC には次の管理機能があります。


- 1 [ダイナミックドメイン名システム \(DDNS\) の登録](#)
- 1 [ウェブインタフェース、コンソールリダイレクト経由のローカル RACADM コマンドラインインタフェース、Telnet/SSH 接続による SM-CLP コマンドラインを使用したリモートシステムの管理と監視](#)
- 1 [Microsoft Active Directory® 認証のサポート - 標準スキーマまたは拡張スキーマを使用して iDRAC のユーザー ID とパスワードを Active Directory で集中化](#)
- 1 [コンソールリダイレクト - リモートシステムにキーボード、ビデオ、マウスの機能を提供](#)
- 1 [仮想メディア - 管理下サーバーが管理ステーションのローカルメディアドライブまたはネットワーク共有フォルダの ISO CD/DVD イメージにアクセス可能](#)
- 1 [監視 \(モニター\) - システム情報やコンポーネントのステータスにアクセス可能](#)
- 1 [システムイベントログへのアクセス - システムイベントログ \(SEL\)、iDRAC のログ、およびオペレーティングシステムの状態とは関係なく、クラッシュしたシステムや応答しないシステムの前回クラッシュ画面にアクセス可能](#)
- 1 [Dell OpenManage™ ソフトウェアの統合 - Dell OpenManage Server Administrator または IT Assistant から iDRAC ウェブインタフェースの起動が可能](#)
- 1 [iDRAC 警告 - 電子メールメッセージまたは SNMP トラップによって管理下ノードの不具合を警告](#)
- 1 [リモート電源管理 - シャットダウンやリセットなどのリモート電源管理機能を管理コンソールから提供](#)
- 1 [Intelligent Platform Management Interface \(IPMI\) のサポート](#)
- 1 [Secure Sockets Layer \(SSL\) 暗号化 - ウェブインタフェースからセキュアリモートシステム管理を提供](#)
- 1 [パスワードレベルのセキュリティ管理 - リモートシステムへの不正アクセスを防止](#)
- 1 [役割 \(ロール\) ベースの権限 - さまざまなシステム管理タスクに応じて割り当て可能な権限](#)

iDRAC のセキュリティ機能

iDRAC には次のセキュリティ機能があります。

- 1 [Microsoft Active Directory \(オプション\) またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証](#)
- 1 [システム管理者が各ユーザーに特定の権限を設定できる役割 \(ロール\) ベースの権限](#)
- 1 [ウェブインタフェースまたは SM-CLP を使用したユーザー ID とパスワードの設定](#)

- 1 SM-CLP とウェブインタフェースは SSL 3.0 標準を使って 128 ビットおよび 40 ビット(128 ビットが認められていない国の場合)暗号化をサポートします。
- 1 ウェブインターフェースまたは SM-CLP を使用したセッションタイムアウトの設定(秒単位)
- 1 設定可能な IP ポート(該当する場合)

 **メモ:** Telnet は SSL 暗号化をサポートしていません。

- 1 暗号化トランスポート層を使用してセキュリティを強化するセキュアシェル(SSH)
- 1 IP アドレスごとのログイン失敗制限により制限を越えた IP アドレスのログインを阻止
- 1 iDRAC に接続するクライアントの IP アドレス範囲を制限

対応プラットフォーム

iDRAC は、Dell PowerEdge M1000-e システムエンクロージャ内の以下の PowerEdge システムに対応しています。

- 1 PowerEdge M600
- 1 PowerEdge M605
- 1 PowerEdge M805
- 1 PowerEdge M905

最新の対応プラットフォームについては、iDRAC の Readme ファイルと、Dell のサポートウェブサイト support.dell.com にある『Dell PowerEdge 互換性ガイド』を参照してください。

対応オペレーティングシステム

[表 1-1](#) は、iDRAC でサポートされているオペレーティングシステムのリストです。

最新情報については、Dell のサポートウェブサイト support.dell.com の『Dell OpenManage Server Administrator 互換性ガイド』を参照してください。

表 1-1 対応 OS

オペレーティングシステムファミリー	オペレーティングシステム
Microsoft Windows	Microsoft® Windows Server® 2003 R2 Standard/Enterprise(32 ビット x86)エディション SP2 Microsoft Windows Server 2003 Web, Standard, および Enterprise(32 ビット x86)エディション SP2 Microsoft Windows Server 2003 Standard/Enterprise(x64)エディション SP2 Microsoft Windows Storage Server 2003 R2 Express, Workgroup, Standard, および Enterprise x64 エディション Microsoft Windows Server 2008 Web, Standard, および Enterprise(32 ビット x86)エディション Microsoft Windows Server 2008 Web, Standard, Enterprise, および Datacenter(x64)エディション メモ: Windows Server 2003 SP1 をインストールする場合は、DCOM のセキュリティ設定に注意してください。詳細については、Microsoft のサポートウェブサイト support.microsoft.com/kb/903220 で記事番号 903220 を参照してください。
Red Hat® Linux®	Enterprise Linux WS, ES, および AS(バージョン 4)(x86 および x86_64) Enterprise Linux 5(x86 および x86_64)
SUSE® Linux	Enterprise Server 9 Update 2 および Update 3(x86_64) Enterprise Server 10(Gold)(x86_64)

対応ウェブブラウザ

[表 1-2](#) は、iDRAC のクライアントとしてサポートされているウェブブラウザのリストです。

最新の対応プラットフォームについては、iDRAC の Readme ファイルと、Dell のサポートウェブサイト support.dell.com にある『Dell OpenManage 互換性ガイド』を参照してください。


 **メモ:** セキュリティに重大な欠陥があるため、SSL 2.0 のサポートは中止になりました。ブラウザを正しく動作させるには、SSL 3.0 対応に設定する必要があります。

表 1-2 対応ウェブブラウザ

Operating System(オペレーティングシステム)	対応ウェブブラウザ
Windows	Internet Explorer 6.0 Service Pack 2(SP2) (Windows XP および Windows 2003 R2 SP2 のみ) Internet Explorer 7.0(Windows Vista, Windows XP, Windows 2003 R2 SP2, Windows Server 2008 のみ) Mozilla Firefox 2.0(Windows, Java vKVM/vMedia コンソールのみ)
Linux	Mozilla Firefox 1.5(32 ビット) (SUSE Linux[バージョン 10]のみ) Mozilla Firefox 2.0(Red Hat Enterprise Linux 4 および 5[32 ビットまたは 64 ビット]および Suse Linux Enterprise Server 10[32 ビットまたは 64 ビット])

対応リモートアクセス接続

表 1-3 は接続機能のリストです。

表 1-3 対応リモートアクセス接続

接続	機能
iDRAC NIC	<ul style="list-style-type: none"> 10Mbps/100Mbps/1Gbps Ethernet(CMC GB Ethernet ポート経由) DHCP のサポート SNMP トラップと電子メールによるイベント通知 iDRAC 設定、システム起動、リセット、電源投入、シャットダウンコマンドなどの操作に使用する SM-CLP (Telnet または SSH)コマンドシェルをサポート impitool や ipmishell などの IPMI ユーティリティのサポート

iDRAC のポート

表 1-4 は、iDRAC が接続を待ち受けるポートのリストです。表 1-5 は、iDRAC がクライアントとして使用するポートです。この情報は、ファイアウォールのポートを開いて iDRAC へのリモートアクセスを許可する場合に必要です。

表 1-4 iDRAC サーバリスニングポート

ポート番号	機能
22*	セキュアシェル (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668*, 3669*	仮想メディアサービス
3770*, 3771*	仮想メディアセキュアサービス
5900*	コンソールリダイレクトキーボード / マウス
5901*	コンソールリダイレクトビデオ
*設定可能なポート	

表 1-5 iDRAC クライアントポート

ポート番号	機能
25	SMTP
53	DNS
68	DHCP で割り当てた IP アドレス
69	TFTP
162	SNMP トラップ
636	LDAPS
3269	グローバルカタログ(GC)用 LDAPS


その他のマニュアル

この『ユーザーズガイド』のほかに、次の文書にもシステム内の iDRAC のセットアップと操作に関する追加情報が含まれています。

- 1 iDRAC オンラインヘルプでは、ウェブインタフェースの使用法について説明しています。
- 1 『Dell Chassis Management Controller ユーザーガイド』は、PowerEdge サーバーを含むシャーシの全モジュールを管理するコントローラの使い方について記載されています。
- 1 『Dell OpenManage IT Assistant ユーザーズガイド』は、IT Assistant の使用法について説明しています。
- 1 『Dell OpenManage Server Administrator ユーザーズガイド』は、Server Administrator のインストールと使用法について説明しています。
- 1 『Dell Update Packages ユーザーズガイド』は、システムアップデート対策としての Dell Update Packages の入手とその使用法について説明しています。

次のシステム文書にも、iDRAC をインストールするシステムに関する詳細が含まれています。

- 1 『製品情報ガイド』には、安全と規制に関する説明が記載されています。保証情報については、本書に含まれている場合と、別のマニュアルが付属する場合があります。
- 1 『ラック取り付けガイド』および『ラック取り付け手順』では、システムをラックに取り付ける方法を説明しています。
- 1 『はじめに』では、システムの機能、システムのセットアップ、および技術仕様の概要を説明しています。
- 1 『ハードウェアオーナーズマニュアル』では、システムの機能、トラブルシューティングの方法、およびコンポーネントの取り付け方や交換方法について説明しています。
- 1 システム管理ソフトウェアのマニュアルでは、ソフトウェアの機能、動作条件、インストール、および基本操作について説明しています。
- 1 OS のマニュアルでは、OS ソフトウェアのインストール手順(必要な場合)や設定方法、および使い方について説明しています。
- 1 別途購入されたコンポーネントのマニュアルでは、これらのオプション装置の取り付けや設定について説明しています。
- 1 システム、ソフトウェア、またはマニュアルの変更について記載されたアップデート情報がシステムに付属していることがあります。

 **メモ:** このアップデート情報には他の文書の内容を差し替える情報が含まれていることがあるので、必ず最初にお読みください。

- 1 リリースノートまたは readme ファイルには、システムやマニュアルに加えられたアップデートの情報や、上級ユーザーや技術者のための高度な技術情報が記載されています。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC の設定

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [作業を開始する前に](#)
- [iDRAC の設定に使用するインタフェース](#)
- [設定タスク](#)
- [CMC ウェブインタフェースを使用したネットワークの設定](#)
- [FlexAddress メザニンカードのファブリック接続の表示](#)
- [iDRAC ファームウェアのアップデート](#)

本項では、iDRAC へのアクセスの確立方法と、iDRAC を使える管理環境に設定する方法を説明します。

作業を開始する前に

iDRAC を設定する前に、次のマニュアルを用意します。

- 1 Dell Chassis Management Controller ファームウェアユーザーガイド
- 1 Dell PowerEdge Installation and Server Management CD
- 1 Dell Systems Management Consoles CD
- 1 Dell PowerEdge Service and Diagnostic Utilities CD
- 1 Dell PowerEdge Documentation CD

iDRAC の設定に使用するインタフェース

iDRAC を設定するには、iDRAC 設定ユーティリティ、iDRAC ウェブインタフェース、ローカル RACADM CLI、または SM-CLP CLI を使用できます。管理下サーバーにオペレーティングシステムと Dell PowerEdge サーバー管理ソフトウェアをインストールすると、ローカル RACADM CLI が使用可能になります。[表 2-1](#) は、これらのインタフェースについて説明しています。

セキュリティを強化するために、iDRAC 設定ユーティリティまたはローカル RACADM CLI からの iDRAC 設定へのアクセスは、RACADM コマンド ([「RACADM サブコマンドの概要」](#)を参照) または GUI ([「設定へのローカルアクセスの有効化と無効化」](#)を参照) を使って無効にできます。

● **注意:** 複数の設定インタフェースを同時に使用すると、予想外の結果が生じることがあります。

表 2-1 設定インタフェース

インタフェース	説明
iDRAC 設定ユーティリティ	起動時にアクセスできる設定ユーティリティは、新しい PowerEdge サーバーをインストールする場合に便利です。ネットワークや基本的なセキュリティ機能の設定や、その他の機能を有効にするときに使用してください。
iDRAC ウェブインタフェース	iDRAC ウェブインタフェースは、iDRAC をインタラクティブに管理しながら、管理下サーバーを監視できるブラウザベースの管理アプリケーションです。システム正常性の監視、システムイベントログの表示、ローカル iDRAC ユーザーの管理、CMC ウェブインタフェースやコンソールリダイレクトセッションの開始などの日常的なタスクに使用する主要インタフェースです。
CMC ウェブインタフェース	CMC ウェブインタフェースは、シャーシの監視と管理のほかに、管理下サーバーのステータスの表示、iDRAC のネットワーク設定、管理下サーバーの起動、停止、リセットなどにも使用できます。
シャーシ LCD パネル	iDRAC を搭載したシャーシの LCD パネルは、シャーシ内のサーバーの大まかなステータスを表示するために使用できます。CMC の初期設定中、設定ウィザードを使用して iDRAC ネットワークの DHCP 設定を有効にできます。
ローカル RACADM	ローカル RACADM コマンドラインインタフェースは管理下サーバーで実行されます。このインタフェースには、iKVM または iDRAC ウェブインタフェースから開始したコンソールリダイレクトセッションからアクセスします。RACADM は、Dell OpenManage Server Administrator のインストール時に管理下サーバーにインストールされます。 RACADM コマンドは、iDRAC のほぼすべての機能へのアクセスを提供します。センサーデータや、システムイベントログのレコード、iDRAC で管理される現在のステータスや設定値を調べることができます。さらに、iDRAC 設定値の変更、ローカルユーザーの管理、機能の有効 / 無効、管理下サーバーのシャットダウンや再起動などの電源機能の実行も可能です。
IVM-CLI	iDRAC 仮想メディアコマンドラインインタフェース (IVM-CLI) は、管理下サーバーに管理ステーション上のメディアへのアクセスを提供します。複数の管理下サーバーにオペレーティングシステムをインストールするスクリプトの作成に便利です。
SM-CLP	SM-CLP は、iDRAC に組み込まれたサーバー管理ワークグループサーバー管理 - コマンドラインプロトコル (SM-CLP) の実装です。SM-CLP コマンドラインには、Telnet や SSH を使用して iDRAC にログインするとアクセスできます。 SM-CLP コマンドは、ローカル RACADM コマンドの便利なサブセットを実装しています。これらのコマンドは管理ステーションのコマンドラインから実行できるため、スクリプトの記述に便利です。コマンドの出力は、XML などの明確なフォーマットで取得でき、スクリプトの記述や、既存のレポートツールや管理ツールとの統合を円滑にします。 RACADM コマンドと SM-CLP コマンドの比較については、 「RACADM と SM-CLP との対応付け」 を参照してください。
IPMI	IPMI は、iDRAC などの組み込み管理サブシステムが他の組み込みシステムや管理アプリケーションと通信するための標準的な方法を定義しています。 IPMI のプラットフォームイベントフィルタ (PEF) やプラットフォームイベントトラップ (PET) の設定には、iDRAC ウェブインタフェース、SM-CLP、または RACADM コマンドを使用できます。


PEF は、ある状態を検出したときに、選択可能な処置(たとえば管理下サーバーの再起動)を iDRAC に実行させます。PET は、特定のイベントまたは状態を検出したときに電子メールまたは IPMI 警告を送信するよう iDRAC に命令します。

また iDRAC では、IPMI オーバー LAN を有効にしている場合に `ipmitool` や `ipmishell` などの標準的な IPMI ツールも使用できます。

設定タスク

本項では、管理ステーション、iDRAC、管理下サーバーの設定タスクについて概説します。実行するタスクには、iDRAC をリモートで使用するための設定、使用する iDRAC 機能の設定、管理下サーバーへのオペレーティングシステムのインストール、管理ステーションおよび管理下サーバーへの管理ソフトウェアのインストールなどがあります。

タスクの下に、各タスクの実行に使用可能な設定タスクが一覧になっています。

 **メモ:** このガイドの設定手順を実行する前に、CMC および I/O モジュールをシャーシに取り付けて設定する必要があります。また、PowerEdge サーバーもシャーシ内に物理的に設置する必要があります。


管理ステーションの設定

Dell OpenManage ソフトウェア、ウェブブラウザ、その他のソフトウェアユーティリティをインストールして、管理ステーションを設定します。


- 1 [管理ステーションの設定](#) を参照してください。


iDRAC ネットワークの設定

iDRAC ネットワークを有効にし、IP、ネットマスク、ゲートウェイ、DNS アドレスを設定します。

 **メモ:** iDRAC 設定ユーティリティまたはローカル RACADM CLI からの iDRAC 設定へのアクセスは、RACADM コマンド([「RACADM サブコマンドの概要」](#)を参照)または GUI ([「設定へのローカルアクセスの有効化と無効化」](#)を参照)を使って無効にできます。

 **メモ:** iDRAC ネットワーク設定を変更すると、iDRAC との現在のネットワーク接続がすべて終了します。

 **メモ:** LCD パネルを使用してサーバーを設定するオプションは、CMC の初期設定中のみで使用できます。いったんシャーシを導入すると、LCD パネルを使用して iDRAC を再設定することはできません。

 **メモ:** LCD パネルは、iDRAC ネットワークを設定するために DHCP を有効にする際にも使用できます。静的アドレスを割り当てるには、iDRAC 設定ユーティリティまたは CMC ウェブインタフェースを使用します。

- 1 シャーシの LCD パネル - 『Dell Chassis Management Controller ファームウェアユーザーガイド』を参照してください。
- 1 iDRAC 設定ユーティリティ - 「[LAN](#)」を参照してください。
- 1 CMC ウェブインタフェース - 「[CMC ウェブインタフェースを使用したネットワークの設定](#)」を参照してください。
- 1 RACADM - 「[cfdlanNetworking](#)」を参照してください。

iDRAC ユーザーの設定

ローカル iDRAC のユーザーと権限を設定します。iDRAC では、ファームウェアに 16 のローカルユーザーを表示するテーブルがあります。これらのユーザーにユーザー名、パスワード、および役割(ロール)を設定できます。

- 1 iDRAC 設定ユーティリティ(システム管理ユーザーのみの設定) - 「[LAN ユーザー設定](#)」を参照してください。
- 1 iDRAC ウェブインタフェース - 「[iDRAC ユーザーの追加と設定](#)」を参照してください。
- 1 RACADM - 「[iDRAC ユーザーの追加](#)」を参照してください。

Active Directory の設定

ローカル iDRAC ユーザーに加え、iDRAC ユーザーログインの認証には Microsoft® Active Directory® も使用できます。

- 1 「[Microsoft Active Directory での iDRAC の使用](#)」を参照してください。

IP フィルタおよび IP ブロックの設定

ユーザー認証に加え、定義した範囲外の IP アドレスからの接続を拒否したり、設定した時間枠内に複数回認証に失敗した IP アドレスからの接続を一時的にブロックして、不正なアクセスを防止できます。

- 1 iDRAC ウェブインタフェース - 「[IP フィルタおよび IP ブロックの設定](#)」を参照してください。
- 1 RACADM - 「[IP フィルタ\(IPRange\)の設定](#)」、「[IP ブロックの設定](#)」を参照してください。

プラットフォームイベントの設定

プラットフォームイベントは、iDRAC が管理下サーバーのセンサーから「警告」状態または「重要」状態を検知した場合に発生します。

プラットフォームイベントフィルタ(PEF)を設定して、検出するイベントを選択します(たとえば、あるイベントが検出されたときに管理下サーバーを再起動する)。

- 1 iDRAC ウェブインタフェース - 「[プラットフォームイベントフィルタ \(PEF\) の設定](#)」を参照してください。
- 1 RACADM - 「[PEF の設定](#)」を参照してください。

プラットフォームイベントトラップ(PET)を設定して、IPMI ソフトウェアを搭載した管理ステーションなどの IP アドレスに警告通知を送信したり、指定の電子メールアドレスに電子メールを送信します。

- 1 iDRAC ウェブインタフェース - 「[プラットフォームイベントトラップ\(PET\)の設定](#)」を参照してください。
- 1 RACADM - [PET の設定](#)

設定へのローカルアクセスの有効化と無効化

ネットワーク設定やユーザー権限などの重要な設定パラメータへのアクセスは、無効にすることができます。アクセスを無効にすると、再起動を行ってもその設定が保持されます。設定への書き込みアクセスは、ローカル RACADM プログラムと iDRAC 設定ユーティリティの両方で(起動時に)ブロックされます。設定パラメータへのウェブアクセスが妨げられることはなく、いつでも設定データを表示できます。iDRAC ウェブインタフェースの詳細については、「[設定へのローカルアクセスの有効化と無効化](#)」を参照してください。cfgRac Tuning コマンドの詳細については、「[cfgRacTuning](#)」を参照してください。

シリアルオーバー LAN の設定

シリアルオーバー LAN(SOL)は、管理下サーバーのシリアルポート I/O をネットワーク上にリダイレクトできる IPMI 機能です。SOL は、iDRAC のコンソールリダイレクト機能を有効にします。

- 1 iDRAC ウェブインタフェース - 「[設定へのローカルアクセスの有効化と無効化](#)」を参照してください。
- 1 「[GUI コンソールリダイレクトの使用](#)」も参照してください。

iDRAC サービスの設定

iDRAC ネットワークサービス(Telnet、SSH、ウェブサーバーインタフェースなど)を有効 / 無効にしたり、ポートや他のサービスパラメータを再設定します。

- 1 iDRAC ウェブインタフェース - 「[iDRAC サービスの設定](#)」を参照してください。
- 1 RACADM - 「[ローカル RACADM を使用した iDRAC Telnet および SSH サービスの設定](#)」を参照してください。

セキュアソケットレイヤ(SSL)の設定

iDRAC ウェブサーバーの SSL の設定

- 1 iDRAC ウェブインタフェース - 「[SSL \(Secure Sockets Layer\)](#)」を参照してください。
- 1 RACADM - 「[cfgRacSecurity](#)」、「[sslicsrqen](#)」、「[sslicertupload](#)」、「[sslicertdownload](#)」、「[sslicertview](#)」を参照してください。

仮想メディアの設定

PowerEdge サーバーにオペレーティングシステムをインストールできるように、仮想メディア機能を設定します。仮想メディアを使用すると、管理下サーバーは管理ステーション上のメディアデバイスや、ネットワーク共有フォルダ内の ISO CD/DVD イメージに、それらが管理下サーバーにあるかのようにアクセスできます。

- 1 iDRAC ウェブインタフェース - 「[仮想メディアの設定と使用法](#)」を参照してください。
- 1 iDRAC 設定ユーティリティ - 「[仮想メディア](#)」を参照してください。

管理下サーバーソフトウェアのインストール

仮想メディアを使用して PowerEdge サーバーに Microsoft Windows または Linux オペレーティングシステムをインストールし、PowerEdge 管理下サーバーに Dell OpenManage ソフトウェアをインストールして、前回クラッシュ画面機能を設定します。

- 1 コンソールリダイレクト - 「[管理下サーバーへのソフトウェアのインストール](#)」を参照してください。
- 1 IVM-CLI - 「[仮想メディアコマンドラインインタフェースユーティリティの使用](#)」を参照してください。

管理下サーバーへの前回クラッシュ画面機能の設定

オペレーティングシステムのクラッシュまたはフリーズ後に iDRAC が画面イメージをキャプチャできるように管理下サーバーを設定します。

- 1 管理下サーバー - 「[管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定](#)」, 「[Windows の自動再起動オプションを無効にする](#)」を参照してください。

CMC ウェブインタフェースを使用したネットワークの設定

- 📌 **メモ:** CMC から iDRAC ネットワーク設定を行うには、シャーン設定の Administrator 権限が必要です。
- 📌 **メモ:** デフォルトの CMC ユーザーは root で、デフォルトのパスワードは calvin です。
- 📌 **メモ:** CMC の IP アドレスは、システム → リモートアクセス → CMC の順にクリックすると iDRAC ウェブインタフェースに表示されます。このページから CMC ウェブインタフェースを起動することもできます。

1. ウェブブラウザに <https://<CMC IP アドレス>> または <https://<CMC DNS 名>> 形式の URL を入力して、CMC ウェブユーザーインタフェースにログインします。
2. CMC のユーザー名とパスワードを入力して、OK をクリックします。
3. 左列の Chassis(シャーン)の隣にあるプラス(+)記号をクリックし、Servers(サーバー)をクリックします。
4. **セットアップ** → **ネットワーク導入** をクリックします。
5. LAN を有効にする 見出しの下のサーバーの隣のチェックボックスをオンにしてサーバーの LAN を有効にします。
6. IPMI オーバー LAN を有効にする 見出しの下にあるサーバーの隣のチェックボックスをオンかオフにして、IPMI オーバー LAN の有効 / 無効を切り替えます。
7. DHCP を有効にする 見出しの下のサーバーの隣のチェックボックスをオンかオフにして、サーバーの DHCP を有効または無効にします。
8. DHCP が無効になっている場合は、サーバーの静的 IP アドレス、ネットマスク、およびデフォルトのゲートウェイを入力します。
9. ページ下の **適用** をクリックします。

FlexAddress メザニンカードのファブリック接続の表示

M1000e には、マルチレベル / マルチスタンダードの高度なネットワーキングシステムである FlexAddress(フレックスアドレス)が含まれています。FlexAddress では、管理下サーバーの各ポート接続に、シャーン割り当ての永続的なワールドワイドネームと MAC アドレス(WWN/MAC)を使用できます。

- 📌 **注意:** 管理下サーバーの電源を投入できなくなるようなエラーを防ぐために、各ポートとファブリック接続には正しいタイプのメザニンカードをインストールする必要があります。

FlexAddress 機能の設定は、CMC ウェブインタフェースを使って行います。FlexAddress 機能とその設定の詳細は、『Dell Chassis Management Controller ファームウェアバージョン 1.20 ユーザーガイド』を参照してください。

FlexAddress 機能を有効にしてキャビネットに対して設定したら、システム → プロパティ → WWN/MAC をクリックして、インストールされているメザニンカード、カードが接続されているファブリックとポート、ファブリックポートの位置、ファブリックのタイプ、およびインストールされている組み込み Ethernet およびオプションのメザニンカードポートそれぞれのサーバー設定またはシャーン割り当ての MAC アドレスを一覧表示します。

FlexAddress が設定されている場合に、インストールされているメザニンカードのリストとそのタイプを表示するには、システム → プロパティ → 概要をクリックします。

iDRAC ファームウェアのアップデート

iDRAC ファームウェアをアップデートすると、iDRAC フラッシュメモリに新しいファームウェアイメージがインストールされます。次のいずれかの方法でファームウェアをアップデートできます。

- 1 SM-CLP load コマンド
- 1 iDRAC ウェブインタフェース
- 1 Dell アップデートパッケージ(Linux または Microsoft Windows 用)
- 1 DOS iDRAC ファームウェアアップデートユーティリティ
- 1 CMC ウェブインタフェース(iDRAC ファームウェアが破損している場合のみ)

ファームウェアまたはアップデートパッケージのダウンロード


ファームウェアを support.dell.com からダウンロードします。ファームウェアイメージは、さまざまなアップデート方法に対応するように複数のフォーマットで入手可能です。


iDRAC ウェブインタフェースまたは SM-CLP を使用して iDRAC ファームウェアをアップデートする場合や、CMC ウェブインタフェースを使用して iDRAC を復旧する場合には、自己解凍式アーカイブとしてパッケージ化されているバイナリイメージをダウンロードします。

管理下サーバーから iDRAC ファームウェアをアップデートするには、アップデートする iDRAC のサーバーで実行しているオペレーティングシステム専用の Dell アップデートパッケージ(DUP)をダウンロードします。

DOS iDRAC ファームウェアアップデートユーティリティを使用して iDRAC ファームウェアをアップデートするには、自己解凍式のアーカイブファイルにパッケージ化されたアップデートユーティリティとバイナリイメージの両方をダウンロードします。

ファームウェアアップデートの実行


 **メモ:** iDRAC ファームウェアアップデートが開始すると、既存の iDRAC セッションがすべて切断され、アップデートプロセスが完了するまで新しいセッションは実行できません。

 **メモ:** シャーシのファンは iDRAC ファームウェアアップデート中 100% で稼働します。アップデートが完了すると、正常なファン速度制御が再開されます。これは正常な動作で、センサー情報を CMC に送信できないときにサーバーをオーバーヒートから保護するように設計されています。


Linux または Microsoft Windows 用の Dell アップデートパッケージを使用するには、管理下サーバーでオペレーティングシステム専用の DUP を実行してください。


SM-CLP load コマンドを使用する場合は、簡易ファイル転送プロトコル(TFTP)サーバーが iDRAC に配信できるディレクトリにファームウェアのバイナリイメージを保存してください。「[SM-CLP を使用した iDRAC ファームウェアのアップデート](#)」を参照してください。

iDRAC ウェブインタフェースまたは CMC ウェブインタフェースを使用する場合は、ウェブインタフェースを実行している管理ステーションにアクセスできるディスクにファームウェアのバイナリイメージを格納してください。「[iDRAC ファームウェアのアップデート](#)」を参照してください。

 **メモ:** iDRAC ウェブインタフェースを使用すると、iDRAC の設定を出荷時のデフォルト設定にリセットすることもできます。

iDRAC ファームウェアアップデートの完了前に進行が中断した場合など、CMC が iDRAC ファームウェアの破損を検出した場合にのみ、CMC ウェブインタフェースを使用してファームウェアをアップデートできます。「[CMC を使用した iDRAC ファームウェアのリカバリ](#)」を参照してください。

 **メモ:** CMC が iDRAC のファームウェアをアップデートすると、iDRAC は SSL 証明書の新しい SHA1 および MD5 キーを生成します。このキーはオープンしているウェブブラウザのキーとは異なるため、ファームウェアアップデートの完了後に iDRAC に接続されているブラウザウィンドウはすべて閉じてください。ブラウザウィンドウを閉じないと、**無効な証明書** というエラーメッセージが表示されます。

 **メモ:** iDRAC ファームウェアをバージョン 1.20 から以前のバージョンにバックデートする(戻す)場合は、ファームウェアが互換性のある ActiveX プラグインバージョンをインストールできるように、Windows ベースの管理ステーションにある既存の Internet Explorer ActiveX ブラウザプラグインを削除する必要があります。ActiveX プラグインを削除するには、`c:\%WINDIR%\Downloaded Program Files` で **DELL IMC KVM Viewer** ファイルを削除してください。

DOS アップデートユーティリティの使用

DOS アップデートユーティリティを使用して iDRAC ファームウェアをアップデートするには、管理下サーバーを DOS で起動し、`idrac16d` コマンドを実行してください。コマンドの構文は次のとおりです。

```
idrac16d [-f] [-i=<ファイル名>] [-l=<ログファイル>]
```


オプションなしで実行すると、`idrac16d` コマンドは現在のディレクトリにあるファームウェアイメージファイル `firmimg.imc` を使って iDRAC ファームウェアをアップデートします。

オプションは次のとおりです。

`-f` - アップデートを強制します。`-f` オプションは、ファームウェアを以前のイメージにダウングレードする場合に使用できます。

`-i=<ファイル名>` - ファームウェアのイメージが含まれているファイル名イメージを指定します。このオプションは、ファームウェアのファイル名をデフォルト名 `firmimg.imc` から変更した場合に必要です。

`-l=<ログファイル>` - アップデートアクティビティからの出力をログします。このオプションはデバッグに使用します。

 **注意:** `idrac16d` コマンドに入力する引数を間違えた場合や、`-h` オプションを入力した場合は、使用法の出力に追加オプションの `-nopresconfig` が表示されます。このオプションは、設定情報を保存せずにファームウェアをアップデートする場合に使用します。IP アドレス、ユーザー、パスワードなどの iDRAC の既存の設定情報をすべて削除してしまうため、このオプションは**使用しない**でください。

デジタル署名の検証


デジタル署名はファイルの署名者の身元を認証するために使用され、署名後に内容が変更されていないことを証明します。

デジタル署名を検証する Gnu Privacy Guard (GPG) をまだシステムにインストールしていない場合は、これをインストールしてください。標準的な検証方法を使用するには、次の手順に従います。

1. Dell Linux GPG 公開キーがまだない場合は、lists.us.dell.com に移動し、**Dell GPG 公開キー** リンクをクリックしてダウンロードします。ファイルをローカルシステムに保存します。デフォルト名は `linux-security-publickey.txt` です。

2. 次のコマンドを実行して、公開キーを gpg 信用データベースにインポートします。

```
gpg --import <公開キーのファイル名>
```

 **メモ:** プロセスを完了するには秘密キーが必要です。

3. 疑わしいキー警告を回避するには、Dell GPG 公開キーの信用レベルを変更します。

e. 次のコマンドを入力します。

```
gpg --edit-key 23B66A9D
```

- f. GPG キーエディタ内で、fpr と入力します。次のメッセージが表示されます。

```
pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Product Group) <linux-security@dell.com>
Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
( pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Product Group) <linux-security@dell.com>
Primary キーのフィンガープリント: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D)
```

インポートしたキーのフィンガープリントが上記と一致していれば、キーの正確なコピーを入手したことになります。

- g. GPG キーエディタに「trust」と入力します。次のメニューが表示されます。

```
Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from
different sources, etc.)
```

```
1 = I don't know or won't say
2 = I do NOT trust
3 = I trust marginally
4 = I trust fully
5 = I trust ultimately
m = back to the main menu
```

Your decision?


- h. 5 <Enter> と入力します。次のプロンプトが表示されます。

```
Do you really want to set this key to ultimate trust? (y/N)
( このキーを絶対的な信用に設定しますか? (y/N) )
```

- i. y <Enter> と入力して選択を確認します。
j. quit <Enter> と入力して、GPG キーエディタを終了します。

公開キーのインポートと検証は 1 回だけ実行します。

4. 必要なパッケージ(例、Linux DUP または自己解凍式アーカイブ)と関連する署名ファイルを Dell のサポートウェブサイト support.dell.com/support/downloads からダウンロードします。

 **メモ:** 各 Linux アップデートパッケージには、個別の署名ファイルがあり、同じウェブページにアップデートパッケージとして表示されます。検証には、アップデートパッケージおよびそれに関連する署名ファイルの両方が必要です。デフォルトでは、署名ファイルの名前は DUP のファイル名と同じで、拡張子は .sign です。たとえば、Linux DUP の名前が PEM600_BIOS_LX_2.1.2.BIN の場合は、その署名ファイル名は PEM600_BIOS_LX_2.1.2.BIN.sign になります。iDRAC ファームウェアイメージには、ファームウェアイメージと共に自己解凍式アーカイブに含まれる .sign ファイルが関連付けられています。ファイルをダウンロードするには、ダウンロードリンクを右クリックし、ファイルオプションの **名前を付けて保存...** を選択します。

5. アップデートパッケージの検証:

```
gpg --verify <Linux アップデートパッケージの署名ファイル名> <Linux アップデートパッケージのファイル名>
```

次に、PowerEdge M600 BIOS アップデートパッケージを検証する手順の例を示します。

1. 次の 2 ファイルを support.dell.com からダウンロードします。

```
1 PEM600_BIOS_LX_2.1.2.BIN.sign
1 PEM600_BIOS_LX_2.1.2.BIN
```

2. 次のコマンドラインを実行して公開キーをインポートします。

```
gpg --import <linux-security-publickey.txt>
```

次の出力メッセージが表示されます。

```
gpg: key 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed
gpg: Total number processed: 1
gpg: unchanged: 1
```

3. Dell 公開キーの GPG 信用レベルを設定します。(まだ設定していない場合)

- a. 次のコマンドを入力します。

```
gpg --edit-key 23B66A9D
```

- b. コマンドプロンプトで、次のコマンドを入力します。

```
fpr
trust
```

- c. 5 <Enter> と入力して、メニューから **絶対的に信用する** を選択します。
d. y <Enter> と入力して選択を確認します。
e. quit <Enter> と入力して、GPG キーエディタを終了します。


これで、Dell 公開キーの検証が完了します。

4. 次のコマンドを実行して、PEM600 BIOS パッケージのデジタル署名を検証します。

```
gpg --verify PEM600_BIOS_LX_2.1.2.BIN.sign PEM600_BIOS_LX_2.1.2.BIN
```

次の出力メッセージが表示されます。

```
gpg: Signature made Fri Jul 11 15:03:47 2008 CDT using DSA key ID 23B66A9D
gpg: Good signature from "Dell, Inc. (Product Group) <linux-security@dell.com>"
```

 **メモ:** 「手順 3」で示したようにキーを検証しなかった場合は、次の追加メッセージが表示されます。

```
gpg: 警告: このキーは信頼性のある署名で認証されていません。
gpg: この署名が所有者のものかどうか識別できません。
Primary キーのフィンガープリント: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
```

ブラウザのキャッシュをクリアします。

最新の iDRAC の機能を使用するには、ブラウザのキャッシュをクリアして、システムに格納されている古い ウェブページをすべて削除する必要があります。

Internet Explorer

1. Internet Explorer を起動します。
2. ツール をクリックして、**インターネットオプション** をクリックします。
インターネットオプション ウィンドウが表示されます。
3. **全般** タブをクリックします。
4. **インターネット一時ファイル** で、**ファイルの削除** をクリックします。
ファイルの削除 ウィンドウが表示されます。
5. **すべてのオフラインコンテンツを削除** をクリックしてチェックし、**OK** をクリックします。
6. **OK** をクリックして、**インターネットオプション** ウィンドウを閉じます。

Firefox.

1. Firefox を起動します。
2. **編集** → **プリファランス** をクリックします。
3. **Privacy(プライバシー)** タブをクリックします。
4. **Clear Cache Now(今すぐキャッシュをクリア)** をクリックします。
5. **Close(閉じる)** をクリックします。

[目次ページに戻る](#)

[目次ページに戻る](#)

管理ステーションの設定

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [管理ステーションの設定手順](#)
- [管理ステーションのネットワーク要件](#)
- [対応ウェブブラウザの設定](#)
- [Java Runtime Environment \(JRE\) のインストール](#)
- [Telnet または SSH クライアントのインストール](#)
- [TFTP サーバーのインストール](#)
- [Dell OpenManage IT Assistant のインストール](#)

管理ステーションは、シャーシ内の PowerEdge サーバーとその他のモジュールの監視と管理に使用するコンピュータです。本項では、iDRAC と連動する管理ステーションを設定するソフトウェアのインストールと設定タスクについて説明します。iDRAC の設定を開始する前に、本項の手順に従って必要なツールのインストールと設定を行ってください。

管理ステーションの設定手順

管理ステーションを設定するには、次の手順を実行してください。

1. 管理ステーションネットワークを設定します。
2. 対応ウェブブラウザをインストールして設定します。
3. Java Runtime Environment (JRE)をインストールします(Windows の場合はオプション)。
4. 必要に応じて Telnet または SSH クライアントをインストールします。
5. 必要に応じて TFTP サーバーをインストールします。
6. Dell OpenManage IT Assistant をインストールします(オプション)。

管理ステーションのネットワーク要件

iDRAC にアクセスするには、管理ステーションが「GB1」というラベルの CMC RJ45 接続ポートと同じネットワーク上に存在する必要があります。管理ステーションが LAN 経由で iDRAC にアクセスできても管理下サーバーにはアクセスできないように、管理下サーバーのネットワークから CMC ネットワークを切り離すことも可能です。


iDRAC コンソールリダイレクト機能(「[GUI コンソールリダイレクトの使用](#)」を参照)を使用すると、サーバーのポートにネットワークアクセスできない場合でも、管理下サーバーのコンソールにアクセスできます。iDRAC 機能を使用すると、コンピュータの再起動など、管理下サーバーの一部の管理機能も実行できます。ただし、管理下サーバーでホストされるネットワークやアプリケーションサービスにアクセスするには、管理コンピュータに追加の NIC が必要な場合があります。

対応ウェブブラウザの設定

この項では、iDRAC ウェブインタフェースと併用する対応ウェブブラウザの設定手順について説明します。対応ウェブブラウザについては、「[対応ウェブブラウザ](#)」のリストを参照してください。

ウェブブラウザのオープン

iDRAC ウェブインタフェースは、幅 800 ピクセル × 高さ 600 ピクセル以上の画面解像度を使い、対応ウェブブラウザで表示するようにデザインされています。インタフェースを表示して全機能にアクセスするには、必要に応じて解像度を 800 × 600 ピクセル以上に設定したり、ブラウザのサイズを変更してください。

 **メモ:** Internet Explorer 6 を使用している場合は、状況によって(特に、ファームウェアのアップデート後の最初のセッション時に)、メインブラウザウィンドウのページが一部だけ表示され、**完了、エラーが発生しました**というメッセージがステータスバーに表示されます。このエラーは、接続上の問題がある場合にも発生します。これは Internet Explorer 6 の既知の問題です。この場合は、ブラウザを閉じてから、再スタートしてください。

ウェブインタフェースに接続するウェブブラウザの設定


プロキシサーバー経由でインターネットに接続している管理ステーションから iDRAC のウェブインタフェースに接続する場合は、このサーバーからインターネットにアクセスするようにウェブブラウザを設定する必要があります。

Internet Explorer のウェブブラウザがプロキシサーバーにアクセスするように設定するには、次の手順を実行してください。

1. ウェブブラウザのウィンドウを開きます。

2. ツール をクリックして、インターネットオプション をクリックします。

インターネットオプション ウィンドウが表示されます。

 **メモ:** Internet Explorer のデフォルトのセキュリティレベルは、バージョンによって異なります。システムを正しく機能させるために、**詳細設定** タブをクリックして、**インストールオンデマンドを有効にする(その他)**、**サードパーティ製のブラウザ拡張を有効にする**、**Sun Java を有効にする**、および **SSL 3.0 を使用する** にチェックマークが付いていることを確認します(オプション名はバージョンによって異なります)。設定を変更した場合は、Internet Explorer を再スタートします。

3. 接続タブをクリックします。
4. ローカルエリアネットワーク(LAN)設定 で LAN 設定 をクリックします。
5. プロキシサーバーを使用 チェックボックスがオンになっている場合は、ローカルアドレスにはプロキシサーバーを使用しない チェックボックスをオンにします。
6. OK を 2 度クリックします。

信用できるドメインリストへの iDRAC の追加

ウェブブラウザを使って iDRAC ウェブインタフェースにアクセスする際、iDRAC の IP アドレスが信用するドメインのリストにない場合は、IP アドレスをリストに加えるように要求されることがあります。追加が完了すると、更新 をクリックまたはウェブブラウザを再起動し、iDRAC ウェブインタフェースへの接続を確立します。

他言語のウェブインタフェースの表示

iDRAC ウェブインタフェースは、次のオペレーティングシステム言語に対応しています。

- 1 英語 (en-us)
- 1 フランス語 (fr)
- 1 ドイツ語 (de)
- 1 スペイン語 (es)
- 1 日本語 (ja)
- 1 簡体字中国語 (zh-cn)

かつこの ISO 識別子は、サポートされている特定言語のタイプを示します。他の方言や言語でのインタフェースの使用はサポートされておらず、意図したように動作しない可能性があります。一部の対応言語で全機能を表示するには、ブラウザウィンドウを 1024 ピクセル幅にサイズ変更する必要があります。

iDRAC ウェブインタフェースは、前述の特定言語タイプに対して、ローカライズされたキーボードを使って操作するようにデザインされています。コンソールリダイレクトといった iDRAC ウェブインタフェースの一部の機能では、特定の機能や文字にアクセスするために追加手順が必要になる場合があります。こうした状況でのローカライズされたキーボードの使い方の詳細は、「[ビデオビューアの使用](#)」を参照してください。他のキーボードの使用はサポートされておらず、予期せぬ問題が発生する可能性があります。

Internet Explorer 6.0(Windows)

Internet Explorer で iDRAC ウェブインタフェースを他の言語で表示するには、次の手順を実行してください。

1. ツール をクリックして、インターネットオプション を選択します。
2. インターネットオプション ウィンドウで 言語 をクリックします。
3. 言語の優先順位 ウィンドウで 追加 をクリックします。
4. 言語の追加 ウィンドウでサポートされている言語を選択します。
複数の言語を選択するには、<Ctrl> を押しながら選択します。
5. 優先言語を選択して 上に移動 をクリックし、その言語をリストの先頭に移動します。
6. 言語設定 ウィンドウで OK をクリックします。
7. OK をクリックします。

Firefox 1.5(Linux)

Firefox 1.5 で iDRAC ウェブインタフェースを他の言語で表示するには、次の手順を実行してください。

1. **編集**→**設定** の順にクリックし、**詳細設定** タブをクリックします。
2. **言語** セクションで **選択** をクリックします。
3. **追加する言語を選択...** をクリックします。
4. 対応言語を選択し、**追加** をクリックします。
5. 使用する言語を選択し、**上へ移動** をクリックしてその言語をリストの一番上に移動します。
6. 言語メニューで **OK** をクリックします。
7. **OK** をクリックします。

Firefox 2.0(Linux または Windows)

Firefox 2.0 で iDRAC ウェブインタフェースを他の言語で表示するには、次の手順を実行してください。

1. **ツール→オプション**をクリックして、**詳細設定** タブをクリックします。
2. **言語** で **選択** をクリックします。
言語 ウィンドウが表示されます。
3. **追加する言語を選択...** ドロップダウンメニューで、対応言語をクリックしてハイライトし、**追加** をクリックします。
4. 使用する言語をクリックして選択し、**上へ移動** をクリックしてその言語をリストの一番上に移動します。
5. **OK** をクリックして、**言語** ウィンドウを閉じます。
6. **OK** をクリックして、**言語** ウィンドウを閉じます。

Linux のロケール設定

コンソールリダイレクトビューアで正しく表示するには、UTF-8 文字コードが必要です。文字化けしている場合は、ロケールを確認し、必要に応じて文字コードをリセットしてください。

次の手順は、簡体字中国語 GUI の Red Hat® Enterprise Linux® クライアントで文字コードを設定する方法です。

1. コマンド端末を開きます。
2. locale と入力し、<Enter> を押します。次のような出力画面が表示されます。

```
LANG=zh_CN.UTF-8
LC_CTYPE=zh_CN.UTF-8
LC_NUMERIC=zh_CN.UTF-8
LC_TIME=zh_CN.UTF-8
LC_COLLATE=zh_CN.UTF-8
LC_MONETARY=zh_CN.UTF-8
LC_MESSAGES=zh_CN.UTF-8
LC_PAPER=zh_CN.UTF-8
LC_NAME=zh_CN.UTF-8
LC_ADDRESS=zh_CN.UTF-8
LC_TELEPHONE=zh_CN.UTF-8
LC_MEASUREMENT=zh_CN.UTF-8
LC_IDENTIFICATION=zh_CN.UTF-8
LC_ALL=
```

3. 値に「zh_CN.UTF-8」が含まれる場合は、変更する必要はありません。値に「zh_CN.UTF-8」が含まれない場合は、手順 4 に進みます。
4. テキストエディタで /etc/sysconfig/i18n ファイルを編集します。
5. ファイルに次の変更を加えます。

現在のエントリ:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CN.GB2312:zh_CN:zh"
```

アップデート後のエントリ:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CN.GB2312:zh_CN:zh"
```

6. ログアウトしてから、オペレーティングシステムにログインします。

他の言語から切り換える場合、この修正が反映されていることを確認してください。有効になっていない場合は、この手順を繰り返します。


Firefox のホワイトリスト機能を無効にする

Firefox には、プラグインをホストする各サイトにプラグインをインストールするときにユーザーの許可を求める「ホワイトリスト」と呼ばれるセキュリティ機能があります。ホワイトリスト機能が有効な場合、ビューアのバージョンは同じでも iDRAC にアクセスするたびにコンソールリダイレクトビューアのインストールが要求されます。

ホワイトリスト機能を無効にし、プラグインの不要なインストールを回避するには、次の手順を実行してください。

1. Firefox ウェブブラウザのウィンドウを開きます。
2. アドレスフィールドに `about:config` と入力し、<Enter> を押します。
3. Preference Name 列で、`xpinstall.whitelist.required` を見つけてダブルクリックします。
Preference Name、Status、Type、Value の値が太字で表示されます。Status の値は `user set` に変わり、Value の値は `false` に変わります。
4. Preferences→Name 列で、`xpinstall.enabled` を見つけます。
Value が `true` になっていることを確認します。なっていない場合は、`xpinstall.enabled` をダブルクリックして Value を `true` に設定します。

Java Runtime Environment (JRE) のインストール


 **メモ:** Internet Explorer ブラウザを使用している場合、コンソールビューア用に ActiveX コントロールが提供されます。JRE をインストールし、ビューアの起動前に iDRAC ウェブインタフェースでコンソールビューアを設定すると、Internet Explorer で Java コンソールビューアも使用できます。詳細については、「[iDRAC ウェブインタフェースでのコンソールリダイレクトの設定](#)」を参照してください。

ビューアを起動する前に、代わりに Java Viewer を使用する選択もできます。

Firefox ブラウザを使用している場合、コンソールリダイレクト機能を使用するには JRE (または Java Development Kit [JDK]) をインストールする必要があります。コンソールビューアは、iDRAC ウェブインタフェースから管理ステーションにダウンロードされ、管理ステーション上で Java Web Start によって起動されます。


[java.sun.com](#) へアクセスし、JRE または JDK をインストールします。バージョン 1.6 (Java 6.0) 以降が推奨されます。

Java Web Start プログラムが、JRE または JDK とともに自動的にインストールされます。ファイル `jviewer.jnlp` がデスクトップにダウンロードされて、何を実行するかを尋ねるダイアログボックスが表示されます。必要に応じて、ブラウザで `jnlp` 拡張タイプを Java Web Start アプリケーションと関連付けてください。**プログラムを指定して開く** オプションを選択し、JRE インストールディレクトリの `bin` サブディレクトリにある `javaws` アプリケーションを選択します。

 **メモ:** JRE または JDK のインストール後、`jnlp` ファイルタイプが Java Web Start と関連付けられていない場合は、この関連を手動で設定できます。Windows (`javaws.exe`) の場合は、**スタート→コントロールパネル→Appearance and Themes→フォルダオプション** をクリックします。ファイルの種類 タブで、登録されているファイルの種類 から `jnlp` をハイライトして、**変更** をクリックします。Linux (`javaws`) の場合は、Firefox をスタートし、**編集→プリファレンス→ダウンロード** をクリックしてから、**アクションの表示と編集** をクリックします。


Linux の場合は、JRE または JDK をインストールしたら、使用システムの PATH の前に Java bin ディレクトリへのパスを追加してください。たとえば、Java が `/usr/java` にインストールされている場合は、次の行をローカルの `.bashrc` または `/etc/profile` に追加します。

```
PATH=/usr/java/bin:$PATH; export PATH
```

 **メモ:** ファイルにはすでに PATH 修正行が含まれているかも知れません。入力したパス情報によって衝突が起きないように注意してください。

Telnet または SSH クライアントのインストール

デフォルトで、iDRAC の Telnet サービスは無効に、SSH サービスは有効になっています。Telnet はセキュアではないプロトコルのため、SSH クライアントをインストールできない場合、またはネットワーク接続がセキュアな場合にのみ使用してください。

 **メモ:** iDRAC へのアクティブな Telnet または SSH 接続は、1 度に 1 つのみが可能です。アクティブな接続が存在する場合、他の接続試行は拒否されます。

iDRAC での Telnet

Telnet は、Microsoft® Windows® および Linux オペレーティングシステムに含まれており、コマンドシェルから実行できます。オペレーティングシステムに組み込まれている標準バージョンのほか、さらに便利な機能の付いた有料 / 無料の Telnet クライアントをインストールすることもできます。

管理ステーションで Windows XP または Windows 2003 を実行している場合は、iDRAC の Telnet セッションで文字の不具合が発生する可能性があります。リターンキーが応答しなかったり、パスワードプロンプトが表示されないなど、ログインのフリーズ状態が発生することがあります。

この問題を解決するには、hotfix 824810 を Microsoft サポートウェブサイト support.microsoft.com からダウンロードしてください。詳細については、Microsoft 技術情報の記事 824810 を参照してください。

Telnet セッションのための Backspace キーの設定

一部の Telnet クライアントでは、<Backspace> キーを使用すると予想外の結果が生じることがあります。たとえば、セッションが ^h をエコーすることがあります。Microsoft と Linux の telnet クライアントではほとんどの場合、<Backspace> キーの使用を設定できます。

Microsoft telnet クライアントで <Backspace> キーを使えるように設定するには、次の手順を実行してください。

1. コマンドプロンプトウィンドウを開きます(必要な場合)。
2. telnet セッションを実行していない場合は、次のように入力します。

```
telnet
```

telnet セッションを実行している場合は、<Ctrl><]> を押します。

3. コマンドプロンプトで、次のコマンドを入力します。

```
set bsasdel
```

次のメッセージが表示されます。

Backspace will be sent as delete. (Backspace が Delete として送信されます。)

Linux の telnet セッションで <Backspace> キーを使えるように設定するには、次の手順を実行してください。

1. シェルを開いて次のように入力します。

```
stty erase ^h
```


2. コマンドプロンプトで、次のコマンドを入力します。

```
telnet
```

iDRAC での SSH

セキュアシェル(SSH)は、Telnet セッションと同じ機能を持つコマンドライン接続ですが、セキュリティを強化するためセッションのネゴシエーションと暗号化機能を備えています。iDRAC は、パスワード認証付きの SSH バージョン 2 に対応しています。iDRAC の場合、SSH はデフォルトで有効になっています。

管理下サーバーの iDRAC に接続する際に、管理ステーションで PuTTY(Windows)または OpenSSH(Linux)を使用できます。ログイン時にエラーが発生した場合は、ssh クライアントからエラーメッセージが発行されます。メッセージのテキストはクライアントによって異なり、iDRAC によって制御されたものではありません。

 **メモ:** OpenSSH は Windows の VT100 または ANSI 端末エミュレータから実行してください。Windows のコマンドプロンプトから OpenSSH を実行した場合は、一部の機能を使用できません(複数のキーが機能せず、グラフィックが表示されません)。

1 度にサポートされる Telnet または SSH セッションは 1 つだけです。セッションタイムアウトは、「[iDRAC プロパティデータベースのグループとオブジェクトの定義](#)」で説明したように、cfgSsnMgtSshIdleTimeout プロパティによって制御されます。

iDRAC 5 SSH の実装では、「[表 3-1](#)」に示すように複数の暗号化スキームがサポートされています。



 **メモ:** SSHv1 はサポートされていません。

表 3-1 暗号化スキーム

スキームの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024(ランダム)ビット(NIST 仕様)
対称暗号	1 AES256-CBC 1 RIJNDael256-CBC 1 AES192-CBC 1 RIJNDael192-CBC 1 AES128-CBC 1 RIJNDael128-CBC 1 BLOWFISH-128-CBC 1 3DES-192-CBC 1 ARCFOUR-128
メッセージの整合性	1 HMAC-SHA1-160 1 HMAC-SHA1-96 1 HMAC-MD5-128

	1 HMAC-MD5-96
認証	1 パスワード

TFTP サーバーのインストール

 **メモ:** SSL 証明書の転送および新規 iDRAC ファームウェアのアップロードに iDRAC ウェブインタフェースのみを使用する場合、TFTP サーバーは不要です。

簡易ファイル転送プロトコル (TFTP) は、ファイル転送プロトコル (FTP) を簡単にしたものです。iDRAC とのファイル転送に、SM-CLP および RACADM コマンドラインインタフェースと併用されます。

iDRAC とのファイルのコピーが必要になるのは、iDRAC ファームウェアをアップデートする場合か、iDRAC に証明書をインストールする場合のみです。これらのタスクを実行するときに SM-CLP または RACADM を使用する場合は、iDRAC が IP 番号または DNS 名でアクセスできるコンピュータで TFTP サーバーを実行している必要があります。

TFTP サーバーが既にリッスンしているかどうかを調べるには、Windows または Linux オペレーティングシステムの `netstat -a` コマンドを使用できます。TFTP のデフォルトポートはポート 69 です。サーバーが実行していない場合は、次の選択肢があります。

- 1 ネットワーク上で TFTP サービスを実行している別のコンピュータを検索する
- 1 Linux を使用している場合は、ディストリビューションで提供される TFTP サーバーをインストールする
- 1 Windows を使用している場合は、有料 / 無料の TFTP サーバーをインストールする

Dell OpenManage IT Assistant のインストール

システムには Dell OpenManage System Management Software Kit が同梱されています。このキットには次のコンポーネントが含まれますが、この限りではありません。

- 1 『Dell Systems Management Consoles CD』- Dell OpenManage IT Assistant をはじめとする最新の Dell システム管理コンソール製品のすべてが含まれています。
- 1 『Dell PowerEdge Service and Diagnostic Utilities CD』- システムの設定に必要なツールを提供し、システムのファームウェア、診断およびドライバを配布します。
- 1 『Dell PowerEdge Documentation CD』- システム、システム管理ソフトウェア製品、周辺機器および RAID コントローラなどについて説明した最新のマニュアルが含まれています。
- 1 Dell のサポートウェブサイトおよび Readme ファイル - Dell 製品に関する最新情報については、Readme ファイルおよび Dell のサポートウェブサイト support.dell.com を確認してください。

Dell OpenManage IT Assistant を含む管理コンソールソフトウェアを管理ステーションにインストールするには、『Dell System Management Consoles CD』を使用します。このソフトウェアのインストール手順については、『クイックインストールガイド』を参照してください。

[目次ページに戻る](#)

[目次ページに戻る](#)

管理下サーバー の設定

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [管理下サーバーへのソフトウェアのインストール](#)
- [管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定](#)
- [Windows の 自動再起動オプションを無効にする](#)

本項では、リモート管理機能を強化する管理下サーバーの設定タスクについて説明します。これらのタスクには、Dell Open Manage Server Administrator ソフトウェアのインストールおよび管理下サーバーの前回クラッシュ画面キャプチャ設定が含まれます。

管理下サーバーへのソフトウェアのインストール

Dell 管理ソフトウェアには、次の機能が含まれています。

- 1 ローカル RACADM CLI - 管理下システムから iDRAC の設定および管理を可能にします。設定タスクおよび管理タスクのスクリプトをサポートする強力なツールです。
- 1 iDRAC の前回クラッシュ画面機能を使用するには Server Administrator が必要です。
- 1 Server Administrator - ネットワーク上のリモートホストからリモートシステムを管理できるウェブインタフェース。
- 1 Server Administrator Instrumentation Service - 業界標準のシステム管理エージェントによって収集される詳細なエラー情報およびパフォーマンス情報へのアクセスを提供し、シャットダウン、起動、セキュリティを含む監視下システムのリモート管理を可能にします。
- 1 Server Administration Storage Management Service - 内蔵グラフィカル表示でストレージ管理情報を表示します。
- 1 Server Administrator ログ - システム、監視下ハードウェアイベント、POST イベント、システム警告に対して発行される、またはこれらによって発行されるコマンドのログを表示します。ログはホームページで表示したり、レポートとして印刷または保存したり、指定のサービス担当者に電子メールで送信できます。

Server Administrator をインストールするには、「Dell PowerEdge Installation and Server Management CD」を使用します。このソフトウェアのインストール手順については、『クイックインストールガイド』を参照してください。

管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定

iDRAC は、管理下システムのクラッシュ原因についてトラブルシューティングを支援するために前回クラッシュ画面をキャプチャし、ウェブインタフェースに表示できます。前回クラッシュ画面機能を有効にするには、次の手順を実行します。

1. 管理下サーバーソフトウェアをインストールします。管理下サーバーソフトウェアのインストールの詳細については、『Server Administrator ユーザーズガイド』を参照してください。
2. Microsoft® Windows® オペレーティングシステムを実行している場合、Windows の **起動と回復** で自動的に再起動する 機能が選択解除されていることを確認してください。
『[Windows の 自動再起動オプションを無効にする](#)』を参照してください。
3. iDRAC ウェブインタフェースで前回クラッシュ画面(デフォルトでは無効)を有効にします。

iDRAC ウェブインタフェースで前回クラッシュ画面機能を有効にするには、**システム** → **リモートアクセス** → **iDRAC** → **ネットワーク/セキュリティ** → **サービス** をクリックし、自動システム回復エージェント設定の見出しの下にある **有効** チェックボックスを選択します。

ローカル RACADM を使用して前回クラッシュ画面機能を有効にするには、管理下システムでコマンドプロンプトを開き、次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
```

4. Server Administrator ウェブインタフェースで、**自動リカバリ** タイマーを有効にし、**自動リカバリ** 処置を **リセット**、**電源オフ**、または **パワーサイクル(電源再投入)** に設定します。

自動リカバリ の設定手順の詳細については、『Server Administrator ユーザーズガイド』を参照してください。前回クラッシュ画面を確実にキャプチャするには、**自動リカバリ** タイマーを 60 秒以上に設定する必要があります。デフォルト設定は 480 秒です。

管理下サーバーの電源がオフの場合、**自動リカバリ** 処置が **シャットダウン** または **パワーサイクル** に設定されていると、前回クラッシュ画面を使用できません。

Windows の 自動再起動オプションを無効にする

iDRAC が前回クラッシュ画面をキャプチャできるようにするには、Microsoft Windows Server® または Windows Vista® を実行している管理下サーバーの **自動再起動** オプションを無効にします。

1. Windows **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. **詳細** タブをクリックします。
3. **起動と回復** で **設定** をクリックします。

4. **自動的に再起動する** チェックボックスを選択解除します。

5. **OK** を 2 度クリックします。

[目次ページに戻る](#)

[目次ページに戻る](#)

ウェブインタフェースを使用した iDRAC の設定

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [ウェブインタフェースへのアクセス](#)
- [iDRAC NIC の設定](#)
- [プラットフォームイベントの設定](#)
- [IPMI の設定](#)
- [iDRAC ユーザーの追加と設定](#)
- [SSL とデジタル証明書を使用した iDRAC 通信のセキュリティ](#)
- [Active Directory 証明書の設定と管理](#)
- [設定へのローカルアクセスの有効化と無効化](#)
- [シリアルオーバー LAN の設定](#)
- [iDRAC サービスの設定](#)
- [iDRAC ファームウェアのアップデート](#)

iDRAC は、iDRAC プロパティとユーザーの設定、リモート管理タスクの実行、リモート(管理下)システムの不具合のトラブルシューティングが可能なウェブインタフェースを提供します。日常のシステム管理に、iDRAC のウェブインタフェースを使用してください。この章では、iDRAC のウェブインタフェースを使って一般的なシステム管理タスクを実行する方法について説明し、関連情報へのリンクも掲載しています。

ほとんどのウェブインタフェース設定タスクは、ローカル RACADM コマンドまたは SM-CLP コマンドでも実行できます。

ローカル RACADM コマンドは、管理下サーバーから実行できます。ローカル RACADM の詳細については、「[ローカル RACADM コマンドラインインタフェースの使用](#)」を参照してください。

SM-CLP コマンドは、Telnet または SSH 接続によってリモートアクセス可能なシェルにて実行できます。SM-CLP の詳細については、「[iDRAC SM-CLP コマンドラインインタフェースの使用](#)」を参照してください。

ウェブインタフェースへのアクセス

iDRAC ウェブインタフェースにアクセスするには、次の手順を実行してください。

1. サポートされているウェブブラウザのウィンドウを開きます。

詳細については、「[対応ウェブブラウザ](#)」を参照してください。

2. **アドレス** フィールドに、`https://<iDRAC IP アドレス>` を入力し、Enter キーを押します。

デフォルトの HTTPS ポート番号(ポート 443)が変更されている場合は、次のように入力します。

`https://<iDRAC IP アドレス>:<ポート番号>`

iDRAC IP アドレス は iDRAC 用の IP アドレスで、ポート番号 は HTTPS ポート番号です。

iDRAC **ログイン** ウィンドウが表示されます。

ログイン

iDRAC ユーザーまたは Microsoft® Active Directory® ユーザーとして ログインできます。デフォルトのユーザー名とパスワードはそれぞれ `root` と `calvin` です。

iDRAC にログインするには、システム管理者から **iDRAC へのログイン** 権限が与えられている必要があります。

ログインするには、次の手順に従ってください。

1. **ユーザー名** フィールドで、以下のいずれかを入力します。

- 1 iDRAC ユーザー名。

ローカルユーザーのユーザー名は大文字と小文字が区別されます。たとえば、`root`、`it_user`、`john_doe` などです。

- 1 Active Directory ユーザー名。


Active Directory 名は、`<ドメイン>\<ユーザー名>`、`<ドメイン>/<ユーザー名>`、`<ユーザー>@<ドメイン>` のいずれかの形式で入力できます。大文字と小文字の区別はありません。たとえば、`dell.com\john_doe` または `JOHN_DOE@DELL.COM` などです。


2. **パスワード** フィールドに、iDRAC のユーザーパスワードまたは Active Directory のユーザーパスワードを入力します。パスワードでは大文字と小文字が区別されます。


3. **OK** をクリックするか、Enter キーを押します。

ログアウト

- セッションを閉じるには、メインウィンドウの右上にある **ログアウト** をクリックします。
- ブラウザウィンドウを閉じます。

 **メモ:** ログインするまで **ログアウト** ボタンは表示されません。

 **メモ:** 正常にログアウトせずにブラウザを閉じると、セッションはタイムアウトになるまで開いたままになることがあります。ログアウトボタンをクリックしてセッションを終了することをお勧めします。この手順でログアウトしない場合、タイムアウトになるまでセッションがアクティブなままになることがあります。

 **メモ:** Microsoft Internet Explorer で、ウィンドウの右上端の閉じるボタン("x")を使用して iDRAC ウェブインタフェースを閉じると、アプリケーションエラーが発生する可能性があります。この不具合を修正するには、Microsoft サポートウェブサイト support.microsoft.com から、最新の Internet Explorer 用累積セキュリティアップデートをダウンロードしてください。

複数のブラウザタブとウィンドウの使用


新しいタブやウィンドウを開いたときのウェブブラウザの動作は、バージョンによって異なります。それぞれのウィンドウは新しいセッションですが、それぞれの新しいタブは新しいセッションではありません。Microsoft Internet Explorer 6 はタブをサポートしないため、オープンしたブラウザウィンドウのそれぞれが新しい iDRAC ウェブインタフェースセッションになります。Internet Explorer 7 では、ウィンドウに加えてタブを開くことができます。各タブは、最後にオープンしたタブの特性を継承します。たとえば、あるユーザーがパワーユーザー権限で 1 つのタブにログインした後、Administrator 権限で別のタブにログインすると、オープンしたどちらのタブも Administrator 権限を持ちます。いずれか 1 つのタブを閉じると、すべての iDRAC ウェブインタフェースタブが終了します。


Firefox におけるタブとウィンドウの動作は、Internet Explorer 7 と同じです。

iDRAC NIC の設定

ここでは、iDRAC がすでに設定され、ネットワーク上でアクセス可能である状態を想定しています。初期 iDRAC ネットワークの設定に関しては、「[iDRAC ネットワークの設定](#)」を参照してください。

ネットワークおよびIPMI LAN の設定

 **メモ:** 次の手順を実行するには、iDRAC の **設定** 権限が必要です。

 **メモ:** ほとんどの DHCP サーバーは、予約テーブルにクライアントの ID トークンを保存するためのサーバーを必要とします。このトークンはクライアント(例:iDRAC)が DHCP ネゴシエーション中に提供します。iDRAC は、1 バイトのインタフェース番号(O)に続く 6 バイトの MAC アドレスを使用して、クライアント ID オプションを提供します。

- システム** → **リモートアクセス** → **iDRAC** をクリックします。
- ネットワーク / セキュリティ** タブをクリックして **ネットワーク設定** ページを開きます。
[表 5-1](#) と [表 5-2](#) に、**ネットワーク** ページの **ネットワーク設定** と **IPMI LAN 設定** について説明します。
- 必要な設定を入力したら、**適用** をクリックします。
- 適切な ボタンをクリックして続行します。「[表 5-3](#)」を参照してください。

表 5-1 ネットワークの設定

設定	説明
NIC を有効にする	選択すると、NIC が有効になり、このグループの残りのコントロールがアクティブになることを示します。NIC が無効になっている場合、ネットワーク経由の iDRAC とのすべての通信はブロックされます。 デフォルトは オフ です。
メディアアクセスコントロール (MAC) アドレス	ネットワークの各ノードを固有に識別するメディアアクセスコントロール (MAC) アドレスを表示します。MAC アドレスは変更できません。
NIC IP アドレスに DHCP を使用	iDRAC に動的ホスト構成プロトコル (DHCP) サーバーから NIC 用の IP アドレスを取得するように指示します。また、 静的 IP アドレス 、 静的サブネットマスク 、 静的ゲートウェイ コントロールを無効にします。 デフォルトは オフ です。
静的 IP アドレス	iDRAC NIC の静的 IP アドレスを入力または編集できます。この設定を変更するには、 DHCP を使用 (NIC IP アドレス用) チェックボックスを選択解除します。
静的サブネットマスク	iDRAC NIC のサブネットマスクを入力または編集できます。この設定を変更するには、まず DHCP を使用 (NIC IP アドレス用) チェックボックスを選択解除します。
静的ゲートウェイ	iDRAC NIC の静的ゲートウェイを入力または編集できます。この設定を変更するには、まず DHCP を使用 (NIC IP アドレス用) チェックボックスを選択解除します。
DHCP を使用して DNS サーバーアドレスを取得する	DHCP を使用して DNS サーバーアドレスを取得する チェックボックスを選択し、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、 静的優先 DNS サーバー および 静的代替 DNS サーバー フィールドに IP アドレスを入力します。

	<p>デフォルトは オフ です。</p> <p>メモ: DHCP を使用して DNS サーバーアドレスを取得する チェックボックスが選択されている場合、IP アドレスを 静的優先 DNS サーバー および 静的代替 DNS サーバー フィールドに入力することはできません。</p>
静的優先 DNS サーバー	優先 DNS サーバーの静的 IP アドレスの入力または編集ができます。この設定を変更するには、まず DHCP を使用して DNS サーバーアドレスを取得する チェックボックスを選択解除します。
静的代替 DNS サーバー	二次 DNS サーバー IP アドレスは、DHCP を使って DNS サーバーアドレスを取得する が 選択されていない 場合に使用します。代替 DNS サーバーが存在しない場合は、IP アドレスとして「0.0.0.0」を入力します。
DNS に iDRAC を登録	DNS サーバーに iDRAC 名を登録します。 デフォルトは 無効 です。
DNS iDRAC 名	DNS に iDRAC を登録 が選択されている場合にのみ iDRAC 名を表示します。デフォルト名は idrac-サービスタグで、サービスタグは Dell サーバーのサービスタグ番号を示します。例: idrac-00002
DNS ドメイン名に DHCP を使用	デフォルトの DNS ドメイン名を使用します。このチェックボックスが選択されておらず、DNS 上の iDRAC を登録 オプションが選択されている場合は、DNS ドメイン名 フィールドで DNS ドメイン名を変更します。 デフォルトは 無効 です。 メモ: DNS ドメイン名に DHCP を使用 チェックボックスを選択する場合は、DHCP の使用 (NIC IP アドレス用) チェックボックスが選択されている必要があります。
DNS ドメイン名	デフォルトの DNS ドメイン名は空白です。DNS ドメイン名に DHCP を使用 チェックボックスが選択されている場合はこのオプションがグレー表示になり、フィールドは変更できません。
コミュニティ文字列	iDRAC から送信される 簡易ネットワーク管理プロトコル (SNMP) の警告トラップで使用するコミュニティ文字列を示します。SNMP 警告トラップは、プラットフォームイベントの発生時に iDRAC によって送信されます。デフォルトは public です。
SMTP サーバーアドレス	プラットフォームイベント発生時に電子メール警告を送信するために iDRAC が通信する 簡易メール転送プロトコル (SMTP) サーバーの IP アドレス。デフォルトは 127.0.0.1 です。


表 5-2 IPMI LAN の設定

設定	説明
IPMI オーバー LAN を有効にする	選択されている場合、IPMI LAN チャネルが有効であることを示します。デフォルトは オフ です。
チャネル権限レベルの制限	LAN チャネルで受け入れられるユーザーの最大権限レベルを設定します。 システム管理者 (Administrator) 、 オペレータ 、 ユーザー のオプションから 1 つを選択します。デフォルトは システム管理者 (Administrator) です。
暗号キー	暗号キーの文字形式の設定では、0 ~ 20 の 16進法の文字を使用します (空白は使用できません)。デフォルトは空白です。

表 5-3 ネットワーク設定ページのボタン

ボタン	説明
詳細設定	ネットワークセキュリティ ページを開いて、IP 範囲と IP ブロックの属性を入力できます。
印刷	画面に表示されている ネットワーク設定 ページのデータを印刷します。
更新	ネットワーク設定 ページを再ロードします。
適用	ネットワーク設定ページに追加された新規設定を保存します。 メモ: NIC の IP アドレス設定を変更すると、すべてのユーザーセッションが終了します。ユーザーは、更新後の IP アドレス設定を使って iDRAC ウェブインタフェースに再接続する必要があります。その他の変更では NIC をリセットする必要があり、このため接続が一時的に途絶える場合があります。

IP フィルタおよびIP ブロックの設定

 **メモ:** 次の手順を実行するには、iDRAC の **設定** 権限が必要です。

1. **システム** → **リモートアクセス** → iDRAC の順にクリックし、**ネットワーク/セキュリティ** タブをクリックして **ネットワーク設定** ページを開きます。
2. **詳細設定** をクリックして、ネットワークセキュリティ設定を行います。
[表 5-4](#) に、**ネットワークセキュリティ** ページの設定を示します。
3. 設定が終了したら、**適用** をクリックします。
4. 適切な ボタンをクリックして続行します。「[表 5-5](#)」を参照してください。

表 5-4 ネットワークセキュリティページの設定

設定	説明
IP 範囲を有効にする	IP 範囲のチェック機能を有効します。これにより、iDRAC にアクセスできる IP アドレスの範囲を定義できます。デフォルトは オフ です。
IP 範囲のアドレス	受け入れる IP サブネットアドレスを指定します。デフォルトは 192.168.1.0 です。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。デフォルトは 255.255.255.0 です。
IP ブロックを有効にする	事前に選択した時間帯で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。デフォルトは オフ です。
IP ブロックエラーカウン	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。デフォルトは 10 です。
IP ブロックエラー時間	IP ブロックペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間帯を秒で指定します。デフォルトは 3600 です。
IP ブロックペナルティ時間	ログイン失敗回数が制限値を超えた IP アドレスからのログインを拒否する時間を秒で指定します。デフォルトは 3600 です。

表 5-5 ネットワークセキュリティページのボタン

ボタン	説明
印刷	画面に表示中の ネットワークセキュリティ ページのデータを印刷します。
更新	ネットワークセキュリティ ページを再ロードします。
適用	ネットワークセキュリティ ページに追加された新規設定を保存します。
ネットワークページに戻る	ネットワーク ページに戻ります。

プラットフォームイベントの設定

プラットフォームイベントの設定では、特定のイベントメッセージが返されたときに iDRAC が選択した処置を実行するように設定します。処置には、処置の必要なし、システムの再起動、システムの電源を入れ直す、システムの電源を切る、警告の生成(プラットフォームイベントトラップ [PET]、電子メール)があります。

表 5-6 に、フィルタ可能なプラットフォームイベントを示します。


表 5-6 フィルタ可能なプラットフォームイベント

索引	プラットフォームイベント
1	バッテリー警告アサート
2	バッテリー重要アサート
3	低電圧重要アサート
4	温度警告アサート
5	温度重要アサート
6	冗長性低下
7	冗長性喪失
8	プロセッサ警告アサート
9	プロセッサ重要アサート
10	プロセッサ不在アサート
11	イベントログ重要アサート
12	ウォッチドッグ重要アサート

プラットフォームイベント(例、バッテリー警告アサート)が発生すると、システムイベントが生成され、システムイベントログ (SEL) に記録されます。このイベントが有効にされているプラットフォームイベントフィルタ (PEF) と一致し、警告 (PET または電子メール) を生成するようにフィルタを設定している場合、1 つまたは複数の設定されている送信先に PET または電子メール警告が送信されます。


同じプラットフォームイベントフィルタで別の動作(システムの再起動など)を実行するように設定すると、その動作が行われます。

プラットフォームイベントフィルタ (PEF) の設定

 **メモ:** プラットフォームイベントトラップまたは電子メール警告設定を行う前に、プラットフォームイベントフィルタを設定してください。

- iDRAC ウェブインタフェースにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
- システム** をクリックし **警告管理** タブをクリックします。


- プラットフォームイベントページで、該当するイベントの **警告の生成** チェックボックスをクリックし、**警告の生成** を有効にします。

 **メモ:** [警告の生成] 列の見出しの横にあるチェックボックスをクリックすると、すべてのイベントに対する 警告の生成を有効 / 無効にできます。

- 各イベントに対し、有効にする処置の下にあるラジオボタンをクリックします。各イベントに対し 1 つの処置のみ設定できます。
- 適用** をクリックします。


 **メモ:** 設定されている有効な宛先(PET または電子メール)に警告を送信するためには、**警告の生成** を有効にする必要があります。

プラットフォームイベントトラップ(PET)の設定


 **メモ:** SNMP 警告を追加したり有効 / 無効にするには、iDRAC の **設定** 権限が必要です。iDRAC の **設定** 権限がない場合、次のオプションは使用できません。

- 対応ウェブブラウザを使ってリモートシステムにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
- 「[プラットフォームイベントフィルタ \(PEF\) の設定](#)」の手順に必ず従ってください。
- PET の送信先 IP アドレスを設定します。

- アクティブにする **送信先番号** の横にある **有効** チェックボックスをクリックします。
- 送信先の IP アドレス** ボックスに IP アドレスを入力します。

 **メモ:** 送信先コミュニティ文字列は iDRAC コミュニティと同じ文字列であることが必要です。


- 適用** をクリックします。

 **メモ:** トラップを確実に送信するには、**ネットワーク設定** ページの **コミュニティ文字列** の値を設定します。**コミュニティ文字列** の値は、iDRAC から送信される簡易ネットワーク管理プロトコル(SNMP)の警告トラップで使用するコミュニティ文字列を示します。SNMP 警告トラップは、プラットフォームイベントの発生時に iDRAC によって送信されます。**コミュニティ文字列** のデフォルト設定は、Public です。

- 必要に応じて **送信** をクリックし、設定した警告をテストします。
- 残りの送信先番号に対しても、ステップ a ~ d を繰り返します。

電子メール警告の設定

- 対応ウェブブラウザを使ってリモートシステムにログインします。
- 「[プラットフォームイベントフィルタ \(PEF\) の設定](#)」の手順に必ず従ってください。
- 電子メール警告設定を指定します。
 - 警告管理** タブで、**電子メール警告設定** をクリックします。
- 電子メール警告の宛先を指定します。
 - 電子メール警告番号** 列で、送信先番号をクリックします。4 つの電子メール送信先に警告を送信できます。
 - 有効** チェックボックスが選択されていることを確認します。
 - 宛先の電子メールアドレス** フィールドに有効な電子メールアドレスを入力します。
 - 適用** をクリックします。

 **メモ:** テストメールを正しく送信するには、**ネットワーク設定** ページで **SMTP サーバーアドレス** を設定する必要があります。プラットフォームイベントが発生すると、設定した IP アドレスにある **SMTP サーバー** は iDRAC と通信して電子メール警告を送信します。


- 必要に応じて **送信** をクリックし、設定した電子メール警告をテストします。
- 残りの電子メール警告設定にも ステップ a ~ ステップ e の手順を繰り返します。

IPMI の設定

- 対応ウェブブラウザを使ってリモートシステムにログインします。

2. IPMI オーバー LAN を設定します。


- a. システム→リモートアクセス→iDRAC の順にクリックして、ネットワーク / セキュリティをクリックします。
- b. IPMI LAN 設定 の ネットワーク設定 ページで、IPMI オーバー LAN を有効にする を選択します。
- c. 必要に応じて、IPMI LAN チャンネルの権限を更新します。

 **メモ:** この設定によって、IPMI オーバー LAN インタフェースから実行できる IPMI コマンドが決まります。詳細については、IPMI 2.0 の仕様を参照してください。

IPMI LAN 設定 で **チャンネル権限レベルの制限** ドロップダウンメニューをクリックし、**システム管理者 (Administrator)**、**オペレータ**、**ユーザー** のいずれかを選択して **適用** をクリックします。

- d. 必要なら IPMI LAN チャンネルの暗号キーを設定します。

 **メモ:** iDRAC IPMI は RMCP+ プロトコルに対応しています。


 **メモ:** 暗号キーは、最大 20 文字の偶数の 16 進数文字で指定する必要があります。

IPMI LAN 設定 の **暗号キー** フィールドに暗号キーを入力します。

- e. **適用** をクリックします。

3. IPMI シリアルオーバー LAN (SOL)を設定します。

- a. システム→リモートアクセス→iDRAC をクリックします。
- b. ネットワークセキュリティタブをクリックして、シリアルオーバー LAN をクリックします。
- c. シリアルオーバー LAN 設定 ページで **シリアルオーバー LAN を有効にする** チェックボックスを選択して、シリアルオーバー LAN を有効にします。
- d. IPMI SOL ポーレートをアップデートします。

 **メモ:** シリアルコンソールを LAN 経由でリダイレクトする場合は、SOL のポーレートが管理下サーバーのポーレートと同じであることを確認してください。


ポーレートドロップダウンメニューをクリックして、19.2 kbps、57.6 kbps、115.2 kbps からデータ速度を選択します。

- e. **適用** をクリックします。

iDRAC ユーザーの追加と設定


iDRAC を使用してシステムを管理し、システムのセキュリティを維持するには、特定の管理者権限(またはロール[役割]ベースの権限)を持つ固有のユーザーを作成します。

iDRAC のユーザーを追加して設定するには、次の手順を実行してください。

 **メモ:** 次の手順を実行するには、iDRAC の **設定** 権限が必要です。

1. システム→リモートアクセス→iDRAC の順にクリックして、ネットワーク/セキュリティタブをクリックします。
2. ユーザー ページを開き、ユーザーを設定します。

ユーザー ページには、各ユーザーの **ユーザー ID**、**状態**、**ユーザー名**、**IPMI LAN 権限**、**iDRAC 権限**、**シリアルオーバー LAN** が表示されます。

 **メモ:** ユーザー 1 は IPMI の匿名ユーザー用に予約されており、変更できません。

3. **ユーザー ID** 列で、ユーザー ID をクリックします。
4. **ユーザーの設定** ページで、ユーザーのプロパティと権限を設定します。

[表 5-7](#)は、iDRAC ユーザー名とパスワードを設定するための **一般** 設定について説明しています。

[表 5-8](#)に、ユーザーの LAN 権限を設定するための **IPMI ユーザー権限**について説明します。

[表 5-9](#)では、IPMI LAN 権限と **iDRAC ユーザー権限**を設定するための **ユーザーグループ権限**について説明しています。

[表 5-10](#)では、iDRAC **グループ**権限について説明しています。iDRAC **ユーザー権限** を **システム管理者 (Administrator)**、**パワーユーザー**、**ゲストユーザー** に追加すると、iDRAC **グループ** が **カスタムグループ**に変わります。

5. 設定が完了したら、**適用** をクリックします。
6. 適切な ボタンをクリックして続行します。「[表 5-11](#)」を参照してください。

表 5-7 一般プロパティ

プロパティ	説明
ユーザー ID	16 個ある設定済みユーザー ID 番号の 1 つが入っています。このフィールドは、編集できません。
ユーザーを有効にする	選択されている場合、iDRAC へのユーザーのアクセスが有効であることを示します。選択解除されている場合、ユーザーアクセスは無効であることを示します。
ユーザー名	iDRAC ユーザー名は最大 16 文字で指定します。各ユーザーは固有のユーザー名を持つ必要があります。 メモ: iDRAC のユーザー名に / (フォワードスラッシュ) や . (ピリオド) を含めることはできません。 メモ: ユーザー名を変更した場合は、新しい名前は次のユーザーログイン時までユーザーインターフェースに表示されません。
パスワードの変更	新しいパスワードと新しいパスワードの確認 フィールドを有効にします。選択しないと、ユーザーのパスワードを変更することはできません。
新しいパスワード	iDRAC ユーザーのパスワードの編集を有効にします。20 文字以内でパスワードを入力します。文字は表示されません。
新しいパスワードの確認	確認のために iDRAC ユーザーのパスワードを再入力します。

表 5-8 IPMI LAN ユーザー権限

プロパティ	説明
許可される最高 LAN ユーザー権限	IPMI LAN チャネルでのユーザーの最大権限を、なし、システム管理者 (Administrator)、オペレータ、ユーザーの中から指定します。
シリアルオーバー LAN を有効にする	IPMI シリアルオーバー LAN を使用できます。選択すると、この権限が有効になります。

表 5-9 iDRAC ユーザー権限

プロパティ	説明
iDRAC グループ	ユーザーの最大 iDRAC ユーザー権限をシステム管理者 (Administrator)、パワーユーザー、ゲストユーザー、カスタム、なしの中から指定します。 iDRAC グループ 権限については、「表 5-10」を参照してください。
iDRAC へのログイン	iDRAC にログインできます。
iDRAC の設定	iDRAC を設定できます。
ユーザーの設定	特定ユーザーのシステムアクセスを許可できるようにします。
ログのクリア	iDRAC のログをクリアできます。
サーバーコントロールコマンドの実行	RACADM コマンドを実行できます。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告 (電子メールと PET) を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

表 5-10 iDRAC グループ権限

ユーザーグループ	許可する権限
システム管理者 (Administrator)	iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバーコントロールコマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
パワーユーザー	iDRAC へのログイン、ログのクリア、サーバーコントロールコマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告。
ゲストユーザー	iDRAC へのログイン
カスタム	次の権限を組み合わせで選択します。iDRAC へのログイン、iDRAC の設定、ユーザーの設定、ログのクリア、サーバー処置コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
なし	権限の割り当てなし

表 5-11 ユーザー設定ページのボタン

ボタン	動作
印刷	画面に表示されているユーザー設定 ページのデータを印刷します。
更新	ユーザー設定 ページを再ロードします。
適用	ユーザー設定に追加された新規設定を保存します。
ユーザー ページに戻る	ユーザーページに戻ります。

SSL とデジタル証明書を使用した iDRAC 通信のセキュリティ

ここでは、iDRAC に組み込まれているデータセキュリティ機能について説明します。

- 1 SSL (Secure Sockets Layer)
- 1 証明書署名要求 (CSR)
- 1 SSL メインメニューへのアクセス
- 1 新しい CSR の生成
- 1 サーバー証明書のアップロード
- 1 サーバー証明書の表示

SSL (Secure Sockets Layer)

iDRAC には、業界標準の SSL セキュリティプロトコルを使用してネットワーク上で暗号化データを送信するように設定されたウェブサーバーが含まれています。公開キーと秘密キーの暗号化技術を基盤とする SSL は、ネットワークでの盗聴を防ぐためにクライアントとサーバー間に認証された暗号化通信を提供する技術として広く普及しています。

SSL 対応システムは、次のタスクを実行できます。

- 1 SSL 対応クライアントに自らを認証する
- 1 クライアントがサーバーに対して自らを認証できるようにする
- 1 両システムが暗号化接続を確立できるようにする

暗号化プロセスは高度なデータ保護を提供します。iDRAC では、北米のインターネットブラウザで使用できる暗号化の最も安全な方式である 128 ビットの SSL 暗号化標準を導入しています。

iDRAC のウェブサーバーは、Dell の署名入り SSL デジタル証明書(サーバー ID)を提供します。インターネット上で高いセキュリティを確保するには、ウェブサーバーの SSL 証明書を、有名な認証局によって署名された証明書と交換してください。署名された証明書を取得するには、まず、iDRAC ウェブインタフェースを使用して企業情報を掲載した証明書署名要求(CSR)を生成します。生成した CSR を VeriSign や Thawte などの CA に送信します。

証明書署名要求 (CSR)

CSR は、認証局 (CA) に対してセキュアサーバー証明書の発行を求めるデジタル要求です。セキュアなサーバー証明書によって、サーバーのクライアントは接続しているサーバーの身元を信用できるほか、サーバーとの暗号化セッションをネゴシエートできます。

認証局は、IT 業界で認められたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を満たしています。CA には、Thawte や VeriSign などがあります。CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ基準を満たしていれば、ネットワークおよびインターネットを介したトランザクションを行う申請者を固有に識別するデジタル署名済みの証明書を発行します。

CA が CSR を承認して証明書を送信したら、それを iDRAC ファームウェアにアップロードする必要があります。iDRAC ファームウェアに保管されている CSR 情報は、証明書に含まれている情報に一致する必要があります。

SSL メインメニューへのアクセス

- 1 システム → リモートアクセス → iDRAC の順にクリックして、ネットワーク / セキュリティ タブをクリックします。
- 2 SSL をクリックして SSL メインメニュー ページを開きます。

SSL メインメニュー ページを使用して CSR を生成し、CA に送信します。CSR 情報は iDRAC ファームウェアに保存されます。

表 5-12 に、CSR の生成時に使用可能なオプションについて説明します。

表 5-13 に、SSL メインメニュー ページ上のボタンについて説明します。

表 5-12 SSL メインメニューオプション

フィールド	説明
新規証明書署名要求 (CSR) の生成	オプションを選択し、次へ をクリックして 証明書署名要求 (CSR) の生成 ページを開きます。 メモ: 新しい CSR は、ファームウェアにある古い CSR を上書きします。CA が CSR を受け入れるためには、ファームウェアにある CSR が CA から返された証明書に一致する必要があります。
サーバー証明書のアップロード	オプションを選択し、次へ をクリックして 証明書のアップロード ページを開き、CA から送信された証明書をアップロードします。

	メモ: iDRAC で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER でエンコードされた証明書は受け入れられません。
サーバー証明書の表示	オプションを選択し、 次へ をクリックして サーバー証明書の表示 ページを開き、既存のサーバー証明書を表示します。

表 5-13 SSL メインメニューボタン

ボタン	説明
印刷	画面に表示されている SSL メインメニュー ページのデータを印刷します。
更新	SSL メインメニュー ページを再ロードします。
次へ	SSL メインメニュー ページの情報を処理し、次のステップに進みます。

新しい証明書署名要求の生成

メモ: 新しい CSR はファームウェアに保存されている古い CSR データを上書きします。ファームウェアの CSR は、CAから返された証明書と一致している必要があります。一致しない場合、iDRAC は証明書を受け入れません。

- SSL メインメニュー ページで、**新規証明書署名要求 (CSR) の生成** を選択して、**次へ** をクリックします。
- 証明書署名要求 (CSR) の生成** ページで、各 CSR 属性の値を入力します。
[表 5-14](#) に、**証明書署名要求 (CSR) の生成** ページのオプションを示します。
- CSR を作成するには、**生成** をクリックします。
- CSR ファイルをローカルコンピュータに保存するには、**ダウンロード** をクリックします。
- 適切な ボタンをクリックして続行します。「[表 5-15](#)」を参照してください。

表 5-14 証明書署名要求 (CSR) の生成 ページのオプション

フィールド	説明
共通名 (コモンネーム)	証明する名前 (通常は www.xyzcompany.com のようなウェブサーバーのドメイン名)。英数字、ハイフン、下線、ピリオドのみが有効です。スペースは使用できません。
組織名	この組織に関連付けられた名前 (たとえば「XYZ Corporation」)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
部門名	部門など組織単位に関連付ける名前 (例、Information Technology)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
地域	証明する会社が所在する都市や地域 (たとえば「Minatoku」)。英数字とスペースのみが有効です。下線や他の文字で単語を区切らないでください。
都道府県名	証明書を申請している組織がある都道府県 (たとえば「Tokyo」)。英数字とスペースのみが有効です。略語は使用しないでください。
国番号	証明書を申請している組織が所在する国の名前。
電子メール	CSR に関連付けられている電子メールアドレス。組織の電子メールアドレスまたは CSR に関連付ける電子メールアドレスを入力します。このフィールドは任意選択です。

表 5-15 証明書署名要求 (CSR) の生成 ページのボタン

ボタン	説明
印刷	画面に表示中の 証明書署名要求の生成 ページのデータを印刷します。
更新	証明書署名要求の生成 ページを再ロードします。
生成	CSR を生成し、指定のディレクトリに保存するようユーザーに指示します。
ダウンロード	証明書をローカルコンピュータにダウンロードします。
SSL メインメニューに戻る	SSL メインメニュー ページに戻ります。

サーバー証明書のアップロード

- SSL メインメニュー ページで **サーバー証明書のアップロード** を選択して、**次へ** をクリックします。
証明書のアップロード ページが開きます。
- ファイルパス** フィールドで証明書へのパスを入力するか、**参照** をクリックして証明書ファイルのある場所へ移動します。

メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスおよび正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

3. **適用** をクリックします。
4. 適切な ボタンをクリックして続行します。「表 5-16」を参照してください。

表 5-16 証明書のアップロードページのボタン

ボタン	説明
印刷	画面に表示されている 証明書のアップロード ページのデータを印刷します。
更新	証明書のアップロード ページを再ロードします。
適用	証明書を iDRAC ファームウェアに適用します。
SSL メインメニューに戻る	SSL メインメニュー ページに戻ります。

サーバー証明書の表示

1. SSL メインメニュー ページで **サーバー証明書の表示** を選択して **次へ** をクリックします。

[表 5-17](#) に、**証明書** ウィンドウに表示されるフィールドと説明を示します。

2. 適切な ボタンをクリックして続行します。「表 5-18」を参照してください。


表 5-17 証明書情報


フィールド	説明
シリアルナンバー	証明書のシリアル番号
タイトル情報	タイトルによって入力された証明書の属性
発行者情報	発行者によって返された証明書の属性
有効期間の開始	証明書の発行日
有効期間の終了	証明書の失効日

表 5-18 サーバー証明書の表示ページのボタン

ボタン	説明
印刷	画面に表示中の サーバー証明書の表示 ページのデータを印刷します。
更新	サーバー証明書の表示 ページを再ロードします。
SSL メインメニューに戻る	SSL メインメニュー ページに戻ります。

Active Directory 証明書の設定と管理

 **メモ:** Active Directory を設定して Active Directory 証明書をアップロード、ダウンロード、表示するには、**iDRAC の設定** 権限が必要です。

 **メモ:** Active Directory 設定および、Active Directory を標準スキーマまたは拡張スキーマで設定する方法の詳細に関しては、「[Microsoft Active Directory での iDRAC の使用](#)」を参照してください。

Active Directory **メインメニュー** にアクセスするには、次の手順を実行してください。

1. **システム** → **リモートアクセス** → **iDRAC** の順にクリックして、**ネットワーク/セキュリティ** タブをクリックします。
2. **Active Directory** をクリックして **Active Directory メインメニュー** ページを開きます。
[表 5-19](#) に、Active Directory **メインメニュー** ページのオプションを示します。
3. 適切な ボタンをクリックして続行します。表 5-20 を参照してください。

表 5-19 Active Directory メインメニューページのオプション

フィールド	説明
-------	----

Active Directory の設定	Active Directory の ルートドメイン名、Active Directory 認証タイムアウト、Active Directory スキーマの選択、iDRAC 名、iDRAC ドメイン名、ロール(役割)グループ、グループ名、グループのドメインを設定します。
Active Directory CA 証明書のアップロード	iDRAC に Active Directory 証明書をアップロードします。
iDRAC サーバー証明書をダウンロードする	Windows Download Manager は iDRAC サーバー証明書をシステムにダウンロードします。
Active Directory CA 証明書の表示	iDRAC にアップロードされた Active Directory 証明書を表示します。

表 5-20 Active Directory メインメニューページのボタン

ボタン	定義
印刷	画面に表示されている Active Directory メインメニュー ページのデータを印刷します。
更新	Active Directory メインメニュー ページを再ロードします。
次へ	Active Directory メインメニュー ページの情報を処理し、次のステップに進みます。

Active Directory の設定 (標準スキーマと拡張スキーマ)

- Active Directory メインメニュー ページで、Active Directory の設定 を選択し、次へ をクリックします。
- Active Directory 設定 ページで、Active Directory 設定を入力します。
[表 5-21](#) に、Active Directory の設定と管理 ページの設定を示します。
- 適用 をクリックして設定を保存します。
- 適切な ボタンをクリックして続行します。「[表 5-22](#)」を参照してください。
- Active Directory 標準スキーマのロール(役割)グループを設定するには、個々のロール(役割)グループ (1~5) をクリックします。「[表 5-23](#)」および「[表 5-24](#)」を参照してください。


 **メモ:** Active Directory 設定 ページの設定を保存するには、カスタムロールグループ ページに進む前に 適用 をクリックします。

表 5-21 Active Directory 設定ページの設定

設定	説明
Active Directory を有効にする	選択されている場合、Active Directory は有効です。デフォルトは 無効 です。
ルートドメイン名	Active Directory のルートドメイン名。このデフォルトは空白です。 名前は x.y から成る有効なドメイン名にします。x は文字間に空白スペースのない 1 ~ 254 の ASCII 文字列で、y は com, edu, gov, int, mil, net, org などの有効なドメインタイプです。デフォルトは空白です。
タイムアウト	Active Directory のクエリが完了するのを待つ時間(秒)。最小値は 15 秒以上です。デフォルト値は 120 です。
標準スキーマを使用	Active Directory に標準スキーマを使用します。
拡張スキーマを使用	Active Directory に拡張スキーマを使用します。
iDRAC 名	Active Directory で iDRAC を固有に識別する名前。このデフォルトは空白です。 名前には 1 ~ 254 文字の ASCII 文字列を使用し、空白スペースは使用できません。
iDRAC ドメイン名	Active Directory iDRAC オブジェクトが属するドメインの DNS 名。このデフォルトは空白です。 名前は x.y から成る有効なドメイン名にします。x は文字間に空白スペースのない 1 ~ 254 の ASCII 文字列で、y は com, edu, gov, int, mil, net, org などの有効なドメインタイプです。
ロール(役割)グループ	iDRAC に関連付けられたロール(役割)グループのリスト。 ロール(役割)グループの設定を変更するには、ロールグループリストでそのロールグループの番号をクリックします。
グループ名	iDRAC に関連付けられた Active Directory でロール(役割)グループを識別する名前。このデフォルトは空白です。
グループドメイン	ロール(役割)グループの属するドメインタイプ。

表 5-22 Active Directory 設定ページのボタン

ボタン	説明
印刷	画面に表示されている Active Directory 設定 ページのデータを印刷します。

更新	Active Directory 設定 ページを再ロードします。
適用	Active Directory 設定 ページに追加された新規設定を保存します。
Active Directory メインメニュー に戻る	Active Directory メインメニュー ページに戻ります。

表 5-23 ロール(役割)グループの権限


設定	説明
ロール(役割)グループの権限レベル	ユーザーの最大 iDRAC ユーザー権限を システム管理者 (Administrator) 、 パワーユーザー 、 ゲストユーザー 、 カスタム 、 なし から指定します。 ロール(役割)グループ 権限については、「表 5-24」を参照してください。
iDRAC へのログイン	グループに iDRAC へのログインアクセスを許可します。
iDRAC の設定	iDRAC を設定するグループ権限を許可します。
ユーザーの設定	ユーザーを設定するグループ権限を許可します。
ログのクリア	ログをクリアするグループ権限を許可します。
サーバーコントロールコマンドの実行	サーバーコントロールコマンドを実行するグループ権限を許可します。
コンソールリダイレクトへのアクセス	コンソールリダイレクトへのグループアクセスを許可します。
仮想メディアへのアクセス	仮想メディアへのグループアクセスを許可します。
テスト警告	グループがテスト警告(電子メールおよび PET)を特定のユーザーに送信できます。
診断コマンドの実行	診断コマンドを実行するグループ権限を許可します。

表 5-24 ロール(役割)グループの権限

プロパティ	説明
システム管理者 (Administrator)	iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバーコントロールコマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
パワーユーザー	iDRAC へのログイン、ログのクリア、サーバーコントロールコマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告。
ゲストユーザー	iDRAC へのログイン
カスタム	次の権限を組み合わせて選択します。iDRAC へのログイン、iDRAC の設定、ユーザーの設定、ログのクリア、サーバー処置コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
なし	権限の割り当てなし

Active Directory CA 証明書のアップロード

- Active Directory **メインメニュー** ページで、Active Directory CA **証明書**をアップロードするを選択して **次へ** をクリックします。
- 証明書のアップロード** ページで、**ファイルパス** フィールドに証明書のファイルパスを入力するか、**参照** をクリックして証明書ファイルまで移動します。

 **メモ:** アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスおよび正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインコントローラの SSL 証明書が同じ認証局によって署名されており、iDRAC にアクセスする管理ステーションにこの証明書があることを確認してください。

- 適用** をクリックします。
- 適切なボタンをクリックして続行します。「表 5-25」を参照してください。

表 5-25 証明書のアップロードページのボタン

ボタン	説明
印刷	画面に表示されている 証明書のアップロード ページのデータを印刷します。
更新	証明書のアップロード ページを再ロードします。
適用	証明書を iDRAC ファームウェアに適用します。
Active Directory メインメニュー に戻る	Active Directory メインメニュー ページに戻ります。

iDRAC サーバー証明書のダウンロード

- Active Directory **メインメニュー** ページで、iDRAC **サーバー証明書**をダウンロードするを選択して **次へ** をクリックします。

2. ファイルをシステムのディレクトリに保存します。
3. **ダウンロードが完了しました** ウィンドウで**閉じる**をクリックします。

Active Directory CA 証明書の表示

Active Directory メインメニュー ページを使用して、iDRAC の CA サーバー証明書を表示します。

1. Active Directory メインメニュー ページで、Active Directory の **CA 証明書を表示する** を選択して **次へ** をクリックします。

[表 5-26](#) に、**証明書** ウィンドウに表示されるフィールドと説明を示します。

2. 適切な ボタンをクリックして続行します。「[表 5-27](#)」を参照してください。


表 5-26 Active Directory CA 証明書の情報

フィールド	説明
シリアルナンバー	証明書のシリアル番号
タイトル情報	タイトルによって入力された証明書の属性
発行者情報	発行者によって返された証明書の属性
有効期間の開始	証明書の発行日。
有効期間の終了	証明書の有効期限日。

表 5-27 Active Directory の CA 証明書の表示ページのボタン

ボタン	説明
印刷	画面に表示されている Active Directory の CA 証明書 ページのデータを印刷します。
更新	Active Directory の CA 証明書の表示 ページを再ロードします。
Active Directory メインメニューに戻る	Active Directory メインメニュー ページに戻ります。

設定へのローカルアクセスの有効化と無効化

 **メモ:** デフォルトでは、設定へのローカルアクセスは**有効**になっています。

設定へのローカルアクセスを有効にする

1. システム → リモートアクセス → iDRAC → ネットワーク/セキュリティ の順にクリックします。
2. **ローカル設定** で、iDRAC で**ローカルユーザーによる設定のアップデートを無効にする** をクリックしてチェックを外し、アクセスを有効にします。
3. **適用** をクリックします。
4. 適切な ボタンをクリックして続行します。

設定へのローカルアクセスを無効にする

1. システム → リモートアクセス → iDRAC → ネットワーク/セキュリティ の順にクリックします。
2. **ローカル設定** で、iDRAC で**ローカルユーザーによる設定のアップデートを無効にする** をクリックしてチェックし、アクセスを無効にします。
3. **適用** をクリックします。
4. 適切な ボタンをクリックして続行します。

シリアルオーバー LAN の設定

1. システム→リモートアクセス→iDRAC→ネットワーク/セキュリティをクリックします。
2. シリアルオーバー LAN をクリックしてシリアルオーバー LAN 設定 ページを開きます。
[表 5-28](#) に、シリアルオーバー LAN の設定 ページの設定を示します。
3. 適用 をクリックします。
4. 必要なら、詳細設定を指定します。指定しない場合は、適切なボタンをクリックして続行します(「[表 5-29](#)」を参照)。

詳細設定を指定するには、次の手順を実行してください。

- a. 詳細設定 をクリックします。
- b. シリアルオーバー LAN 詳細設定 ページで、必要に応じて詳細を指定します(「[表 5-30](#)」を参照)。
- c. 適用 をクリックします。
- d. 適切なボタンをクリックして続行します(「[表 5-31](#)」を参照)。

表 5-28 シリアルオーバー LAN の設定 ページの設定

設定	説明
シリアルオーバー LAN を有効にする	チェックボックスが選択されている場合、シリアルオーバー LAN が有効であることを示します。
ボーレート	データ速度を示します。データ速度を 19.2 kbps、57.6 kbps、 115.2 kbps の中から選択します。

表 5-29 シリアルオーバー LAN の設定 ページのボタン

ボタン	説明
印刷	画面に表示中のシリアルオーバー LAN 設定 ページのデータを印刷します。
更新	シリアルオーバー LAN 設定 ページを再ロードします。
詳細設定	シリアルオーバー LAN の設定 詳細設定 ページを開きます。
適用	シリアルオーバー LAN 設定 ページの表示中に行った新しい設定を保存します。




表 5-30 シリアルオーバー LAN の設定 詳細設定 ページの設定

設定	説明
文字累積間隔	SQL 文字データパッケージの一部を送信するまでに iDRAC が待機する時間。時間は秒で測定されます。
文字送信しきい値	iDRAC は、このしきい値に設定した文字数を受け取ると、文字を含む SQL 文字データパッケージを送信します。しきい値は文字数で測定されます。

表 5-31 シリアルオーバー LAN の設定 詳細設定 ページのボタン

ボタン	説明
印刷	画面に表示されているシリアルオーバー LAN 設定 詳細設定 ページのデータを印刷します。
更新	シリアルオーバー LAN 設定 詳細設定 ページを再ロードします。
適用	シリアルオーバー LAN 設定 詳細設定 ページの表示中に行った新しい設定を保存します。
シリアルオーバー LAN の設定 ページに戻る	シリアルオーバー LAN 設定 ページに戻ります。

iDRAC サービスの設定

-  **メモ:** これらの設定を変更するには、iDRAC の設定 権限が必要です。
-  **メモ:** サービスに変更を適用すると、変更は瞬時に反映されます。既存の接続は、警告なしで終了されることがあります。
-  **メモ:** BMU と通信する Microsoft Windows 提供の Telnet クライアントには、既知の問題があります。ハイパーターミナルや PuTTY といった他の Telnet クライアントを使用してください。

1. システム→リモートアクセス→iDRAC の順にクリックして、ネットワーク/セキュリティ タブをクリックします。

2. サービス をクリックして サービス 設定ページを開きます。
3. 必要に応じて、次のサービスを設定します。
 1. ウェブサーバー - ウェブサーバーの設定については「[表 5-32](#)」を参照
 1. SSH - SSH 設定については「[表 5-33](#)」を参照
 1. Telnet - Telnet 設定については「[表 5-34](#)」を参照
 1. 自動システムリカバリエージェント - 自動システムリカバリエージェントの設定については「[表 5-35](#)」を参照
4. 適用 をクリックします。
5. 適切な ボタン をクリックして続行します。「[表 5-36](#)」を参照してください。

表 5-32 ウェブサーバーの設定

設定	説明
有効	iDRAC ウェブサーバーを有効または無効にします。チェックボックスが選択されている場合、ウェブサーバーが有効であることを示します。デフォルトは 有効 です。
最大セッション数	システムで許可される同時セッションの最大数。このフィールドは編集できません。同時セッションは 4 セッションまで可能です。
現在のセッション数	システムの現在のセッション数(最大セッション数 以下)。このフィールドは編集できません。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更はすぐに有効になり、ウェブサーバーはリセットされます。タイムアウト時間の範囲は 60~1920 秒です。デフォルトは 300 秒です。
HTTP ポート番号	ブラウザ接続で iDRAC が通信するポート。デフォルトは 80 です。
HTTPS ポート番号	セキュアなブラウザ接続で iDRAC が通信するポート。デフォルトは 443 です。

表 5-33 SSH の設定

設定	説明
有効	SSH を有効または無効にします。チェックボックスが選択されている場合、SSH は有効であることを示します。
最大セッション数	システムで許可される同時セッションの最大数。1 セッションのみサポートされています。
アクティブセッション数	システムの現在のセッション数。
タイムアウト	セキュアなアイドルタイムアウト(秒)。タイムアウト時間の範囲は 60~1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは 300 秒です。
ポート番号	SSH 接続で iDRAC が通信するポート。デフォルトは 22 です。

表 5-34 Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。選択されている場合、Telnet は有効です。
最大セッション数	システムで許可される同時セッションの最大数。1 セッションのみサポートされています。
アクティブセッション数	システムの現在のセッション数。
タイムアウト	telnet のアイドルタイムアウト(秒)。タイムアウト時間の範囲は 60~1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは 0 です。
ポート番号	Telnet 接続で iDRAC が通信するポート。デフォルトは 23 です。

表 5-35 自動システムリカバリエージェントの設定

設定	説明
有効	自動システムリカバリエージェントを有効にします。

表 5-36 サービスページのボタン

ボタン	説明
印刷	サービス ページを印刷します。
更新	サービス ページを更新します。
変更の適用	サービス ページの設定を適用します。

iDRAC ファームウェアのアップデート

注意: iDRAC ファームウェアのアップデートが完了前に中断されるなどで、iDRAC ファームウェアが破損された場合、CMC を使って iDRAC を回復(リカバリ)できます。手順については、『CMC ファームウェアユーザーガイド』を参照してください。

メモ: ファームウェアアップデートは、デフォルトで現在の iDRAC 設定を保持します。アップデートプロセス中、iDRAC 設定を出荷時のデフォルト設定にリセットできるオプションがあります。設定を出荷時のデフォルト設定にすると、アップデート完了時に外部ネットワークアクセスが無効になります。iDRAC 設定ユーティリティまたは CMC ウェブインタフェースを使ってネットワークを有効にし、設定する必要があります。

1. iDRAC ウェブインタフェースを起動します。
2. **システム**→**リモートアクセス**→iDRAC の順にクリックして、**アップデート** タブをクリックします。

メモ: ファームウェアをアップデートするには、iDRAC がアップデートモードになっている必要があります。このモードでは、アップデートプロセスをキャンセルした場合でも iDRAC は自動的にリセットされます。

3. **ファームウェアアップデート** ページで、**次へ** をクリックしてアップデートプロセスを開始します。
4. **ファームウェアアップデート - アップロード(1/4 ページ)** ウィンドウで、**参照** をクリックするか、ダウンロードしたファームウェアイメージへのパスを入力します。

次に、例を示します。

C:\Updates\iV1.0\<イメージ名>

デフォルトのファームウェアイメージ名は `firmimg.imc` です。

5. **次へ** をクリックします。
 1. ファイルは iDRAC にアップロードされます。これは数分かかる場合があります。
または
 1. ファームウェアアップグレードのプロセスを終了する場合は、この時点で **キャンセル** をクリックします。**キャンセル** をクリックすると、iDRAC は正常な動作モードにリセットされます。
6. **ファームウェアアップデート - 検証(2/4 ページ)** ウィンドウには、アップロードしたイメージファイルで実行された検証の結果が表示されます。
 1. イメージファイルが正しくアップロードされ、すべての検証チェックに合格した場合、ファームウェアイメージが **確認されたことを示すメッセージ** が表示されます。
または
 1. イメージが正しくアップロードされなかったり、検証チェックに合格しない場合、ファームウェアアップデートは **ファームウェアアップデート - アップロード(1/4 ページ)** ウィンドウに戻ります。iDRAC のアップグレードを再試行するか、**キャンセル** をクリックして iDRAC を正常な動作モードにリセットします。
7. **メモ:** **設定の保存** チェックボックスを選択解除すると、iDRAC はデフォルト設定にリセットされます。デフォルト設定では LAN は無効になっています。iDRAC ウェブインタフェースにログインできません。BIOS POST 中に iDRAC 設定ユーティリティを使用して CMC ウェブインタフェースまたは iKVM で LAN 設定を再設定する必要があります。
7. デフォルトでは、アップグレード後も iDRAC で現在の設定を保存するための **設定の保存** チェックボックスが選択されています。設定を保存しない場合は、**設定の保存** チェックボックスを選択解除します。
8. **アップデートの開始** をクリックして、アップグレードプロセスを開始します。アップグレードプロセスには割り込まないでください。
9. **ファームウェアアップデート - アップデート(3/4 ページ)** ウィンドウには、アップグレードのステータスが表示されます。ファームウェアアップグレード操作の進行状況は、**進行状況** 列にパーセントで表示されます。
10. ファームウェアアップデートが完了すると、**ファームウェアアップデート - アップデート結果(4/4 ステップ)** ウィンドウが表示され、iDRAC は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC に再接続する必要があります。

CMC を使用した iDRAC ファームウェア のリカバリ

通常、iDRAC ファームウェアは iDRAC ウェブインタフェース、もしくは support.dell.com よりダウンロード可能なオペレーティングシステム特有のアップデートパッケージなどの iDRAC アイテムを使用してアップデートします。

iDRAC ファームウェアのアップデートが完了前に中断されるなどで iDRAC ファームウェアが破損した場合、CMC ウェブインタフェースを使ってファームウェアをアップデートできます。

CMC が iDRAC ファームウェアの破損を検知した場合、iDRAC は CMC ウェブインタフェースの **アップデート可能なコンポーネント** ページにリストされます。

メモ: CMC ウェブインタフェースの使用に関する手順については、『CMC ファームウェアユーザーガイド』を参照してください。

iDRAC ファームウェアをアップデートするには、次の手順を実行してください。

1. support.dell.com から管理コンピュータに最新の iDRAC ファームウェアをダウンロードします。
2. CMC のウェブベースのインタフェースにログインします。
3. システムツリーでシャーシをクリックします。
4. アップデートタブをクリックします。アップデート可能なコンポーネントページが表示されます。CMC からリカバリ可能な iDRAC であれば、これを搭載したサーバーがリストに含まれます。
5. サーバー-n(n は回復[リカバリ]する iDRAC のサーバー番号)をクリックします。
6. 参照 をクリックしてダウンロードした iDRAC ファームウェアイメージを検索し、開く をクリックします。
7. ファームウェアアップデートを開始する をクリックします。

ファームウェアイメージファイルが CMC にアップロードされると、iDRAC はそのイメージを使って自らをアップデートします。

[目次ページに戻る](#)


[目次ページに戻る](#)

Microsoft Active Directory での iDRAC の使用

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [拡張スキーマと標準スキーマの長所と短所](#)
- [拡張スキーマ Active Directory の概要](#)
- [Active Directory 標準スキーマの概要](#)
- [ドメインコントローラの SSL を有効にする](#)
- [Active Directory を使用した iDRAC へのログイン](#)
- [よくあるお問い合わせ \(FAQ\)](#)

ディレクトリサービスは、ネットワーク上のユーザー、コンピュータ、プリンタ、その他のデバイスを制御するために必要な全情報に共通するデータベースを管理しています。会社で Microsoft® Active Directory® サービスソフトウェアを使用している場合は、iDRAC にアクセスできるように設定し、Active Directory ソフトウェアで既存のユーザーに iDRAC のユーザー権限を追加して制御できます。

 **メモ:** Microsoft Windows® 2000 および Windows Server® 2003 オペレーティングシステムでは Active Directory を使用して iDRAC のユーザーを認識できます。

Active Directory を使用すると、iDRAC でのユーザーアクセスを次の 2 通りの方法で定義できます。拡張スキーマソリューションを使うと、Dell が定義した Active Directory オブジェクトを使用でき、標準スキーマソリューションを使うと、Active Directory のグループオブジェクトのみを使用できます。

拡張スキーマと標準スキーマの長所と短所

Active Directory を使用して iDRAC へのアクセスを設定する場合は、拡張スキーマソリューションか標準スキーマソリューションかを選択する必要があります。

拡張スキーマソリューションを使用する場合の長所は次のとおりです。

- 1 すべてのアクセスコントロールオブジェクトを Active Directory で管理可能。
- 1 権限レベルの異なる iDRAC でユーザーアクセスを設定する際の最大限の柔軟性。

標準スキーマソリューションを使用する場合の長所は次のとおりです。

- 1 標準スキーマでは Active Directory オブジェクトのみが使用されるためスキーマ拡張が不要。
- 1 Active Directory 側での設定が簡単。

拡張スキーマ Active Directory の概要

拡張スキーマの Active Directory を有効にする方法は 3 通りあります。

- 1 iDRAC ウェブインタフェースを使用 ([「ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する方法」](#)を参照)。
- 1 RACADM CLI ツールを使用 ([「RACADM を使用して拡張スキーマ Active Directory で iDRAC を設定する方法」](#)を参照)。
- 1 SM-CLP コマンドラインを使用 ([「SM-CLP を使用して拡張スキーマ Active Directory で iDRAC を設定する方法」](#)を参照)。

Active Directory スキーマ拡張

Active Directory データは、属性とクラスの分散データベースです。Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。ユーザークラスは、データベースに保存されるクラスの一例です。ユーザークラスの属性の例としては、ユーザーの名、姓、電話番号などがあります。会社は、自社環境に特有のニーズを満たすための固有の属性とクラスを追加することで、Active Directory データベースを拡張できます。Dell では、このスキーマにリモート管理の認証と許可をサポートするための属性とクラスを加えて、機能を拡張しました。

既存の Active Directory スキーマに追加した属性やクラスは、それぞれ固有の ID で定義する必要があります。業界で固有の ID を維持するため、Microsoft は Active Directory オブジェクト識別子 (OID) のデータベースを管理して、会社がスキーマに拡張を追加する際に、それが固有なもので互いに競合しないことが保証されるように図っています。Microsoft Active Directory のスキーマを拡張するにあたり、Dell は、[表 6-1](#) に示すように、ディレクトリサービスに追加した属性とクラスについて固有の OID、固有の拡張子、固有にリンク付けられた属性 ID を受け取りました。

表 6-1 Dell Active Directory のオブジェクト識別子

Active Directory サービスクラス	Active Directory OID
Dell の拡張子	dell
Dell ベース OID	1.2.840.113556.1.8000.1280
RAC LinkID 範囲	12070 ~ 12079

RAC スキーマ拡張の概要

Dell では、さまざまな顧客環境に柔軟に対応できるように、ユーザーが達成したい成果に応じて設定できるプロパティを用意しています。Dell は、関連、デバイス、権限のプロパティを加えて、このスキーマを拡張しました。関連プロパティは、特定の権限セットを持つユーザーまたはグループを 1 台または複数台の RAC デバイスにリンクするために使用します。このモデルでは、ユーザー、RAC 権限、およびネットワーク上の RAC デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

Active Directory オブジェクトの概要

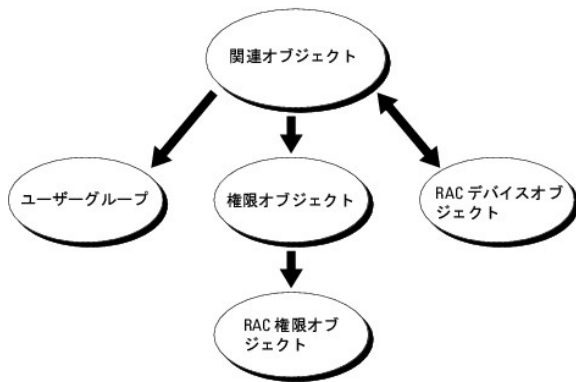
認証と許可のために Active Directory に統合するネットワーク上の物理 RAC の 1 台につき、少なくとも 1 個ずつ関連オブジェクトと RAC デバイスオブジェクトを作成しておきます。関連オブジェクトは必要なだけいくつでも作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数にも制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバーでもかまいません。

ただし、各関連オブジェクトは 1 つの権限オブジェクトにしかリンクできず、ユーザー、ユーザーグループ、RAC デバイスオブジェクトを 1 つの権限オブジェクトにしかリンクできません。この例では、Administrator (システム管理者) は特定の RAC で各ユーザーの権限を制御できます。

RAC デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための RAC ファームウェアへのリンクです。RAC をネットワークに追加した場合、システム管理者は RAC とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と認可を実行できるようにする必要があります。ユーザーが認証できるためには、システム管理者が RAC を少なくとも 1 つの関連オブジェクトに追加する必要があります。

図 6-1 は、関連オブジェクトがすべての認証と認可に必要な関連付けを提供する仕組みを示しています。

図 6-1 Active Directory オブジェクトの典型的なセットアップ



メモ: RAC 権限オブジェクトは DRAC 4 と iDRAC の両方に適用されます。

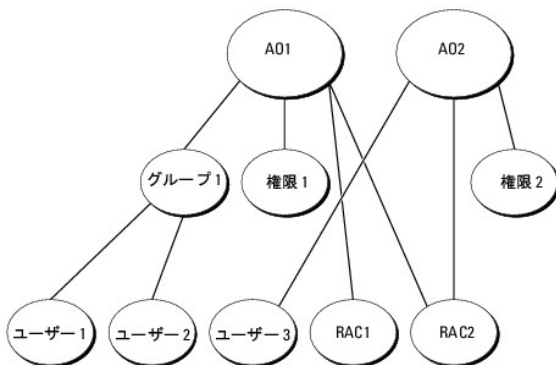
作成する関連オブジェクトの数に制限はありません。ただし、RAC (iDRAC) で認証と許可を実行するには、関連オブジェクトを少なくとも 1 つ作成する必要があり、Active Directory と統合するネットワーク上の各 RAC (iDRAC) に RAC デバイスオブジェクトが 1 つ必要です。

関連オブジェクトに含むことができるユーザー、グループ、RAC デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる権限オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは RAC に「権限」のある「ユーザー」を接続します。

Active Directory オブジェクトは、単一ドメインにも複数ドメインにも設定できます。たとえば、iDRAC が 2 つ (RAC1 と RAC2)、既存の Active Directory ユーザーが 3 台 (ユーザー 1、ユーザー 2、ユーザー 3) あるとします。ユーザー 1 とユーザー 2 に両方の iDRAC への Administrator 権限を与え、ユーザー 3 に RAC2 カードへのログイン権限を与えることにします。図 6-2 に、このシナリオで Active Directory オブジェクトを設定する方法を示します。

別のドメインからユニバーサルグループを追加する場合、ユニバーサルスコープで関連オブジェクトを作成します。Dell Schema Extender Utility で作成されたデフォルトの関連オブジェクトはドメインローカルグループであり、他のドメインからのユニバーサルグループとは連動しません。

図 6-2 単一ドメインでの Active Directory オブジェクトの設定



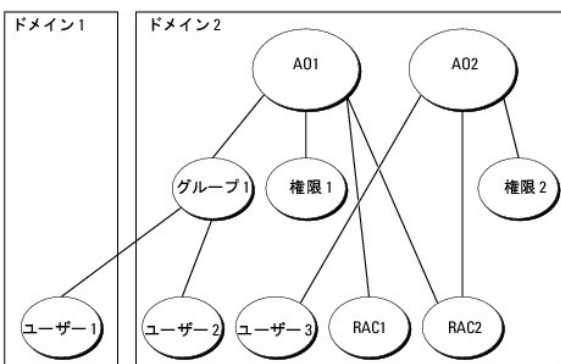
単一ドメインでオブジェクトを設定するシナリオでは、次のタスクを実行します。

1. 関連オブジェクトを 2 つ作成します。
2. 2 つの iDRAC を表す 2 つの RAC デバイスオブジェクト(RAC1 と RAC2)を作成します。
3. 2 つの権限オブジェクト(権限 1 と権限 2)を作成し、権限 1 にはすべての権限 (Administrator)、権限 2 にはログイン権限を与えます。
4. ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。
5. グループ 1 をメンバーとして関連オブジェクト 1 (AO1)に、権限 1 を権限オブジェクトとして AO1 に、そして RAC1、RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。
6. ユーザー 3 をメンバーとして関連オブジェクト 2 (AO2)に、権限 2 を権限オブジェクトとして AO2 に、RAC2 を RAC デバイスとして AO2 に追加します。

詳細については、「[Active Directory への iDRAC ユーザーと権限の追加](#)」を参照してください。

図 6-3 に、複数ドメインの Active Directory オブジェクトの例を示します。このシナリオでは、iDRAC 2 つ(RAC1 および RAC2)、既存の Active Directory ユーザーが 3 つ(ユーザー 1、ユーザー 2、およびユーザー 3)あります。ユーザー 1 はドメイン 1 に存在し、ユーザー 2 とユーザー 3 はドメイン 2 に存在しています。このシナリオでは、両方の iDRAC の Administrator 権限を持つユーザー 1 とユーザー 2 を設定し、RAC2 カードへのログイン権限を持つユーザー 3 を設定します。

図 6-3 複数ドメインでの Active Directory オブジェクトの設定



複数ドメインのシナリオでオブジェクトを設定するには、次の手順を実行してください。

1. ドメインのフォレスト機能がネイティブまたは Windows 2003 モードになっていることを確認します。
2. 2 つの関連オブジェクト AO1(ユニバーサルスコープの)と AO2 をいずれかのドメインに作成します。
図 6-3 に、ドメイン 2 のオブジェクトを示します。
3. 2 つの iDRAC を表す 2 つの RAC デバイスオブジェクト(RAC1 と RAC2)を作成します。
4. 2 つの権限オブジェクト(権限 1 と権限 2)を作成し、権限 1 にはすべての権限 (Administrator)、権限 2 にはログイン権限を与えます。
5. ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。グループ 1 のグループスコープはユニバーサルでなければなりません。
6. グループ 1 をメンバーとして関連オブジェクト 1 (AO1)に、権限 1 を権限オブジェクトとして AO1 に、そして RAC1、RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。
7. ユーザー 3 をメンバーとして関連オブジェクト 2 (AO2)に、権限 2 を権限オブジェクトとして AO2 に、RAC2 を RAC デバイスとして AO2 に追加します。

iDRAC にアクセスするための拡張スキーマ Active Directory の設定

Active Directory を使って iDRAC にアクセスする前に、次の手順を実行して、Active Directory ソフトウェアと iDRAC を設定する必要があります。

1. Active Directory スキーマを拡張します(「[Active Directory スキーマの拡張](#)」を参照)。
2. Active Directory ユーザーおよびコンピュータのsnapインを拡張します(「[Active Directory ユーザーとコンピュータsnapインへの Dell 拡張のインストール](#)」を参照)。
3. iDRAC ユーザーとその権限を Active Directory に追加します(「[Active Directory への iDRAC ユーザーと権限の追加](#)」を参照)。
4. SSL を各ドメインコントローラで有効にします(「[ドメインコントローラの SSL を有効にする](#)」を参照)。
5. iDRAC ウェブインタフェースまたは RACADM を使用して、iDRAC Active Directory プロパティを設定します(「[ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する方法](#)」または「[RACADM を使用して拡張スキーマ Active Directory で iDRAC を設定する方法](#)」を参照)。

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Dell の組織単位、スキーマのクラスと属性、サンプル権限、および関連オブジェクトが Active Directory スキーマに追加されます。スキーマを拡張するには、ドメインフォレストのスキーママスター FSMO(Flexible Single Master Operation)ロール(役割)オーナーのスキーマ Administrator 権限が必要です。

次のいずれかの方法でスキーマを拡張できます。

- 1 Dell Schema Extender ユーティリティ
- 1 LDIF スクリプトファイル

LDIF スクリプトファイルを使用すると、Dell の組織単位はスキーマに追加されません。


LDIF ファイルおよび Dell の Schema Extender は、それぞれ『Dell Systems Management Consoles CD』の次のディレクトリにあります。

- 1 CD ドライブ: ¥support¥OMActiveDirectory Tools¥RAC4-5¥LDIF_Files
- 1 CD ドライブ: ¥support¥OMActiveDirectory Tools¥RAC4-5¥Schema_Extender

LDIF ファイルを使用するには、LDIF_Files ディレクトリにある readme の説明を参照してください。Dell Schema Extender を使用して Active Directory スキーマを拡張するには、「[Dell Schema Extender の使用](#)」を参照してください。

Schema Extender または LDIF ファイルのコピーと実行はどの場所からでもできます。

Dell Schema Extender の使用

 **注意:** Dell Schema Extender(スキーマ拡張ユーティリティ) は、SchemaExtenderOem.ini ファイルを使用します。Dell Schema Extender ユーティリティが正しく機能するように、このファイルの名前は変更しないでください。

1. ようこそ 画面で、**次へ** をクリックします。
2. 警告を読んでから、もう一度 **次へ** をクリックします。
3. **資格情報で現在のログの使用** を選択するか、スキーマ Administrator 権限でユーザー名とパスワードを入力します。
4. Dell Schema Extender を実行するには、**次へ** をクリックします。
5. **完了** をクリックします。

スキーマが拡張されます。スキーマの拡張を確認するには、Microsoft Management Console(MMC)と Active Directory スキーマスナップインを使用して、次の存在を確認します。

- 1 クラス(「[表 6-2](#)」～「[表 6-7](#)」を参照)。
- 1 属性(「[表 6-8](#)」)

MMC で Active Directory のスキーマスナップインを有効にして使用する方法については、Microsoft のマニュアルを参照してください。

表 6-2 Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられるオブジェクト識別番号(OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 6-3 dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.1
説明	Dell RAC デバイスを表します。RAC デバイスは Active Directory では dellRacDevice として設定する必要があります。この設定を使って、iDRAC は Lightweight Directory Access Protocol(LDAP)クエリを Active Directory に送信できます。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 6-4 dellAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.2
説明	Dell 関連オブジェクトを表します。この関連オブジェクトはユーザーとデバイスを結び付けます。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	dellProductMembers dellPrivilegeMember

表 6-5 dellRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	IDRAC デバイスの権限(許可権限)を定義します。
クラスの種類	補助クラス
SuperClasses	なし
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

表 6-6 dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	Dell の権限(許可権限)のコンテナクラスとして使用されます。
クラスの種類	構造体クラス
SuperClasses	ユーザー
属性	dellRAC4Privileges

表 6-7 dellProduct クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.5
説明	すべての Dell 製品が派生するメインクラス。
クラスの種類	構造体クラス
SuperClasses	コンピュータ
属性	dellAssociationMembers

表 6-8 Active Directory スキーマに追加された属性のリスト

属性名 / 説明	割り当てられる OID/ 構文オブジェクト識別子	単一値
dellPrivilegeMember この属性に属する dellPrivilege オブジェクトのリスト	1.2.840.113556.1.8000.1280.1.1.2.1 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers このロール(役割)に属する dellRacDevices オブジェクトのリスト。この属性は dellAssociationMembers パックワードリンクへのフォワードリンクです。 リンク ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

dellIsLoginUser ユーザーにデバイスへのログイン権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin ユーザーにデバイスのカード設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin ユーザーにデバイスのユーザー設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser ユーザーにデバイスのコンソールリダイレクト権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser ユーザーにデバイスの仮想メディア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser ユーザーにデバイスのテスト警告ユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion スキーマのアップデートに現在のスキーマバージョンが使用されます。	1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType この属性は dellRacDevice オブジェクトの現在の Rac タイプで dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers のリスト。この属性は dellProductMembers リンク属性へのバックワードリンクです。 リンク ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール

Active Directory でスキーマを拡張する場合は、RAC (iDRAC) デバイス、ユーザーとユーザーグループ、RAC の関連、RAC の権限を管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『Dell Systems Management Consoles CD』を使用してシステム管理ソフトウェアをインストールした場合、インストール過程で **Active Directory ユーザーおよびコンピュータスナップインへの Dell 拡張** オプションを選択すると、スナップインを拡張できます。システム管理ソフトウェアのインストールの手順については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。

Active Directory ユーザーとコンピュータスナップインの詳細については、Microsoft のマニュアルを参照してください。

Administrator Pack のインストール

Active Directory iDRAC オブジェクトを管理している各システムに Administrator Pack をインストールする必要があります。Administrator Pack をインストールしないと、コンテナ内の Dell RAC オブジェクトを表示できません。

詳細については、「[Active Directory ユーザーとコンピュータのスナップインを開く](#)」を参照してください。

Active Directory ユーザーとコンピュータのスナップインを開く

Active Directory ユーザーとコンピュータスナップインを開くには、次の手順に従います。

1. ドメインコントローラにログインしている場合は、**スタート**→**管理ツール**→**Active Directory ユーザーとコンピュータ**の順にクリックします。

ドメインコントローラにログインしていない場合は、適切な Microsoft Administrator Pack がローカルシステムにインストールされている必要があります。この Administrator Pack をインストールするには、**スタート**→**ファイル名を指定して実行**の順にクリックし、MMC と入力して <Enter> を押します。

Microsoft Management Console (MMC) が表示されます。

2. **コンソール 1** ウィンドウで、**ファイル** (または Windows 2000 を実行しているシステムでは**コンソール**) をクリックします。
3. **スナップインの追加と削除** をクリックします。
4. **Active Directory ユーザーとコンピュータ** スナップインを選択して **追加** をクリックします。
5. **閉じる** をクリックして OK をクリックします。

Active Directory への iDRAC ユーザーと権限の追加


Dell の拡張 Active Directory ユーザーとコンピュータスナップインを使用して、RAC、関連、および権限オブジェクトを作成すると、iDRAC ユーザーと権限を追加できます。各オブジェクトタイプを追加するには、次の手順に従います。

1. RAC デバイスオブジェクトの作成
1. 権限オブジェクトの作成
1. 関連オブジェクトの作成
1. 関連オブジェクトへのオブジェクトの追加

RAC デバイスオブジェクトの作成

1. MMC **コンソールルート** ウィンドウでコンテナを右クリックします。
2. Select **新規**→**Dell RAC オブジェクト** を選択します。
新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。この名前は、[ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する方法の手順 a](#) で入力する iDRAC 名と同一でなければなりません。
4. **RAC デバイスオブジェクト** を選択します。
5. **OK** をクリックします。

権限オブジェクトの作成

 **メモ:** 権限オブジェクトは、関係する関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールのルート**(MMC) ウィンドウでコンテナを右クリックします。
2. **新規**→**Dell RAC オブジェクト** の順に選択します。
新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **権限オブジェクト** を選択します。
5. **OK** をクリックします。
6. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。
7. **RAC 権限** タブをクリックして、ユーザーに与える権限を選択します (詳細は「[iDRAC ユーザー権限](#)」を参照)。

関連オブジェクトの作成

関連オブジェクトはグループから派生し、グループタイプが含まれている必要があります。関連スコープは関連オブジェクトのセキュリティグループの種類を指定します。関連オブジェクトを作成する場合は、追加するオブジェクトの種類に適用される関連スコープを選択します。

たとえば、**ユニバーサル**を選択すると、関連オブジェクトは Active Directory ドメインがネイティブモード以上で機能している場合にのみ使用可能になります。

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。
2. **新規**→ **Dell RAC オブジェクト** の順に選択します。
新規オブジェクト ウィンドウが開きます。
3. 新しいオブジェクトの名前を入力します。
4. **関連オブジェクト** を選択します。
5. **関連オブジェクト** のスコープを選択します。
6. **OK** をクリックします。

関連オブジェクトへのオブジェクトの追加

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーまたはユーザーグループ、権限オブジェクト、RAC デバイスまたは RAC デバイスグループ間の関連付けができます。Windows 2000 モード以降のシステムを使用している場合は、ユニバーサルグループを使ってユーザーまたは RAC オブジェクトでドメインを拡張する必要があります。

ユーザーおよび RAC デバイスのグループを追加できます。Dell 関連グループと Dell に関連しないグループを作成する手順は同じです。

ユーザーまたはユーザーグループの追加

1. **関連オブジェクト** を右クリックし、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限オブジェクト タブをクリックして、RAC デバイスに認証するときにユーザーまたはユーザーグループの権限を定義する関連に、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは 1 つだけです。

権限の追加

1. **権限オブジェクト** タブを選択し、**追加** をクリックします。
2. 権限オブジェクト名を入力し、**OK** をクリックします。

製品 タブをクリックして、1 台または複数台の RAC デバイスを関連に追加します。関連デバイスは、ネットワークに接続している RAC デバイスのうち、定義したユーザーまたはユーザーグループが使用できるものを指定します。関連オブジェクトには複数の RAC デバイスを追加できます。

RAC デバイスまたは RAC デバイスグループの追加

RAC デバイスまたは RAC デバイスグループを追加するには、次の手順に従います。

1. **製品** タブを選択して **追加** をクリックします。
2. RAC デバイスまたは RAC デバイスグループの名前を入力し、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。

ウェブインターフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する方法

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC ウェブインターフェースにログインします。

3. システム→リモートアクセスの順にクリックします。
4. 設定タブをクリックして、Active Directoryを選択します。
5. Active Directory メインメニュー ページで、Active Directory の設定 を選択し、次へ をクリックします。
6. 全般設定セクションで、以下の操作を行います。
 - e. Active Directory を有効にする チェックボックスをオンにします。
 - f. ルートドメイン名 を入力します。ルートドメイン名 はフォレストのルートドメインの完全修飾名です。
 - g. タイムアウト の時間を秒単位で入力します。
7. Active Directory スキーマの選択セクションで 拡張スキーマの使用 をクリックします。
8. 拡張スキーマの設定セクションでは、以下の操作を行います。
 - a. DRAC 名 を入力します。この名前は、ドメインコントローラで作成した RAC オブジェクトの共通名と同じにしてください(「[RAC デバイスオブジェクトの作成](#)」の「[手順 3](#)」を参照)。
 - b. DRAC ドメイン名 を入力します(例、iDRAC.com)。NetBIOS 名を使用しないでください。DRAC ドメイン名 は、RAC デバイスオブジェクトがあるサブドメインの完全修飾ドメイン名です。
9. 適用 をクリックして Active Directory の設定を保存します。
10. Active Directory メインメニューに戻る をクリックします。
11. ドメインフォレストのルート CA 証明書を iDRAC にアップロードします。
 - a. Active Directory CA 証明書をアップロードする ラジオボタンを選択して、次へ をクリックします。
 - b. 証明書のアップロード ページで、証明書のファイルパスを入力するか、証明書ファイルの場所まで移動します。

 **メモ:** アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスおよび正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインコントローラの SSL 証明書はルート CA によって署名されている必要があります。iDRAC にアクセスする管理ステーション上でルート CA 証明書を使用可能にします(「[ドメインコントローラルート CA 証明書のエクスポート](#)」を参照)。

 - c. 適用 をクリックします。

iDRAC のウェブサーバーは、適用 をクリックすると自動的に再起動します。
12. iDRAC Active Directory 機能の設定を完了するには、ログアウトしてから iDRAC にログインします。
13. システム→リモートアクセスの順にクリックします。
14. 設定タブをクリックし、ネットワーク をクリックします。
15. ネットワーク設定 で DHCP を使用 (NIC IP アドレス用) が選択されている場合は、DHCP を使用して DNS サーバーアドレスを取得 を選択します。

DNS サーバーの IP アドレスを手動で入力するには、DHCP を使用して DNS サーバーアドレスを取得する チェックボックスをオフにし、一次および代替 DNS サーバーの IP アドレスを入力します。

16. 変更の適用 をクリックします。

これで iDRAC 拡張スキーマ Active Directory 機能の設定が完了しました。

RACADM を使用して拡張スキーマ Active Directory で iDRAC を設定する方法

ウェブインタフェースでなく RACADM CLI ツールを使用して、拡張スキーマで iDRAC Active Directory 機能を設定するには、次のコマンドを使用します。

1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacDomain <RAC FQDN>
racadm config -g cfgActiveDirectory -o cfgADRootDomain <ルート FQDN>
racadm config -g cfgActiveDirectory -o cfgADRacName <RAC 共通名>
```

```
racadm sslcertupload -t 0x2 -f <ルート CA 証明書 TFTP-URI>
```

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. iDRAC で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。


```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <二次 DNS IP アドレス>
```

4. <Enter> を押して、iDRAC Active Directory 機能の設定を完了します。

SM-CLP を使用して拡張スキーマ Active Directory で iDRAC を設定する方法

 **メモ:** ルート CA 証明書を取得でき、iDRAC サーバー証明書を保存できる TFTP サーバーを実行している必要があります。

SM-CLP を使用して拡張スキーマで iDRAC の Active Directory 機能を設定するには、次のコマンドを使用します。

1. Telnet または SSH を使用して iDRAC にログインし、次の SM-CLP コマンドを入力します。

```
cd /system/spl/oem Dell_adservice1

set enablestate=1

set oem Dell_schematype=1

set oem Dell_adracdomain=<RAC FQDN>

set oem Dell_adrootdomain=<ルート FQDN>

set oem Dell_adracname=<RAC 共通名>

set /system1/spl/oem Dell_ssl oem Dell_certtype=AD

load -source <ActiveDirectory 証明書 TFTP URI> /system1/spl/oem Dell_ssl

set /system1/spl/oem Dell_ssl oem Dell_certtype=SSL

dump -destination <DRAC サーバー証明書 TFTP URI> /system1/spl/oem Dell_ssl
```

2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の SM-CLP コマンドを入力します。

```
->cd /system1/spl/enetport1/lanendpt1/ipendpt1
dnsendpt1 oem Dell_serversfromdhcp=1
```

3. iDRAC で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の SM-CLP コマンドを入力します。

```
set /system1/spl/enetport1/lanendpt1/Y
ipendpt1/dnsendpt1 oem Dell_serversfromdhcp=0

->cd /system1/spl/enetport1/lanendpt1/ipendpt1
dnsendpt1/remotesapl dnsserveraddress=<一次 DNS IP アドレス>

->cd /system1/spl/enetport1/lanendpt1/ipendpt1
dnsendpt1/remotesapl dnsserveraddress=<二次 DNS IP アドレス>
```

Active Directory 標準スキーマの概要

[図 6-4](#) に示すように、Active Directory を統合するために標準スキーマを使用する場合は、Active Directory と iDRAC の両方で設定が必要になります。Active Directory 側では、標準グループオブジェクトがロール(役割)グループとして使用されます。iDRAC へのアクセス権を持つユーザーがロール(役割)グループのメンバーとなります。指定した iDRAC へのアクセスをこのユーザーに与えるには、ロール(役割)グループ名とそのドメイン名を特定の iDRAC で設定する必要があります。拡張スキーマソリューションとは異なり、ロール(役割)と権限レベルは Active Directory でなく、各 iDRAC で定義されます。各 iDRAC について、5 つまでのロール(役割)グループを設定および定義できます。[表 5-10](#) は、ロール(役割)グループの権限レベルを、[表 6-9](#) はロール(役割)グループのデフォルト設定を示したものです。

図 6-4 Microsoft Active Directory と標準スキーマを使用して iDRAC を設定する方法

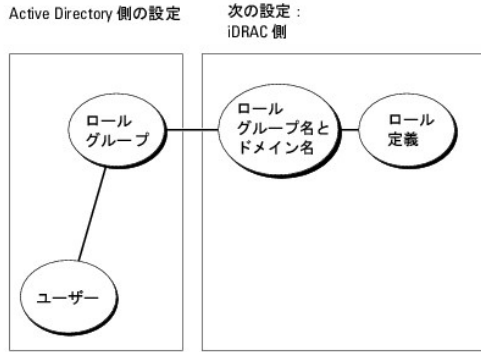


表 6-9 ロール(役割)グループのデフォルト権限

デフォルトの権限レベル	許可する権限	ビットマスク
Administrator(システム管理者)	iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。	0x000001ff
パワーユーザー	iDRAC へのログイン、ログのクリア、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告。	0x000000f9
ゲストユーザー	iDRAC へのログイン	0x00000001
なし	権限の割り当てなし	0x00000000
なし	権限の割り当てなし	0x00000000

メモ: ビットマスク値の使用は、RACADM で標準スキーマを設定する場合に限ります。

Active Directory で標準スキーマを有効にするには、次の 2 通りの方法があります。

1. iDRAC ウェブユーザーインターフェースの使用。「[標準スキーマ Active Directory とウェブインターフェースを使用して iDRAC を設定する方法](#)」を参照してください。
1. RACADM CLI ツールの使用。「[標準スキーマ Active Directory と RACADM を使用して iDRAC を設定する方法](#)」を参照してください。

iDRAC にアクセスするために標準スキーマ Active Directory を設定する方法

Active Directory ユーザーが iDRAC にアクセスできるためには、まず次の手順に従って Active Directory を設定する必要があります。

1. Active Directory サーバー(ドメインコントローラ)で、Active Directory ユーザーとコンピュータスナップインを開きます。
2. グループを作成するか、既存のグループを選択します。ウェブインターフェース、RACADM、または SM-CLP を使用してグループ名とドメイン名を iDRAC で設定する必要があります(「[標準スキーマ Active Directory とウェブインターフェースを使用して iDRAC を設定する方法](#)」または「[標準スキーマ Active Directory と RACADM を使用して iDRAC を設定する方法](#)」を参照)。
3. iDRAC にアクセスする Active Directory グループのメンバーとして Active Directory ユーザーを追加します。

標準スキーマ Active Directory とウェブインターフェースを使用して iDRAC を設定する方法

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC ウェブインターフェースにログインします。
3. システム → リモートアクセス → iDRAC の順にクリックして、設定 タブをクリックします。
4. Active Directory を選択して Active Directory メインメニュー ページを開きます。
5. Active Directory メインメニュー ページで、Active Directory の設定 を選択し、次へ をクリックします。
6. 全般設定セクションでは以下の操作を行います。
 - a. Active Directory を有効にする チェックボックスをオンにします。
 - b. ルートドメイン名 を入力します。ルートドメイン名 はフォレストのルートドメインの完全修飾名です。
 - c. タイムアウト の時間を秒単位で入力します。

7. Active Directory スキーマの選択セクションで **標準スキーマの使用** をクリックします。
8. **適用** をクリックして Active Directory の設定を保存します。
9. I標準スキーマ設定セクションの **ロール(役割)グループ** 列で **ロール(役割)グループ** をクリックします。
ロール(役割)グループの設定 ページが表示されます。このページには、ロール(役割)グループの **グループ名**、**グループドメイン**、**ロール(役割)グループの権限** が含まれています。
10. **グループ名** を入力します。iDRAC に関連付けられた Active Directory でロール(役割)グループを識別するグループ名。
11. **グループドメイン** を入力します。**グループドメイン** はフォレストのルートドメインの完全修飾名です。
12. **ロール(役割)グループの権限** で、グループの権限を設定します。
[表 5-10](#) に**ロール(役割)グループの権限** を示します。
 権限を変更すると、既存の **ロール(役割)グループの権限** (Administrator[システム管理者]、パワーユーザー、ゲストユーザー)は、変更した権限に基づいてカスタムグループまたは適切な**ロール(役割)グループの権限** に変更されます。
13. **適用** をクリックして、ロール(役割)グループの設定を保存します。
14. Active Directory の **設定と管理に戻る** をクリックします。
15. Active Directory **メインメニューに戻る** をクリックします。
16. ドメインフォレストのルート CA 証明書を iDRAC にアップロードします。
 - a. **Active Directory CA 証明書をアップロードする** ラジオボタンを選択して、**次へ** をクリックします。
 - b. **証明書のアップロード** ページで、証明書のファイルパスを入力するか、証明書ファイルの場所まで移動します。
 **メモ:** アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスおよび正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインコントローラの SSL 証明書はルート CA によって署名されている必要があります。iDRAC にアクセスする管理ステーション上でルート CA 証明書を使用可能にします([「ドメインコントローラルート CA 証明書のエクスポート](#)」を参照)。

 - c. **適用** をクリックします。
 iDRAC のウェブサーバーは、**適用** をクリックすると自動的に再起動します。
17. iDRAC Active Directory 機能の設定を完了するには、ログアウトしてから iDRAC にログインします。
18. **システム** → **リモートアクセス** の順にクリックします。
19. **設定** タブをクリックし、**ネットワーク** をクリックします。
20. **ネットワーク設定** で **DHCP を使用 (NIC IP アドレス用)** が選択されている場合、**DHCP を使用** を選択して **DNS サーバーアドレスを取得** を選択します。
 DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、一次および代替 DNS サーバーの IP アドレスを入力します。
21. **変更の適用** をクリックします。
 これで iDRAC 標準スキーマ Active Directory 機能の設定が完了しました。

標準スキーマ Active Directory と RACADM を使用して iDRAC を設定する方法

ウェブインタフェースでなく RACADM CLI を使用して、標準スキーマで iDRAC Active Directory 機能を設定するには、次のコマンドを使用します。


1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。


```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgActiveDirectory -o cfgADRootDomain <ルート FQDN>
racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupName <ロール(役割)グループの共通名>
racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupDomain <RAC FQDN>
```

```
racadm config -g cfgStandardSchema -i <索引> -o cfgSSADRoleGroupPrivilege <権限ビットマスク>

racadm sslcertupload -t 0x2 -f <ルート CA 証明書 TFTP-URI>

racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書 TFTP-URI>
```

 **メモ:** ビットマスク値については、「表 B-1」を参照してください。

2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```


3. iDRAC で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <二次 DNS IP アドレス>
```

標準スキーマ Active Directory と SM-CLP を使用して iDRAC を設定する方法

 **メモ:** 証明書は SM-CLP ではアップロードできません。iDRAC ウェブインタフェースまたはローカル RACADM コマンドを使用してください。

SM-CLP を使用して標準スキーマで iDRAC の Active Directory 機能を設定するには、次のコマンドを使用します。

1. Telnet または SSH を使用して iDRAC にログインし、次の SM-CLP コマンドを入力します。

```
cd /system/spl/oem Dell_ adservice1

set enablestate=1

set oem Dell_ schematype=2

set oem Dell_ adracdomain=<RAC FQDN>
```

2. 次の 5 つの Active Directory ロール(役割)グループそれぞれに次のコマンドを入力します。

```
set /system1/spl/groupN oem Dell_ groupname=<ロール (役割) グループ N 共通名>

set /system1/spl/groupN oem Dell_ groupdomain=<RAC FQDN>

set /system1/spl/groupN oem Dell_ groupprivilege=<ユーザー権限ビットマスク>
```

N は 1 ~ 5 の数字です。

3. Active Directory SSL 証明書を設定するには、次のコマンドを入力します。

```
set /system1/spl/oem Dell_ ssl1 oem Dell_ certtype=AD

load -source <ActiveDirectory 証明書 TFTP URI> /system1/spl/oem Dell_ ssl1

set /system1/spl/oem Dell_ ssl1 oem Dell_ certtype=SSL

dump -destination <iDRAC サーバー証明書 TFTP URI> /system1/spl/oem Dell_ ssl1
```

4. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の SM-CLP コマンドを入力します。

```
set /system1/spl/enetport1/lanendpt1/Y

ipendpt1/dnsendpt1 oem Dell_ serversfromdhcp=1
```

5. iDRAC で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の SM-CLP コマンドを入力します。

```
set /system1/spl/enetport1/lanendpt1/Y

ipendpt1/dnsendpt1 oem Dell_ serversfromdhcp=0

->cd /system1/spl/enetport1/lanendpt1/ipendpt1

dnsendpt1/remotesapl dnsserveraddress=<一次 DNS IP アドレス>

->cd /system1/spl/enetport1/lanendpt1/ipendpt1


dnsendpt1/remotesapl dnsserveraddress=<二次 DNS IP アドレス>
```

ドメインコントローラの SSL を有効にする

Microsoft Enterprise ルート CA を使ってすべてのドメインコントローラを SSL 証明書に自動的に割り当てる場合は、次の手順に従って各ドメインコントローラで SSL を有効にする必要があります。

- ドメインコントローラに Microsoft エンタープライズのルート CA をインストールします。
 - スタート→コントロールパネル→プログラムの追加と削除の順に選択します。
 - Windows コンポーネントの追加と削除を選択します。
 - Windows コンポーネント ウィザードで、証明書サービス チェックボックスをオンにします。
 - CA の種類 でエンタープライズのルート CA を選択して 次へ をクリックします。
 - この CA の共通名 を入力して 次へ をクリックし、完了 をクリックします。
- 各コントローラの SSL 証明書をインストールして、各ドメインコントローラで SSL を有効にします。
 - スタート→管理ツール→ドメインセキュリティポリシー をクリックします。
 - 公開キーのポリシー フォルダを展開し、自動証明書要求の設定 を右クリックして自動証明書要求 をクリックします。
 - 自動証明書要求の設定ウィザード で 次へ をクリックし、ドメインコントローラ を選択します。
 - 次へ をクリックして、完了 をクリックします。

ドメインコントローラルート CA 証明書のエクスポート

 **メモ:** システムで Windows 2000 が実行されている場合は、次の手順は異なっている可能性があります。

- Microsoft Enterprise CA サービスを実行しているドメインコントローラを見つけます。
- スタート→ファイル名を指定して実行 の順にクリックします。
- ファイル名を指定して実行 のフィールドに「mmc」と入力し、OK をクリックします。
- コンソール 1 (MMC) ウィンドウで、ファイル (または Windows 2000 マシンではコンソール) をクリックし、スナップインの追加と削除 を選択します。
- スナップインの追加と削除 ウィンドウで 追加 をクリックします。
- スタンドアロンスナップイン ウィンドウで 証明書 を選択して 追加 をクリックします。
- コンピュータ アカウントを選択して 次へ をクリックします。
- ローカルコンピュータを選択して 完了 をクリックします。
- OK をクリックします。
- コンソール 1 ウィンドウで、証明書 フォルダを展開し、パーソナル フォルダを展開して、証明書 フォルダをクリックします。
- ルート CA 証明書を見つけて右クリックし、すべてのタスク を選択して エクスポート... をクリックします。
- 証明書のエクスポート ウィザードで 次へ を選択し、いいえ、秘密キーをエクスポートしない を選択します。
- 次へ をクリックし、フォーマットとして Base-64 エンコード X.509 (.cer) を選択します。
- 次へ をクリックし、システムのディレクトリに証明書を保存します。
- 手順 14 に保存した証明書を iDRAC にアップロードします。

RACADM を使って証明書をアップロードするには、「[ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する方法](#)」を参照してください。



ウェブインタフェースを使って証明書をアップロードするには、次の手順を実行します。

- サポートされているウェブブラウザのウィンドウを開きます。
- iDRAC ウェブインタフェースにログインします。
- システム→リモートアクセス をクリックし、設定 タブをクリックします。
- セキュリティ をクリックして セキュリティ証明書メインメニュー ページを開きます。
- セキュリティ証明書メインメニュー ページで サーバー証明書のアップロード を選択して、適用 をクリックします。

- f. **証明書のアップロード** 画面で、次のいずれかの手順を実行します。
 - o **参照** をクリックして、証明書を選択します。
 - o **値** フィールドで証明書のパスを入力します。
- g. **適用** をクリックします。

iDRAC ファームウェア SSL 証明書のインポート

次の手順を使って、すべてのドメインコントローラの信頼された証明書のリストに iDRAC ファームウェア SSL 証明書をインポートします。

-  **メモ:** システムで Windows 2000 が実行されている場合は、次の手順は異なっている可能性があります。
-  **メモ:** iDRAC ファームウェア SSL 証明書が既知の CA によって署名されている場合は、この手順を実行する必要はありません。

iDRAC の SSL 証明書は、iDRAC のウェブサーバーで使用される証明書と同じです。すべての iDRAC は、デフォルトの自己署名済み証明書付きで出荷されます。

iDRAC ウェブインタフェースを使用して証明書にアクセスするには、**設定** → **Active Directory** → **iDRAC サーバー証明書をダウンロードする** を選択します。

1. ドメインコントローラで、MMC **コンソール** ウィンドウを開き、**証明書** → **信頼できるルート認証局**の順に選択します。
2. **証明書** を右クリックし、**すべてのタスク** を選択して **インポート** をクリックします。
3. **次へ** をクリックして SSL 証明書ファイルまで参照します。
4. 各ドメインコントローラの**信頼できるルート認証局**に RAC SSL 証明書をインストールします。

独自の証明書をインストールした場合は、その証明書に署名する CA が **信頼できるルート認証局** リストにあるかどうか確認してください。この認証局がリストにない場合、それを使用するすべてのドメインコントローラにインストールする必要があります。

5. **次へ** をクリックし、証明書の種類に基づいて証明書の保存場所を Windows に自動的に選択させるか、希望の場所まで参照します。
6. **完了** をクリックして OK をクリックします。

Active Directory を使用した iDRAC へのログイン

ウェブインタフェースを使用して iDRAC にログインするのに、Active Directory を使用できます。次のフォーマットのいずれかを使ってユーザー名を入力します。

<ユーザー名@ドメイン>

または


<ドメイン>/<ユーザー名>

または

<ドメイン>\<ユーザー名>

ユーザー名は 1~256 バイトの ASCII 文字列です。

ユーザー名、ドメイン名ともに空白スペースや特殊文字(¥, /, @ など)は使用できません。

-  **メモ:** 「Americas」などの NetBIOS ドメイン名は名前解決できないため、指定できません。

よくあるお問い合わせ(FAQ)

[表 6-10](#) は、よくあるお問い合わせとその回答です。

表 6-10 Active Directory との iDRAC の使用:
よくあるお問い合わせ(FAQ)

質問	回答
複数のツリー全体で Active Directory を使って iDRAC にログインできますか？	はい。iDRAC の Active Directory クエリアルゴリズムでは、1 つのフォレストで複数のツリーをサポートします。
混在モード(フォレストのドメインコントローラが、Microsoft Windows NT® 4.0、Windows 2000、または Windows Server 2003 など、異なるオペレーティングシステムを実行する場合)において、Active Directory を使って iDRAC にログインできますか？	はい。混在モードでは、iDRAC クエリプロセスが使用するすべてのオブジェクト(ユーザー、RAC デバイスオブジェクト、関連オブジェクト)は、同一のドメインになければなりません。
	Dell 拡張の Active Directory ユーザーとコンピュータスナップインは混在モードの場合、ドメイン間

	でオブジェクトを作成するために、モードを確認し、ユーザー制限を行います。
Active Directory との iDRAC の使用は複数のドメイン環境をサポートしていますか？	はい。ドメインフォレストの機能レベルは、ネイティブか Windows 2003 モードであることが必要です。また、関連オブジェクト、RAC ユーザーオブジェクト、および RAC デバイスオブジェクト(関連オブジェクトを含む)にあるグループはユニバーサルグループでなければなりません。
これらの Dell 拡張オブジェクト(Dell 関連オブジェクト、Dell RAC デバイス、および Dell 権限オブジェクト)をいくつかのドメインに分散できますか？	関連オブジェクトと権限オブジェクトは同じドメインの中に置く必要があります。この 2 種類のオブジェクトは、Dell 拡張の Active Directory ユーザーとコンピュータのスナップインによって、強制的に同一のドメインに作成されます。その他のオブジェクトは別のドメインに作成することができます。
ドメインコントローラの SSL 設定に何か制限はありますか？	はい。フォレストにある Active Directory サーバーの SSL 証明書は、すべて同じルート CA によって署名される必要があります。これは、iDRAC でアップロード可能な信用できる CA SSL 証明書は 1 つのみであるためです。
新しい RAC 証明書を作成しアップロードしましたが、ウェブインタフェースが起動しません。	<p>RAC 証明書の生成に Microsoft 証明書サービスを使用している場合、証明書の作成時に ウェブ証明書 ではなく誤って ユーザー証明書 を選択してしまった可能性があります。</p> <p>回復(リカバリ)するには、CSR を生成してから新しいウェブ証明書を Microsoft Certificate Services を使って作成し、管理下サーバーの RACADM CLI を用いてロードするには、次の RACADM コマンドを使用します。</p> <pre>racadm sslcsrgen [-g] [-u] [-f {filename}]</pre> <pre>racadm sslcertupload -t 1 -f {web_sslcert}</pre>
Active Directory 認証を使って iDRAC にログインできない場合、どうすればよいですか？この問題はどのようにトラブルシューティングできますか？	<ol style="list-style-type: none"> 1. ログインに NetBIOS 名でなく、正しいユーザードメイン名が使用されていることを確認します。 2. ローカル iDRAC ユーザーアカウントがある場合は、ローカルの資格情報を使用して iDRAC にログインします。 <p>ログインした後、次の手順を実行してください。</p> <ol style="list-style-type: none"> a. iDRAC Active Directory 設定 ページにある Active Directory を有効にする ボックスが選択されているのを確認します。 b. iDRAC ネットワーク設定 ページの DNS 設定が正しいことを確認します。 c. Active Directory ルート CA から iDRAC に Active Directory 証明書をアップロードしたことを確認します。 d. ドメインコントローラの SSL 証明書の有効期限が切れていないことを確認します。 e. DRAC 名、ルードメイン名、および DRAC/MC ドメイン名 が Active Directory の環境設定と一致していることを確認します。 f. iDRAC のパスワードが 127 文字以下であることを確認します。iDRAC は最大 256 文字のパスワードをサポートしていますが、Active Directory がサポートしているパスワードは最大 127 文字です。

[目次ページに戻る](#)

[目次ページに戻る](#)

管理下サーバーの設定と正常性の表示

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [システム概要](#)
- [WWN/MAC の概要](#)
- [システムの正常性](#)

システム概要

システム→プロパティ→概要をクリックして、メインシステムエンクロージャと Integrated Dell Remote Access Controller の情報を取得します。

メインシステムエンクロージャ

システム情報

iDRAC ウェブインタフェースのこの部分は、管理下サーバーについて次の基本情報を提供します。

- 1 説明 - 管理下サーバーのモデル番号や名前。
- 1 BIOS バージョン - 管理下サーバーの BIOS のバージョン番号。
- 1 サービスタグ - 管理下サーバーのサービスタグ番号。
- 1 ホスト名 - 管理下サーバーに関連する DNS ホスト名。
- 1 OS 名 - 管理下サーバーにインストールされているオペレーティングシステムの名前。

I/O メザニンカード

iDRAC ウェブインタフェースのこの部分は、管理下サーバーにインストールされている I/O メザニンカードとストレージコントローラカードについて、次の情報を提供します。

- 1 I/O メザニンカード - 管理下サーバーにインストールされている I/O メザニンカードをリストします。
- 1 カードタイプ - インストールされているメザニンカード / 接続の物理タイプ。
- 1 モデル名 - インストールされているメザニンカードのモデル番号、タイプ、または説明。
- 1 内蔵ストレージカード - インストールされているストレージコントローラカードのモデル番号または名前。

オートリカバリ

iDRAC ウェブインタフェースのこの部分は、Manage Server Administrator によって設定された管理下サーバーのオートリカバリ機能の現在の動作モードを詳述します。

- 1 リカバリ処置 - システム障害やハンクが検出されたときに実行する処置。使用できる処置は、**処置なし**、**ハードリセット**、**パワーダウン**、**パワーサイクル(電源再投入)**です。
- 1 初期カウントダウン - システムハンク検出後、iDRAC がリカバリ処置を実行するまでの時間(秒単位)。
- 1 現カウントダウン - カウントダウンタイマーの現在の値(秒単位)。


iDRAC(Integrated Dell Remote Access Controller)

iDRAC 情報

iDRAC ウェブインタフェースのこの部分は、iDRAC 自体について次の情報を提供します。

- 1 日付 / 時刻 - iDRAC の現在の日付と時刻(最後のページリフレッシュ時点)
- 1 ファームウェアのバージョン - 管理下サーバーにインストールされている iDRAC ファームウェアの現在のバージョン。
- 1 ファームウェアのアップデート - iDRAC ファームウェアが最後にアップデートされた日時。
- 1 ハードウェアのバージョン - 管理下サーバーの Primary(一時)プレーナー(回路基板)のバージョン番号。
- 1 IP アドレス - iDRAC(管理下サーバーではない)に関連付けられた IP アドレス。

- 1 ゲートウェイ - iDRAC に設定されたネットワークゲートウェイの IP アドレス。
- 1 サブネットマスク - iDRAC に設定された TCP/IP サブネットマスク。
- 1 MAC アドレス - iDRAC の LOM (LAN on Motherboard) ネットワークインタフェースコントローラに関連付けられた MAC アドレス。
- 1 DHCP 有効 - iDRAC が DHCP サーバーからその IP アドレスと関連情報をフェッチするように設定されている場合は有効になります。
- 1 優先 DNS アドレス 1 - 現在アクティブな Primary(一時)DNS サーバーに設定されます。
- 1 代替 DNS アドレス 2 - 代替の DNS サーバーアドレスに設定されます。


 **メモ:** この情報は、iDRAC → **プロパティ** → **iDRAC 情報** から入手できます。

WWN/MAC の概要

システム → **プロパティ** → **WWN/MAC** をクリックすると、インストールされている I/O メザニカードと関連するネットワークファブリックの現在の構成を表示できます。FlexAddress(フレックスアドレス)機能が有効な場合は、グローバルに割り当てられた(シャーン割り当ての)永続的 MAC アドレスが各 LOM のハードウェアに組み込まれた値を置き換えます。

システムの正常性

システム → **プロパティ** → **正常性** をクリックして、iDRAC と iDRAC が監視するコンポーネントの正常性に関する重要な情報を表示します。**重要度**行は、各コンポーネントのステータスを示します。ステータスアイコンのリストとその意味は、「[表 14-3](#)」を参照してください。**コンポーネント** 行のコンポーネント名をクリックして、コンポーネントに関する詳細を表示します。

 **メモ:** コンポーネントの情報は、ウィンドウの左側のペインでコンポーネント名をクリックしても表示できます。コンポーネントは左側のペインで、選択されているタブや画面とは関係なく常に表示されます。

iDRAC

iDRAC 情報ページには、正常性ステータス、名前、ファームウェアバージョン、ネットワークパラメータといった iDRAC に関する重要な詳細が多数リストされます。ページ上部の適切なタブをクリックすると、追加情報が表示されます。

CMC

CMC ページには、Chassis Management Controller の正常性ステータス、ファームウェアバージョン、および IP アドレスが表示されます。また、CMC **ウェブインタフェースの始動** ボタンをクリックしても、CMC ウェブインタフェースを始動できます。

バッテリー


バッテリーページには、管理下システムのリアルタイムクロック(RTC)と CMOS 設定データのストレージを維持するシステム基板のコインセルバッテリーのステータスと値が表示されます。

温度

温度プローブ情報ページには、オンボード室温プローブのステータスと測定値が表示されます。警告または失敗状態の最低および最高温度のしきい値が、プローブの現在の正常性ステータスとともに表示されます。

電圧

電圧プローブ情報ページには、電圧プローブのステータスと測定値が表示され、オンボード電圧レールと CPU コアセンサーのステータスといった情報が提供されます。

 **メモ:** サーバーのモデルによっては、警告または失敗状態の温度しきい値やプローブの正常性ステータスは表示されません。

電源モニター

電源モニターページでは、次のような電源のモニターおよび統計情報を表示できます。

- 1 電源モニター - サーバーによって使用されている電力量(システム基板電流モニターが報告)をワット単位で表示します。
- 1 電力追跡統計情報 - **計測開始時刻**が最後にリセットされてからシステムによって使用された電力量に関する情報を表示します。
- 1 ピーク統計情報 - **計測開始時刻**が最後にリセットされてからシステムによって使用されたピーク電力量に関する情報を表示します。

CPU

CPU 情報ページは、管理下サーバーの各 CPU の正常性について報告します。正常性ステータスには、多数の熱、電源、機能テストが一覧表示されます。

POST

POST コードページには、管理下サーバーのオペレーティングシステムを起動する前の、最終システム POST コード(16 進数)が表示されます。

他の正常性


他の正常性ページからは、次のシステムログにアクセスできます。

システムイベントログ - 管理下システムで発生するシステムの重要イベントが表示されます。

POST コード - 管理下サーバーのオペレーティングシステムを起動する前の、最終システム POST コード(16 進数)が表示されます。

最終クラッシュ - 一番最近のクラッシュ画面と時刻を表示します。

起動キャプチャ - 最後の 3 つの起動画面を再生します。

 **メモ:** この情報は、システム→プロパティ→ログからも利用できます。

[目次ページに戻る](#)

[目次ページに戻る](#)

GUI コンソールリダイレクトの使用

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [概要](#)
- [コンソールリダイレクトの使用](#)
- [ビデオビューアの使用](#)
- [よくあるお問い合わせ\(FAQ\)](#)


本項では、iDRAC コンソールリダイレクト機能の使用法について説明します。

概要

iDRAC コンソールリダイレクト機能を使用すると、ローカルのコンソールにリモートからグラフィックモードまたはテキストモードでアクセスできます。この機能を使用すると、1 つの場所から単一または複数の iDRAC システムを制御できます。

日常的なメンテナンスを各サーバーの前に座って行う必要はありません。デスクトップまたはラップトップコンピュータを使ってリモートからサーバーを管理できます。また、リモートから即座に他のユーザーと情報を共有することもできます。

コンソールリダイレクトの使用

 **メモ:** コンソールリダイレクトセッションを開いたとき、管理下サーバーはそのコンソールがリダイレクトされていることを示しません。

コンソールリダイレクト ページでは、ローカルの管理ステーションのキーボード、ビデオ、およびマウスを使ってリモートシステムを管理し、リモート管理下サーバーでそのデバイスを制御できます。この機能を仮想メディア機能と併用すると、リモートでソフトウェアのインストールを実行できます。

コンソールリダイレクトセッションには次の規則が適用されます。

- 1 同時にサポートされているコンソールリダイレクトセッションは最大 2 つです。両セッションで、同じ管理下サーバーコンソールを同時に表示します。
 - 1 管理下システムのウェブブラウザからコンソールリダイレクトセッションを開始しないでください。
 - 1 1 MB/秒以上のネットワーク帯域幅が必要です。
- 2 番目のユーザーがコンソールリダイレクトセッションを要求すると、最初のユーザーは通知を受け取り、アクセス拒否、ビデオのみ許可、またはフル共有アクセスを許可するオプションから選択できます。2 番目のユーザーには、別のユーザーがコントロールしていることが通知されます。1 番目のユーザーが 30 秒以内に応答しないと、2 番目のユーザーには自動的にフルアクセスが許可されます。2 つのセッションが同時にアクティブな期間には、アクティブセッションを持つ他方のユーザーを識別するメッセージが、各ユーザーの画面の右上角に表示されます。3 番目のアクティブセッションは許可されません。3 番目のユーザーがコンソールリダイレクトセッションを要求すると、1 番目や 2 番目のユーザーのセッションを中断することなく、アクセスは拒否されます。
- 1 番目と 2 番目のいずれのユーザーも Administrator 権限を持っていない場合は、1 番目のユーザーのアクティブセッションが終了すると、2 番目のユーザーのセッションも自動的に終了します。

サポートされている画面解像度とリフレッシュレート

[表 8-1](#) は、管理下システムで実行しているコンソールリダイレクトセッションでサポートされている画面解像度と、そのリフレッシュレートを示しています。

表 8-1 サポートされている画面解像度とリフレッシュレート

画面解像度	リフレッシュレート (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

管理ステーションの設定

管理ステーションでコンソールリダイレクトを使用するには、次の手順を実行してください。

1. 対応ウェブブラウザをインストールして設定します。詳細については、以下の項を参照してください。
 - 1 [対応ウェブブラウザ](#)
 - 1 [対応ウェブブラウザの設定](#)

- Firefox を使用している場合、または Internet Explorer で Java ビューアを使用する場合は、Java Runtime Environment (JRE) をインストールします。「[Java Runtime Environment \(JRE\) のインストール](#)」を参照してください。
- 画面解像度は 1280x1024 ピクセル以上に設定することをお勧めします。

注意: アクティブなコンソールリダイレクトセッションがあり、推奨解像度以下の画面で iKVM に接続している場合、ローカルコンソールでサーバーを選択すると、サーバーのコンソール解像度がリセットされることがあります。サーバーで Linux オペレーティングシステムを実行している場合は、ローカルモニターで X11 コンソールが表示されない可能性があります。iKVM で <Ctrl><Alt><F1> キーを押すと、Linux がテキストコンソールに切り替わります。

iDRAC ウェブインタフェースでのコンソールリダイレクトの設定

iDRAC ウェブインタフェースでコンソールリダイレクトを設定するには、次の手順を実行してください。

- システム をクリックし、コンソール タブをクリックします。
- 設定 をクリックして **コンソールリダイレクトの設定** ページを開きます。
- コンソールリダイレクトのプロパティを設定します。表 8-2 は、コンソールリダイレクトの設定について説明しています。
- 設定が完了したら、適用 をクリックします。
- 適切なボタンをクリックして続行します。「表 8-3」を参照してください。

表 8-2 コンソールリダイレクトの設定プロパティ

プロパティ	説明
有効	クリックして、コンソールリダイレクトを有効または無効にします。 チェックボックスがオン の場合は、コンソールリダイレクトが有効です。 チェックボックスがオフ の場合は、コンソールリダイレクトが無効です。 デフォルトは 有効 です。
最大セッション数	コンソールリダイレクトの最大セッション数(1 または 2)が表示されます。コンソールリダイレクトで許可する最大セッション数を変更するには、ドロップダウンメニューを使用します。デフォルトは 2 です。
アクティブセッション数	アクティブなコンソールセッション数を表示します。このフィールドは読み取り専用です。
キーボードとマウスポート番号	コンソールリダイレクトのキーボード/マウスオプションへの接続に使用するネットワークポート番号。トラフィックは常に暗号化されます。別のプログラムでデフォルトのポートが使用されている場合は、この番号を変更しなければならない可能性があります。デフォルトは 5900 です。
ビデオポート番号	コンソールリダイレクトの画面サービスへの接続に使用されるネットワークポート番号。別のプログラムでデフォルトのポートが使用されている場合は、この設定を変更しなければならない可能性があります。デフォルトは 5901 です。
ビデオ暗号化有効	チェックボックスがオン の場合は、ビデオ暗号化が有効です。ビデオポートを経由するすべてのトラフィックは、暗号化されます。 チェックボックスがオフ の場合は、ビデオ暗号化が無効です。ビデオポートを経由するトラフィックは暗号化されません。 デフォルトは、 暗号化 されます。 暗号化を無効にすると、低速なネットワークのパフォーマンスを改善できる場合があります。
マウスモード	管理下サーバーが Windows オペレーティングシステム環境で実行されている場合は、Windows を選択します。 サーバーが Linux 環境で実行されている場合は、Linux を選択します。 サーバーが Windows または Linux オペレーティングシステム環境で実行されていない場合は、なしを選択します。 デフォルトは Windows です。
IE 用コンソールブラウザタイプ	Windows オペレーティングシステム上で Internet Explorer を使用している場合は、次のビューアから選択できます。 ActiveX - The ActiveX コンソールリダイレクト ビューア Java - Java コンソールリダイレクト ビューア メモ: Internet Explorer のバージョンによっては、追加のセキュリティ制限をオフにする必要があります(「 仮想メディアの設定と使用法 」を参照)。 メモ: Java ビューアを使用するには、クライアントシステムに Java Runtime Environment がインストールされている必要があります。
ローカルコンソールを無効にする	チェックボックスがオンの場合は、コンソールリダイレクト中 iKVM モニターへの出力は無効になります。これにより、 コンソールリダイレクト を使って実行したタスクは、管理下サーバーのローカルモニターに表示されなくなります。

メモ: コンソールリダイレクトで仮想メディアを使用する方法については、「[仮想メディアの設定と使用法](#)」を参照してください。

コンソールリダイレクトの設定 ページには、表 8-5 に示すボタンがあります。

表 8-3 コンソールリダイレクトの設定ページのボタン

ボタン	定義
印刷	コンソールリダイレクトの設定 ページを印刷します。
更新	コンソールリダイレクトの設定 ページを再ロードします。
適用	コンソールリダイレクトに追加された新規設定を保存します。

SM-CLP コマンドラインインターフェイスでのコンソールリダイレクトの設定

コンソールリダイレクトセッションの開始

コンソールリダイレクトセッションを開くと、Dell 仮想 KVM ビューアアプリケーションが開始し、リモートシステムのデスクトップがビューアに表示されます。この仮想 KVM ビューアアプリケーションを使用すると、ローカル管理ステーションからリモートシステムのマウスとキーボードの機能を制御できます。


ウェブインターフェイスでコンソールリダイレクトセッションを開くには、次の手順を実行してください。

1. システム をクリックし、コンソール タブをクリックします。
2. コンソールリダイレクト ページで、表 8-4 に示す情報を使用してコンソールリダイレクトセッションが使用可能であることを確認します。

表示されているプロパティ値の設定を変更する場合は、「[iDRAC ウェブインターフェイスでのコンソールリダイレクトの設定](#)」を参照してください。

表 8-4 コンソールリダイレクトページの情報

プロパティ	説明
コンソールリダイレクト有効	はい / いいえ
ビデオ暗号化有効	はい / いいえ
最大セッション数	サポートされているコンソールリダイレクトの最大セッション数を表示します。
現在のセッション数	現在アクティブなコンソールリダイレクトセッション数を表示します。
マウスモード	現在有効なマウスアクセラレータが表示されます。マウスアクセラレータ モードは、管理下サーバーにインストールされているオペレーティングシステムの種類に応じて選択する必要があります。
コンソールのプラグインタイプ	現在設定されているプラグインタイプが表示されます。 Active-X - Active-X ビューアが起動します。Active-X ビューアは、Windows オペレーティングシステム上で実行する場合、Internet Explorer でのみ使用できます。 Java - Java ビューアが起動します。Java ビューアは、Internet Explorer を含め、どのブラウザでも使用できます。クライアントが Windows 以外のオペレーティングシステムで実行されている場合は、Java ビューアを使用する必要があります。Windows オペレーティングシステム環境で、Internet Explorer を使用して iDRAC にアクセスする場合は、プラグインタイプに Active-X または Java のどちらかを選択できます。
ローカルコンソール	ローカルコンソールが無効になっていない場合は、チェックボックスがオフです。チェックボックスがオンの場合は、シャーンで iKVM 接続を使用しているユーザーがコンソールにアクセスできません。


 **メモ:** コンソールリダイレクトで仮想メディアを使用する方法については、「[仮想メディアの設定と使用法](#)」を参照してください。


コンソールリダイレクト ページには、表 8-5 に示すボタンがあります。

表 8-5 コンソールリダイレクトページのボタン

ボタン	定義
更新	コンソールリダイレクトの設定 ページを再ロードします。
ビューアの起動	目的のリモートシステムのコンソールリダイレクトセッションを開きます。
印刷	コンソールリダイレクトの設定 ページを印刷します。

3. コンソールリダイレクトセッションが使用可能な場合は、ビューアの起動 をクリックします。

 **メモ:** アプリケーションが起動した後、メッセージボックスがいくつか表示される場合があります。アプリケーションへの不正アクセスを防ぐために、これらのメッセージボックスは 3 分間内に参照する必要があります。そうしないと、アプリケーションの再起動を要求されます。

 **メモ:** 以下の手順の途中で **セキュリティ警告** ウィンドウが表示された場合は、その内容を読んでから、はい をクリックして続行します。

管理ステーションが iDRAC に接続し、Dell デジタル KVM ビューアアプリケーションにリモートシステムのデスクトップが表示されます。

4. 2 つのマウスポインタ(1 つはリモートシステム用、もう 1 つはローカルシステム用)がビューアウィンドウに表示されます。リモートのマウスポインタがローカルのマウスポインタに従うように 2 つのマウスポインタを同期する必要があります。「[マウスポインタの同期](#)」を参照してください。

ビデオビューアの使用

ビデオビューアは管理ステーションと管理下サーバー間のユーザーインターフェースを提供するので、管理ステーション側から管理下サーバーのデスクトップを表示して、マウスやキーボードの機能を制御できます。リモートシステムに接続すると、ビデオビューアが別のウィンドウで開始します。

ビデオビューアは、カラーモード、マウスの同期、スナップショット、キーボードマクロ、仮想メディアへのアクセスなど、さまざまなコントロール調整機能を提供します。これらの機能の詳細については、[ヘルプ](#)をクリックしてください。

コンソールリダイレクトセッションを開始し、ビデオビューアが表示されたら、カラーモードの調整やマウスポインタの同期が必要になる場合があります。

[表 8-6](#) は、ビューアで使用可能なメニューオプションについて説明しています。

表 8-6 ビューアメニューバーの選択項目

メニュー項目	項目	説明
ビデオ	一時停止	コンソールリダイレクトを一時停止します。
	再開	コンソールリダイレクトを再開します。
	更新	ビューアの画面イメージを再描画します。
	現在の画面のキャプチャ	現在のリモートシステム画面を Windows 上の .bmp ファイルまたは Linux 上の .png ファイルにキャプチャします。ダイアログボックスが表示され、指定した場所にファイルを保存できます。
	全画面	ビデオビューアを全画面表示モードに拡大するには、 ビデオ メニューから 全画面表示 を選択します。
	終了	コンソールの使用を終了し、(リモートシステムのログアウト手順に従って)ログアウトしたら、 ビデオ メニューから 終了 を選択して ビデオビューア ウィンドウを閉じます。
キーボード	右 <Alt> キーを押し続ける	右 <Alt> キーと組み合わせるキーを入力する前にこのアイテムを選択します。
	左 <Alt> キーを押し続ける	左 <Alt> キーと組み合わせるキーを入力する前にこのアイテムを選択します。
	左 <Windows> キー	左 <Windows> キーと組み合わせる文字を入力する前に 押し続ける を選択します。左 <Windows> キーのキーストロークを送信するには、 押し放す を選択します。
	右 <Windows> キー	右 <Windows> キーと組み合わせる文字を入力する前に 押し続ける を選択します。右 <Windows> キーのキーストロークを送信するには、 押し放す を選択します。
	マクロ	マクロを選択するか、マクロに指定されたホットキーを入力すると、リモートシステムでそのアクションが実行されます。ビデオビューアは、次のマクロを提供しています。 <ul style="list-style-type: none"> 1 Ctrl-Alt-Del 1 Alt-Tab 1 Alt-Esc 1 Ctrl-Esc 1 Alt-スペース 1 Alt-Enter 1 Alt-ハイフン 1 Alt-F4 1 PrtScn 1 Alt-PrtScn 1 F1 1 Pause 1 Alt+m
キーボードのバスマスルー	キーボードのバスマスルーモードでは、クライアント上のすべてのキーボード機能をサーバーにリダイレクトできます。	
マウス	カーソルの同期	マウス メニューでは、クライアントのマウスがサーバーのマウスにリダイレクトされるようにカーソルを同期できます。
オプション	カラーモード	ネットワーク上でパフォーマンスを向上させるための色彩度を選択できます。たとえば、仮想メディアからソフトウェアをインストールする場合は、コンソールビューアが使用するネットワーク帯域幅を減らし、メディアからのデータ転送に使用する帯域幅を増やすように、最も彩度の低い色(3 ビットグレー)を選択できます。
		カラーモードは、15 ビットカラー、7 ビットカラー、4 ビットカラー、4 ビットグレー、3 ビットグレーに設定できます。
メディア	仮想メディアウィザード	メディア メニューでは、仮想メディアウィザードへのアクセスが提供され、以下のようなデバイスまたはイメージにリダイレクトできます。 <ul style="list-style-type: none"> 1 フロッピードライブ 1 CD 1 DVD 1 ISO フォーマットのイメージ 1 USB フラッシュドライブ 仮想メディアの機能については、「 仮想メディアの設定と使用法 」を参照してください。 仮想メディアを使用するには、コンソールビューアウィンドウをアクティブにしている必要があります。
ヘルプ	-	ヘルプ メニューをアクティブにします。

マウスポインタの同期

コンソールリダイレクトを使用してリモートの PowerEdge システムに接続する場合、リモートシステムのマウスアクセラレータ速度が管理ステーションのマウスポインタと同期せず、ビデオビューアウィンドウに 2 つのマウスポインタが表示されることがあります。

マウスポインタを同期するには、**マウス**→**カーソルの同期**の順にクリックするか、<Alt><M> キーを押します。


[カーソルの同期] メニューアイテムは切り替え式です。メニューのアイテムの横にチェックマークがあり、マウスの同期がアクティブであることを確認してください。


Red Hat® Linux® または Novell® SUSE® Linux を使用している場合は、ビューアを起動する前に必ず Linux 用のマウスモードに設定してください。設定の詳細については、「[iDRAC ウェブインタフェースでのコンソールリダイレクトの設定](#)」を参照してください。iDRAC コンソールリダイレクト画面でマウスの矢印を制御するには、オペレーティングシステムのデフォルトのマウス設定が使用されます。

ローカルコンソールを無効 / 有効にする

iDRAC ウェブインタフェースを使用して iKVM 接続を無効にするように iDRAC を設定できます。ローカルコンソールが無効になると、黄色のステータスドットがサーバーリスト(OSCAR)に表示され、コンソールが iDRAC でロックされていることを示します。ローカルコンソールが有効なときは、ステータスドットが緑色で表示されます。

管理下サーバーのコンソールへの排他的アクセスを確保する場合は、ローカルコンソールを無効にし、また **コンソールリダイレクトページ** で **最大セッション数** を 1 に再設定する必要があります。

 **メモ:** ローカルコンソール機能は、PowerEdge SC1435 および 6950 以外のすべての x9xx PowerEdge システムでサポートされています。

 **メモ:** サーバー上のローカルビデオを無効にする(オフにする)と、iKVM に接続しているモニター、キーボード、マウスが無効になります。

ローカルコンソールを無効または有効にするには、次の手順を実行してください。

- 管理ステーションで、対応ウェブブラウザを開いて iDRAC にログインします。詳細については、「[ウェブインタフェースへのアクセス](#)」を参照してください。
- システム** をクリックし、**コンソール** タブをクリックして、**設定** をクリックします。
- サーバー上のローカルビデオを無効にする(オフにする)場合は、**コンソールリダイレクトの設定** ページで、**ローカルコンソールを無効にする** チェックボックスをオンにし、**適用** をクリックします。デフォルト値は **オフ** です。
- サーバー上のローカルビデオを有効にする(オンにする)場合は、**コンソールリダイレクトの設定** ページで、**ローカルコンソールを無効にする** チェックボックスをオフにし、**適用** をクリックします。

コンソールリダイレクト ページにローカルサーバービデオのステータスが表示されます。

よくあるお問い合わせ(FAQ)

[表 8-7](#) は、よくあるお問い合わせとその回答です。

表 8-7 コンソールリダイレクトの使用:よくあるお問い合わせ(FAQ)

質問	回答
サーバー上のローカルビデオがオフになっている場合に、新しいリモートコンソールビデオセッションを開始できますか。	はい。
ローカルビデオをオフにするように要求してからサーバー上のローカルビデオがオフになるまで 15 秒もかかるのはなぜですか。	ビデオがオフに切り替わる前に、ローカルユーザーが必要に応じて別の操作を実行できるように配慮されています。
ローカルビデオをオンにする場合に、遅延時間は発生しますか。	いいえ。ローカルビデオを オン にする要求を iDRAC が受信すると、ビデオは瞬時にオンになります。
ローカルユーザーはビデオをオフにすることもできますか。	はい。ローカルユーザーは ローカル RACADM CLI を使ってビデオをオフにできます。
ローカルユーザーはビデオをオンにすることもできますか。	いいえ。ローカルコンソールを無効にすると、ローカルユーザーのキーボードとマウスは無効になるため、設定を変更することはできません。
ローカルビデオをオフに切り替えると、ローカルキーボードとマウスもオフに切り替わりませんか。	はい。
ローカルコンソールをオフにすると、リモートコンソールセッションのビデオはオフになりますか。	いいえ。ローカルビデオのオン / オフを切り替えても、リモートコンソールセッションには影響しません。
iDRAC ユーザーがローカルサーバービデオをオン / オフにするために必要な権限は何ですか。	iDRAC の設定権限を持つユーザーであれば、ローカルコンソールをオン / オフにできます。
ローカルサーバービデオの現在のステータスを取得するにはどのようにしますか。	ステータスは iDRAC のウェブインタフェースの コンソールリダイレクトの設定 ページに表示されます。 RACADM CLI コマンドの <code>racadm getconfig -g cfgRacTuning</code> は、 <code>cfgRacTuneLocalServerVideo</code> のオブジェクトにステータスを表示します。 ステータスは、iKVM OSCAR モニターにも表示されます。ローカルコンソールが有効な場合、サーバー名の横に緑色のステータスが表示されます。無効な場合は、ローカルコンソールが iDRAC によってロックされていることを示す黄色のドットが表示されます。
コンソールリダイレクトウィンドウからシステム画面の下部が見えませんか。	管理ステーションのモニターの解像度が 1280x1024 に設定されていることを確認してください。

コンソールウィンドウが文字化けします。	Linux のコンソールビューアには UTF-8 文字コードが必要です。ロケールを確認し、必要に応じて文字コードをリセットしてください。詳細については、「 Linux のロケール設定 」を参照してください。
Windows 2000 オペレーティングシステムをロードすると、管理下サーバーの画面に何も表示されないのはなぜですか。	管理下サーバーに正しい ATI ビデオドライバがありません。『Dell PowerEdge Installation and Server Management CD』を使用してビデオドライバをアップデートしてください。
コンソールリダイレクトを実行しているときに DOS でマウスが同期しないのはなぜでしょうか。	Dell BIOS はマウスドライバを PS/2 マウスとしてエミュレートしています。設計上、PS/2 マウスはマウスポインタの相対位置を使用するため、同期のずれが生じます。iDRAC には USB マウスドライバが搭載されているので、マウスポインタの絶対位置と正確な追跡が可能です。iDRAC が USB の絶対的なマウスの位置を Dell BIOS に通知しても、BIOS エミュレーションによって相対的な位置に戻されるため、動作は変わりません。この問題を修正するには、コンソールリダイレクトの設定でマウスモードを なし に設定してください。
Linux テキストコンソールでマウスが同期しないのはなぜでしょうか。	仮想 KVM は USB マウスドライバを必要としますが、USB マウスドライバは X-Window オペレーティングシステムでしか使用できません。
マウスの同期の問題がまだ解決しません。	コンソールリダイレクトセッションの開始前に、オペレーティングシステム用に正しいマウスが選択されていることを確認します。 マウス メニューで、 マウスの同期 が選択されていることを確認します。マウスの同期を切り替えるには、 マウス → マウスの同期 の順に選択するか、<Alt><M> キーを押します。同期が有効になっている場合、 マウス メニューで選択項目の横にチェックマークが表示されます。
iDRAC コンソールリダイレクトを使ってリモートから Microsoft® オペレーティングシステムをインストール中に、キーボードやマウスを使用できないのはなぜですか。	BIOS でコンソールリダイレクトが有効になっているシステムで、Microsoft の対応オペレーティングシステムをリモートからインストールすると、EMS 接続メッセージが表示され、続行する前に OK を選択するように要求されます。リモートでマウスを使って OK を選択することはできません。ローカルシステムで OK を選択するか、リモートで管理下サーバーを再起動し、再インストールしてから、BIOS でコンソールリダイレクトをオフにする必要があります。 このメッセージは、コンソールリダイレクトが有効になったことをユーザーに知らせるために Microsoft によって生成されます。このメッセージが表示されないようにするには、オペレーティングシステムをリモートインストールする前に、必ずコンソールリダイレクトを BIOS でオフにしてください。
管理ステーションの Num Lock インジケータにリモートサーバーの Num Lock のステータスが反映されないのはなぜですか。	iDRAC からアクセスした場合、管理ステーションの Num Lock インジケータは必ずしもリモートサーバーの Num Lock 状態と一致するとは限りません。Num Lock の状態は、管理ステーションの Num Lock の状態にかかわらず、リモートセッションが接続されたときのリモートサーバーの設定に依存します。
ローカルホストからコンソールリダイレクトセッションを確立すると、複数のセッションビューア ウィンドウが表示されるのはなぜですか。	コンソールリダイレクトセッションをローカルシステムから設定しているからです。この操作はサポートされていません。
コンソールリダイレクトセッションを実行中に、ローカルユーザーが管理下サーバーにアクセスした場合、警告メッセージが表示されますか。	いいえ。ローカルユーザーがシステムにアクセスした場合は、双方がシステムを制御できます。
コンソールリダイレクトセッションを実行するために必要な帯域幅はどれくらいですか。	良好なパフォーマンスを得るためには、5 MB/秒の接続を推奨します。最低限必要なパフォーマンスを得るためには 1 MB/秒の接続が必要です。
管理ステーションでコンソールリダイレクトを実行するために最低限必要なシステム要件を教えてください。	管理ステーションには、256 MB 以上の RAM を搭載した Intel Pentium III 500 MHz プロセッサが必要です。

[目次ページに戻る](#)

仮想メディアの設定と使用法

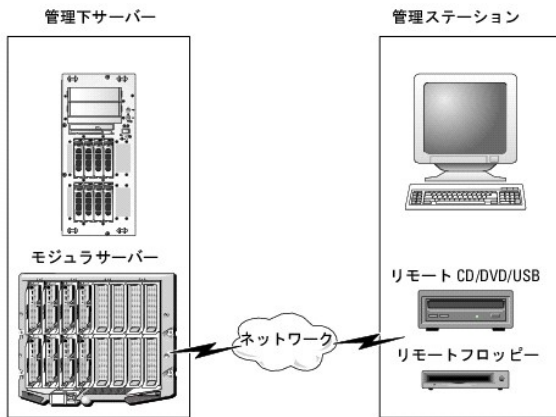
Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [概要](#)
- [仮想メディアの設定](#)
- [仮想メディアの実行](#)
- [よくあるお問い合わせ\(FAQ\)](#)

概要

コンソールリダイレクトビューアからアクセスする **仮想メディア** 機能は、ネットワーク上のリモートシステムに接続しているメディアへのアクセスを管理下サーバーに提供します。図 9-1 は、**仮想メディア** の全体的なアーキテクチャを示します。

図 9-1 仮想メディアの全体的なアーキテクチャ



仮想メディア を使用すると、管理下サーバーの起動から、アプリケーションのインストール、ドライバのアップデート、新しいオペレーティングシステムのインストールまで、仮想 CD/DVD およびディスクドライブからリモートで実行できます。

メモ: **仮想メディア** は 128 Kbps 以上のネットワーク帯域幅を必要とします。

仮想メディア は、管理下サーバーのオペレーティングシステムと BIOS に 2 つのデバイス(フロッピーディスクデバイスと光学ディスクデバイス)を定義します。

管理ステーションは、物理的なメディアまたはイメージファイルをネットワークを介して提供します。**仮想メディア** が接続していると、管理下サーバーからのすべての仮想 CD/ フロッピードライブのアクセス要求がネットワーク経由で管理ステーションに転送されます。**仮想メディア** への接続は、物理デバイスへのメディアの挿入と同様に表示されます。仮想メディアが接続していないとき、管理下サーバーの仮想デバイスは、ドライブにメディアがインストールされていない 2 台のドライブに見えます。

表 9-1 に、仮想フロッピーと仮想光学ドライブにサポートされているドライブ接続をリストします。

メモ: 接続中に **仮想メディア** を変更すると、システムの起動順序が停止する可能性があります。

表 9-1 サポートされているドライブ接続

サポートされている仮想フロッピードライブ接続	サポートされている仮想光学ドライブ接続
レガシー 1.44 フロッピードライブ(1.44 フロッピーディスクセット)	CD-ROM、DVD、CDRW、CD-ROM メディアとのコンボドライブ
USB フロッピードライブ(1.44 フロッピーディスクセット)	ISO9660 フォーマットの CD-ROM/DVD イメージファイル
1.44 フロッピーイメージ	CD-ROM メディアのある USB CD-ROM ドライブ
USB リムーバブルディスク	

Windows ベースの管理ステーション

Microsoft® Windows® オペレーティングシステムを実行している管理ステーションで **仮想メディア** 機能を実行するには、Internet Explorer と ActiveX コントロールプラグインの対応バージョンをインストールします(対応ウェブブラウザを参照)。ブラウザのセキュリティを **中** 以下に設定し、Internet Explorer が署名付き ActiveX コントロールをダウンロードしてインストールできるようにします。

Internet Explorer のバージョンによっては、ActiveX のセキュリティ設定をカスタマイズする必要があります。

1. Internet Explorer をスタートします。
2. ツール→ インターネットオプション をクリックし、セキュリティ タブをクリックします。
3. セキュリティ設定 を表示または変更するゾーンを選択してください。で、希望するゾーンをクリックして選択します。
4. このゾーンのセキュリティのレベル で、レベルのカスタマイズ をクリックします。
セキュリティ設定 ウィンドウが表示されます。
5. ActiveX コントロールとプラグイン で、次の設定が 有効にする になっていることを確認します。
 - 1 スクリプトレットの許可
 - 1 ActiveX コントロールに対して自動的にダイアログを表示
 - 1 署名された ActiveX コントロールのダウンロード
 - 1 未署名の ActiveX コントロールのダウンロード
6. OK をクリックして変更を保存し、セキュリティ設定 ウィンドウを閉じます。
7. OK をクリックして、インターネットオプション ウィンドウを閉じます。
8. Internet Explorer を再スタートします。

ActiveX をインストールするには、Administrator 権限が必要です。ActiveX コントロールをインストールする前に、Internet Explorer でセキュリティ警告が表示される場合があります。ActiveX コントロールのインストールを実行するには、表示されるセキュリティ警告に答えて ActiveX コントロールを許可します。

Linux ベースの管理ステーション

Linux オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Firefox の対応バージョンをインストールします。詳細については、「[対応ウェブブラウザ](#)」を参照してください。

コンソールリダイレクトプラグインを実行するには、Java Runtime Environment (JRE) が必要です。JRE は、java.sun.com からダウンロードできます。JRE バージョン 1.6 以降が推奨されます。

仮想メディアの設定

1. iDRAC ウェブインタフェースにログインします。
2. ナビゲーションツリーでシステム を選択し、コンソール タブをクリックします。
3. 設定→ 仮想メディア の順にクリックして仮想メディアを設定します。
[表 9-2](#) は 仮想メディア の設定値の説明です。
4. 設定が終了したら、適用 をクリックします。
5. 適切なボタンをクリックして続行します。「[表 9-3](#)」を参照してください。

表 9-2 仮想メディアの設定値

Attribute(属性)	Value(値)
仮想メディアの連結	<p>連結 - 瞬時に 仮想メディア をサーバーに連結します。</p> <p>分離 - 瞬時に 仮想メディア からサーバーを分離します。</p> <p>自動連結 - 仮想メディアセッションが開始している場合のみ、 仮想メディア をサーバーに連結します。</p>
最大セッション数	許可されている 仮想メディア の最大セッション数を表示します。これは常に 1 です。
アクティブセッション数	仮想メディアの現在のセッション数を表示します。
仮想メディア暗号化の有効	チェックボックスをクリックして、 仮想メディア 接続の暗号化を有効または無効にします。チェックボックスがオンの場合は、暗号化が有効で、チェックボックスがオフの場合は、暗号化が無効です。
仮想メディアポート番号	仮想メディア サービスへの暗号化なしの接続に使用されるネットワークポート番号。 仮想メディア サービスへの接続には、指定したポート番号から始まる 2 つの連続ポートが使用されます。指定したポートに続くポート番号を、その他の iDRAC サービスに設定することはできません。デフォルトは 3668 です。

仮想メディア SSL ポート番号	仮想メディア サービスへの暗号化接続に使用されるネットワークポート番号。仮想メディア サービスへの接続には、指定したポート番号から始まる 2 つの連続ポートが使用されます。指定したポートに続くポート番号を、その他の iDRAC サービスに設定することはできません。デフォルトは 3670 です。
フロッピーのエミュレーション	仮想メディア がサーバーにフロッピードライブとして表示されるか USB キーとして表示されるかを示します。フロッピーのエミュレーションのチェックボックスがオンの場合、仮想メディア デバイスはサーバーでフロッピーデバイスとして表示されます。オフの場合は、USB キードライブとして表示されます。
ブートワンスを有効にする	ブートワンスオプションを有効にするには、このボックスをオンにします。このオプションは、サーバーが 1 度起動した後で 仮想メディア セッションを終了します。このオプションは、自動展開の際に便利です。

表 9-3 仮想メディア設定ページのボタン

ボタン	説明
印刷	画面に表示されている コンソール設定 ページのデータを印刷します。
更新	コンソール設定 ページを再ロードします。
適用	コンソール設定 ページに追加された新しい設定を保存します。

仮想メディアの実行

- **注意:** 仮想メディアセッションの実行中は、`racreset` コマンドを使用しないでください。使用すると、データ損失などの不測の結果が生じます。
- **注意:** 仮想メディアにアクセス中、[コンソールビューア] ウィンドウアプリケーションはアクティブなままである必要があります。

- 管理ステーションで対応ウェブブラウザを開きます。「[対応ウェブブラウザ](#)」を参照してください。
- iDRAC ウェブインタフェースをスタートします。[ウェブインタフェースへのアクセス](#)。
- ナビゲーションツリーで **システム** を選択し、**コンソール** タブをクリックします。

コンソールリダイレクト ページが表示されます。表示されている属性値を変更する場合は、「[仮想メディアの設定](#)」を参照してください。

- ☑ **メモ:** このデバイスは仮想フロッピーとして仮想化できるので、**フロッピーイメージファイル** が **フロッピードライブ** (該当する場合) の下に表示されることがあります。1 台のオプティカルドライブと 1 つのフロッピーを同時に選択するか、1 台のドライブだけを選択することができます。
- ☑ **メモ:** 管理下サーバー上の仮想デバイスドライブ文字は、管理ステーション上の物理ドライブ文字とは一致しません。
- ☑ **メモ:** Internet Explorer の 拡張セキュリティが設定されている Windows オペレーティングシステムクライアントでは、**仮想メディア** が正しく機能しないことがあります。この問題を解決するには、Microsoft オペレーティングシステムのマニュアルを参照するか、システム管理者にお問い合わせください。

- ビューアの起動** をクリックします。

- ☑ **メモ:** Linux では、ファイル `viewer.jsp` がデスクトップにダウンロードされ、ファイルの処置について尋ねるダイアログボックスが表示されます。**プログラムを指定して開く** オプションを選択し、JRE インストールディレクトリの `bin` サブディレクトリにある `javaws` アプリケーションを選択します。

iDRACView アプリケーションが別のウィンドウで起動します。

- メディア** → **仮想メディアウィザード...** をクリックします。

[メディアリダイレクト] ウィザードが開きます。

- [ステータス] ウィンドウを表示します。メディアが接続している場合は、別のメディアソースに接続する前に切断してください。切断するメディアの右にある **接続解除** ボタンをクリックします。

- 接続するメディアタイプの横にあるラジオボタンを選択します。

フロッピー / USB ドライブ セクションのラジオボタンを 1 つと、**CD/DVD ドライブ** セクションのラジオボタンを 1 つ選択できます。

フロッピーイメージまたは ISO イメージを接続する場合は、(ローカルコンピュータ上の) イメージのパスを入力するか、**参照** ボタンでイメージを参照します。

- 選択した各メディアタイプの横にある接続ボタン** をクリックします。

メディアは接続し、[ステータス] ウィンドウがアップデートされます。

- 閉じる** ボタンをクリックします。

仮想メディアの切断

- メディア** → **仮想メディアウィザード...** をクリックします。

2. 切断する メディアの横にある **接続解除** をクリックします。

メディアは切断され、[ステータス] ウィンドウがアップデートされます。

3. **Close** (閉じる) をクリックします。

仮想メディアからの起動

システム BIOS を使用すると、仮想オプティカルドライブまたは仮想フロッピードライブから起動できるようになります。POST 中、BIOS セットアップウィンドウを開き、仮想ドライブが有効になっており、正しい順序で表示されていることを確認します。

BIOS 設定を変更するには、次の手順を実行してください。

1. 管理下サーバーを起動します。

2. <F2> を押して BIOS 設定ウィンドウを開きます。

3. 起動順序をスクロールして、<Enter> キーを押します。

ポップアップウィンドウに、仮想オプティカルデバイス と仮想フロッピードライブのリストがその他の標準起動デバイスと共に表示されます。

4. 仮想ドライブが有効で、ブータブルメディア (起動メディア) の最初のデバイスとして表示されていることを確認してください。必要に応じて、画面の指示に従って起動順序を変更します。

5. 変更を保存して終了します。

管理下サーバーが再起動します。

管理下サーバーは起動順序に従って、ブータブル (起動) デバイスからの起動を試みます。仮想デバイスが接続済みでブータブルメディアが存在している場合、システムはこの仮想デバイスで起動します。起動メディアがない場合は、ブータブルメディアのない物理デバイスの場合と同様にデバイスを無視します。

仮想メディアを使用したオペレーティングシステムのインストール

本項では、管理ステーションに手動でインタラクティブにオペレーティングシステムをインストールする方法について説明します。完了までに数時間かかる場合があります。**仮想メディア** を使用してスクリプトでオペレーティングシステムをインストールする手順では 15 分以内で完了します。詳細については、「[オペレーティングシステムの導入](#)」を参照してください。

1. 次の点を確認します。

- 1 管理ステーションの CD ドライブにオペレーティングシステムのインストール CD が挿入されている。
- 1 ローカルの CD ドライブが選択されている。
- 1 仮想ドライブに接続している。

2. 「[仮想メディアからの起動](#)」の起動手順に従って、BIOS がインストール元の CD ドライブから起動するように設定されていることを確認してください。

3. 画面の指示に従ってセットアップを完了します。

サーバーのオペレーティングシステムが実行しているときの仮想メディアの使用

Windows ベースシステム

Windows システムでは、仮想メディアドライブは連結されると自動的にマウントされ、ドライブ文字が設定されます。

Windows からの仮想ドライブの使い方は、物理ドライブの場合とほぼ同じです。仮想メディアウィザードを使用してメディアに接続し、ドライブをクリックしてその内容を参照すると、そのシステムでメディアが使用できるようになります。

Linux ベースのシステム

システムのソフトウェア構成によっては、仮想メディアドライブが自動的にマウントされない場合があります。ドライブが自動的にマウントされない場合は、Linux の `mount` コマンドを使ってドライブを手動でマウントします。

よくあるお問い合わせ (FAQ)

[表 9-4](#) は、よくあるお問い合わせとその回答です。

表 9-4 仮想メディアの使い方:よくあるお問い合わせ(FAQ)

質問	回答
仮想メディアのクライアントの接続が時々切断されます。どうしてでしょうか。	ネットワークのタイムアウトが発生すると、iDRAC ファームウェアはサーバーと仮想ドライブ間のリンクを切断して接続を中断します。 仮想メディアの設定を iDRAC ウェブインタフェースまたはローカル RACADM コマンドで変更した場合、設定変更が適用されると、接続しているすべてのメディアが切断されます。 仮想ドライブに再接続するには、仮想メディアウザードを使用します。
どのオペレーティングシステムが iDRAC をサポートしていますか。	対応オペレーティングシステムについては、「 対応オペレーティングシステム 」のリストを参照してください。
どのウェブブラウザが iDRAC をサポートしていますか。	対応ウェブブラウザについては、「 対応ウェブブラウザ 」のリストを参照してください。
時々クライアントの接続が切れるのはなぜですか。	<ol style="list-style-type: none"> 1 ネットワークが低速であるか、クライアントシステムの CD ドライブで CD を交換した場合は、クライアントの接続が途切れることがあります。たとえば、クライアントシステムの CD ドライブで CD を交換した場合、新しい CD には自動開始機能が備わっている可能性があります。この場合、クライアントシステムが CD の読み込み準備に時間がかかりすぎて、ファームウェアがタイムアウトになり、接続が途切れることがあります。接続が途切れた場合は、GUI から再接続して、その前の操作を続けることができます。 1 ネットワークのタイムアウトが発生した場合、iDRAC ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。また、ウェブインタフェースまたは RACADM コマンドの入力によって、他の人が仮想メディアの設定を変更した可能性があります。仮想ドライブに再接続するには、仮想メディア 機能を使用します。
Windows オペレーティングシステムのインストールに時間がかかりすぎるようです。どうしてでしょうか。	『Dell PowerEdge Installation and Server Management CD』と低速ネットワーク接続を使用して Windows オペレーティングシステムをインストールする場合、ネットワークレイテンジによって iDRAC ウェブインタフェースへのアクセスに時間がかかることがあります。インストールウィンドウにインストールプロセスが表示されていないのに、インストールが進行しています。
フロッピードライブまたは USB メモリキーの内容を見ているのですが、同じドライブを使って仮想メディア接続を確立しようとすると、接続エラーメッセージが表示されて再試行を求められます。どうしてでしょうか。	仮想フロッピードライブへの同時アクセスはできません。ドライブの仮想化を試みる前にドライブの内容を表示するアプリケーションを閉じてください。
仮想デバイスをブータブル(起動)デバイスとして設定するにはどうしますか。	管理下サーバーの [BIOS セットアップ] にアクセスして起動メニューに進みます。仮想 CD、仮想フロッピー、または仮想フラッシュを見つけて、必要に応じてデバイスの起動順序を変更します。たとえば、CD ドライブから起動するには、その CD ドライブを起動順序の最初のドライブとして設定してください。
どのタイプのメディアから起動できますか。	iDRAC では、以下のブータブルメディアから起動できます。 <ol style="list-style-type: none"> 1 CDROM/DVD データメディア 1 ISO 9660 イメージ 1 1.44 フロッピーディスクまたはフロッピーイメージ 1 オペレーティングシステムがリムーバブルディスクとして認識した USB キー 1 USB キーイメージ
USB キーをブータブルにするには、どうしますか。	support.dell.com で、Dell USB キーをブータブルにするための Windows プログラム、Dell 起動ユーティリティを検索してください。 Windows 98 起動ディスクでの起動、および起動ディスクから USB キーへのシステムファイルのコピーも可能です。たとえば、DOS プロンプトで次のコマンドを入力します。 <code>sys a: x: /s</code> x: は、ブータブルにする USB キーです。 Dell 起動ユーティリティを使用して、ブータブル USB キーを作成することもできます。このユーティリティは Dell ブランドの USB キーとしか互換性がありません。ユーティリティをダウンロードするには、ウェブブラウザを開き、Dell のサポートウェブサイト support.dell.com で R122672.exe を検索してください。
Red Hat® Enterprise Linux® または SUSE® Linux オペレーティングシステムを実行しているシステムでは、仮想フロッピーデバイスを検索できません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。	一部の Linux バージョンは仮想フロッピードライブと仮想 CD ドライブを同じ方法で自動マウントしません。仮想フロッピードライブをマウントするには、Linux が仮想フロッピードライブに割り当てたデバイスノードを検索します。仮想フロッピードライブを正しく見つけてマウントするには、次の手順を実行してください。 <ol style="list-style-type: none"> 1. Linux コマンドプロンプトウィンドウを開き、次のコマンドを入力します。 <code>grep "Virtual Floppy" /var/log/messages</code> 2. そのメッセージの最後のエントリを探し、その時刻を書きとめます。 3. Linux のプロンプトで次のコマンドを入力します。 <code>grep "hh:mm:ss" /var/log/messages</code> このコマンドで、 hh:mm:ss は、手順 1 で grep から返されたメッセージのタイムスタンプです。 4. 手順 3 で、grep コマンドの結果を読み、DELL 仮想フロッピー のデバイス名を探します。 5. 仮想フロッピードライブに接続していることを確認します。 6. Linux のプロンプトで次のコマンドを入力します。 <code>mount /dev/sdx /mnt/floppy</code> このコマンドで、 /dev/sdx はステップ 4 で見つけたデバイス名です。 /mnt/floppy はマウントポイントです。
仮想フロッピードライブでサポートされているファイルシステムの種類を教えてください。	仮想フロッピードライブは、FAT16 または FAT32 ファイルシステムをサポートしています。

iDRAC ウェブインタフェースを使用してファームウェアのアップデートをリモートで実行すると、サーバーの仮想ドライブが削除されました。どうしてでしょうか。	ファームウェアのアップデートによって iDRAC がリセットされ、リモート接続が切断して仮想ドライブがアンマウントされます。iDRAC リセットが完了すると、ドライブは再表示されます。
---	--

[目次ページに戻る](#)

[目次ページに戻る](#)

ローカル RACADM コマンドラインインタフェースの使用

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [RACADM コマンドの使用](#)
- [RACADM サブコマンド](#)
- [RACADM ユーティリティを使用した iDRAC の設定](#)
- [iDRAC 設定ファイルの使用](#)
- [複数の iDRAC の設定](#)

ローカル RACADM コマンドラインインタフェース (CLI) は、管理下サーバーから iDRAC の管理機能へのアクセスを提供します。RACADM を使用すると、iDRAC ウェブインタフェースと同じ機能にアクセスできます。RACADM はスクリプトで使用して複数のサーバーと iDRAC の設定を簡易化する一方、ウェブインタフェースはインタラクティブな管理に便利です。

ローカル RACADM コマンドは、管理下サーバーから iDRAC へのアクセスにネットワーク接続を使用しません。つまり、最初の iDRAC ネットワーク設定にローカル RACADM コマンドを使用できます。

複数の iDRAC を設定する方法については、「[複数の iDRAC の設定](#)」を参照してください。

この項には次の情報が記載されています。

- 1 コマンドプロンプトからの RACADM の使用
- 1 `racadm` コマンドを使用した iDRAC の設定
- 1 RACADM 設定ファイルを使用した複数の iDRAC の設定

RACADM コマンドの使用

コマンドプロンプトまたはシェルプロンプトからローカル (管理下サーバー上) で RACADM コマンドを実行します。

管理下サーバーにログインし、コマンドシェルを起動して、ローカル RACADM コマンドを次のフォーマットで入力します。

```
racadm <サブコマンド> -g <グループ> -o <オブジェクト> <値>
```

オプションを使用しなければ、RACADM コマンド によって一般的な使用情報が表示されます。RACADM サブコマンド一覧を表示するには、次のように入力します。

```
racadm help
```

サブコマンドのリストには、iDRAC でサポートされるコマンドがすべて含まれています。

サブコマンドのヘルプを取得するには、次のように入力します。

```
racadm help <サブコマンド>
```

このコマンドによって、サブコマンドの構文とコマンドラインオプションが表示されます。

RACADM サブコマンド

表 10-1 は、RACADM で実行できる各 RACADM サブコマンドについて説明しています。構文と有効なエントリを含む RACADM サブコマンドの詳細については、「[RACADM サブコマンドの概要](#)」のリストを参照してください。

表 10-1 RACADM サブコマンド

コマンド	説明
<code>clrraclog</code>	iDRAC のログをクリアします。クリアすると、ログがクリアされたときのユーザーと時刻を示すエントリが 1 つ作成されます。
<code>clrsele</code>	管理下サーバーのシステムイベントログの エントリをクリアします。
<code>config</code>	iDRAC を設定します。
<code>getconfig</code>	現在の iDRAC 設定のプロパティを表示します。
<code>getniccfg</code>	コントローラの現在の IP 設定を表示します。
<code>getraclog</code>	iDRAC のログを表示します。
<code>getractime</code>	iDRAC の時刻を表示します。
<code>getssninfo</code>	アクティブセッションに関する情報を表示します。
<code>getsvctag</code>	サービスタグを表示します。
<code>getsysinfo</code>	IP 設定、ハードウェアモデル、ファームウェアバージョンおよびオペレーティングシステム情報を含む iDRAC および管理下サーバーに関する情報を表示します。
<code>gettracelog</code>	iDRAC トレースログ を表示します。-i と共に使用すると、iDRAC のトレースログ内のエントリ数を表示します。
<code>help</code>	iDRAC サブコマンドを一覧にします。

help <サブコマンド>	指定したサブコマンドの使用ステートメントを一覧にします。
racreset	iDRAC をリセットします。
racresetcfg	iDRAC をデフォルト設定にリセットします。
serveraction	管理下サーバーの電源管理操作を実行します。
setniccfg	コントローラの IP 設定を指定します。
sslcertdownload	CA 証明書をダウンロードします。
sslcertupload	CA 証明書またはサーバー証明書を iDRAC にアップロードします。
sslcertview	iDRAC に CA 証明書またはサーバー証明書を表示します。
sslcsrngen	SSL CSR を生成してダウンロードします。
testemail	iDRAC NIC で iDRAC に電子メールを送信させます。
testtrap	iDRAC NIC で iDRAC に SNMP 警告を送信させます。

RACADM ユーティリティを使用した iDRAC の設定

この項では、RACADM を使用して、さまざまな iDRAC 設定タスクを実行する方法を説明します。

現在の iDRAC 設定の表示

RACADM `getconfig` サブコマンドは、iDRAC から現在の設定を取得します。設定値は、1 つまたは複数の オブジェクト を含む グループ に編成され、オブジェクトには 値 があります。

グループとオブジェクトの詳細については、「[iDRAC プロパティデータベースのグループとオブジェクトの定義](#)」を参照してください。

全 iDRAC グループのリストを表示するには、次のコマンドを入力します。

```
racadm getconfig -h
```


特定のグループのオブジェクトと値を表示するには、次のコマンドを入力します。


```
racadm getconfig -g <グループ>
```


たとえば、`cfgLanNetworking` グループのオブジェクト設定をすべて表示するには、次のコマンドを入力します。

```
racadm getconfig -g cfgLanNetworking
```

RACADM を使用した iDRAC ユーザーの管理

 **注意:** `racresetcfg` コマンドを使用すると、すべての 設定パラメータが元のデフォルトにリセットされるため、注意してください。それまでに行った変更がすべて失われます。

 **メモ:** 新しい iDRAC を設定している場合や、`racadm racresetcfg` コマンドを実行した場合、現在のユーザーは `root` (ルート)のみで、パスワードは `calvin` になります。

 **メモ:** ユーザーは経時的に有効にしたり、無効にしたりできます。その結果、ユーザーが各 iDRAC に異なる索引番号を持つ場合があります。

iDRAC のプロパティデータベースには、最大 15 のユーザーを設定できます。(16 番目のユーザーは、IPMI LAN ユーザー用に予約されています。)手動で iDRAC ユーザーを有効にする前に、現在のユーザーが存在しているかどうか確認してください。


コマンドプロンプトで次のコマンドを入力すると、ユーザーが存在するかどうかわかります。

```
racadm getconfig -u <ユーザー名>
```

または

1 ~ 16 の各索引に 1 回ずつ次のコマンドを入力します。

```
racadm getconfig -g cfgUserAdmin -i <索引>
```

 **メモ:** また、`racadm getconfig -f <ファイル名>` と入力し、生成した `<ファイル名>` ファイルを表示することもできます。このファイルにはすべてのユーザーと、その他の iDRAC 設定パラメータが含まれます。

複数のパラメータとオブジェクト ID が現在値と共に表示されます。対象オブジェクトは次の 2 つです。

```
# cfgUserAdminIndex=nn
```

```
cfgUserAdminUserName=
```

`cfgUserAdminUserName` オブジェクトに値がない場合は、`cfgUserAdminIndex` オブジェクトで示されるその索引番号は使用可能です。「=」の後に名前が表示された場合は、索引がそのユーザー名に割り当てられています。

iDRAC ユーザーの追加

新しいユーザーを iDRAC に追加するには、次の手順を実行してください。

1. ユーザー名を設定します。
2. パスワードを設定します。
3. ログインを iDRAC ユーザー権限に設定します。
4. ユーザーを有効にします。

例

次の例は、パスワードが「123456」で iDRAC へのログイン権限のある「John」という新しいユーザーを追加する方法を示しています。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2 0x00000001
racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

新規ユーザーを検証するには、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 2
```

権限のある iDRAC ユーザーを有効にする

ユーザーに特定の管理者権限(役割[ロール]ベース)を与えるには、`cfgUserAdminPrivilege` プロパティを、[表 10-2](#) に示した値から構成されるビットマスクに設定します。

表 10-2 ユーザー権限を表すビットマスク

ユーザー権限	権限ビットマスク
iDRAC へのログイン	0x00000001
iDRAC の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100

たとえば、ユーザーに **iDRAC の設定**、**ユーザーの設定**、**ログのクリア**、**コンソールリダイレクトへのアクセス** 権限を与えるには、`0x00000002`、`0x00000004`、`0x00000008`、`0x00000010` の値を追加してビットマップ `0x0000002E` を構成します。続いて、次のコマンドを入力して権限を設定します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

iDRAC ユーザーの削除

RACADM を使用している場合は、ユーザーを手動で個別に無効にする必要があります。設定ファイルを使用してユーザーを削除することはできません。

次の例では、RAC ユーザーの削除に使用できるコマンド構文を示します。


```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <索引> ""
```

二重引用符(“)のヌル文字列は、指定した索引のユーザー設定を削除して、出荷時のデフォルトにリセットするように iDRAC に指示します。

電子メール警告のテスト

iDRAC 電子メール警告機能を使用すると、管理下サーバーで重要なイベントが発生したときに電子メール警告を受信できます。次の例は、電子メール警告機能をテストして、iDRAC が電子メール警告をネットワークを介して正しく送信できることを確認する方法を示しています。

```
racadm testemail -i 2
```


 **メモ:** 電子メール警告機能をテストする前に、SMTP と 電子メール警告のオプション が設定されていることを確認してください。詳細については、「[電子メール警告の設定](#)」を参照してください。

iDRAC SNMP トラップ警告機能のテスト

iDRAC SNMP トラップ警告機能を使用すると、管理下サーバーで発生したシステムイベントを受信するための SNMP トラップリスナーを設定できます。

次の例は、SNMP トラップ警告機能をテストする方法を示しています。

```
racadm testtrap -i 2
```

 **メモ:** iDRAC SNMP トラップ警告機能をテストする前に、SNMP とトラップのオプションが正しく設定されていることを確認してください。これらのオプションを設定するには、`testtrap` および `testemail` サブコマンドの説明を参照してください。

iDRAC ネットワークプロパティの設定

使用可能なネットワークプロパティのリストを生成するには、次のように入力します。

```
racadm getconfig -g cfgLanNetworking
```


DHCP を使用して IP アドレスを取得するには、次のコマンドを使って `cfgNicUseDhcp` オブジェクトを記述し、この機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

コマンドは、起動時に <Ctrl><E> の入力を求められたときの iDRAC 設定ユーティリティと同じ設定機能を提供します。iDRAC 設定ユーティリティを使用したネットワークプロパティ設定の詳細については、「[LAN](#)」を参照してください。

次に、LAN ネットワークプロパティの設定に入力できるコマンドの例を示します。

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

 **メモ:** `cfgNicEnable` を 0 に設定すると、DHCP が有効の場合でも iDRAC LAN は無効になります。

IPMI の設定

1. 次のコマンドを入力して、IPMI オーバー LAN を設定します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

 **メモ:** この設定によって、IPMI オーバー LAN インタフェースから実行できる IPMI コマンドが決まります。詳細については、IPMI 2.0 の仕様を参照してください。

- a. 次のコマンドを入力して、IPMI チャンネル権限をアップデートします。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <レベル>
```

<レベル> は次のいずれかです。


- 2(ユーザー)
- 3(オペレーター)

- 4(Administrator: システム管理者)

たとえば、IPMI LAN チャンネル権限を 2(ユーザー) に設定するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

- 必要に応じて、次のようなコマンドを使用して IPMI LAN チャンネルの暗号化キーを設定します。


 **メモ:** iDRAC IPMI は RMCP+ プロトコルに対応しています。詳細については、IPMI 2.0 仕様を参照してください。

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <キー>
```

<キー> は有効な 16 進数形式の 20 文字からなる暗号化キーです。

- 次のコマンドを使用して、IPMI シリアルオーバー LAN(SOL)を設定します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

 **メモ:** IPMI SOL 最低権限レベルは、IPMI SOL をアクティブにするために最低限必要な権限を決定します。詳細については、IPMI 2.0 の仕様を参照してください。

- 次のコマンドを使用して IPMI SOL の最小権限レベルをアップデートします。


```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <レベル>
```

<レベル> は次のいずれかです。

- 2(ユーザー)
- 3(オペレータ)
- 4(Administrator: システム管理者)

例えば、IPMI の権限を 2(ユーザー)に設定する場合は、次のコマンドを入力します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

 **メモ:** シリアルコンソールを LAN 経由でダイレクトする場合、SOL ボーレートが管理下サーバーのボーレートと同じであることを確認してください。

- 次のコマンドを使用して IPMI SOL のボーレートをアップデートします。


```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <ボーレート>
```

<ボーレート> は 19200、57600、115200 bps のいずれかになります。

次に、例を示します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

- コマンドプロンプトで次のコマンドを入力して SOL を有効にします。

 **メモ:** SOL は個々のユーザーに対して有効または無効にできます。

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

<ID> はユーザーの固有の ID です。

PEF の設定

各プラットフォーム警告に対し iDRAC が講じる処置を設定できます。[表 10-3](#) は、可能な処置と RACADM でこれらを識別するための値のリストです。

表 10-3 プラットフォームイベントの処置

動作	Value(値)
処置は不要	0
電源オフ	1
再起動	2
パワーサイクル(電源再投入)	3

- 次のコマンドを使用して PEF 処置を設定します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <索引> <処置値>
```

<索引> は PEF 索引(「表 5-6」を参照)で、<処置値> は「表 10-3」から取得した値です。

たとえば、プロセッサの重大なイベントが検出されたときに、PEF がシステムを再起動して IPMI 警告を送信できるようにするには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
```

PET の設定

1. 次のコマンドを使用してグローバル警告を有効にします。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. 次のコマンドを使用して PET を有効にします。

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <索引> <0|1>
```

<索引> は PET の送信先索引で、0 は PET を無効に、1 は PET を有効にします。

たとえば、PET を索引 4 で有効にするには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```

3. 次のコマンドを使用して PET ポリシーを設定します。

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <索引> <IP アドレス>
```

<索引> は PET の送信先索引で、<IP アドレス> は、プラットフォームイベント警告を受け取るシステムの宛先 IP アドレスです。

4. コミュニティ名の文字列を設定します。

コマンドプロンプトで、次のコマンドを入力します。

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名前>
```

<名前> は PET コミュニティ名です。

電子メールアラートの設定

1. 次のコマンドを入力してグローバル警告を有効にします。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. 次のコマンドを入力して電子メール警告を有効にします。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <索引> <0|1>
```

<索引> は電子メール送信先索引で、0 は電子メール警告を無効に、1 は電子メール警告を有効にします。電子メールの送信先索引は 1~4 の値が可能です。

たとえば、PET を索引 4 で有効にするには、次のコマンドを入力します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

3. 次のコマンドを使用して電子メールのオプションを設定します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <電子メールアドレス>
```

1 は電子メール送信先の索引で、<電子メールアドレス> は、プラットフォームイベント警告を受け取る送信先電子メールアドレスです。

4. カスタムメッセージを設定するには、次のコマンドを入力します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <索引> <カスタムメッセージ>
```

<索引> は電子メール送信先索引で、<カスタムメッセージ> はカスタムメッセージです。

5. 必要に応じて、次のコマンドを使用して設定した電子メール警告をテストします。

```
racadm testemail -i <索引>
```

<索引> は、テストする電子メール送信先索引です。

IP フィルタ(IPRange)の設定

IP アドレスフィルタ(または IP 範囲チェック)を使用すると、ユーザーが特定した範囲内にある IP アドレスのクライアントワークステーションや管理ワークステーションからのみ IDRAC へのアクセスを許可できます。その他のすべてのログイン要求は拒否されます。

IP フィルタは着信ログインの IP アドレスを、次の `cfgRacTuning` プロパティで指定する IP アドレス範囲と比較します。

- 1 `cfgRacTuneIpRangeAddr`
- 1 `cfgRacTuneIpRangeMask`

`cfgRacTuneIpRangeMask` プロパティは着信 IP アドレスと `cfgRacTuneIpRangeAddr` プロパティの両方に適用されます。結果が同じ場合は、着信ログイン要求に IDRAC へのアクセスが許可されます。この範囲外の IP アドレスからのログイン要求にはエラーが返されます。

次の式の値がゼロに等しい場合は、ログインに進みます。

```
cfgRacTuneIpRangeMask & (<着信 IP アドレス> ^ cfgRacTuneIpRangeAddr)
```

& は数量のビットワイズ AND で ^ はビットワイズ XOR です。

`cfgRacTuning` プロパティの全リストは、「[cfgRacTuning](#)」を参照してください。

表 10-4 IP アドレスフィルタ(IPRange)のプロパティ

プロパティ	説明
<code>cfgRacTuneIpRangeEnable</code>	IP アドレスのチェック機能を有効にします。
<code>cfgRacTuneIpRangeAddr</code>	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。 このプロパティはビットワイズ and と <code>cfgRacTuneIpRangeMask</code> を使用して、許可する IP アドレスの上位ビットを決定します。IP アドレスの上位ビットにこのビットパターンが含まれるすべての IP アドレスにログインが許可されます。この範囲外の IP アドレスからのログインはエラーになります。各プロパティのデフォルト値は、192.168.1.0 ~ 192.168.1.255 のアドレス範囲からのログインを許可しています。
<code>cfgRacTuneIpRangeMask</code>	IP アドレスの有意ビット位置を定義します。マスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。

IP フィルタの設定

ウェブインタフェースで IP フィルタを設定するには、次の手順を実行してください。

1. システム→リモートアクセス→IDRAC→ネットワーク/セキュリティの順にクリックします。
2. ネットワーク設定 ページで、詳細設定 をクリックします。
3. IP 範囲有効 チェックボックスを選択し、IP 範囲のアドレスと IP 範囲のサブネットマスクを入力します。
4. 適用 をクリックします。

次の例では、ローカル RACADM を使用して IP フィルタを設定します。

 **メモ:** RACADM と RACADM コマンドの詳細については、「[ローカル RACADM コマンドラインインタフェースの使用](#)」を参照してください。

1. 次の RACADM コマンドは 192.168.0.57 以外のすべての IP アドレスをブロックします。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1  
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57  
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```
2. ログインを 4 つの連続する IP アドレスに限定するには(192.168.0.212~192.168.0.215)、次のようにマスクの最下位の 2 ビットを除くすべてを選択します。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1  
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212  
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

範囲マスクの最後のバイトは 252 に設定されています。10 進数では 11111100b に相当します。

IP フィルタのガイドライン

IP フィルタを有効にする場合は、次のガイドラインに従ってください。

- 1 `cfgRacTuneIpRangeMask` は必ずネットマスク形式で設定してください。最重要ビットがすべて(マスクのサブネットを定義)する 1 で、下位ビットではすべて 0 になります。
- 1 必要な範囲の基底アドレスを `cfgRacTuneIpRangeAddr` の値として使用します。このアドレスの 32 ビットのバイナリ値は、マスクにゼロがある下位ビットがすべてゼロになります。


IP ブロックの設定

IP ブロックは、事前に選択した時間内に特定の IP アドレスからのログイン失敗回数が過剰になったのを動的に判断し、そのアドレスが iDRAC にログインするのをブロックします。

IP ブロックには次の機能が含まれます。

- 1 許可するログイン失敗回数 (`cfgRacTuneIpBlkFailCount`)
- 1 これらの失敗の時間枠 (秒) (`cfgRacTuneIpBlkFailWindow`)
- 1 許可する合計失敗回数を超過してブロックされた IP アドレスのセッション確立が阻止される秒数 (`cfgRacTuneIpBlkPenaltyTime`)

特定の IP アドレスからのログイン失敗が累積すると、それらは内部カウンタに登録されます。ユーザーがログインに成功すると、失敗履歴がクリアされて、内部カウンタがリセットされます。

 **メモ:** クライアント IP アドレスからのログイン試行が拒否されると、SSH クライアントに「ssh exchange identification: Connection closed by remote host (SSH ID: リモートホストが接続を閉じました)」というメッセージが表示される場合があります。

`cfgRacTune` プロパティの全リストは、「[iDRAC プロパティデータベースのグループとオブジェクトの定義](#)」を参照してください。

[ログイン再試行制限のプロパティ](#) に、ユーザー定義のパラメータを示します。

表 10-5 ログイン再試行制限のプロパティ

プロパティ	定義
<code>cfgRacTuneIpBlkEnable</code>	IP ブロック機能を有効にします。 一定時間内に (<code>cfgRacTuneIpBlkFailWindow</code>) 1 つの IP アドレスからの失敗が連続すると (<code>cfgRacTuneIpBlkFailCount</code>)、以降そのアドレスからのセッション確立試行がすべて一定の時間 (<code>cfgRacTuneIpBlkPenaltyTime</code>) 拒否されます。
<code>cfgRacTuneIpBlkFailCount</code>	ログイン試行を拒否するまでの IP アドレスのログイン失敗回数を設定します。
<code>cfgRacTuneIpBlkFailWindow</code>	失敗した試行がカウントされる時間枠 (秒)。失敗回数がこの制限値を超えると、カウンタはリセットされます。
<code>cfgRacTuneIpBlkPenaltyTime</code>	ログイン失敗回数の制限を超えた IP アドレスからのログイン試行を拒否する時間を秒で指定します。

IP ブロックを有効にする

次の例では、クライアントが 1 分間に 5 回ログイン試行に失敗した場合に、5 分間のクライアント IP アドレスのセッション確立を阻止します。


```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1  
  
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5  
  
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60  
  
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```


次の例は、1 分以内に失敗が 3 回を超えた場合に、1 時間ログイン試行を阻止します。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1  
  
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3  
  
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60  
  
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

ローカル RACADM を使用した iDRAC Telnet および SSH サービスの設定

Telnet/SSH コンソールは、RACADM コマンドを使用してローカル (管理下サーバー上) で設定できます。

 **メモ:** この項のコマンドを実行するには、iDRAC の設定 権限が必要です。

 **メモ:** iDRAC で Telnet または SSH 設定を変更した場合、既存のすべてのセッションは、警告なく終了します。

ローカル RACADM から Telnet/SSH コンソールを有効にするには、管理下サーバーにログインし、コマンドプロンプトで次のコマンドを入力します。

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
```

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Telnet または SSH サービスを無効にするには、値を 1 から 0 に変更します。

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0
```

```
racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

iDRAC の Telnet ポート番号を変更するには、次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <新しいポート番号>
```

たとえば、Telnet ポートをデフォルトの 22 から 8022 に変更するには、次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

使用可能な RACADM CLI コマンドの全リストは、「[ローカル RACADM コマンドラインインタフェースの使用](#)」を参照してください。

iDRAC 設定ファイルの使用

iDRAC 設定ファイルは、iDRAC データベースの値が含まれたテキストファイルです。RACADM `getconfig` サブコマンドを使用して iDRAC の現在の値が含まれた設定ファイルを生成できます。ファイルを編集し、RACADM `config -f` サブコマンドを使用してファイルを iDRAC にロードし直すか、設定を他の iDRAC にコピーできます。

iDRAC 設定ファイルの作成

設定ファイルは、フォーマットされていないプレーンテキストファイルです。有効なファイル名なら何でも使用できますが、推奨される拡張子は `.cfg` です。

設定ファイルの特徴は以下の通りです。


- 1 テキストエディタで作成可能
- 1 RACADM `getconfig` サブコマンドで iDRAC から取得
- 1 RACADM `getconfig` サブコマンドで iDRAC から取得して編集

RACADM `getconfig` コマンドで設定ファイルを取得するには、管理下サーバーのコマンドプロンプトで次のコマンドを入力します。

```
racadm getconfig -f myconfig.cfg
```

このコマンドは、現在のディレクトリにファイル `myconfig.cfg` を作成します。

設定ファイルの構文

 **注意:** Windows の Notepad や Linux の vi など、プレーンテキストエディタで設定ファイルを編集します。racadm ユーティリティは ASCII テキストのみを解析します。フォーマットすると、パーサが混乱して iDRAC データベースが破損する可能性があります。

この項では設定ファイルのフォーマットについて説明します。

- 1 # で始まる行はコメントです。

コメントは、行の最初の列で開始する必要があります。その他の列にある # の文字は、単に # 文字として処理されます。

例:

```
#  
  
# これはコメントです。  
  
[cfgUserAdmin]  
  
cfgUserAdminPrivilege=4
```

- 1 すべてのグループエントリは、[] の文字で囲む必要があります。

グループ名を示す開始の [文字は、一列目で始まる必要があります。このグループ名はそのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。[iDRAC プロパティデータベースのグループとオブジェクトの定義](#) で定義したように、設定データはグループに分類されています。

次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

例:

```
[cfgLanNetworking] (グループ名)  
  
cfgNicIpAddress=143.154.133.121 (オブジェクト名)
```


- 1 パラメータは、object、=、値 の間に空白を入れずに「object=値」のペアとして指定されます。

値の後の空白スペースは無視されます。値の文字列内にあるスペースは変更されません。= の右側の文字はすべてそのまま解釈されます(たとえば 2 番目の =、または#、[、] など)。

- 1 パーサは、索引オブジェクトエントリを無視します。

ユーザーは使用する索引を指定できません。索引がすでに存在する場合は、それが使用されます。索引がない場合は、そのグループで最初に使用可能な索引に新しいエントリが作成されず。


racadm getconfig -f <ファイル名> コマンドは、索引オブジェクトの前にコメントを配置するため、ここでコメントを確認できます。

 **メモ:** 次のコマンドを使用すると、索引グループを手動で作成できます。
racadm config -g <グループ名> -o <アンカー付きオブジェクト> -i <索引> <固有アンカー名>

- 1 索引付きグループの行は設定ファイルから削除できません。

次のコマンドを使用して、手動で索引オブジェクトを削除する必要があります。

```
racadm config -g <グループ名> -o <オブジェクト名> -i <索引> ""
```

 **メモ:** NULL 文字列(2 つの "" 文字)は、指定したグループの索引を削除するように iDRAC に命令します。

索引付きグループの内容を表示するには、次のコマンドを使用します。

```
racadm getconfig -g <グループ名> [-i <索引>]
```

- 1 索引付きグループの場合、オブジェクトアンカーは [] の組の後ろになる最初のオブジェクトでなければなりません。次は、現在の索引付きグループの例です。

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<ユーザー名>
```

- 1 パーサーが索引付けされたグループを見つけた場合、これはさまざまな索引との差を表すアンカー付きオブジェクトの値です。

パーサーは、iDRAC からそのグループのすべての索引を読み取ります。グループ内のオブジェクトはすべて iDRAC が 設定されたときに簡単な変更が加えられたものです。変更されたオブジェクトが新しい索引を表す場合、設定中にその iDRAC の索引が作成されます。

- 1 設定ファイルで索引を指定することはできません。

索引は作成と削除が繰り返されるため、グループは次第に使用中の索引と未使用索引で断片化して行く可能性があります。索引が存在する場合は、変更されます。索引が存在しない場合は、最初に使用できる索引が使用されます。この方法では、管理されているすべての RAC 間で索引を正確に一致させる必要のない場合に、索引付きエントリを追加できるという柔軟性が得られます。新しいユーザーは、最初に使用可能な索引に追加されます。すべての索引が一杯で新しいユーザーを追加しなければならない場合は、1 つの iDRAC で正しく解析および実行される設定ファイルが別の iDRAC でも正しく実行されるとは限りません。

設定ファイルの iDRAC IP アドレスの変更

設定ファイルの iDRAC IP アドレスを変更する場合は、不要な <変数>=<値> のエントリをすべて削除します。IP アドレス変更に関連する 2 つの <変数>=<値> エントリを含め、"[]" が付いた実際の変数グループのラベルのみが残ります。

次に、例を示します。

```
#
# オブジェクトグループ"cfgLanNetworking"
```

```
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

このファイルは次のようにアップデートされます。

```
#
# オブジェクトグループ"cfgLanNetworking"
```


```
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
```

コメント、以下の行は無視されます


```
cfgNicGateway=10.35.9.1
```

iDRAC への設定ファイルのロード

`racadm config -f <ファイル名>` コマンドは、有効なグループとオブジェクト名が存在し、構文ルールに従っていることを検証するために設定ファイルを解析します。ファイルにエラーがあれば、コマンドはファイルの内容で iDRAC データベースをアップデートします。

 **メモ:** 構文のみを検証し、iDRAC データベースをアップデートしない場合は、`config` サブコマンドに `-c` オプションを追加します。

設定ファイルのエラーには、検出された行番号のフラグと、その問題を説明した簡単なメッセージが付ききます。設定ファイルで iDRAC をアップデートする前に、すべてのエラーを修正する必要があります。

 **注意:** `racresetcfg` サブコマンドを使用すると、データベースと iDRAC NIC は元のデフォルトの設定にリセットされ、ユーザーとユーザー設定はすべて削除されます。root (ルート) ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。

`racadm config -f <ファイル名>` コマンドを実行する前に、`racreset` サブコマンドを使用して iDRAC をデフォルト設定にリセットできます。ロードする設定ファイルに目的のオブジェクト、ユーザー、索引、他のパラメータがすべて含まれていることを確認してください。

設定ファイルで iDRAC をアップデートするには、管理下サーバーのコマンドプロンプトで次のコマンドを実行します。

```
racadm config -f <ファイル名>
```

コマンドが完了したら、`RACADM getconfig` サブコマンドを実行すると、アップデートが正常に終了したことを確認できます。

複数の iDRAC の設定

設定ファイルを使用して、同じプロパティの他の iDRAC を設定できます。複数の iDRAC を設定するには、次の手順に従ってください。

1. 他の iDRAC にコピーしたい設定がある iDRAC から設定ファイルを作成します。管理下サーバーのコマンドプロンプトで次のコマンドを入力します。

```
racadm getconfig -f <ファイル名>
```

<ファイル名> は `myconfig.cfg` など、iDRAC プロパティを保存するファイルの名前です。

詳細については、「[iDRAC 設定ファイルの作成](#)」を参照してください。

 **メモ:** 一部の設定ファイルには、他の iDRAC にファイルをエクスポートする前に変更が必要な固有の iDRAC 情報(静的 IP アドレスなど)が含まれています。

2. 前の手順で作成した設定ファイルを編集し、コピーしたくない設定を削除またはコメントアウトします。
3. 設定したい iDRAC がある管理下サーバーのそれぞれにアクセスできるネットワークドライブに、編集した設定ファイルをコピーします。
4. 各 iDRAC に次の設定を行います。

- a. 管理下サーバーにログインし、コマンドプロンプトを開始します。
- b. iDRAC の設定をデフォルト設定から変更するには、次のコマンドを入力します。

```
racadm racreset
```

- c. 次のコマンドを使用して、設定ファイルを iDRAC にロードします。

```
racadm config -f <ファイル名>
```

<ファイル名> は、作成した設定ファイルの名前です。ファイルが作業ディレクトリにない場合は、完全パスを含めてください。

- d. 次のコマンドを入力して、設定済みの iDRAC をリセットします。

```
racadm reset
```

[目次ページに戻る](#)


[目次ページに戻る](#)

iDRAC SM-CLP コマンドラインインタフェースの使用

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [SM-CLP を使用したシステム管理](#)
- [iDRAC SM-CLP サポート](#)
- [SM-CLP の機能](#)
- [MAP アドレス領域の移動](#)
- [show パープの使用](#)
- [iDRAC SM-CLP の例](#)
- [Telnet または SSH によるシリアルオーバー LAN\(SOL\)の使用](#)

本項では、iDRAC に組み込まれている Server Management Workgroup(SMWG) Server Management Command Line Protocol(SM-CLP)について説明します。

 **メモ:** ここでは、ユーザーが Systems Management Architecture for Server Hardware (SMASH) イニシアチブおよび SMWG SM-CLP 仕様に精通していることを前提としていません。これらの仕様の詳細については、Distributed Management Task Force (DMTF) のウェブサイト www.dmtf.org を参照してください。

iDRAC SM-CLP は DMTF と SMWG が提唱するプロトコルで、システム管理 CLI 実装の標準となっています。その原動力は、システム管理コンポーネントの標準化の基盤となることを目標に定義された SMASH アーキテクチャです。SMWG SM-CLP は DMTF が提唱する全体的な SMASH 作業のサブコンポーネントです。

SM-CLP は、ローカルの RACADM コマンドラインインタフェースが提供する機能のサブセットを別のアクセスパスで提供します。SM-CLP は iDRAC 内で実行されますが、RACADM は管理下サーバーで実行されます。また、RACADM は Dell 専用のインタフェースであるのに対し、SM-CLP は業界標準のインタフェースです。RACADM および SM-CLP コマンドのマッピングについては、「[RACADM と SM-CLP との対応付け](#)」を参照してください。

SM-CLP を使用したシステム管理

iDRAC SM-CLP によって、コマンドラインまたはスクリプトから次のシステム機能を管理できます。

- 1 サーバーの電源管理 - システムのオン、シャットダウン、再起動
- 1 システムイベントログ(SEL)管理 - SEL レコードの表示やクリア
- 1 iDRAC ユーザーのアカウント管理
- 1 Active Directory 設定
- 1 iDRAC LAN 設定
- 1 SSL 証明書署名要求(CSR)の生成
- 1 仮想メディア設定
- 1 Telnet または SSH でのシリアルオーバー LAN(SOL)リダイレクト

iDRAC SM-CLP サポート

SM-CLP は iDRAC ファームウェアからホストされ、Telnet 接続と SSH 接続をサポートしています。iDRAC SM-CLP インタフェースは DMTF 組織が提供する SM-CLP 仕様バージョン 1.0 に基づいています。

以下の項では、iDRAC からホストされる SM-CLP 機能の概要を述べます。

SM-CLP の機能

SM-CLP 仕様は、CLI を使用した単純なシステム管理に使用できる標準的な SM-CLP パープの共通セットを提供しています。

SM-CLP はパープとターゲットの概念を発展させて、CLI を使用したシステム設定機能を提供します。パープは実行する処理を指し、ターゲットはその処理を実行するエンティティ(またはオブジェクト)を決定します。

以下は SM-CLP コマンドラインの構文です。

<パープ> [<オプション>] [<ターゲット>] [<プロパティ>]

[表 11-1](#) は、iDRAC CLI がサポートするパープのリスト、各コマンドの構文、およびパープがサポートするオプションのリストを示しています。

表 11-1 サポートされている SM-CLP CLI パープ

パープ	説明	オプション
cd	シェルを使用して管理下システムのアドレス領域を移動します。	-default, -examine, -help, -output, -version

	構文: cd [オプション] [ターゲット]	
delete	オブジェクトのインスタンスを削除します。 構文: delete [オプション] [ターゲット]	-examine, -help, -output, -version
dump	バイナリイメージを MAP から URI に移動します。 dump -destination <URI> [オプション] [ターゲット]	-destination, -examine, -help, -output, -version
exit	SM-CLP シェルのセッションを終了します。 構文: exit [オプション]	-help, -output, -version
help	SM-CLP コマンドのヘルプを表示します。 help	-examine, -help, -output, -version
load	バイナリイメージを URI から MAP に移動します。 構文: load -source <URI> [オプション] [ターゲット]	-examine, -help, -output, -source, -version
reset	ターゲットをリセットします。 構文: reset [オプション] [ターゲット]	-examine, -help, -output, -version
set	ターゲットのプロパティを設定します。 構文: set [オプション] [ターゲット] <プロパティ名>=<値>	-examine, -help, -output, -version
show	ターゲットのプロパティ、パーブ、およびサブターゲットを表示します。 構文: set [オプション] [ターゲット] <プロパティ 名>=<値>	-all, -default, -display, -examine, -help, -level, -output, -version
start	ターゲットを開始します。 構文: start [オプション] [ターゲット]	-examine, -force, -help, -output, -version
stop	ターゲットをシャットダウンします。 構文: stop [オプション] [ターゲット]	-examine, -force, -help, -output, -state, -version, -wait
version	ターゲットのバージョン属性を表示します。 構文: version [オプション]	-examine, -help, -output, -version

表 11-2 は、SM-CLP オプションについて説明しています。表に示されているように、一部のオプションには省略形があります。

表 11-2 サポートされている SM-CLP オプション

SM-CLP オプション	説明
-all, -a	実行可能な機能のすべてを実行するようにパーブに指示します。
-destination	dump コマンドのイメージを保存する場所を指定します。 構文: -destination <URI>
-display, -d	コマンド出力をフィルタします。 構文: -display <プロパティ ターゲット パーブ>[, <プロパティ ターゲット パーブ>]*
-examine, -x	コマンドを実行せずにコマンド構文を確認するようにコマンドプロセッサに指示します。
-help, -h	パーブのヘルプを表示します。
-level, -l	指定ターゲット下の追加レベルでターゲットで動作するようパーブに指示します。

	構文: -level <n all>
-output, -o	出力のフォーマットを指定します。 構文: -output <text clpcsv clpxml>
-source	load コマンドのイメージ場所を指定します。 構文: -source <URI >
-version, -v	SMASH-CLP バージョン番号を表示します。

MAP アドレス領域の移動

メモ: SM-CLP アドレスパスでスラッシュ(/)とバックスラッシュ(\)は置き換え可能です。ただし、コマンドラインの最後のバックスラッシュは次の行のコマンドに続き、コマンドが解析されると無視されます。

SM-CLP で管理できるオブジェクトは Manageability Access Point (MAP) アドレス領域と呼ばれる階層空間に分類されたターゲットで表されます。アドレスパスは、アドレス領域のルートからアドレス領域のオブジェクトへのパスを指定します。

ルートターゲットは、スラッシュ(/)またはバックスラッシュ(\)で表されます。これは、iDRAC にログインするときのデフォルトの開始ポイントです。cd パープブを使用してルートから移動します。たとえば、システムイベントログ (SEL) で 3 番目のレコードに移動するには、次のコマンドを入力します。

```
->cd /system1/sp1/logs1/record3
```

ターゲットなしで cd パープブを入力し、アドレス領域の現在の場所を検索します。... の機能は、Windows および Linux の場合と同様です。.. は、親レベルを参照し、. は、現在のレベルを参照します。

ターゲット

表 11-3 は、SM-CLP で使用可能なターゲットの一覧です。

表 11-3 SM-CLP のターゲット

ターゲット	定義
/system1/	管理下システムターゲット
/system1/sp1	サービスのプロセッサ。
/system1/sol1	シリアルオーバー LAN のターゲット。
/system1/sp1/account1 ~ /system1/sp1/account16	16 のローカル iDRAC ユーザーアカウント。account1 が root アカウント。
/system1/sp1/enetport1	iDRAC NIC の MAC アドレス。
/system1/sp1/enetport1/lanendpt1/ ipendpt1	iDRAC IP、ゲートウェイ、ネットマスクの設定。
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	iDRAC DNS サーバーの設定。
/system1/sp1/group1 ~ /system1/sp1/group5	Active Directory 標準スキーマのグループ。
/system1/sp1/logs1	ログ収集ターゲット。
/system1/sp1/logs1/record1	管理下システムの SEL レコードの個々のインスタンス
/system1/sp1/logs1/records	管理下システムの SEL ターゲット。
/system1/sp1/oemdel_lracsecurity1	証明書署名要求の生成に使用するパラメータのストレージ。
/system1/sp1/oemdel_ssl1	SSL 証明書要求の状態。
/system1/sp1/oemdel_vmsservice1	仮想メディアの設定と状態。

show パープブの使用

ターゲットの詳細を知るには、show パープブを使用します。このパーブは、その場所で許可されているターゲットのプロパティ、サブターゲット、および SM-CLP パープブのリストを表示します。

-display オプションの使用

show -display オプションで、コマンドの出力を 1 つまたは複数のプロパティ、ターゲット、パーブに制限できます。たとえば、現在の場所のプロパティとターゲットのみを表示する場合は、次のコマンド

ドを使用します。

```
show -d properties,targets /system1/sp1/account1
```

特定のプロパティのみを表示するには、次のコマンドのように修飾します。

```
show -d properties=(userid,username) /system1/sp1/account1
```

1 つのプロパティのみを表示する場合は、括弧は省略できます。

-level オプションの使用

`show -level` オプションは、指定ターゲットの下の他のレベルに `show` を実行します。たとえば、`account1` の `username` および `userid` プロパティを、`/system1/sp1` の下の `account16` ターゲットから表示する場合は、次のコマンドを入力します。

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

アドレス領域のすべてのターゲットとプロパティを表示するには、次のコマンドのように `-l all` オプションを使用します。

```
show -l all -d properties /
```

-output オプションの使用

`-output` オプションは、SM-CLP パープの出力の 4 つのフォーマット(`text`、`clpcsv`、`keyword`、`clpxml`)の 1 つを指定します。

デフォルトのフォーマットは `text` (テキスト) で、最も読みやすい出力です。`clpcsv` フォーマットはカンマ区切りの値のフォーマットで、表計算プログラムへの読み込みに適しています。`keyword` (キーワード) フォーマットは、キーワード=値 のペアを 1 行に 1 つずつのリストとして出力します。`clpxml` フォーマットは、**応答** XML 要素を含む XML ドキュメントです。DMTF は `clpcsv` および `clpxml` フォーマットを指定しており、これらの仕様は DMTF ウェブサイト (www.dmtf.org) で参照できます。

次の例は、SEL の内容を XML で出力する方法を示しています。

```
show -l all -output format=clpxml /system1/sp1/logs1
```

iDRAC SM-CLP の例

以下のサブセクションでは、SM-CLP を使用して次の処理を実行する例を示します。

- 1 サーバーの電源管理
- 1 SEL の管理
- 1 MAP ターゲットのナビゲーション
- 1 システムプロパティの表示
- 1 iDRAC IP アドレス、サブネットマスク、ゲートウェイアドレスの設定

iDRAC SM-CLP インタフェースの使い方の詳細については、「[iDRAC SMCLP プロパティデータベース](#)」を参照してください。

サーバーの電源管理

[表 11-4](#) は、SM-CLP を使用して管理下サーバーの電源管理操作を実行する例を示しています。

表 11-4 サーバーの電源管理操作

操作	構文
SSH インタフェースを使用して iDRAC にログインする	>ssh 192.168.0.120 >login: root >password:
サーバーの電源を切る	->stop /system1 system1 has been stopped successfully
電源オフの状態からサーバーの電源を入れる	->start /system1 system1 has been started successfully
サーバーを再起動する	->reset /system1 system1 has been reset successfully

SEL 管理

表 11-5 は、SM-CLP を使用して、管理下システムで SEL 関連の操作を実行する例を示しています。

表 11-5 SEL の管理操作

操作	構文
SEL の表示	<pre>->show /system1/spl/logs1</pre> <p>Targets: record1 record2 record3 record4 record5</p> <p>Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5</p> <p>Verbs: cd delete exit help show version</p>
SEL レコードの表示	<pre>->show /system1/spl/logs1/record4 ufip=/system1/spl/logs1/log1/record4</pre> <p>Properties: Caption=Not defined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted ElementName=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI SEL CreationClassName=CIM_LogRecord RecordID=4 MessageTimeStamp=16:37:10,January 13,2007</p> <p>Verbs: cd exit help show version</p>
SEL のクリア	<pre>->delete /system1/spl/logs1 All records deleted successfully</pre>

MAP ターゲットのナビゲーション

表 11-6 は、cd パープを使用して MAP をナビゲートする例を示しています。すべての例で、最初のデフォルトターゲットは / であると想定されます。

表 11-6 Map ターゲットのナビゲーション操作

操作	構文
システムターゲットまでナビゲートして再起動する	<pre>->cd system1 ->reset</pre> <p>メモ: 現在のデフォルトターゲットは / です。</p>
SEL ターゲットまでナビゲートしてログレコードを表示する	<pre>->cd system1 ->cd spl ->cd logs1 ->show</pre> <pre>->cd system1/spl/logs1 ->show</pre>
現在のターゲットを表示する	<pre>->cd .</pre>
1 つ上のレベルへ移動する	<pre>->cd ..</pre>
シェルを終了する	<pre>->exit</pre>

iDRAC IP アドレス、サブネットマスク、ゲートウェイアドレスの設定

SM-CLP を使用して iDRAC ネットワークプロパティをアップデートするには、2 段階のプロセスがあります。

1. `/system1/sp1/enetport1/lanendpt1/ipendpt1`: で NIC プロパティの新しい値を設定します。
 - o `oemdel1_nicenable` - iDRAC ネットワークを有効にするには 1、無効にするには 0 に設定します。
 - o `ipaddress` - IP アドレス
 - o `subnetmask` - サブネットマスク
 - o `oemdel1_usedhcp` - DHCP の使用を有効にして `ipaddress` および `subnetmask` プロパティを設定するには 1、静的な値を設定するには 0 に設定します。
2. `committed` プロパティを 1 に設定して新しい値をコミットします。

commit プロパティの値が 1 の場合、プロパティの現在の設定はアクティブです。いずれかのプロパティを変更すると、commit プロパティが 0 にリセットされ、その値がコミットされていないことを示します。

メモ: commit プロパティは、`/system1/sp1/enetport1/lanendpt1/ipendpt1` MAP 場所のプロパティのみに影響します。その他の SM-CLP コマンドはすべて瞬時に有効になります。

メモ: ローカル RACADM を使用して iDRAC ネットワークプロパティを設定する場合、ローカル RACADM はネットワーク接続に依存しないため、変更内容は瞬時に反映されます。

変更をコミットすると、新しいネットワーク設定が有効になり、Telnet または SSH セッションが終了します。このコミット手順を導入すると、SM-CLP コマンドをすべて完了するまでセッションの終了を延期できます。

表 11-7 は、SM-CLP を使用した iDRAC プロパティの設定例を示しています。

表 11-7 SM-CLP を使用した iDRAC ネットワークプロパティの設定

操作	構文
iDRAC NIC プロパティの場所へ移動します。	<code>-->cd /system1/sp1/enetport1/lanendpt1/ipendpt1</code>
新しい IP アドレスを設定します。	<code>-->set ipaddress=10.10.10.10</code>
サブネットマスクを設定します。	<code>-->set subnetmask=255.255.255.255</code>
DHCP フラグをオンにします。	<code>-->set oemdel1_usedhcp=1</code>
NIC を有効にします。	<code>-->set oemdel1_nicenable=1</code>
変更をコミットします。	<code>-->set committed=1</code>

SM-CLP を使用した iDRAC ファームウェアのアップデート

SM-CLP を使用して iDRAC をアップデートするには、Dell アップデートパッケージの TFTP URI を把握している必要があります。

SM-CLP を使用してファームウェアをアップデートするには、次の手順を実行してください。

1. Telnet または SSH を使用して iDRAC にログインします。
2. 次のコマンドを入力して、現在のファームウェアバージョンを確認します。

```
version
```

3. 次のコマンドを入力します。

```
load -source tftp://<TFTP サーバー>/<アップデートパス> /system1/sp1
```

<TFTP サーバー> は TFTP サーバーの DNS 名または IP アドレス、<アップデートパス> は TFTP サーバー上のアップデートパッケージのパスです。

開いている Telnet または SSH セッションは終了します。ファームウェアアップデートが完了するまで数分かかる場合があります。

4. 新しいファームウェアが書き込まれたことを確認するには、新しい Telnet または SSH セッションを起動し、version コマンドをもう一度入力します。

Telnet または SSH によるシリアルオーバー LAN(SOL)の使用

管理ステーションの Telnet または SSH コンソールを使用して iDRAC に接続し、管理下サーバーのシリアルポートをコンソールにリダイレクトします。この機能は、シリアルストリームとネットワークパケット間の変換に `solproxy` などのユーティリティを必要とする IPMI SOL の代わりになります。iDRAC SOL の実装によって、シリアルとネットワーク間の変換は iDRAC 内で行われるため、追加のユーティリティは不要になります。

使用する Telnet または SSH コンソールは、管理下サーバーのシリアルポートから届くデータを解釈して応答できる必要があります。通常、シリアルポートは ANSI- または VT100- ターミナルをエミュレートするシェルに接続しています。

Telnet を使用すると、IPMI LAN SOL ポート 2100 に接続します。シリアルコンソールは自動的に Telnet コンソールにリダイレクトされます。

SSH または Telnet を使用すると、SM-CLP に接続する場合と同様に iDRAC に接続できます。その後、SOL リダイレクトは `/system1/sol1` ターゲットから開始できます。

iDRAC での Telnet および SSH クライアントの使用については、「[Telnet または SSH クライアントのインストール](#)」を参照してください。

Microsoft Windows のハイパーターミナルでの SOL オーバー Telnet の使用

1. **スタート**→**プログラム**→**アクセサリ**→**通信**→**ハイパーターミナル** の順に選択します。
2. 接続用の名前を入力し、アイコンを選択して OK をクリックします。
3. **接続方法** フィールドのリストから TCP/IP(Winsock) を選択します。
4. **ホストアドレス** フィールドに iDRAC の DNS 名または IP アドレスを入力します。
5. **ポート番号** フィールドに Telnet ポート番号 を入力します。
6. **OK** をクリックします。


SOL セッションを終了するには、ハイパーターミナルの切断アイコンをクリックします。

Linux での SOL オーバー Telnet の使用

Linux 管理ステーションで Telnet から SOL を起動するには、次の手順を実行してください。

1. シェルを起動します。
2. 次のコマンドで iDRAC に接続します。

```
telnet <iDRAC IP アドレス>
```

 **メモ:** Telnet サービスのポート番号をデフォルトのポート 23 から変更した場合は、telnet コマンドの末尾にポート番号を追加します。

3. 次のコマンドを入力して SOL を起動します。

```
start /system1/sol1
```

これで、管理下サーバーのシリアルポートに接続します。

SOL を終了する準備ができたなら、<Ctrl>+<+] と入力します (コントロールを押しながら右の角括弧を入力して放します)。Telnet のプロンプトが表示されます。quit と入力して Telnet を終了します。

SOL オーバー SSH の使用

/system1/sol1 ターゲットによって、管理下サーバーのシリアルポートを SSH コンソールにリダイレクトできます。

1. OpenSSH または PuTTY を使用して iDRAC に接続します。
2. 次のコマンドを入力して SOL を起動します。

```
start /system1/sol1
```

これで、管理下サーバーのシリアルポートに接続します。SM-CLP コマンドは使用できなくなりました。

SOL リダイレクトを終了する場合は、<Enter>、<Esc>、<T> の順に各キーを続けて押します。SSH セッションが終了します。

いったん SOL を開始すると、SM-CLP に戻ることはできません。SSH セッションを終了し、新しいセッションを起動して SM-CLP を使用する必要があります。

[目次ページに戻る](#)

[目次ページに戻る](#)

iVM-CLI を使用したオペレーティングシステムの導入

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [作業を開始する前に](#)
- [起動イメージファイルの作成](#)
- [導入の準備](#)
- [オペレーティングシステムの導入](#)
- [仮想メディアコマンドラインインタフェースユーティリティの使用](#)

仮想メディアコマンドラインインタフェース (iVM-CLI) ユーティリティは、管理ステーションからリモートシステムの iDRAC に仮想メディアの機能を提供するコマンドラインインタフェースです。iVM-CLI とスクリプト方式を使用すると、ネットワーク内の複数のリモートシステムにオペレーティングシステムを導入できます。

本項では、企業のネットワークに iVM-CLI ユーティリティを統合する方法について説明します。

作業を開始する前に

iVM-CLI ユーティリティを使用する前に、リモートのターゲットシステムと企業のネットワークが以下の項で述べる要件を満たしていることを確認してください。

リモートシステム要件

- 1 各リモートシステムで iDRAC が設定されている。

ネットワーク要件

ネットワーク共有に以下のコンポーネントが含まれている。

- 1 オペレーティングシステムファイル
- 1 必要なドライバ
- 1 オペレーティングシステムの起動イメージファイル

イメージファイルは、業界標準のブータブルフォーマットのオペレーティングシステム CD か CD/DVD ISO イメージである必要があります。

起動イメージファイルの作成

イメージファイルをリモートシステムに導入する前に、サポートされているシステムがそのファイルから起動できることを確認してください。イメージファイルをテストするには、iDRAC ウェブユーザーインターフェースを使用してイメージファイルをテストシステムに転送してから、システムを再起動します。

以下の項では、Linux と Windows システム用のイメージファイルの作成方法について説明します。

Linux システム用のイメージファイルの作成

Linux システム用にブータブルイメージファイルを作成するには、データ複製ユーティリティ (dd) を使用します。

ユーティリティを実行するには、コマンドプロンプトを開いて次のように入力します。

```
dd if=<入力デバイス> of=<出力ファイル>
```

次に、例を示します。

```
dd if=/dev/sdc0 of=mycd.img
```

Windows システム用のイメージファイルの作成

Windows イメージファイル用のデータ複製ユーティリティを選択する際、イメージファイルと CD/DVD ブートセクターをコピーするユーティリティを選択してください。

導入の準備

リモートシステムの設定

1. 管理ステーションからアクセスできるネットワーク共有フォルダを作成します。
2. オペレーティングシステムファイルをネットワーク共有フォルダにコピーします。
3. オペレーティングシステムをリモートシステムに導入するためのブータブルな設定済み展開イメージファイルがある場合は、このステップをスキップしてください。

設定済みのブータブルな展開イメージファイルがない場合は、このファイルを作成します。オペレーティングシステムの導入手順に使用されるプログラムやスクリプトをすべて含めます。

たとえば、Microsoft® Windows® オペレーティングシステムを導入する場合は、Microsoft Systems Management Server (SMS) で使用される導入方法に類似するプログラムをイメージファイルに含めることができます。

イメージファイルを作成するときは、以下の操作を行ってください。

- 1 標準的なネットワークベースのインストール手順に従う
 - 1 対象システムのそれぞれが同じ導入プロセスを起動して実行するように、展開イメージを「読み取り専用」とマークする
- 1 次のいずれかの手順を実行してください。
 - 1 `ipmitool` と仮想メディアコマンドラインインタフェース (IVM-CLI) を既存のオペレーティングシステム導入アプリケーションに統合します。ユーティリティを使用する際の手引きとして `ivmdeploy` サンプルスクリプトを使用します。
 - 1 オペレーティングシステムの導入には、既存の `ivmdeploy` スクリプトを使用します。

オペレーティングシステムの導入

リモートシステムにオペレーティングシステムを導入するには、IVM-CLI と `ivmdeploy` スクリプトを使用します。

始める前に、IVM-CLI ユーティリティに含まれている `ivmdeploy` サンプルスクリプトを確認してください。このスクリプトは、ネットワーク内のリモートシステムにオペレーティングシステムを導入するために必要な詳しい手順を説明しています。

以下の手順は、ターゲットのリモートシステムにオペレーティングシステムを導入するための概要です。

1. `ip.txt` テキストファイルに、導入するリモートシステムの iDRAC IP アドレス (1 行に 1 つの IP アドレス) を入力します。
2. ブータブルオペレーティングシステム CD または DVD をクライアントメディアドライブに挿入します。
3. コマンドラインで `ivmdeploy` を実行します。

`ivmdeploy` スクリプトを実行するには、コマンドプロンプトで次のコマンドを入力します。

```
ivmdeploy -r ip.txt -u <iDRAC ユーザー> -p <iDRAC パスワード> -c {<iso9660-img> | <パス>}
```

このコマンドで、

- 1 <iDRAC ユーザー> は iDRAC ユーザー名です (例: `root`)。
- 1 <iDRAC パスワード> は iDRAC ユーザーのパスワードです (例: `calvin`)。
- 1 <iso9660-img> は、オペレーティングシステムインストール CD または DVD の ISO9660 イメージのパスです。
- 1 <パス> は、オペレーティングシステムインストール CD または DVD に含まれるデバイスのパスです。


`ivmdeploy` スクリプトは、コマンドラインオプションを IVMCLI ユーティリティに渡します。これらのオプションの詳細については、「[コマンドラインオプション](#)」を参照してください。このスクリプトの `-r` オプションの処理方法は、IVMCLI `-r` オプションとは若干異なります。`-r` オプションの引数が既存のファイル名である場合、スクリプトは指定したファイルから iDRAC IP アドレスを読み取り、各行に IVMCLI ユーティリティを一度実行します。`-r` オプションの引数が既存のファイル名でない場合は、単独の iDRAC のアドレスになります。この場合、`-r` は IVMCLI ユーティリティの説明と同様に機能します。

`ivmdeploy` スクリプトは、CD/DVD または CD/DVD ISO9660 イメージからのインストールのみをサポートしています。フロッピーディスクまたはフロッピーディスクイメージからのインストールが必要な場合は、スクリプトを変更して IVMCLI `-f` オプションを使用してください。

仮想メディアコマンドラインインタフェースユーティリティの使用

仮想メディアコマンドラインインタフェース (IVM-CLI) ユーティリティは、管理ステーションから iDRAC に仮想メディアの機能を提供するスクリプト可能なコマンドラインインタフェースです。

IVM-CLI ユーティリティは次の機能を提供します。

 **メモ:** 読み取り専用のイメージファイルを仮想化するとき、複数セッションで同一イメージメディアを共有できる。物理ドライブを仮想化するとき、1 度に 1 つのセッションが指定の物理ドライブにアクセスできる。

- 1 仮想メディアプラグインに対応したリムーバブルデバイスまたはイメージファイル

- 1 iDRAC ファームウェアのブートワンス機能が有効の場合の自動終了
- 1 セキュアソケットレイヤ(SSL)を使用した iDRAC 通信のセキュリティ保護

ユーティリティを実行する前に、iDRAC に対し仮想メディアのユーザー権限があることを確認してください。

オペレーティングシステムが Administrator 権限、オペレーティングシステムに固有の権限またはグループメンバーシップをサポートしている場合は、iVM-CLI コマンドを実行するためにも Administrator 権限が必要です。

クライアントシステムの管理者 (Administrator) は、ユーザーグループと権限を制御するので、このユーティリティを実行できるユーザーも制御することになります。

Windows システムの場合は、iVM-CLI ユーティリティのパワーユーザー権限が必要です。

Linux システムでは、Administrator 権限がなくても、`sudo` コマンドを使って iVM-CLI ユーティリティにアクセスできます。このコマンドは、Administrator (システム管理者) 以外のアクセス権を一元的に与える手段となり、すべてのユーザーコマンドをログに記録します。iVM-CLI グループにユーザーを追加または編集する場合、Administrator (システム管理者) は `visudo` コマンドを使用します。Administrator 権限がないユーザーは、`sudo` コマンドを iVM-CLI コマンドライン (または iVM-CLI スクリプト) の接頭辞として追加すると、リモートシステムの iDRAC にアクセスしてユーティリティを実行できます。

iVM-CLI ユーティリティのインストール

iVM-CLI ユーティリティは『Dell OpenManage™ Systems Management Consoles CD』にあります。この CD は Dell OpenManage System Management Software キットに同梱されています。ユーティリティをインストールするには、『Systems Management Consoles CD』をシステムの CD ドライブに挿入し、画面の説明に従ってください。

『Systems Management Consoles CD』には、診断、ストレージ管理、リモートアクセスサービス、RACADM ユーティリティなどの最新のシステム管理ソフトウェア製品が含まれています。システム管理ソフトウェアの最新の製品情報が含まれた Readme ファイルも付いています。

さらに、『Systems Management Consoles CD』には、`ivmdeploy` (iVM-CLI および RACADM ユーティリティを使用して、複数のリモートシステムにソフトウェアを導入する方法を説明するサンプルスクリプト) が含まれています。



メモ: `ivmdeploy` スクリプトは、インストール時にディレクトリに存在する他のファイルに依存しています。別のディレクトリからスクリプトを使用する場合は、一緒にすべてのファイルをコピーする必要があります。

コマンドラインオプション

iVM-CLI インタフェースは、Windows と Linux システムで共通しています。このユーティリティのオプションは RACADM ユーティリティのオプションと整合性があります。たとえば、iDRAC IP アドレスを指定するオプションでは、RACADM でも iVM-CLI ユーティリティでも同じ構文が必要です。

iVM-CLI コマンドのフォーマットは以下のとおりです。

```
iVMCLI [パラメータ] [オペレーティングシステムシェルオプション]
```

コマンドライン構文では、大文字と小文字が区別されます。詳細については、「[iVM-CLI パラメータ](#)」を参照してください。

リモートシステムのコマンドが受け入れられ、iDRAC が接続を許可した場合は、次のどちらかが発生するまでコマンドの実行が続行します。

- 1 何らかの理由で iVM-CLI 接続が終了した場合。
- 1 オペレーティングシステムのコントロールを使用して処理が手動で中止された場合。たとえば、Windows でタスク マネージャを使うと処理を終了できます。

iVM-CLI パラメータ

iDRAC の IP アドレス

```
-r <iDRAC IP アドレス>[:<iDRAC SSL ポート>]
```

このパラメータは、iDRAC の IP アドレスと SSL ポートを提供します。これらは、ユーティリティがターゲット iDRAC と仮想メディア接続を確立するために必要です。無効な IP アドレスまたは DDNS 名を入力すると、エラーメッセージが表示されてコマンドは終了します。

<iDRAC IP アドレス> は有効な固有の IP アドレスまたは iDRAC 動的ドメインネームシステム (DDNS) 名です (サポートしている場合)。<iDRAC SSL ポート> を省くと、ポート 443 (デフォルトポート) が使用されます。iDRAC のデフォルト SSL ポートを変更していない限り、オプションの SSL ポートは不要です。

iDRAC ユーザー名

```
-u <iDRAC ユーザー名>
```

このパラメータは仮想メディアを実行する iDRAC ユーザー名を提供します。

<iDRAC ユーザー名> には、次の属性が必要です。

- 1 有効なユーザー名
- 1 iDRAC 仮想メディアユーザー権限

iDRAC の認証に失敗した場合は、エラーメッセージが表示されてコマンドが終了します。

iDRAC ユーザーパスワード

```
-p <iDRAC ユーザーパスワード>
```

このパラメータは、指定した iDRAC ユーザーのパスワードを提供します。

iDRAC の認証に失敗した場合は、エラーメッセージが表示されてコマンドが終了します。

フロッピー / ディスクデバイスまたはイメージファイル

```
-f {<device-name> | <イメージファイル>}
```

ここで、<デバイス名> は有効なドライブ文字 (Windows システム) またはマウント可能ファイルシステムパーティション番号などを含む有効なデバイスファイル名 (Linux システム) です。<イメージファイル> は有効なイメージファイルのファイル名とパスです。

このパラメータは、仮想フロッピー / ディスクメディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

```
-f c:\temp\myfloppy.img (Windows システム)
```

```
-f /tmp/myfloppy.img (Linux システム)
```

イメージファイルが書き込み保護されていない場合、仮想メディアはそのファイルに書き込むことができます。上書きしてはならないフロッピーイメージファイルへの書き込みを保護するようにオペレーティングシステムで設定します。

たとえば、デバイスは次のように指定します。

```
-f a:¥ (Windows システム)
```

```
-f /dev/sdb4 # デバイス上の 4 番目のパーティション /dev/sdb (Linux システム)
```

デバイスに書き込み保護機能がある場合は、その機能を使用して仮想メディアがメディアに書き込めないようにしてください。

フロッピーメディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出されたら、エラーメッセージが表示されてコマンドが終了します。

CD/DVD デバイスまたはイメージファイル

```
-c {<デバイス名> | <イメージファイル>}
```

<デバイス名> は有効な CD/DVD ドライブ文字 (Windows システム) または有効な CD/DVD デバイスファイル名 (Linux システム) で、<イメージファイル> は有効な ISO-9660 イメージファイルのファイル名とパスです。

このパラメータは、仮想 CD/DVD-ROM メディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

```
-c c:\temp\mydvd.img (Windows システム)
```

```
-c /tmp/mydvd.img (Linux システム)
```

たとえば、デバイスは次のように指定します。

```
-c d:¥ (Windows システム)
```

```
-c /dev/cdrom (Linux システム)
```

CD/DVD メディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出されたら、エラーメッセージが表示されてコマンドが終了します。

スイッチオプションしかない場合を除き、このコマンドを使って少なくとも 1 つのメディアタイプ (フロッピーまたは CD/DVD ドライブ) を指定します。指定しないと、エラーメッセージが表示されてコマンドが終了します。

バージョン表示

```
-v
```

このパラメータは iVM-CLI ユーティリティのバージョンを表示するために使用します。その他の非スイッチオプションが提供されていない場合、コマンドはエラーメッセージなしで終了します。

ヘルプの表示

```
-h
```

このパラメータは iVM-CLI ユーティリティのパラメータの概要を表示します。その他の非スイッチオプションが提供されていない場合、コマンドはエラーなしで終了します。

手動表示

-m

このパラメータは、可能なオプションすべてに関する説明が記載された iVMM-CLI ユーティリティの詳細ページを表示します。

暗号化データ

-e

このパラメータがコマンドラインに含まれていると、iVMM-CLI は SSL-暗号化チャネルを使用して、管理ステーションとリモートシステムの iDRAC 間でデータを転送します。このパラメータがコマンドラインに含まれていない場合は、データ転送が暗号化されません。

iVMM-CLI オペレーティングシステムのシェルオプション

iVMM-CLI のコマンドラインでは、次のオペレーティングシステムの機能を使用できます。

- 1 stderr/stdout redirection - 印刷されたユーティリティの出力をファイルにリダイレクトします。

たとえば、大なり記号(>)の後にファイル名を入力すると、iVMM-CLI ユーティリティの印刷出力で指定したファイルが上書きされます。



メモ: iVMM-CLI ユーティリティは標準入力 (stdin) からは読み取りません。このため、stdin リダイレクションは不要です。

- 1 バックグラウンド実行 - iVMM-CLI ユーティリティはデフォルトではフォアグラウンドで実行します。オペレーティングシステムのコマンドシェル機能を使用すると、ユーティリティをバックグラウンドで実行できます。たとえば、Linux オペレーティングシステムでは、コマンドに続いてアンバーサンド(&)を指定すると、プログラムから新しいバックグラウンドプロセスが生成されます。

後者の方法はスクリプトプログラムの場合に便利です。iVMM-CLI コマンドの新しいプロセスが開始した後、スクリプトを継続できます(そうでない場合は、iVMM-CLI プログラムが終了するまでスクリプトがブロックされます)。iVMM-CLI の複数のインスタンスがこの方法で開始し、コマンドインスタンスの 1 つ以上を手動で終了しなければならない場合は、オペレーティングシステムに固有の機能を使用して、プロセスをリストにして終了します。

iVMM-CLI の戻りコード

0 = エラーなし

1 = 接続できない

2 = iVMM-CLI コマンドラインエラー

3 = RAC ファームウェア接続の切断

エラーが発生した場合は、標準エラー出力に英語のみのテキストメッセージも表示されます。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC 設定ユーティリティの使用

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [概要](#)
- [iDRAC 設定ユーティリティの起動](#)
- [iDRAC 設定ユーティリティの使用](#)

概要

iDRAC 設定ユーティリティは、iDRAC および管理下サーバーのパラメータを表示および設定できる起動前の設定環境です。具体的には、以下のことが可能です。


- 1 iDRAC および Primary(一次)バックプレーンのファームウェアリビジョン番号を表示する
- 1 iDRAC ローカルエリアネットワークを設定する、有効または無効にする
- 1 IPMI オーバー LAN を有効または無効にする
- 1 LAN プラットフォームイベントトラップ(PET)送信先を有効にする
- 1 仮想メディアデバイスを接続または切断する
- 1 システム管理者のユーザー名およびパスワードを変更する
- 1 iDRAC 設定を出荷時のデフォルトに戻す
- 1 システムイベントログ(SEL)メッセージを表示する、またはログからメッセージをクリアする

iDRAC 設定ユーティリティを使用して実行できるタスクは、iDRAC または OpenManage ソフトウェアで提供される他のユーティリティ(ウェブインタフェース、SM-CLP コマンドラインインタフェース、ローカル RACADM コマンドラインインタフェース)を使用しても実行できるほか、基本的なネットワーク設定は最初の CMC 設定時に CMC LCD でも実行できます。

iDRAC 設定ユーティリティの起動

最初、または iDRAC をデフォルト設定にリセット後に iDRAC 設定ユーティリティにアクセスするには、iKVM に接続したコンソールを使用する必要があります。

- 1 iKVM コンソールに接続したキーボードで、Print Screen キーを押して iKVM の On Screen Configuration and Reporting(OSCAR)メニューを表示します。上向き矢印 キーと下向き矢印キーを使用してサーバーが実装されているスロットをハイライトし、Enter キーを押します。
- 2 サーバーの前面にある電源ボタンを押してサーバーの電源を入れるか、再起動します。
- 3 <Ctrl-E> を押して **5 秒以内にリモートアクセスのセットアップを**というメッセージが表示されたら、すぐに <Ctrl><E> を押します。

 **メモ:** Ctrl-E キーを押す前にオペレーティングシステムがロードを開始した場合は、起動が完了するのを待ってからシステムを再起動して、もう一度やり直してください。

iDRAC 設定ユーティリティが表示されます。最初の 2 行に、iDRAC ファームウェアと Primary(一時)バックプレーンファームウェアのリビジョンに関する情報が表示されます。リビジョンレベルは、ファームウェアアップグレードが必要かどうかを決定するのに役立ちます。

iDRAC ファームウェアは、ウェブインタフェース、SM-CLP など、外部インタフェースに関連するファームウェアの一部です。一次バックプレーンファームウェアは、サーバーのハードウェア環境とインタフェースし、それを監視するファームウェアの一部です。

iDRAC 設定ユーティリティの使用

ファームウェアのリビジョンメッセージの下の iDRAC 設定ユーティリティの残りの部分は、上向き矢印キーと下向き矢印キーを使用してアクセスできるメニューアイテムです。

- 1 メニュー項目からサブメニューまたは編集可能なテキストフィールドが表示されたら、Enter キーを押してその項目にアクセスし、設定が終了したら Esc キーを押します。
- 1 項目には / いいえ、有効 / 無効 など選択可能な値がある場合は、左向き矢印 キーまたは右向き矢印キー、スペース キーを押して値を選択します。
- 1 編集不可能な項目は青色で表示されます。項目によっては、他の選択内容によって編集可能になるものがあります。
- 1 画面の下部に現在の項目の操作手順が表示されます。F1 キーを押すと現在の項目のヘルプを表示できます。
- 1 iDRAC 設定ユーティリティの使用を終えたら、Esc キーを押して 終了 メニューを表示します。このメニューでは、変更の保存または無視を選択できるほか、ユーティリティに戻ることもできます。

次の項では、iDRAC 設定ユーティリティのメニュー項目について説明します。

LAN

左向き矢印、右向き矢印、スペースキーを使用して **有効** または **無効** を選択します。

iDRAC LAN は、デフォルト設定では無効になっています。ウェブインタフェース、SM-CLP コマンドラインインタフェースへの Telnet/SSH アクセス、コンソールリダイレクト、仮想メディアなど iDRAC アイテムの使用を許可する場合、LAN が有効になっている必要があります。

LAN を無効にすると、次の警告が表示されます。

LAN チャンネルがオフの場合、iDRAC 帯域外（アウトバンド）インタフェースは無効になります。

任意のキーを押してメッセージをクリアし、続行します。

このメッセージでは、LAN が無効になっていると、iDRAC HTTP、HTTPS、Telnet、SSH ポートに直接接続されている装置にアクセスできないだけでなく、管理ステーションから iDRAC に送信される IPMI メッセージなどの帯域外管理ネットワークトラフィックも受信できないことが通知されます。ただし、ローカル RACADM インタフェースは使用可能で、iDRAC LAN の再設定に使用できます。

IPMI オーバー LAN(オン / オフ)

左向き矢印、右向き矢印、スペースキーを押して **オン** または **オフ** を選択します。**オフ** を選択すると、iDRAC は LAN インタフェース経由での IPMI メッセージを受け入れません。

オフ を選択すると、次の警告が表示されます。

LAN チャンネルがオフの場合、iDRAC 帯域外インタフェースは無効になります。

任意のキーを押してメッセージをクリアし、続行します。メッセージの説明に関しては、「[LAN](#)」を参照してください。

LAN パラメータ

LAN パラメータのサブメニューを表示するには、Enter キーを押します。LAN パラメータの設定を終えた後、Esc キーを押すと前のメニューに戻ります。


表 13-1 LAN パラメータ

項目	説明
RMCP+ 暗号化キー	Enter キーを押して値を編集し、終了したら Esc キーを押します。RMCP+ 暗号化キーは、40 文字の 16 進法の文字列(文字 0 ~ 9、a ~ f、A ~ F)です。RMCP+ は認証および暗号化を IPMI に追加する IPMI のエクステンションです。デフォルト値は 0 を 40 個連ねたものです。
IP アドレスソース	DHCP または 静的 を選択します。DHCP を選択すると、DHCP サーバーから Ethernet IP アドレス、サブネットマスク、デフォルトゲートウェイ フィールドが取得されます。ネットワーク上に DHCP が見つからない場合、フィールドはゼロに設定されます。 静的 を選択すると、 Ethernet IP アドレス、サブネットマスク、デフォルトゲートウェイ アイテムは編集可能になります。
Ethernet IP アドレス	IP アドレスソースを DHCP に設定すると、このフィールドには DHCP から取得された IP アドレスが表示されます。 IP アドレスソースを 静的 に設定する場合、iDRAC に割り当てる IP アドレスを入力します。 デフォルトは、192.168.0.120 に、サーバーのスロット番号を加えた値です。
MAC Address	これは、iDRAC ネットワークインタフェースの編集不可能な MAC アドレスです。
サブネットマスク	IP アドレスソースを DHCP に設定すると、このフィールドには DHCP から取得したサブネットマスクアドレスが表示されます。 IP アドレスソースを 静的 に設定している場合は、iDRAC のサブネットマスクを入力します。 デフォルトは 255.255.255.0 です。
デフォルトゲートウェイ	IP アドレスソースを DHCP に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイのアドレスが表示されます。 IP アドレスソースを 静的 に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。 デフォルトは 192.168.0.1 です。
LAN 警告有効	オン を選択するとプラットフォームイベントトラップ(PET)LAN 警告が有効になります。
警告ポリシーエントリ 1	有効 または 無効 を選択すると、最初の送信先がアクティブになります。
警告送信先 1	PET LAN 警告送信先の IP アドレスを入力します。
ホスト名文字列	Enter キーを押して編集します。PET 警告のホスト名を入力します。
DHCP からの DNS サーバー	オン を選択するとネットワーク上の DHCP サービスから DNS サーバーアドレスが取得されます。 オフ を選択すると以下の DNS サーバーアドレスを指定できます。
DNS サーバー 1	DHCP からの DNS サーバーが オフ の場合、最初の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	DHCP からの DNS サーバーが オフ の場合、2 番目の DNS サーバーの IP アドレスを入力します。
iDRAC 名の登録	オン を選択すると DNS サービスに iDRAC 名を登録できます。ユーザーが DNS 内で iDRAC 名を見えないようにするには、 オフ を選択します。
iDRAC 名	iDRAC 名の登録を オン に設定すると、Enter キーを押して 現在の DNS iDRAC 名 テキストフィールドを編集できます。iDRAC 名の編集を終えたら Enter キーを押します。前のメニューに戻るには Esc キーを押します。iDRAC 名は有効な DNS ホスト名でなければなりません。
DHCP からのドメイン名	ネットワーク上の DHCP サービスからドメイン名を取得するには、 オン を選択します。ドメイン名を指定するには、 オフ を選択します。
ドメイン名	DHCP からのドメイン名が オフ の場合、Enter キーを押すと 現在のドメイン名 テキストフィールドを編集できます。編集を終えたら Enter キーを押します。前のメニューに戻るには Esc キーを押します。ドメイン名は、有効な DNS ドメイン(例:mycompany.com)でなければなりません。

仮想メディア

左向き矢印と右向き矢印 キーを使用して **接続** または **切断** を選択します。**接続** を選択すると、仮想メディアデバイスが USB バスに接続され、**コンソールリダイレクト** セッション中に使用可能になります。

切断 を選択すると、ユーザーは **コンソールリダイレクト** セッション中に仮想メディアデバイスにアクセスできません。

 **メモ:** **仮想メディア** 機能で USB フラッシュドライブを使用するには、BIOS 設定ユーティリティで **USB フラッシュドライブのエミュレーションタイプ** を **ハードディスク** に設定してください。BIOS 設定ユーティリティへは、サーバー起動中に F2 キーを押すとアクセスできます。**USB フラッシュドライブのエミュレーションタイプ** が **自動** に設定されていると、フラッシュドライブはシステムでフロッピードライブとして表示されます。

LAN ユーザー設定


LAN ユーザーは iDRAC の Administrator (システム管理者) アカウント (デフォルトで **root**【ルート】) です。LAN ユーザー設定のサブメニューを表示するには、Enter キーを押します。LAN ユーザーの設定を終えて、Esc キーを押すと前のメニューに戻ります。

表 13-2 LAN ユーザー設定ページ

項目	説明
アカウントアクセス	有効 を選択すると Administrator (システム管理者) アカウントが有効になります。 無効 を選択すると Administrator (システム管理者) アカウントが無効になります。
アカウント権限	システム管理者 (Admin) 、 ユーザー 、 オペレータ 、 アクセスなし のいずれかを選択します。
アカウントユーザー名	Enter キーを押してユーザー名を編集し、終了したら Esc キーを押します。デフォルトのユーザー名は root (ルート) です。
パスワードを入力する	Administrator (システム管理者) アカウントの新しいパスワードを入力します。入力時に、文字は表示されません。
パスワードを確認する	Administrator (システム管理者) アカウントの新しいパスワードを再入力します。入力した文字が パスワードを入力する フィールドに入力した文字と一致しない場合はメッセージが表示され、パスワードを再度入力する必要があります。

デフォルトに戻す

デフォルトに戻す メニュー項目を使用すると、iDRAC 設定項目がすべて出荷時のデフォルトに戻されます。これは、システム管理者のユーザーパスワードを忘れた場合や iDRAC をデフォルト設定から再設定する場合に必要な可能性があります。

 **メモ:** デフォルト設定で iDRAC ネットワークは無効になっています。iDRAC 設定ユーティリティで iDRAC ネットワークを有効にするまでネットワーク上で iDRAC を再設定することはできません。

Enter キーを押して項目を選択します。次の警告メッセージが表示されます。

Resetting to factory defaults will restore remote Non-Volatile user settings. Continue? (出荷時のデフォルト設定に戻すとリモートの非揮発性ユーザー設定が復元されます。続行しますか ?)

< NO (Cancel) > (<いいえ (キャンセル) ...>)

< YES (Continue) > (<はい (続行) >)

はい を選択し、Enter キーを押すと iDRAC はデフォルト設定に戻ります。

システムイベントログメニュー

システムイベントログ メニューでは、システムイベントログ (SEL) メッセージを表示したり、ログメッセージをクリアできます。Enter キーを押すと **システムイベントログメニュー** が表示されます。システムはログエントリをカウントし、レコード総数と最新のメッセージを表示します。SEL は、最大 512 のメッセージを保持します。

SEL メッセージを表示するには、**システムイベントログの表示** を選択して Enter キーを押します。左向き矢印 キーを使用すると前の (古い) メッセージに移動し、右向き矢印 キーを押すと次の (新しい) メッセージに移動します。レコード番号を入力するとそのレコードに移動します。SEL メッセージの表示を終了するには Esc キーを押します。

 **メモ:** iDRAC 設定ユーティリティまたは iDRAC ウェブインタフェース内の SEL のみクリアできます。

SEL メッセージをクリアするには、**システムイベントログのクリア** を選択して Enter キーを押します。

SEL メニューの使用を終えて、Esc キーを押すと前のメニューに戻ります。

iDRAC 設定ユーティリティの終了

iDRAC 設定の変更が終了し、Esc キーを押すと Exit (終了) メニューが表示されます。

変更を保存して終了 を選択して Enter キーを押すと変更が保存されます。

変更を保存せずに終了 を選択して Enter キーを押すと変更は保存されません。

セットアップに戻る を選択して Enter キーを押すと iDRAC 設定ユーティリティに戻ります。

[目次ページに戻る](#)

[目次ページに戻る](#)

管理下サーバーのリカバリとトラブルシューティング

Integrated Dell™ リモートアクセス Controller Firmware バージョン 1.2
ユーザーガイド

- [安全第一 - ユーザーとシステム](#)
- [問題の兆候](#)
- [問題解決ツール](#)
- [トラブルシューティングとよくあるお問い合わせ \(FAQ\)](#)

ここでは、iDRAC 機能を使用したリモート管理下サーバーの診断とトラブルシューティングに関連するタスクの実行方法について説明します。本項では以下について説明します。

1. [トラブル指標](#) - 問題の診断に導くメッセージやその他のシステム指標を見つけるのに役立ちます。
1. [不具合解決ツール](#) - システムのトラブルシューティングに使用できる iDRAC ツールについて説明します。
1. [トラブルシューティングとよくあるお問い合わせ \(FAQ\)](#) - 遭遇する可能性のある一般的な状況に対する回答を提供します。

安全第一 - ユーザーとシステム

本項の一部の手順を実行するには、シャーシ、PowerEdge サーバー、または他のハードウェアモジュールに作業を行う必要があります。このガイドおよびシステムマニュアルで説明されている以外のシステムハードウェアの修理は試みないでください。

警告: 修理作業の多くは、認定されたサービス技術者のみが行うことができます。製品マニュアルで許可されている、もしくはオンライン / 電話によるサービスおよびサポートチームによって指示されるトラブルシューティングと簡単な修理のみを行ってください。Dell で認められていない修理 (内部作業) による損傷は、保証の対象となりません。製品に付属のマニュアルに書かれている安全にお使いいただくための注意をお読みになり、指示に従ってください。

問題の兆候

ここでは、システムに問題がある可能性を示す兆候について説明します。

LED インジケータ

システム上の問題の初期兆候は、シャーシまたはシャーシに実装されているコンポーネントの LED に示される可能性があります。次のコンポーネントおよびモジュールにはステータス LED がありません。

1. シャーシ LCD モニター
1. サーバー
1. ファン
1. CMC
1. I/O モジュール
1. 電源装置

シャーシ LCD の単独 LED は、システムコンポーネント全体のステータスを示します。LCD で青色の LED が点灯している場合、システム内で検知されているエラー状態がないことを示します。LCD で黄色の LED が点滅している場合は、1 つまたは複数のエラー状態が検知されたことを示します。

シャーシ LCD で黄色の LED が点滅している場合、LCD メニューを使用してエラーのあるコンポーネントを特定できます。LCD の使い方については、『Dell CMC ファームウェアユーザーガイド』を参照してください。

[表 14-1](#) に、PowerEdge サーバー上の LED とその意味を示します。

表 14-1 サーバーの LED インジケータ

LED インジケータ	意味
緑色に点灯	サーバーの電源が入っている状態です。緑色の LED が点灯していない場合、サーバーの電源が入っていないことを示します。
青色に点灯	iDRAC は正常に動作しています。
黄色に点滅	iDRAC がエラー状態を検知したか、ファームウェアのアップデートを進行中である可能性があります。
青色に点滅	ユーザーがこのサーバーのロケータ ID をアクティブにした状態です。

ハードウェア問題の兆候

モジュールにハードウェアの不具合がある場合の兆候には、以下が含まれます。

- 1 電源が入らない
- 1 ファンのノイズ
- 1 ネットワーク接続の喪失
- 1 バッテリー、温度、電圧、電源モニターのセンサー警告
- 1 ハードドライブエラー
- 1 USB メディアエラー
- 1 落下、浸水、その他の外部要因による物理的損傷

上記のような不具合が発生した場合、次の方法で問題の解決を試みてください。

- 1 モジュールを抜き差しして、再起動する
- 1 モジュールをシャーシ内の別のベイに挿入する
- 1 ハードドライブまたは USB キーを交換する
- 1 電源およびネットワークケーブルを再接続 / 交換する

これらの手順で問題が解決されない場合、『ハードウェアオーナーズマニュアル』でハードウェアデバイスのトラブルシューティング情報を参照してください。

その他の問題の兆候

表 14-2 問題の兆候

注目すべき点:	処置:
システム管理ソフトウェアからの警告メッセージ	システム管理ソフトウェアのマニュアルを参照してください。
システムイベントログのメッセージ	「システムイベントログ (SEL) の確認」 を参照してください。
起動時 POST コードのメッセージ	「POST コードの確認」 を参照してください。
前回クラッシュ画面のメッセージ	「前回のシステムクラッシュ画面の表示」 を参照してください。
LCD のサーバーステータス画面の警告メッセージ	「サーバーステータス画面でのエラーメッセージの確認」 を参照してください。
iDRAC ログのメッセージ	「iDRAC ログの表示」 を参照してください。

問題解決ツール


ここでは、特にリモートで問題解決を試みる場合、システムの問題を診断するのに使用できる iDRAC 機能について説明します。




- 1 システム正常性の確認
- 1 エラーメッセージに対するシステムイベントログの確認
- 1 POST コードの確認
- 1 前回クラッシュ画面の表示
- 1 LCD 上のサーバーステータス画面でエラーメッセージを確認
- 1 iDRAC ログの表示
- 1 システム情報へのアクセス
- 1 シャーシ内の管理下サーバーの識別
- 1 診断コンソールの使用
- 1 リモートシステムの電源管理

システム正常性の確認

iDRAC ウェブインタフェースにログインする際、最初に表示されるページにシステムコンポーネントの正常性状態が表示されます。[表 14-3](#) に、システム正常性インジケータの意味を示します。

表 14-3 システム正常性インジケータ

インジケータ	説明
	緑のチェックマークは、正常(平常)ステータスを示します。

	感嘆符の入った黄色の三角形は、警告(非重要)ステータスを示します。
	赤い X は、重要(エラー)ステータスを示します。
	疑問符のアイコンは、不明なステータスを示します。

正常性 ページのコンポーネントをクリックすると、そのコンポーネントに関する情報が表示されます。バッテリー、温度、電圧、電源モニターに対してはセンサーの読み取り値が表示されます。一部の不具合の診断に役立ててください。iDRAC および CMC 情報ページには、現在のステータスと設定情報が表示されます。

システムイベントログ (SEL) の確認

SEL ログ ページには、管理下サーバーで発生したイベントのメッセージが表示されます。

システムイベントログ を表示するには、次の手順を実行してください。


1. **システム** をクリックし、**ログ** タブをクリックします。
2. **システムイベントログ** をクリックして **システムイベントログ** ページを表示します。
システムイベントログ ページには、システム正常性インジケータ(「表 14-3」を参照)、タイムスタンプ、イベントの説明が表示されます。
3. **システムイベントログ** ページの適切なボタンをクリックして続行します(「表 14-4」を参照)。

表 14-4 SEL ページのボタン

ボタン	動作
印刷	ウィンドウに表示される並び順に SEL を印刷します。
ログのクリア	SEL をクリアします。 メモ: ログのクリア ボタンは、ログのクリア 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、選択したディレクトリに SEL を保存できます。 メモ: Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft® サポートウェブサイト support.microsoft.com から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。
更新	SEL ページを再ロードします。

POST コードの確認

POST コード ページには、オペレーティングシステムの起動前の最後のシステム POST コードが表示されます。POST コードはシステム BIOS から返される進行状況を示すコードで、電源オンリセットからの起動順序の異なる段階を示し、システム起動に関するあらゆるエラーを診断できます。

 **メモ:** LCD モニターまたは『ハードウェアオーナーズマニュアル』の POST コードメッセージ番号の説明文を参照してください。


POST コードを表示するには、次の手順を実行してください。

1. **システム**、**ログ** タブ、**POST コード** の順にクリックします。
POST コード ページには、システム正常性インジケータ(「表 14-3」を参照)、16 進コード、コードの説明が表示されます。
2. POST コード ページの適切なボタンをクリックして続行します(「表 14-5」を参照)。

表 14-5 POST コードのボタン

ボタン	動作
印刷	POST コード ページを印刷します。
更新	POST コード ページを再ロードします。

前回のシステムクラッシュ画面 の表示

 **注意:** Server Administrator および iDRAC ウェブインタフェースで前回クラッシュ画面機能が設定されている必要があります。この機能を設定する手順については、「[管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定](#)」を参照してください。

前回のクラッシュ画面 ページには、システムクラッシュ前に発生したイベントに関する情報を含む最新クラッシュ画面が表示されます。最後にシステムがクラッシュしたときのイメージは、iDRAC の持続ストアに保存され、リモートアクセスできます。

前回クラッシュ画面 ページを表示するには、次の手順を実行してください。

- 1 システム、ログ タブ、**前回クラッシュ** の順にクリックします。

前回クラッシュ画面 ページには、[表 14-6](#) に示すボタンが表示されます。



 **メモ:** 保存されているクラッシュ画面が存在しない場合、**保存** および **削除** ボタンは表示されません。

表 14-6 前回のクラッシュ画面ページのボタン

ボタン	動作
印刷	前回のクラッシュ画面 ページを印刷します。
保存	ポップアップウィンドウが開き、選択したディレクトリに 前回クラッシュ画面 ページを保存できます。
削除	前回のクラッシュ画面 ページを削除します。
更新	前回のクラッシュ画面 ページを再ロードします。

 **メモ:** 自動リカバリタイマーの変動により、システムリセットタイマーの値が高すぎる値で設定されている場合は、**前回クラッシュ画面** をキャプチャできない可能性があります。デフォルト設定は 480 秒です。Server Administrator と IT Assistant でシステムリセットタイマーを 60 秒に設定して、**前回クラッシュ画面** が正しく機能することを確認します。詳細については、「[管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定](#)」を参照してください。

最近の起動順序の表示

起動に問題がある場合は、起動キャプチャページで最後の 3 つの起動順序時に発生した画面アクティビティを表示できます。起動画面の再生は、1 フレーム / 秒の速度で実行されます。[表 14-7](#) には、使用できるコントロール動作がリストされています。


 **メモ:** 再生された起動キャプチャ順序を表示するには、Administrator 権限が必要です。

表 14-7 起動キャプチャオプション

ボタン / オプション	説明
起動順序の選択	ロードして再生する起動順序を選択できます。 <ol style="list-style-type: none"> 1 起動キャプチャ 1 - 一番最近の起動順序をロードします。 1 起動キャプチャ 2 - 起動キャプチャ 1 の前に起きた、2 番目に最近の起動順序をロードします。 1 起動キャプチャ 3 - 起動キャプチャ 2 の前に起きた、3 番目に最近の起動順序をロードします。
名前を付けて保存	現在のシーケンスのすべての起動キャプチャイメージを含む圧縮 .zip ファイルを作成します。この処理を実行するには、Administrator 権限が必要です。
前の画面	前の画面がある場合は、再生コンソールにそれを表示します。
再生	再生コンソールの現在の画面からスクリーンプレイを開始します。
一時停止	再生コンソールに表示されている現在の画面でスクリーンプレイを一時停止します。
停止	スクリーンプレイを停止して、起動順序の最初の画面をロードします。
次の画面	次の画面がある場合は、再生コンソールにそれを表示します。
印刷	画面に表示されている起動キャプチャイメージを印刷します。
更新	起動キャプチャページを再ロードします。

サーバースタータス画面でのエラーメッセージの確認

LED が黄色に点滅し、特定のサーバーにエラーが発生した場合、LCD 上のメインサーバースタータス画面に影響があったサーバーを橙色でハイライトします。LCD ナビゲーションボタンを使用して、影響があるサーバーをハイライト表示し、中央のボタンをクリックします。2 行目にエラーおよび警告メッセージが表示されます。下記の表には、すべてのエラーメッセージおよびその重要度が示されています。

表 14-8 サーバースタータス画面

重要度	メッセージ	原因
警告	システム基板の周辺温度: システム基板の温度センサー、警告イベント	サーバー周辺温度が警告しきい値を超えました。
重要	システム基板の周辺温度: システム基板の温度センサー、エラーイベント	サーバー周辺温度がエラーしきい値を超えました。
重要	システム基板の CMOS バッテリー: システム基板のバッテリーセンサー、エラーがアサートされました	CMOS バッテリーが存在しないか、電圧がありません。

警告	システム基板のシステムレベル: システム基板の電流センサー、警告イベント	電流 が警告しきい値を超えました。
重要	システム基板のシステムレベル: システム基板の電流センサー、エラーイベント	電流 がエラーしきい値を超えました。
重要	CPU<番号> <電圧センサー名>: CPU<番号>の電圧センサー、状態アサートがアサートされました	電圧が許容範囲を超えています。
重要	システム基板 <電圧センサー名>: システム基板の電圧センサー、状態アサートがアサートされました	電圧が許容範囲を超えています。
重要	CPU<番号> <電圧センサー名>: CPU<番号>の電圧センサー、状態アサートがアサートされました	電圧が許容範囲を超えています。
重要	CPU<番号> ステータス: CPU<番号>のプロセッサセンサー、IERR がアサートされました	CPU エラー
重要	CPU<番号> ステータス: CPU<番号>のプロセッサセンサー、熱トリップがアサートされました	CPU が過熱状態
重要	CPU<番号> ステータス: CPU<番号>のプロセッサセンサー、設定エラーがアサートされました	不正なプロセッサタイプまたは間違った位置に取り付けられています。
重要	CPU<番号> ステータス: CPU<番号>のプロセッサセンサー、存在がアサート解除されました	必要な CPU が存在しません。
重要	システム基板 Video Riser: システム基板のモジュールセンサー、デバイスの取り外しがアサートされました	必要なモジュールが取り外されました。
重要	メザニン B<スロット番号> ステータス: メザニン B<スロット番号> のアドインカードセンサー、インストールエラーがアサートされました	I/O ファブリックに間違ったメザニンカードが取り付けられています。
重要	メザニン C<スロット番号> ステータス: メザニン C<スロット番号> のアドインカードセンサー、インストールエラーがアサートされました	I/O ファブリックに間違ったメザニンカードが取り付けられています。
重要	バックプレーンドライブ <番号>: バックプレーンのドライブスロットセンサー、ドライブが取り外されました	ストレージドライブが取り外されました
重要	バックプレーンドライブ <番号>: バックプレーンのドライブスロットセンサー、ドライブ障害がアサートされました	ストレージドライブの障害
重要	システム基板 PFault フェールセーフ: システム基板の電圧センサー、状態アサートがアサートされました	システム基板の電圧が異常レベルに達した場合に、このイベントが生成されます。
重要	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、タイマー期限切れがアサートされました	IDRAC ウォッチドッグのタイマー期限切れ。特に処置は設定されていません。
重要	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、再起動がアサートされました	IDRAC ウォッチドッグは、システムのクラッシュ(ホストからの応答がないためのタイマー期限切れ)を検知し、再起動の処置が設定されています。ÅB
重要	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、電源オフがアサートされました	IDRAC ウォッチドッグは、システムのクラッシュ(ホストからの応答がないためのタイマー期限切れ)を検知し、電源オフの処置が設定されています。ÅB
重要	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、電源の入れ直しがアサートされました	IDRAC ウォッチドッグは、システムのクラッシュ(ホストからの応答がないためのタイマー期限切れ)を検知し、電源入れ直しの処置が設定されています。ÅB
重要	システム基板 SEL: システム基板のイベントログセンサー、ログがいっぱいであることがアサートされました	SEL デバイスは、SEL がいっぱいになる前に 1 つしかエンTRIESを追加できないことを検出しました。ÅB
警告	ECC 訂正可能エラー: メモリセンサー、訂正可能な ECC (<DIMM の位置>) がアサートされました	訂正可能 ECC エラー数が重要レートに達しました。
重要	ECC 訂正不能エラー: メモリセンサー、訂正不能 ECC (<DIMM の位置>) がアサートされました	訂正不能 ECC エラーが検知されました。
重要	I/O チャンネルチェック: 重要なイベントセンサー、I/O チャンネルチェック NMI がアサートされました	I/O チャンネルに重要な割り込みが発生しています。
重要	PCI パリティエラー: 重要なイベントセンサー、PCI PERR がアサートされました	PCI バスにパリティエラーが検知されました。
重要	PCI システムエラー: 重要なイベントセンサー、PCI SERR (<スロット番号または PCI デバイス ID>) がアサートされました	デバイスにより、PCI エラーが検知されました。
重要	SBE ログ無効: イベントログセンサー、訂正可能なメモリエラーのログ無効がアサートされました	ログされるシングルビットエラーの数が多すぎると、シングルビットエラーのログは無効になります。
重要	ログ無効: イベントログセンサー、すべてのイベントログ無効がアサートされました	すべてのエラーログは無効になります。
リカバリ不可	CPU プロトコルエラー: プロセッサセンサー、リカバリ不可へのステータス移行がアサートされました	プロセッサプロトコルがリカバリ不可の状態になりました。
リカバリ不可	CPU バスエラー: プロセッサセンサー、リカバリ不可へのステータス移行がアサートされました	プロセッサバス PERR がリカバリ不可の状態になりました。
リカバリ不可	CPU 初期化エラー: プロセッサセンサー、リカバリ不可へのステータス移行がアサートされました	プロセッサ初期化がリカバリ不可の状態になりました。
リカバリ不可	CPU マシンチェック: プロセッサセンサー、リカバリ不可へのステータス移行がアサートされました	プロセッサマシンチェックがリカバリ不可の状態になりました。
重要	メモリスベア: メモリセンサー、冗長性喪失 (<DIMM の位置>) がアサートされました	メモリスベアの冗長性が無くなりました。
重要	メモリミラー: メモリセンサー、冗長性喪失 (<DIMM の位置>) がアサートされました	メモリミラーの冗長性が無くなりました。
重要	メモリ RAID: メモリセンサー、冗長性喪失 (<DIMM の位置>) がアサートされました	RAID メモリの冗長性が無くなりました。
警告	メモリ追加: メモリセンサー、メモリの存在 (<DIMM の位置>) がアサート解除されました	増設されたメモリモジュールが取り外されました。
警告	メモリ除去: メモリセンサー、メモリの存在 (<DIMM の位置>) がアサート解除されました	メモリモジュールが取り外されました。
重要	メモリ構成エラー: メモリセンサー、構成エラー (<DIMM の位置>) がアサートされました	システムのメモリ構成が正しくありません。
警告	メモリ冗長性低下: メモリセンサー、冗長性低下 (<DIMM の位置>) がアサートされました	メモリの冗長性は低下しましたが、喪失されていません。
重要	PCIE 致命的エラー: 重要なイベントセンサー、バスの致命的エラーがアサートされました	PCIE バスに致命的なエラーが検知されました。
重要	チップセットエラー: 致命的なイベントセンサー、PCI PERR がアサートされました	チップエラーが検出されました。
警告	メモリ ECC 警告: メモリセンサー、OK から 非重要 (<DIMM の場所>) へのステータス移行がアサートされました	訂正可能な ECC エラー率が通常率より増加しました。
重要	メモリ ECC 警告: メモリセンサー、やや重大 から 重要 (<DIMM の場所>) へのステータス移行がアサートされました	訂正可能な ECC エラー率が重要な率に達しました。
重要	POST エラー: POST センサー、メモリ非搭載	システム基板にメモリが搭載されていません
重要	POST エラー: POST センサー、メモリ構成エラー	メモリが検出されましたが、構成不能です。

重要	POST エラー: POST センサー、使用不可メモリエラー	メモリが構成されましたが、使用できません。
重要	POST エラー: POST センサー、シャドウ BIOS にエラーが発生しました	システム BIOS シャドウの障害
重要	POST エラー: POST センサー、CMOS にエラーが発生しました	CMOS の障害
重要	POST エラー: POST センサー、DMA コントローラにエラーが発生しました	DMA コントローラの障害
重要	POST エラー: POST センサー、割り込み信号コントローラにエラーが発生しました	割り込み信号コントローラの障害
重要	POST エラー: POST センサー、タイマー更新が失敗しました	タイマー更新エラー
重要	POST エラー: POST センサー、設定可能インターバルタイマーエラー	設定可能インターバルタイマーのエラー
重要	POST エラー: POST センサー、パリティエラー	パリティエラー
重要	POST エラー: POST センサー、SIO にエラーが発生しました	SIO の障害
重要	POST エラー: POST センサー、キーボードコントローラにエラーが発生しました	キーボードコントローラエラー
重要	POST エラー: POST センサー、システム管理割り込みの初期化に失敗しました	SMI (システム管理割り込み) の初期化エラー。
重要	POST エラー: POST センサー、BIOS シャットダウンテストに失敗しました	BIOS シャットダウンテストエラー
重要	POST エラー: POST センサー、BIOS POST メモリテストに失敗しました	BIOS POST メモリテストエラー
重要	POST エラー: POST センサー、Dell リモートアクセスコントローラの構成に失敗しました	DRAC (Dell Remote Access Controller) の構成エラー
重要	POST エラー: POST センサー、CPU 構成に失敗しました	CPU 構成エラー
重要	POST エラー: POST センサー、不正メモリ構成エラー	メモリ構成が正しくありません
重要	POST エラー: POST センサー、POST にエラーが発生しました	ビデオ初期化後の一般的エラー。
重要	ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性がアサートされました	互換性のないハードウェアが検知されました
重要	ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性 (BMC ファームウェア) がアサートされました	ハードウェアはファームウェアとの互換性がありません。
重要	ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性 (BMC ファームウェアと CPU の不一致) がアサートされました	CPU はファームウェアとの互換性がありません
重要	メモリ過熱: メモリセンサー、訂正可能な ECC <DIMM の位置> がアサートされました	メモリモジュールの過熱
重要	メモリ致命的 SB CRC: メモリセンサー、訂正不能な ECC がアサートされました	South bridge メモリの障害
重要	メモリ致命的 NB CRC: メモリセンサー、訂正不能な ECC がアサートされました	North bridge メモリの障害
重要	ウォッチドッグタイマー: ウォッチドッグセンサー、再起動がアサートされました	ウォッチドッグタイマーがシステムを再起動させました
重要	ウォッチドッグタイマー: ウォッチドッグセンサー、タイマー期限切れがアサートされました	ウォッチドッグタイマーが期限切れになりましたが、処置の必要なし
警告	リンクチューニング: バージョン変更センサー、ソフトウェアまたはファームウェアの変更がアサート解除されました	正常な NIC 操作を可能にするリンクチューニング設定のアップデートに失敗しました
警告	リンクチューニング: バージョン変更センサー、ハードウェアの変更 <デバイスのスロット番号> がアサート解除されました	正常な NIC 操作を可能にするリンクチューニング設定のアップデートに失敗しました
重要	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、仮想 MAC アドレス (バス # デバイス # 機能 #) の設定失敗がアサートされました	このデバイスでは、フレックスアドレスを設定できません
重要	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、デバイスオプション ROM によるリンクチューニングまたはフレックスアドレス (メザニン <位置>) のサポートの失敗がアサートされました	オプション ROM がフレックスアドレスまたはリンクチューニングをサポートしていません。
重要	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、BMC/iDRAC からのリンクチューニングまたはフレックスアドレスデータの取得失敗がアサートされました	BMC/iDRAC からリンクチューニングまたはフレックスアドレス情報の取得に失敗しました。
重要	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、デバイスオプション ROM によるリンクチューニングまたはフレックスアドレス (メザニン XX) のサポートの失敗がアサートされました	このイベントは、NIC 用の PCI デバイスオプション ROM がリンクチューニングまたはフレックスアドレス設定機能をサポートしない場合に生成されます。
重要	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、仮想 MAC アドレス (<場所>) のプログラムの失敗がアサートされました	このイベントは、所定の NIC デバイスの仮想 MAC アドレスのプログラムに BIOS が失敗した場合に生成されます。
重要	I/O 致命的エラー: 致命的 IO グループセンサー、致命的 IO エラー (<場所>)	このイベントは、CPU IERR に関連して生成され、CPU IERR の原因となったデバイスを示します。
警告	PCIe 非致命的エラー: 非致命的な I/O グループセンサー、PCIe エラー (<場所>)	このイベントは CPU IERR に関連して生成されます。

iDRAC ログの表示

iDRAC ログは持続的なログで、iDRAC ファームウェアに保管されています。ログにはユーザーの処置 (ログイン、ログアウト、セキュリティポリシーの変更など) と iDRAC が発行する警告のリストが格納されています。ログがいっぱいになると、最も古いエントリから上書きされます。

システムイベントログ (SEL) には管理下サーバーで発生するイベントのレコードが格納され、iDRAC ログには iDRAC で発生するイベントのレコードが格納されます。

iDRAC ログにアクセスするには、次の手順を実行してください。

- 1 システム → リモートアクセス → iDRAC の順に クリックし、iDRAC ログ をクリックします。

iDRAC ログは、表 14-9 の情報を提供します。

表 14-9 iDRAC ログページ情報

フィールド	説明
日時	日付と時刻 (Dec 19 16:55:47 など)。

	iDRAC のクロックは、管理下サーバーのクロックから設定されます。iDRAC を最初に起動する際に管理下サーバーと通信できない場合は、システム起動の文字列として時刻が表示されます。
ソース	イベントを引き起こしたインタフェース
説明	イベントの概要と iDRAC にログインしたユーザー名。

iDRAC ログページのボタンの使用

iDRAC ログ ページには、次のボタンがあります(「表 14-10」を参照)。

表 14-10 iDRAC ログボタン

ボタン	動作
印刷	iDRAC ログ ページを印刷します。
ログのクリア	iDRAC ログ のエントリをクリアします。 メモ: ログのクリア ボタンは、ログのクリア 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、iDRAC ログ を選択したディレクトリに保存できます。 メモ: Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト support.microsoft.com から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。
更新	iDRAC ログ ページを再ロードします。

システム情報の表示

システム概要 ページには、次のシステムコンポーネントに関する情報が表示されます。

- 1 メインシステムエンクロージャ
- 1 iDRAC(Integrated Dell Remote Access Controller)

システム情報にアクセスするには、システム→プロパティの順にクリックします。

メインシステムエンクロージャ

表 14-11 と 表 14-12 で、メインシステムエンクロージャのプロパティについて説明します。

表 14-11 システム情報フィールド

フィールド	説明
説明	システムの情報を表示します。
BIOS バージョン	システムの BIOS バージョンを表示します。
サービスタグ	システムのサービスタグ番号を表示します。
ホスト名	ホストシステムの名前を表示します。
OS 名	システムで実行されているオペレーティングシステムを表示します。

表 14-12 自動リカバリフィールド

フィールド	説明
リカバリ処置	システムハング が検知されたときに、iDRAC が処置の必要なし、ハードリセット、電源を切る、パワーサイクル のいずれかの処置を実行するように設定できます。
初期カウントダウン	システムハング が検知されてから iDRACがリカバリ処置を実行するまでの秒数。
現在のカウントダウン	カウントダウンタイマーの現在の値(秒)。

iDRAC(Integrated Dell Remote Access Controller)

表 14-13 iDRAC プロパティについて説明しています。

表 14-13 iDRAC 情報フィールド

フィールド	説明
日時	iDRAC の現在の日時を GMT で表示します。
ファームウェアバージョン	iDRAC ファームウェアのバージョンを表示します。
ファームウェアアップデート	ファームウェアが最後にアップデートされた日付を表示します。日付は UTC フォーマットで表示されます (例: Tue, 8 May 2007, 22:18:21 UTC)。
IP アドレス	ネットワークインタフェースを識別する 32 ビットアドレス。値は、143.166.154.127 のようなドット区切りのフォーマットで表示されます。
ゲートウェイ	他のネットワークへのブリッジの役割を果たすゲートウェイの IP アドレス。値は、143.166.150.5 のようなドット区切りのフォーマットです。
サブネットマスク	サブネットマスクは、拡張ネットワークプレフィックスとホスト番号を構成する IP アドレスの一部を示します。値は、255.255.0.0 のようなドット区切りのフォーマットで表示されます。
MAC アドレス	ネットワークで各 NIC を固有に識別するメディアアクセスコントロール (MAC) アドレス (例: 00-00-0c-ac-08)。これは、Dell が割り当てる ID で、編集できません。
DHCP 有効	有効 は、動的ホスト構成プロトコル (DHCP) が有効であることを示します。 無効 は、DHCP が有効でないことを示します。

シャーシ内の管理下サーバーの識別

PowerEdge M1000e シャーシは、最大 16 台のサーバーを収容できます。シャーシ内の特定のサーバーを見つけるために、iDRAC ウェブインタフェースを使用してサーバー上の青色の点滅 LED をオンにできます。LED をオンにする際、LED が点滅している間にシャーシに到達できるように LED を点滅させる秒数を指定できます。0 を入力すると、LED は無効にされるまで点滅し続けます。

サーバーを識別するには、次の手順を実行してください。

1. **システム** → **リモートアクセス** → **iDRAC** → **トラブルシューティング** の順にクリックします。
2. **識別** ページで **サーバーの識別** の横の値ボックスをチェックします。
3. **サーバータイムアウトの識別** フィールドに、LED を点滅させる秒数を入力します。無効にするまで点滅させる場合は 0 を入力します。
4. **適用** をクリックします。

サーバー上の青色の LED が指定した秒数ほど点滅します。

0 を入力して LED を点滅させ続けている場合、次の手順を実行してこれを無効にします。

1. **システム** → **リモートアクセス** → **iDRAC** → **トラブルシューティング** の順にクリックします。
2. **識別** ページで **サーバーの識別** の横の値ボックスを選択解除します。
3. **適用** をクリックします。

診断コンソールの使用

iDRAC には、Microsoft® Windows® や Linux システムに含まれているものと同様なネットワーク診断ツールが標準装備されています (「表 14-14」を参照)。iDRAC ウェブインタフェースを使用して、ネットワークのデバッグツールにアクセスできます。

診断コンソール ページにアクセスするには、次の手順を実行してください。

1. **システム** → **iDRAC** → **トラブルシューティング** の順にクリックします。
2. **診断** タブをクリックします。

表 14-14 に、**診断コンソール** ページに入力できるコマンドを示します。コマンドを入力して **送信** をクリックします。デバッグの結果が **診断コンソール** ページに表示されます。

クリア ボタンをクリックして、前のコマンドで表示した結果をクリアします。

診断コンソール ページを更新するには、**更新** をクリックします。


表 14-14 診断コマンド

コマンド	説明
arp	ARP (Address Resolution Protocol) テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を印刷します。

ping <IP アドレス>	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC から到達可能かどうかを確認します。宛先 IP アドレスをこのオプションの右にあるフィールドに入力してください。ICMP (インターネットコントロールメッセージプロトコル) エコーパケットが現在のルーティングテーブルの内容に基づいて宛先 IP アドレスに送信されます。
gettracelog	iDRAC トレースログ を表示します。詳細については、「 gettracelog 」を参照してください。

リモートシステムの電源管理

iDRAC では、管理下サーバーの電源管理操作をリモートで実行できます。再起動時と電源の投入および切断時に、オペレーティングシステムからシャットダウンをきちんと実行するには、電源管理ページを使用します。

 **メモ:** 電源管理処置を実行するには、**サーバー処置コマンドの実行** 権限が必要です。ユーザー権限の設定方法については、「[iDRAC ユーザーの追加と設定](#)」を参照してください。

1. **システム** をクリックし、**電源管理** タブをクリックします。
2. **電源制御処置** を選択します (例: **システムをリセットする (ウォームブート)**)。
[表 14-15](#) に、電源制御処置について説明します。
3. 選択した処置を実行するには、**適用** をクリックします。
4. 適切な ボタン をクリックして続行します。「[表 14-16](#)」を参照してください。

表 14-15 電源制御処置

システムの電源を入れる	システムの電源をオンにします (システムの電源がオフのときに電源ボタンを押すのと同じ)。
システムの電源を切る	システムの電源をオフにします (システムの電源がオンのときに電源ボタンを押すのと同じ)。
NMI (Non-Masking Interrupt)	オペレーティングシステムに高レベルの割り込みを送信し、重要な診断またはトラブルシューティング動作を可能にするためにシステム動作を一時停止させます。
正常なシャットダウン	オペレーティングシステムを正常にシャットダウンし、システムの電源を切ります。これには、システムによる電源管理を可能にする ACPI (Advanced Configuration and Power Interface) 対応のオペレーティングシステムが必要です。
システムをリセットする (ウォームブート)	電源を切らずにシステムを再起動します (ウォームブート)。
システムの電源を入れ直す	電源を切ってからシステムを再起動します (コールドブート)。

表 14-16 電源管理ページのボタン

ボタン	動作
印刷	画面に表示されている 電源管理 ページのデータを印刷します。
更新	電源管理 ページを再ロードします。
適用	電源管理 ページ表示中に加えた新しい設定を保存します。

トラブルシューティングとよくあるお問い合わせ (FAQ)

[表 14-17](#) に、トラブルシューティングについてよくあるお問い合わせ (FAQ) を掲載します。

表 14-17 トラブルシューティングとよくあるお問い合わせ (FAQ)

質問	回答
サーバー上の LED が黄色で点滅中です。	SEL でメッセージを確認し、SEL をクリアして LED の点滅を停止します。 iDRAC ウェブインタフェースを使用する場合: <ol style="list-style-type: none"> 1 「システムイベントログ (SEL) の確認」を参照してください。 SM-CLP を使用する場合: <ol style="list-style-type: none"> 1 「SEL 管理」を参照してください。 iDRAC 設定ユーティリティを使用する場合: <ol style="list-style-type: none"> 1 「システムイベントログメニュー」を参照してください。
サーバー上で青色の LED が点滅しています。	ユーザーがサーバーのロケータ ID をアクティブにした状態です。シャシ内のサーバーを識別するのに役立つ信号です。この機能についての詳細は、「 シャシ内の管理下サーバーの識別 」を参照してください。
iDRAC の IP アドレスの検索方法は?	CMC ウェブインタフェースを使用する場合:

	<ol style="list-style-type: none"> 1. シャーシ→ サーバー の順にクリックし、セットアップ タブをクリックします。 2. 導入 をクリックします。 3. 表示される表からサーバーの IP アドレスを読み取ります。 <p>KVMを使用する場合:</p> <ol style="list-style-type: none"> 1. サーバーを再起動し、Ctrl+E キーを押して iDRAC 設定ユーティリティに入ります。 <p>または</p> <ol style="list-style-type: none"> 1. BIOS POST 中に表示される IP アドレスに注目します。 <p>または</p> <ol style="list-style-type: none"> 1. OSCAR の「Dell CMC」コンソールを選択してローカルシリアル接続経由で CMC にログインします。 <p>CMC RACADM コマンドはこの接続から発行できます。CMC RACADM サブコマンドのリストは、『CMC ファームウェアユーザーズガイド』を参照してください。</p>
iDRAC の IP アドレスの検索方法は?(続き)	<p>次に、例を示します。</p> <pre>\$ racadm getniccfg -m server-1</pre> <p>DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1</p> <p>ローカル RACADM を使用する場合:</p> <ol style="list-style-type: none"> 1. コマンドプロンプトで次のコマンドを入力します。 <pre>racadm getsysinfo</pre> <p>LCD を使用する場合:</p> <ol style="list-style-type: none"> 1. メインメニューで サーバー をハイライトし、チェックボタンを押します。 2. IP アドレスを検索するサーバーを選択し、チェック ボタンを押します。
CMC の IP アドレスの検索方法は?	<p>iDRAC ウェブインタフェースを使用する場合:</p> <ol style="list-style-type: none"> 1. システム→ リモートアクセス→ CMC の順にクリックします。 <p>概要 ページに CMC の IP アドレスが表示されます。</p> <p>または</p> <ol style="list-style-type: none"> 1. OSCAR の「Dell CMC」コンソールを選択してローカルシリアル接続経由で CMC にログインします。CMC RACADM コマンドはこの接続から発行できます。CMC RACADM サブコマンドのリストは、『CMC ファームウェアユーザーズガイド』を参照してください。 <pre>\$ racadm getniccfg -m chassis</pre> <p>NIC Enabled = 1 DHCP Enabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate</p>
iDRAC ネットワーク接続が機能しません。	<ol style="list-style-type: none"> 1. LAN ケーブルが CMC に接続されていることを確認してください。 1. iDRAC の LAN が有効になっていることを確認してください。
サーバーをシャーシに挿入し、電源ボタンを押したのですが、何も起こりません。	<ol style="list-style-type: none"> 1. サーバーの電源が入るまでに、iDRAC は初期化に約 30 秒かかります。30 秒待ってから電源ボタンをもう一度押してください。 1. CMC の電力バジェットを確認してください。シャーシの電力バジェットを超えている可能性があります。
iDRAC のシステム管理者ユーザー名とパスワードを忘れました。	<p>iDRAC をデフォルト設定に復元する必要があります。</p> <ol style="list-style-type: none"> 1. サーバーを再起動し、Ctrl+E キーを押して iDRAC 設定ユーティリティに切り替えます。 2. 設定ユーティリティメニューで、デフォルトにリセットする をハイライトして Enter キーを押します。 <p>詳細については、『デフォルトに戻す』を参照してください。</p>
サーバースロット名の変更方法は?	<ol style="list-style-type: none"> 1. CMC ウェブインタフェースにログインします。 2. シャーシ ツリーを開き、サーバー をクリックします。 3. セットアップ タブをクリックします。 4. 該当するサーバーの行に、新しいスロット名を入力します。 5. 適用 をクリックします。
iDRAC ウェブインタフェースからコンソールリダイレクトセッションを起動すると ActiveX セキュリティポップアップ画面が表示されます。	<p>iDRAC がクライアントのブラウザで信頼済みサイトでない可能性があります。</p> <p>コンソールリダイレクトセッションを開始するたびにセキュリティポップアップ画面が表示されるのを回避するには、iDRAC を信頼済みサイトリストに追加してください。</p>

	<ol style="list-style-type: none"> 1. ツール→インターネットオプション...→セキュリティ→信頼済みサイトの順にクリックします。 2. サイトをクリックして iDRAC の IP アドレスまたは DNS 名を入力します。 3. 追加をクリックします。
コンソールリダイレクトセッションを開始したとき、ビューアの画面が空白です。	仮想メディア 権限があるが、コンソールリダイレクト 権限がない場合、仮想メディア機能にアクセスできるようビューアを起動できますが、管理下サーバーのコンソールは表示されません。
iDRAC が起動しません。	<p>サーバーを取り外し、挿入し直してください。</p> <p>iDRAC がアップグレード可能なコンポーネントとして表示されているかどうか CMC ウェブインタフェースを確認します。表示される場合は、「CMC を使用した iDRAC フォームウェアのリカバリ」の手順に従ってください。</p> <p>依然問題が修正されない場合は、テクニカルサポートにお問い合わせください。</p>
管理下サーバーの起動を試行すると、電源インジケータは緑色ですが POST またはビデオが表示されません。	<p>これは、次の状態である場合に発生します。</p> <ul style="list-style-type: none"> 1 メモリがインストールされていない、またはアクセス不可能である。 1 CPU がインストールされていない、またはアクセス不可能である。 1 ビデオライザーカードが不在、または接続が不適切である。 <p>また、iDRAC ウェブインタフェースまたは LCD で iDRAC ログのエラーメッセージも確認してください。</p>

[目次ページに戻る](#)

[目次ページに戻る](#)

用語集

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

Active Directory

Active Directory は、ユーザーデータ、セキュリティ、分散リソースのネットワーク管理を自動化する標準化された一元管理システムで、他のディレクトリとの相互動作ができるようにします。Active Directory は、分散ネットワーク環境用に特にデザインされています。

ARP

アドレス解決プロトコル(Address Resolution Protocol)の略語。インターネットアドレスからホストの Ethernet アドレスを求める手法。

ASCII

情報交換用アメリカ標準コード(American Standard Code for Information Interchange)の略語。文字、数字、その他の記号の表示と印刷に使用されるコード表現体系。

BIOS

Basic Input/Output System の略語。周辺デバイスに最も低位レベルのインタフェースを提供し、オペレーティングシステムのメモリへのロードなど、システム起動処理の第一段階を制御するシステムソフトウェアの一部。

バス

コンピュータ内の各種の機能単位を接続する伝導体のセット。バスは、それが運ぶデータの種別によって、データバス、アドレスバス、PCI バスなどと名付けられます。

CA

認証局(CA)は、IT 業界で認知されたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を提供しています。CA には、Thawte や VeriSign などがあります。CA は CSR を受理すると、CSR に含まれる情報を調べ、検証します。応募者が CA のセキュリティ標準を満たしていると、CA はネットワークおよびインターネットを介したトランザクションに対して、応募者を一意に識別する証明書を発行します。

CD

コンパクトディスク(Compact Disc)の略語。

CHAP

Challenge-Handshake Authentication Protocol の略語。PPP サーバーが使用している認証スキームで、接続時またはそれ以降に、接続元の一致を確認します。

CIM

Common Information Model の略語。ネットワーク上でシステムを管理するためのプロトコル。

CLI

コマンドラインインタフェース(Command Line Interface)の略語。

CLP

コマンドラインプロトコル(Command Line Protocol)の略語。

コンソールリダイレクト

コンソールリダイレクトとは、管理下システムのディスプレイ画面、マウス機能およびキーボード機能を管理ステーションの該当するデバイスへ転送する機能のこと。これを使用して管理ステーションの

システムコンソールから管理下システムを制御できます。

CSR

認証署名要求 (Certificate signing request) の略語。

DHCP

ダイナミックホスト設定プロトコル (Dynamic Host Configuration Protocol) の略語。このプロトコルは IP アドレスをローカルエリアネットワーク (LAN) のコンピュータに動的に割り当てる手段を提供します。

DLL

Dynamic Link Library (ダイナミックリンクライブラリ) の略語。小さいプログラムで構成されたライブラリ。システムで実行中の大きいプログラムが必要時に呼び出すことができます。この小さいプログラムは、大きいプログラムがプリンタやスキャナなどの特定のデバイスと通信できるように、DLL プログラム (または DLL ファイル) としてパッケージ化されていることがよくあります。

DDNS

Domain Name System (ドメイン名システム)

DMTF

分散管理タスクフォース (Distributed Management Task Force) の略語。

DNS

ドメイン名システム (Domain Name System) の略語。

DSU

ディスクストレージユニット (Disk Storage Unit) の略語。

拡張スキーマ

Active Directory と併用されるソリューションで iDRAC6 へのユーザーアクセスを特定します。Dell 定義の Active Directory オブジェクトを使用します。

FQDN

完全修飾ドメイン名 (Fully Qualified Domain Names) の略語。Microsoft® Active Directory® は、64 バイト以下の FQDN しかサポートしていません。

FSMO

Flexible Single Master Operation の略語。Microsoft が拡張動作の一律性を保証する方法。

GMT

Greenwich Mean Time (グリニッジ標準時) の略語。世界各地に共通する標準時刻。GMT は一般的にイギリスのロンドン郊外にあるグリニッジ天文台跡を通過する本初子午線 (経度 0°) に基づく平均太陽時を反映するものです。

GPIO

汎用入力 / 出力 (General Purpose Input/Output) の略語。

GRUB

GRand Unified Bootloader の略語。一般的に使用される新しい Linux ローダー。

GUI

グラフィカルユーザーインターフェース(Graphical User Interface)の略語。ユーザーとの対話がすべてテキストによって表示または入力されるコマンド表示メッセージインターフェースとは対照的に、ウインドウ、ダイアログボックス、ボタンなどの要素を使用したコンピュータ表示インターフェースを指します。

ハードウェアログ

iDRAC6 が生成したイベントを記録します。

iAMT

Intel® Active Management Technology(アクティブマネジメントテクノロジー) - コンピュータの電源が入っている / いない、またオペレーティングシステムの応答不在に関わらず、よりセキュアなシステム管理機能を実現します。

ICMB

Intelligent Enclosure Management Bus(インテリジェントエンクロージャ管理バス)の略語。

ICMP

Internet Control Message Protocol の略語。

ID

識別子(Identifier)の略語。一般に、ユーザー識別子(ユーザー ID)またはオブジェクト識別子(オブジェクト ID)を参照するときに使用されます。

iDRAC6

integrated Dell Remote Access Controller の略語。Dell 11G PowerEdge サーバー用の内蔵システムオンチップ監視 / 制御システム。

IP

インターネットプロトコル(Internet Protocol)の略語。TCP/IP のネットワーク層。IP はパケットの経路選択、断片化、再構成などを行います。

IPMB

intelligent platform management bus の略語。システム管理テクノロジーで使用されるバス。

IPMI

Intelligent Platform Management Interface の略語。システム管理テクノロジーの一部。

Kbps

1 秒あたりのキロビット数(Kilobits per second)の略語で、データ転送速度を表します。

LAN

構内通信網またはローカルエリアネットワーク(Local Area Network)の略語。

LDAP

軽量ディレクトリアクセスプロトコル(Lightweight Directory Access Protocol)の略語。

LED

発光ダイオード(light-emitting diode)の略語。

LOM

マザーボードに組み込まれた LAN 接続(Local area network On Motherboard)の略語。

LUN

logical unit の略語(論理装置)。

MAC

媒体アクセス制御(Media Access Control)の略語。ネットワークノードとネットワーク物理層の間のネットワークサブレイヤ。

MAC アドレス

媒体アクセス制御アドレス(Media Access Control address)の略語。NIC の物理コンポーネントに組み込まれる固有アドレス。

管理下サーバー

管理下サーバーは、iDRAC が組み込まれているシステムです。

管理下システム

管理ステーションにより監視されるシステムは、管理下システムと呼ばれています。

管理ステーション

管理ステーションは、iDRAC6 を備えた Dell システムをシステム管理者がリモートで管理するシステムです。

MAP

Manageability Access Point の略語。

Mbps

1 秒あたりのメガビット数(Megabits per second)の略語で、データ転送速度を表します。

MIB

管理情報ベース(Management Information Base)の略語。

MII

Media Independent Interface の略語。

NAS

ネットワーク接続ストレージ(Network Attached Storage)の略語。

NIC

Network Interface Card (ネットワークインタフェースカード)の略語。アダプタ回路基板。コンピュータに搭載されて、ネットワークへの物理的な接続を提供します。

OID

Object Identifiers(オブジェクト識別子)の略語。

PCI

Peripheral Component Interconnect(周辺機器コンポーネント相互接続)の略語。周辺機器をシステムに接続し、それらの周辺機器と通信するための標準インタフェースおよびバス技術です。

POST

電源投入時自己診断(power-on self-test)の略語。コンピュータの電源を入れると、システムによって自動的に一連の診断テストが実行されます。

PPP

Point-to-Point Protocol の略語。一連のポイントツーポイントリンクを通じて、ネットワークレイヤデータグラム(IP パケットなど)の転送に使うインターネット標準プロトコル。

RAM

ランダムアクセスメモリ(Random-Access Memory)の略語。RAM は、システムおよび iDRAC6 上の の読み書き可能な汎用メモリです。

RAM ディスク

ハードディスクをエミュレートするメモリ常驻プログラム。iDRAC6 はメモリに RAM ディスクを保持しています。

RAC

Remote Access Controller の略語。

ROM

読み取り専用メモリ(Read-Only Memory)の略語。データの読み取りはできますが、書き込みはできません。

ロールバック

以前のソフトウェアまたはファームウェア バージョンへ戻すことです。

RPM

Red Hat® Package Manager の略語。Red Hat Enterprise Linux® オペレーションシステム用のパッケージ管理システムで、ソフトウェアパッケージのインストールを支援します。インストールプログラムに似ています。

SAC

Microsoft Special Administration Console の略語。

SAP

サービスアクセスポイント(Service Access Point)の略語。

SEL

システムイベントログ(system event log)の略語。

SMI

システム管理割り込み(Systems Management Interrupt)の略語。

SM-CLP

Server Management-Command Line Protocol の略語(サーバー管理コマンドラインプロトコル)。SM-CLP は、複数のプラットフォームでサーバー管理を主導する DMTF SMASH のサブコンポーネントです。Managed Element Addressing Specification (管理下エレメントアドレス指定仕様書)および SM-CLP マッピング仕様に対する多くのプロファイルに関連する SM-CLP 仕様書は、さまざまなタスク実行用の標準化されたバードとターゲットについて説明しています。

SMTP

簡易メール転送プロトコル(Simple Mail Transfer Protocol)の略語。システム間の電子メールの転送に使用するプロトコル。SMTP は通常、イーザネット上で使用されます。

SMWG

Systems Management Working Group(システム管理ワークグループ)の略語。

SNMP トラップ

IDRAC6 で生成される通知(イベント)で、管理下システムの状況の変化や、ハードウェアの潜在的な問題に関する情報が含まれています。

SSH

セキュアシェル(Secure Shell)の略語。

SSL

セキュアソケットレイヤ(Secure Sockets Layer)の略語。

標準スキーマ

Active Directory と併用されるソリューションで IDRAC6 へのユーザーアクセスを特定します。Active Directory グループオブジェクトのみを使用します。

TAP

Telelocator Alphanumeric Protocol の略語。ページャサービスに要求を送信するために使用するプロトコル。

TCP/IP

Transmission Control Protocol/Internet Protocol の略語。ネットワーク層とトランスポート層のプロトコルを持つ標準 Ethernet プロトコルのセットを指します。

TFTP

簡易ファイル転送プロトコル(Trivial File Transfer Protocol)の略語。デバイスやシステムに起動コードをダウンロードするために使用される簡易ファイル転送プロトコル。

Unified Server Configurator

Dell Unified Server Configurator(USC)は組み込まれている設定ユーティリティで、サーバーのライフサイクル中、システムとストレージの管理タスクを組み込み環境から実行できるようにします。

UPS

無停電電源装置 (Uninterruptible power supply) の略語。

USB

Universal Serial Bus の略語。

USC

Unified Server Configurator の略語。

UTC

協定世界時 (Universal Coordinated Time) の略語。「GMT」を参照してください。

VLAN

仮想構内通信網 (Virtual Local Area Network) の略語。

VNC

仮想ネットワークコンピューティング (Virtual Network Computing) の略語。

VT-100

ビデオ端末 (Video Terminal) 100 の略語。多くの共通端末エミュレーションプログラムによって使用されています。

WAN

広域通信網 (Wide Area Network) の略語。

WS-MAN

Web Services for Management (管理用ウェブサービス) (WS-MAN) プロトコルの略語。WS-MAN は、情報交換用のトランスポートメカニズムです。管理が簡単になるよう、WS-MAN はデバイスがデータを共有するよう汎用言語を提供します。

[目次ページに戻る](#)

[目次ページに戻る](#)

RACADM サブコマンドの概要

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

- [help](#)
- [arp](#)
- [clearasrscreen](#)
- [config](#)
- [getconfig](#)
- [coredump](#)
- [coredumpdelete](#)
- [fwupdate](#)
- [getssninfo](#)
- [getsysinfo](#)
- [gettractime](#)
- [ifconfig](#)
- [netstat](#)
- [ping](#)
- [setniccfg](#)
- [getniccfg](#)
- [getsvctag](#)
- [racdump](#)
- [racreset](#)
- [_racresetcfg](#)
- [serveraction](#)
- [getraclog](#)
- [clrraclog](#)
- [getsel](#)
- [clrsel](#)
- [gettracelog](#)
- [sslcsrgen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [sslkeyupload](#)
- [testemail](#)
- [testtrap](#)
- [vmdisconnect](#)
- [vmkey](#)
- [usercertupload](#)
- [usercertview](#)
- [localConRedirDisable](#)

本項では、RACADM コマンドラインインタフェースで使用できるサブコマンドについて説明します。

help


 **メモ:** このコマンドを使うには、iDRAC へのログイン 権限が必要です。

表 A-1 に、help コマンドについて説明します。

表 A-1 Help コマンド

コマンド	定義
help	RACADM で使用できるすべてのサブコマンドをリストにし、それぞれの短い説明を表示します。

概要

```
racadm help
```

```
racadm help <サブコマンド>
```

説明

help サブコマンドは racadm コマンドで使用できるサブコマンドすべてをリストにし、各サブコマンドにつき一行ずつの説明を表示します。help の後にサブコマンドを入力して、そのサブコマンドの構文を表示することもできます。

出力

racadm help コマンドはすべてのサブコマンドのリストを表示します。

racadm help <サブコマンド> コマンドは、指定したコマンドだけの情報を表示します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM

arp

 **メモ:** このコマンドを使用するには、**診断コマンドの実行** パーミッションが必要です。

[表 A-2](#) にarp コマンドを示します。

表 A-2 arp コマンド

コマンド	定義
arp	ARP テーブルの内容を表示します。ARP テーブル エントリの追加や削除はできません。


概要

racadm arp

対応インターフェース

- 1 リモート RACADM
 - 1 telnet/ssh/シリアル RACADM
-

clearasrscreen

 **メモ:** このサブコマンドを使うには、**ログのクリア** パーミッションが必要です。

[表 A-3](#) にclearasrscreen サブコマンドを示します。

表 A-3 clearasrscreen

サブコマンド	定義
clearasrscreen	メモリにある最後のクラッシュ画面をクリアします。


概要

racadm clearasrscreen

対応インターフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
 - 1 telnet/ssh/シリアル RACADM
-

config

 **メモ:** getconfig コマンドを使うには、iDRAC への**ログイン** 権限が必要です。

[表 A-4](#) に、config および getconfig サブコマンドについて説明します。

表 A-4 config/getconfig

コマンド	定義
------	----

サブコマンド	定義
config	iDRAC6 を設定します。
getconfig	iDRAC6 設定データを取得します。

概要

```
racadm config [-c|-p] -f <ファイル名>
```

```
racadm config -g <グループ名> -o <オブジェクト名> [-i <インデックス>] <値>
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

説明

config サブコマンドにより、iDRAC6 設定パラメータを個々に設定するか、設定ファイルの一部として一括設定できます。データが異なる場合は、その iDRAC6 オブジェクトが新しい値で書き込まれます。

入力

[表 A-5](#) に、**config** サブコマンド オプションについて説明します。

 **メモ:** -f と -p オプションは、シリアル/telnet/ssh コンソールではサポートされていません。

表 A-5 **config** サブコマンドオプションと説明

オプション	説明
-f	-f <ファイル名> オプションを使用すると、 config は <ファイル名> で指定したファイルの内容を読み取り、iDRAC6 を設定します。ファイルの内容は「 構文解析規則 」で指定した形式のデータでなければなりません。
-p	パスワード オプションである -pl は、設定が完了した後、 config に config ファイル -f <ファイル名> に含まれているパスワード エントリを削除させます。
-g	-g <グループ名> (グループオプション) は、-o オプションと一緒に使用する必要があります。<グループ名> は、設定するオブジェクトを含むグループを指定します。
-o	-o <オブジェクト名> <Value> (オブジェクトオプション) は、-g オプションと一緒に使用する必要があります。このオプションは、文字列 <値> で書き込まれるオブジェクト名を指定します。
-i	-i <インデックス> (インデックスオプション) はインデックス付きのグループのみに有効で、固有のグループを指定できます。<index> は 1~16 の 10 進整数です。この場合、索引は「名前付き」の値ではなく、索引値で指定されます。
-c	-c (チェックオプション) は config サブコマンドと一緒に使用し、ユーザーが .cfg ファイルの構文を解析して構文エラーを検出できるようにします。エラーが検出されたら、その行番号とエラーの短い説明が表示されます。iDRAC6 には書き込まれません。このオプションはチェックのみです。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

- 1 無効な構文、グループ名、オブジェクト名、索引、またはその他の無効なデータベースメンバ
- 1 RACADM CLI エラー

このサブコマンドは、.cfg ファイル内にあるオブジェクトの総数のうちいくつかの設定オブジェクトが書き込まれたかを示す数値を返します。


例

```
1 racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100
```

cfgNicIpAddress 設定パラメータ (オブジェクト) の値を 10.35.10.110 に設定します。この IP アドレスオブジェクトは **cfgLanNetworking** グループにあります。

```
1 racadm config -f myrac.cfg
```

iDRAC6 を設定または再設定します。myrac.cfg ファイルは getconfig コマンドから作成できます。myrac.cfg ファイルは、構文解析ルールに従って手動で編集することもできます。

 **メモ:** myrac.cfg ファイルにはパスワード情報は含まれません。この情報をファイルに含めるには、手動で入力する必要があります。設定時に myrac.cfg ファイルからパスワード情報を削除する場合は、-p オプションを使用します。

getconfig

getconfig サブコマンドの説明

getconfig サブコマンドを使うと、ユーザーは個別の iDRAC6 設定パラメータを取得するか、すべての iDRAC6 設定グループを取得してファイルに保存できます。

入力

表 A-6 に、getconfig サブコマンド オプションについて説明します。


 **メモ:** ファイルを指定しないで -f オプションを使用すると、ファイルの内容が端末画面に出力されます。

表 A-6 getconfig サブコマンドオプション

オプション	説明
-f	-f <ファイル名> オプションを getconfig に追加すると、iDRAC6 設定のすべてが設定ファイルに書き込まれます。このファイルは config サブコマンドを使った一括設定用に使用できます。 メモ: -f オプションでは cfgIpmiPet と cfgIpmiPef グループ用のエントリは作成されません。 cfgIpmiPet グループをファイルに取り込むためのトラップ先を少なくとも 1 つ設定する必要があります。
-g	-g <グループ名> (グループ オプション) を使用すると、単一グループの設定を表示できます。グループ名 は、racadm.cfg ファイルで使用されているグループの名前です。グループが索引付きグループの場合は、-i オプションを使用してください。
-h	-h (ヘルプ) オプションは、使用可能な設定グループすべてを表示します。このオプションは、正確なグループ名を覚えていない場合に便利です。
-i	-i <インデックス> (インデックス オプション) は、インデックス付きのグループのみに有効で、固有のグループを指定できます。<インデックス> は 1~16 の 10 進数です。-i <インデックス> を指定しなければ、グループに 1 の値が想定されます。これは複数のエントリを含んだテーブルです。この場合、索引は「名前付き」の値ではなく、索引値で指定されます。
-o	-o <オブジェクト名> (オブジェクトオプション) ではクエリで使用するオブジェクト名を指定します。このオプションは任意選択で、-g オプションと一緒に使用できます。
-u	-u <ユーザー名>、(ユーザー名 オプション) を使うと、指定したユーザーの設定を表示できます。<ユーザー名> オプションはユーザーのログインユーザー名です。
-v	-v オプションは、プロパティの表示で追加の詳細情報を表示するために、-g オプションと一緒に使用します。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

- 1 無効な構文、グループ名、オブジェクト名、索引、またはその他の無効なデータベースメンバ
- 1 RACADM CLI 転送エラー

エラーが発生しなければ、指定した設定の内容が表示されます。

例

```
1 racadm getconfig -g cfgLanNetworking
```

cfgLanNetworking グループ内の設定プロパティ (オブジェクト) をすべて表示します。

```
1 racadm getconfig -f myfile.cfg
```

iDRAC6 のグループ設定オブジェクトすべてを myrac.cfg に保存します。

```
1 racadm getconfig -h
```

iDRAC6 で使用可能な設定グループのリストを表示します。

```
1 racadm getconfig -u root
```

root という名前のユーザーの設定プロパティを表示します。

```
1 racadm getconfig -g cfgUserAdmin -i 2 -v
```

インデックス 2 でのユーザーグループインスタンスを、プロパティ値の詳細情報と一緒に表示します。

概要

```
racadm getconfig -f <ファイル名>
```

```
racadm getconfig -g <グループ名> [-i <索引>]
```


```
racadm getconfig -u <ユーザー名>
```

```
racadm getconfig -h
```

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

coredump

 **メモ:** このコマンドを使用するには、**デバッグコマンドの実行** パーミッションが必要です。

[表 A-7](#) に、**coredump** サブコマンドを示します。

表 A-7 coredump

サブコマンド	定義
coredump	前回の iDRAC6 コア ダンプを表示します。

概要

```
racadm coredump
```

説明

coredump サブコマンドは、RAC で最近発生した重要な問題に関する詳細情報を表示します。coredump 情報はこれらの重要な問題の診断に使用できます。

使用可能な場合、coredump 情報は iDRAC6 の電源を切った後も次の状態が発生するまで保持されます。


- 1 **coredumpdelete** サブコマンドを使って coredump 情報がクリアされた
- 1 RAC で別の重要問題が発生した この場合、coredump 情報は最後に発生した重要エラーに関するものです。

coredumpのクリアに関する詳細は、**coredumpdelete** を参照してください。

対応インターフェース

- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

coredumpdelete

 **メモ:** このコマンドを使用するには、**ログのクリア** または **デバッグコマンドの実行** パーミッションが必要です。

[表 A-8](#) に、**coredumpdelete** サブコマンドを示します。

表 A-8 coredumpdelete


サブコマンド	定義
coredumpdelete	iDRAC6 に保存されているコアダンプを削除します。

概要

```
racadm coredumpdelete
```

説明

coredumpdelete サブコマンドは、現在 RAC に保存されている coredump データをクリアするために使用できます。


 **メモ:** coredumpdelete コマンドを発行したときに coredump が RAC に保存されていないと、成功したというメッセージが表示されます。これは正常な動作です。


coredump の表示に関する詳細は、coredump サブコマンドを参照してください。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

fwupdate

 **メモ:** このコマンドを使うには、iDRAC6 の設定 権限が必要です。

 **メモ:** ファームウェアのアップデートを開始する前に、追加情報について「[iDRAC6 の詳細設定](#)」を参照してください。

[表 A-9](#) に、fwupdate サブコマンドを示します。

表 A-9 fwupdate

サブコマンド	定義
fwupdate	iDRAC6 上のファームウェアをアップデートします。

概要

```
racadm fwupdate -s
```

```
racadm fwupdate -g -u -a <TFTP_サーバー_IP_アドレス> [-d <パス>]
```

```
racadm fwupdate -r
```

説明

fwupdate サブコマンドを使うと、iDRAC6 上のファームウェアをアップデートできます。ユーザーは以下のことができます。

- 1 ファームウェアアップデートプロセスの状態を確認する
- 1 IP アドレスとオプションのパスを指定して TFTP サーバーから iDRAC6 ファームウェアをアップデートする
- 1 ローカル RACADM を使ってローカル ファイル システムから iDRAC6 ファームウェアをアップデートする
- 1 予備ファームウェアのロールバック

対応インターフェース

- 1 ローカル RACADM
- 1 telnet/ssh/シリアル RACADM

入力

表 A-10 に fwupdate サブコマンドのオプションを示します。


 **メモ:** -p オプションはローカル RACADM でのみサポートされています。リモートまたはシリアル/telnet/ssh コンソールではサポートされていません。

表 A-10 fwupdate サブコマンドオプション

オプション	説明
-u	update オプションはファームウェアアップデートファイルのチェックサムを実行して、実際のアップデートプロセスを開始します。このオプションは -g または -p オプションと一緒に使用できます。アップデートの最後に iDRAC6 はソフトリセットを実行します。
-s	status オプションはアップデートプロセスの現在の状態を返します。このオプションは常に単一で使用します。
-g	get オプションは TFTP サーバーからファームウェアアップデートファイルを取得するようにファームウェアに指示します。ユーザーはまた -a と -d オプションも指定する必要があります。-a オプションが指定されていないとデフォルトで、プロパティ cfgRhostsFwUpdateIpAddr と cfgRhostsFwUpdatePath を使ってグループ cfgRemoteHosts に含まれているプロパティを読み込みます。
-a	TFTP アドレス オプションは、TFTP サーバの IP アドレスを指定します。
-d	-d (ディレクトリ) オプションは、ファームウェアアップデートファイルが保存されている TFTP サーバー上または iDRAC6 のホストサーバー上のディレクトリを指定します。
-p	-p (put) オプションは、ファームウェアファイルを管理下システムから iDRAC6 にアップデートするために使用します。-u オプションは -p オプションと一緒に使用する必要があります。
-r	ロールバック オプションを使用して、予備ファームウェアへロールバックします。

出力

どの操作を実行中かを示すメッセージを表示します。

例

```
1 racadm fwupdate -g -u -a 143.166.154.143 -d <パス>
```


この例では、-g オプションは、(-d で指定した) 特定の IP アドレスにある TFTP サーバー上の (-a オプションで指定した) 場所からファームウェアアップデートファイルをダウンロードするように指示します。TFTP サーバーからイメージファイルをダウンロードした後、アップデートプロセスが開始されます。完了時に iDRAC6 がリセットされます。

```
1 racadm fwupdate -s
```

このオプションは、ファームウェアアップデートの現在の状態を読み込みます。

```
1 racadm fwupdate -p -u -d <パス>
```

この例では、アップデートのファームウェアイメージがホストのファイルシステムによって提供されます。

 **メモ:** -p オプションは、fwupdate サブコマンドのリモート RACADM インターフェースではサポートされていません。

getssninfo


 **メモ:** このコマンドを使うには、iDRAC へのログイン 権限が必要です。

表 A-11 に、getssninfo サブコマンドについて説明します。

表 A-11 getssninfo サブコマンド

サブコマンド	定義
getssninfo	Session Manager のセッションテーブルから、1 つまたは複数の現在アクティブまたは保留中のセッションの情報を取得します。

概要

```
racadm getssninfo [-A] [-u <ユーザー名> | *]
```

説明

getssninfo コマンドは、iDRAC6 に接続しているユーザーのリストを返します。概要情報では次の情報が表示されます。

- 1 ユーザー名
- 1 IP アドレス（該当する場合）
- 1 セッションの種類（シリアル、telnet など）
- 1 使用コンソール（例：仮想メディア、仮想 KVM）

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

入力

[表 A-12](#) に、getssninfo サブコマンドオプションについて説明します。

表 A-12 getssninfo サブコマンドオプション

オプション	説明
-A	-A オプションを指定するとデータヘッダは印刷されません。
-u	-u <ユーザー名> ユーザー名オプションは、印刷出力を特定のユーザー名の詳細セッション記録だけに限定します。ユーザー名として「*」記号が入力されている場合は、すべてのユーザーが一覧になります。このオプションを指定すると、概要情報は印刷されません。

例

```
1 racadm getssninfo
```

[表 A-13](#) に racadm getssninfo コマンドの出力例を示します。

表 A-13 getssninfo サブコマンド出力例

ユーザー	IP アドレス	タイプ	Consoles
root	192.168.0.10	Telnet	Virtual KVM

```
1 racadm getssninfo -A
"root" "143.166.174.19" "Telnet" "NONE"
1 racadm getssninfo -A -u *
"root" "143.166.174.19" "Telnet" "NONE"
"bob" "143.166.174.19" "GUI" "NONE"
```

getsysinfo

 **メモ:** このコマンドを使うには、iDRAC へのログイン権限が必要です。

[表 A-14](#) に、racadm getsysinfo サブコマンドについて説明します。

表 A-14 getsysinfo

コマンド	定義
getsysinfo	IDRAC6 情報、システム情報、ウォッチドッグステータス情報を表示します。

概要

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-c] [-4] [-6] [-r]
```

説明

getsysinfo サブコマンドは、RAC 管理下システムに関する情報とウォッチドッグの設定を表示します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

入力

[表 A-15](#) に、getsysinfo サブコマンドオプションについて説明します。

表 A-15 getsysinfo サブコマンドオプション

オプション	説明
-4	IPv4 設定を表示します。
-6	IPv6 設定を表示します。
-c	共通設定を表示します。
-d	IDRAC6 情報を表示します。
-s	システム情報を表示します。
-w	ウォッチドッグ情報を表示します。
-A	ヘッダ / ラベルを印刷しません。

-w オプションを指定しないと、その他のオプションがデフォルトとして使用されます。

出力

getsysinfo サブコマンドは、RAC 管理下システムに関する情報とウォッチドッグの設定を表示します。

出力例

```
RAC Information:
RAC Date/Time = 10/01/2008 09:39:53
Firmware Version = 0.32
Firmware Build = 55729
Last Firmware Update = 09/25/2008 18:08:31
Hardware Version = 0.01
MAC Address = 00:1e:c9:b2:c7:1f

Common settings:
Register DNS RAC Name = 0
DNS RAC Name = IDRAC6
Current DNS Domain =
Domain Name from DHCP = 0

IPv4 settings:
Enabled = 1
Current IP Address = 192.168.0.120
```

```
Current IP Gateway = 192.168.0.1
Current IP Netmask = 255.255.255.0
DHCP Enabled = 0
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0
```

```
IPv6 settings:
Enabled = 0
Current IP Address 1 = 2002:0000:0000::0001
Current IP Gateway = ::
Prefix Length = 64
Autoconfig = 1
DNS Server from DHCPv6 = 0
Current DNS Server 1 = ::
Current DNS Server 2 = ::
```

```
System Information:
System Model = PowerEdge R610
System BIOS Version = 0.2.4
BMC Firmware Version = 0.32
Service Tag = AC056
Host Name =
OS Name =
Power Status = ON
```

```
Watchdog Information:
Recovery Action = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

```
Watchdog Information:
Recovery Action = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

例

```
l racadm getsysinfo -A -s

"System Information:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"

"Microsoft Windows 2000 version 5.0, Build Number 2195, Service Pack 2" "ON"

l racadm getsysinfo -w -s

System Information:
System Model = PowerEdge 2900
System BIOS Version = 0.2.3
BMC Firmware Version = 0.17
Service Tag = 48192
Host Name = racdev103
OS Name = Microsoft Windows Server 2003
Power Status = OFF

Watchdog Information:
Recovery Action = None
Present countdown value = 0 seconds
Initial countdown value = 0 seconds
```

制限

Dell™ OpenManage™ システムが管理下システムにインストールされているときにのみ、`getsysinfo` の出力のホスト名と OS 名フィールドに正確な情報が表示されます。管理下システムに OpenManage がインストールされていないと、これらのフィールドには空白または不正確な値が表示されます。

getractive


 **メモ:** このコマンドを使うには、iDRAC へのログイン 権限が必要です。

表 A-16 に、`getractive` サブコマンドについて説明します。

表 A-16 `getractive`

サブコマンド	定義
<code>getractive</code>	リモートアクセスコントローラから現在の時刻を表示します。

概要

```
racadm gettractime [-d]
```

説明

オプションを何も指定しないと、`gettractime` サブコマンドは時刻を一般的な形式で表示します。

`-d` オプションを指定すると、`gettractime` は時刻を `yyyymmddhhmmss.mmmmmms` 形式で表示します。これは UNIX `date` コマンドで返されるのと同じ形式です。

出力

`gettractime` サブコマンドは出力を 1 行で表示します。

出力例


```
racadm gettractime
Thu Dec 8 20:15:26 2005

racadm gettractime -d
20051208201542.000000
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

ifconfig

 **メモ:** このコマンドを使用するには、**診断コマンドの実行** または **iDRAC の設定** 権限が必要です。

[表 A-17](#) に、`ifconfig` サブコマンドを示します。

表 A-17 `ifconfig`

サブコマンド	定義
<code>ifconfig</code>	ネットワークインタフェーステーブルの内容を表示します。

概要

```
racadm ifconfig
```

netstat

 **メモ:** このコマンドを使用するには、**診断コマンドの実行** パーミッションが必要です。

[表 A-18](#) に、`netstat` サブコマンドを示します。

表 A-18 `netstat`

サブコマンド	定義
--------	----

サブコマンド	定義
netstat	ルーティングテーブルと現在の接続を表示します。


概要

```
racadm netstat
```

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

ping

 **メモ:** このコマンドを使うには、**診断コマンドの実行** または **iDRAC の設定** 権限が必要です。

[表 A-19](#) に、ping サブコマンドを示します。

表 A-19 ping

サブコマンド	定義
ping	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。宛先 IP アドレスが必要です。ICMP（インターネットコントロールメッセージプロトコル）エコーパケットが現在のルーティングテーブルの内容に基づいて宛先 IP アドレスに送信されます。


概要

```
racadm ping <IP アドレス>
```

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM


setniccfg

 **メモ:** setniccfg コマンドを使うには、**iDRAC の設定** 権限が必要です。

[表 A-20](#) に、setniccfg サブコマンドについて説明します。

表 A-20 setniccfg

サブコマンド	定義
setniccfg	コントローラの IP 設定を指定します。

 **メモ:** NIC と Ethernet 管理ポートは同じ意味で使われる場合があります。

概要

```
racadm setniccfg -d
```

```
racadm setniccfg -d6
```

```
racadm setniccfg -s <IPv4アドレス> <ネットマスク> <IPv4 ゲートウェイ>
```

```
racadm setniccfg -s6 <IPv6 アドレス> <IPv6 プレフィクス長> <IPv6 ゲートウェイ>
```

```
racadm setniccfg -o
```

説明

setniccfg サブコマンドは、コントローラの IPアドレスを設定します。

- 1 -d オプションは Ethernet 管理ポートの DHCP を有効にしま (デフォルトでは DHCP は無効です)。
- 1 -d6 オプションは Ethernet 管理ポートの AutoConfig を有効にします。これはデフォルトで有効になっています。
- 1 -s オプションは静的 IP 設定を有効にします。IPv4 アドレス、ネットマスク、ゲートウェイを指定できます。指定しなければ、既存の静的な設定が使用されます。<IPv4 アドレス>、<ネットマスク>および<ゲートウェイ> は、文字列をドットで区切って入力する必要があります。
- 1 -s6 オプションは静的 IPv6 設定を有効にします。IPv6 アドレス、プレフィクス長、および IPv6 ゲートウェイを指定できます。
- 1 -o オプションは Ethernet 管理ポートを完全に無効にします。

出力

setniccfg サブコマンドは操作に失敗した場合にエラーメッセージを表示します。成功した場合は、成功したことを知らせるメッセージが表示されます。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

getniccfg


 **メモ:** getniccfg コマンドを使うには、iDRAC へのログイン 権限が必要です。

表 A-21 に setniccfg と getniccfg サブコマンドを示します。

表 A-21 setniccfg/getniccfg

サブコマンド	定義
getniccfg	コントローラの現在の IP 設定を表示します。

概要

```
racadm getniccfg
```

説明

getniccfg サブコマンドは、現在の Ethernet 管理ポートの設定を表示します。

出力例


getniccfg サブコマンドは操作に失敗した場合にエラーメッセージを表示します。成功した場合は、出力が次の形式で表示されます。

```
NIC Enabled      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
```

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

getsvctag

 **メモ:** このコマンドを使うには、iDRAC へのログイン 権限が必要です。

[表 A-22](#) に getsvctag サブコマンドについて説明します。

表 A-22 getsvctag

サブコマンド	定義
getsvctag	サービスタグを表示します。

概要

racadm getsvctag

説明

getsvctag サブコマンドはホストシステムのサービスタグを表示します。

例

コマンドプロンプトで getsvctag と入力します。出力は次のように表示されます。


```
Y76TP0G
```

成功すると 0、エラーの場合はゼロ以外の値を返します。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

racdump

 **メモ:** このコマンドを使うには、デバッグ パーミッションが必要です。

[表 A-23](#) に racdump サブコマンドを示します。

表 A-23 racdump

サブコマンド	定義
racdump	ステータスおよび一般 iDRAC6 情報を表示します。

概要

racadm racdump

説明

racdump サブコマンドは、ダンプ、ステータスおよび一般 iDRAC 基板情報を取得する単一のコマンドを提供します。


racdump サブコマンドを処理すると、次の情報が表示されます。

- 1 システム / RAC の一般情報
- 1 コアダンプ
- 1 セッション情報
- 1 プロセス情報
- 1 ファームウェアビルド情報

対応インターフェース

- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM


racreset

 **メモ:** このコマンドを使うには、iDRAC の設定 権限が必要です。

[表 A-24](#) racreset サブコマンドについて説明します。

表 A-24 racreset

サブコマンド	定義
racreset	iDRAC6 をリセットします。

 **メモ:** racreset サブコマンドを発行すると、iDRAC6 が使用可能な状態に戻るまでに最大 1 分間かかることがあります。

概要

racadm racreset [hard | soft]

説明

racreset サブコマンドは iDRAC6 にリセットを発行します。リセットイベントは iDRAC6 ログに書き込まれます。

ハードリセットは RAC の深いリセットを行います。ハードリセットは、RAC を回復するための最終手段としてのみ実行してください。

 **メモ:** iDRAC6 のハードリセットを行った後は、「[表 A-25](#)」の説明に従ってシステムを再起動する必要があります。

[表 A-25](#) に、racreset サブコマンドを示します。

表 A-25 racreset サブコマンドオプション

オプション	説明
ハード	ハードリセットはリモートアクセスコントローラ (RAC) の深いリセットを行います。ハードリセットは、回復目的での最終手段として iDRAC6 コントローラをリセットするためにのみ使用してください。
ソフト	ソフトリセットは RAC の正常な再起動を行います。

例

```
1 racadm racreset
```

iDRAC6 のソフトリセットのシーケンスを開始します。


```
1 racadm racreset hard
```

iDRAC6 のハードリセットのシーケンスを開始します。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

racresetcfg

 **メモ:** このコマンドを使うには、iDRAC の **設定** 権限が必要です。

[表 A-26](#) は、**racresetcfg** サブコマンドについて説明しています。

表 A-26 **racresetcfg**

サブコマンド	定義
racresetcfg	iDRAC6 設定全体を工場出荷時のデフォルト値に戻します。

概要


```
racadm racresetcfg
```


対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM


説明

racresetcfg サブコマンドは、ユーザーが設定したデータベースプロパティのエントリをすべて削除します。データベースのすべてのエントリには、カードを最初のデフォルト設定に戻すために使用するデフォルトのプロパティがあります。データベースプロパティのリセット後、iDRAC6 は自動的にリセットされます。

 **メモ:** このコマンドは iDRAC6 の現在の設定を削除し、iDRAC6 とシリアル設定を最初のデフォルト設定に戻します。リセット後のデフォルト名とパスワードはそれぞれ **root** と **calvin** で、IP アドレスは 192.168.0.120 です。ネットワーククライアント（対応ウェブブラウザ、telnet/ssh、リモート RACADM など）から **racresetcfg** を発行する場合は、デフォルトの IP アドレスを使う必要があります。

 **メモ:** デフォルトへのリセットが完了するよう、特定の iDRAC6 ファームウェア プロセスを停止、再起動する必要があります。この動作が完了するまで約 30 秒間、iDRAC6 は応答しなくなります。

serveraction

 **メモ:** このコマンドを使用するには、**サーバー制御コマンドの実行** パーミッションが必要です。

[表 A-27](#) に、**serveraction** サブコマンドについて説明します。

表 A-27 **serveraction**

サブコマンド	定義
--------	----

サブコマンド	定義
serveraction	管理下システムのリセットまたは電源オン / オフ / サイクルを実行します。

概要

racadm serveraction <動作>

説明

serveraction サブコマンドを使うと、ホストシステムの電源管理を行うことができます。 [表 A-28](#) で、serveraction 電源管理オプションについて説明します。

表 A-28 serveraction サブコマンドオプション

文字列	定義
<処置>	処置を指定します。<処置> の文字列のオプションは以下のとおりです。 <ul style="list-style-type: none"> 1 powerdown - 管理下システムの電源を切ります。 1 powerup - 管理下システムの電源を入れます。 1 powercycle - 管理下システムの電源を入れ直します。この動作は、システムのプロントパネルの電源ボタンを押すことでシステムの電源を切ってから入れ直すのと同様です。 1 powerstatus - サーバーの現在の電源状態を表示します（「オン」または「オフ」）。 1 hardreset - 管理下システムのリセット（再起動）を行います。


出力

serveraction サブコマンドは、要求された動作が実行できなかった場合はエラーメッセージを表示し、要求された動作が正常に完了した場合は成功したことを知らせるメッセージを表示します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

getraclog

 **メモ:** このコマンドを使うには、iDRAC へのログイン 権限が必要です。

[表 A-29](#) で、racadm getraclog コマンドについて説明します。

表 A-29 getraclog

コマンド	定義
getraclog -i	iDRAC6 ログのエントリ数を表示します。
getraclog	iDRAC6 ログエントリを表示します。

概要

racadm getraclog -i


racadm getraclog [-A] [-o] [-c count] [-s start-record] [-m]

説明

getraclog -i コマンドは、iDRAC6 ログ内のエントリ数を表示します。

以下のオプションを使うと、`getraclog` コマンドでエントリを読み込むことができます。

- 1 `-A` - ヘッダやラベルなしで出力を表示します。
- 1 `-c` - 返されるエントリの最大数を指定します。
- 1 `-m` - 1 度に 1 画面分の情報を表示し、ユーザーに続行するように指示します（UNIX の `more` コマンドと同様）。
- 1 `-o` - 出力を 1 行に表示します。
- 1 `-s` - 表示する開始レコードを指定します。

 **メモ:** オプションを何も指定しないと、ログ全体が表示されます。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは 1 月 1 日の午前 0 時に始まり、システムが起動するまで進められます。システムが起動した後は、システムのタイムスタンプが使用されます。


出力例

```
Record:      1
Date/Time:   Dec 8 08:10:11
Source:      login[433]
Description: root login from 143.166.157.103
```

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

clrraclog

 **メモ:** このサブコマンドを使うには、**ログのクリア** パーミッションが必要です。


概要

racadm clrraclog

説明

`clrraclog` サブコマンドは、iDRAC6 のログから既存のレコードをすべて削除します。ログがクリアされると、新しいレコードが 1 つ作成されてその日付と時刻が記録されます。

getsel

 **メモ:** このコマンドを使うには、iDRAC への**ログイン** 権限が必要です。

[表 A-30](#) に、`getsel` コマンドについて説明します。

表 A-30 `getsel`

コマンド	定義
<code>getsel -i</code>	システムイベントログ 内のエントリ数を表示します。
<code>getsel</code>	SEL エントリを表示します。

概要

```
racadm getsel -i
```


```
racadm getsel [-E] [-R] [-A] [-o] [-c count] [-s count] [-m]
```

説明

`getsel -i` コマンドは SEL 内のエントリ数を表示します。

以下の `getsel` オプション（`-i` オプションなし）はエントリの読み込みに使います。

- A - ヘッダとラベルなしで表示します。
- c - 返されるエントリの最大数を指定します。
- o - 出力を 1 行に表示します。
- s - 表示する開始レコードを指定します。
- E - 各行の終りに生の SEL を 16 バイトほど 16 進値で出力します。
- R - 生のデータのみ出力します。
- m - 1 度に 1 画面分を表示し、ユーザーに続行するように指示します（UNIX の `more` コマンドと同様）。

 **メモ:** 引数を何も指定しないと、ログ全体が表示されます。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、重要度、説明が表示されます。


例:

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

clrsel

 **メモ:** このサブコマンドを使うには、**ログのクリア** パーミッションが必要です。

概要

```
racadm clrsel
```

説明

`clrsel` コマンドはシステムイベントログ (SEL) から既存のレコードをすべて削除します。

対応インターフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
 - 1 telnet/ssh/シリアル RACADM
-

gettracelog


 **メモ:** このコマンドを使うには、iDRAC へのログイン 権限が必要です。

表 A-31 に、gettracelog サブコマンドについて説明します。

表 A-31 gettracelog

コマンド	定義
gettracelog -i	iDRAC6 トレースログのエントリ数を表示します。
gettracelog	iDRAC6 のトレースログを表示します。

概要

```
racadm gettracelog -i
```

```
racadm gettracelog [-A] [-o] [-c count] [-s startrecord] [-m]
```

説明

gettracelog (-i オプションなし) コマンドはエントリを読み込みます。以下の gettracelog エントリを使ってエントリを読み込みます。

-i - iDRAC6 トレースログのエントリの数を表示します。

-m - 1 度に 1 画面分を表示し、ユーザーに続行するように指示します (UNIX の more コマンドと同様)。

-o - 出力を 1 行に表示します。

-c - 表示するレコード数を指定します。

-s - 表示を開始するレコードを指定します。

-A - ヘッダとラベルを表示しません。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは 1 月 1 日の午前 0 時に始まり、システムが起動するまで進められます。システムが起動した後は、システムのタイムスタンプが使用されます。

例:

```
Record:      1

Date/Time:  Dec 8 08:21:30

Source:      ssnmgrd[175]

Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

sslcsrgen


 **メモ:** このコマンドを使うには、iDRAC の設定 権限が必要です。

表 A-32 に、sslcsrgen サブコマンドについて説明します。

表 A-32 sslcsrgen

サブコマンド	説明
sslcsrgen	RAC から SSL 証明書署名要求 (CSR) を生成してダウンロードします。

概要

```
racadm sslcsrgen [-g] [-f <ファイル名>]
```

```
racadm sslcsrgen -s
```

説明

sslcsrgen サブコマンドを使って、CSR を生成し、クライアントのローカルファイルシステムにファイルをダウンロードできます。CSR は、RAC 上での SSL トランザクションに使用できるカスタム SSL 証明書の作成に使用できます。


オプション

 **メモ:** -f オプションは、シリアル/telnet/ssh コンソールではサポートされていません。

[表 A-33](#) に、**sslcsrgen** サブコマンドオプションについて説明します。

表 A-33 sslcsrgen サブコマンドオプション

オプション	説明
-g	新しい CSR を生成します。
-s	CSR 生成プロセスのステータスを返します (生成進行中、アクティブ、なし)。
-f	CSR をダウンロードする先の場所の <ファイル名> を指定します。

 **メモ:** -f オプションを指定しないと、ファイル名はデフォルトで現在のディレクトリ内の **sslcsr** になります。

オプションを何も指定しないと、生成された CSR はデフォルトでローカルファイルシステムに **sslcsr** としてダウンロードされます。-g オプション は -s オプションと一緒に使用できず、-f オプションは -g オプションと一緒にしか使用できません。

sslcsrgen -s サブコマンドは次のいずれかのステータスコードを返します。

- 1 CSR は正常に生成されました。
- 1 CSR はありません。
- 1 CSR の生成の進行中です。

制限

sslcsrgen サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できず、シリアル、telnet、SSH インタフェースでは使用できません。

 **メモ:** CSR を生成するには、その前に CSR フィールドを RACADM [cfgRacSecurity](#) グループで設定する必要があります。例: `racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany`

例

```
racadm sslcsrgen -s
```


または

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM

sslcertupload

 **メモ:** このコマンドを使うには、iDRAC の **設定** 権限が必要です。

[表 A-34](#) に、sslcertupload サブコマンドについて説明します。

表 A-34 sslcertupload

サブコマンド	説明
sslcertupload	カスタム SSL サーバーまたは CA 証明書をクライアントから RAC にアップロードします。

概要

```
racadm sslcertupload -t <種類> [-f <ファイル名>]
```

オプション

[表 A-35](#) に、sslcertupload サブコマンドオプションについて説明します。

表 A-35 sslcertupload サブコマンドオプション

オプション	説明
-t	アップロードする証明書の種類が CA 証明書かサーバー証明書を指定します。 1 = サーバー証明書 2 = CA 証明書
-f	アップロードする証明書のファイル名を指定します。ファイルを指定しないと、現在のディレクトリ内の sslcert ファイルが選択されます。

sslcertupload コマンドはアップロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

制限

sslcertupload サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できません。sslsrgen サブコマンドはシリアル、telnet、SSH インタフェースでは使用できません。


例

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM

sslcertdownload

 **メモ:** このコマンドを使うには、iDRAC の **設定** 権限が必要です。

[表 A-36](#) に、sslcertdownload サブコマンドについて説明します。

表 A-36 sslcertdownload

サブコマンド	説明
sslcertupload	SSL 証明書を iDRAC6 からクライアントのファイルシステムにダウンロードします。

概要

```
racadm sslcertdownload -t <種類> [-f <ファイル名>]
```

オプション

表 A-37 に、sslcertdownload サブコマンドオプションについて説明します。

表 A-37 sslcertdownload サブコマンドオプション

オプション	説明
-t	ダウンロードする証明書の種類が Microsoft® Active Directory® 証明書かサーバー証明書かを指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-f	アップロードする証明書のファイル名を指定します。-f オプションまたはファイル名が指定されていないと、現在のディレクトリ内の sslcert ファイルが選択されます。

sslcertdownload コマンドはダウンロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

制限

sslcertdownload サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できません。sslsrgen サブコマンドはシリアル、telnet、SSH インタフェースでは使用できません。

例

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM

sslcertview


 **メモ:** このコマンドを使うには、iDRAC の **設定** 権限が必要です。

表 A-38 に、sslcertview サブコマンドについて説明します。

表 A-38 sslcertview

サブコマンド	説明
sslcertview	RAC 上に存在する SSL サーバーまたは CA 証明書を表示します。

概要

```
racadm sslcertview -t <種類> [-A]
```


オプション

表 A-39 に、`sslcertview` サブコマンドオプションについて説明します。

表 A-39 `sslcertview` サブコマンドオプション

オプション	説明
-t	表示する証明書の種類が Microsoft Active Directory 証明書かサーバ証明書を指定します。 1 = サーバ証明書 2 = Microsoft Active Directory 証明書
-A	ヘッダー / ラベルを印刷しません。

出力例

```
racadm sslcertview -t 1

Serial Number          : 00

Subject Information:
Country Code (CC)     : US
State (S)              : Texas
Locality (L)          : Round Rock
Organization (O)      : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)      : iDRAC6 default certificate

Issuer Information:
Country Code (CC)     : US
State (S)              : Texas
Locality (L)          : Round Rock
Organization (O)      : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)      : iDRAC6 default certificate

Valid From             : Jul 8 16:21:56 2005 GMT
Valid To               : Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

sslkeyupload


 **メモ:** このコマンドを使うには、iDRAC の設定 権限が必要です。

表 A-40 に、`sslkeyupload` サブコマンドを示します。

表 A-40 `sslkeyupload`

--	--

サブコマンド	説明
sslkeyupload	SSL キーをクライアントから iDRAC6 にアップロードします。

概要

```
racadm sslkeyupload -t <種類> [-f <ファイル名>]
```

オプション

表 A-41 に、sslkeyupload サブコマンド オプションを示します。

表 A-41 sslkeyupload サブコマンドオプション

オプション	説明
-t	アップロードするキーを指定します。 1 = サーバー証明書の生成に使用する SSL キー
-f	アップロードする SSL キーのファイル名を指定します。

sslkeyupload コマンドはアップロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

制限

sslkeyupload サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できません。シリアル、SSH インタフェースでは使用できません。

例

```
racadm sslkeyupload -t 1 -f c:\sslkey.txt
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM

testemail

表 A-42 に、testemail サブコマンドについて説明します。

表 A-42 testemail の設定

サブコマンド	説明
testemail	RAC の電子メール警告機能をテストします。

概要

```
racadm testemail -i <索引>
```

説明

iDRAC6 から指定の宛先へテスト電子メールを送信します。

テスト電子メールコマンドを実行する前に、RACADM [cfgEmailAlert](#) グループ内の指定したインデックスが有効になっており、正しく設定されていることを確認してください。表 A-43 に、[cfgEmailAlert](#) グループのリストと関連するコマンドを示します。

表 A-43 testemail の設定

動作	コマンド
警告を有効にします。	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
宛先の電子メールアドレスを設定します。	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com
宛先の電子メールアドレスに送信するカスタムメッセージを設定します。	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "これはテストです"
SMTP の IP アドレスが正しく設定されていることを確認します。	racadm config -g cfgRemoteHosts -o cfgRhostsSmtplibAddr -i 192.168.0.152
現在の電子メール警告設定を表示します。	racadm getconfig -g cfgEmailAlert -i <索引> ここで、<索引> は 1~4 の数値です。

オプション

[表 A-44](#) に、testemail サブコマンドオプションについて説明します。

表 A-44 testemail サブコマンド

オプション	説明
-i	テストする電子メール警告の索引を指定します。

出力

なし。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

testtrap

 **メモ:** このコマンドを使うには、警告のテスト パーミッションが必要です。

[表 A-45](#) に、testtrap サブコマンドについて説明します。

表 A-45 testtrap

サブコマンド	説明
testtrap	RAC の SNMP トラップ警告機能をテストします。

概要

```
racadm testtrap -i <索引>
```

説明

testtrap サブコマンドは、iDRAC6 からネットワーク上の指定した宛先トラップリスナーにテストトラップを送信することで RAC の SNMP トラップ警告機能をテストします。

testtrap サブコマンドを実行する前に、RACADM [cfgIpmiPet](#) グループ内の指定した索引が正しく設定されていることを確認してください。

[表 A-46](#) に、[cfgIpmiPet](#)グループに関するコマンドを示します。

表 A-46 cfgEmailAlert コマンド

動作	コマンド
警告を有効にします。	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable 0 -i 1 1
宛先の電子メールの IP アドレスを設定します。	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
現在のテストトラップ設定を表示します。	racadm getConfig -g cfgIpmiPet -i <インデックス> ここで、<索引> は 1~4 の数値です。

入力

[表 A-47](#) に、testtrap サブコマンドオプションについて説明します。


表 A-47 testtrap サブコマンドオプション

オプション	説明
-i	テストに使うトラップ設定の索引を指定します。有効な値は 1~4 です。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

vmdisconnect

 **メモ:** このサブコマンドを使うには、**仮想メディアのアクセス** パーミッションが必要です。

[表 A-48](#) に、vmdisconnect サブコマンドについて説明します。

表 A-48 vmdisconnect

サブコマンド	説明
vmdisconnect	すべての開いているリモートクライアントからの iDRAC6 仮想メディア接続を閉じます。クライアントから閉じます。

概要

```
racadm vmdisconnect
```

説明

vmdisconnect サブコマンドを使うと、他のユーザーの仮想メディアセッションを切断できます。切断すると、そのウェブベースのインタフェースに正しい接続状態が表示されます。これは、ローカルまたはリモート RACADM を使ったのみ使用できます。

vmdisconnect サブコマンドを使うと、iDRAC6 ユーザーはアクティブな仮想メディアセッションをすべて切断できます。アクティブな仮想メディアセッションは、iDRAC6 ウェブ ベース インタフェースで、あるいは RACADM [getsysinfo](#) サブコマンドを使用して表示できます。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM

vmkey


 **メモ:** このサブコマンドを使うには、**仮想メディアのアクセス** パーミッションが必要です。

表 A-49 に、vmkey サブコマンドを示します。

表 A-49 vmkey

サブコマンド	説明
vmkey	仮想メディアキー関連の操作を行います。

概要

racadm vmkey <処置>

<処置> を **リセット** に設定すると、仮想フラッシュメモリはデフォルトサイズの 256 MB にリセットされます。

説明

カスタム仮想メディアキーイメージを RAC にアップロードすると、キーサイズがイメージサイズになります。vmkey サブコマンドは、キーを元のデフォルトサイズ (iDRAC6 上で 256MB) に戻すために使用できます。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/シリアル RACADM

usercertupload


 **メモ:** このコマンドを使うには、**iDRAC の設定** 権限が必要です。

表 A-50 に、usercertupload サブコマンドについて説明します。

表 A-50 usercertupload

サブコマンド	説明
usercertupload	ユーザー証明書またはユーザー CA 証明書をクライアントから iDRAC6 にアップロードします。

概要

racadm usercertupload -t <type> [-f <ファイル名>] -i <index>

オプション

表 A-51 に、usercertupload サブコマンドオプションを示します。

表 A-51 usercertupload サブコマンドオプション

オプション	説明
-------	----

-t	アップロードする証明書の種類が CA 証明書かサーバー証明書を指定します。 1 = ユーザー証明書 2 = ユーザー CA 証明書
-f	アップロードする証明書のファイル名を指定します。ファイルを指定しないと、現在のディレクトリ内の <code>sslcert</code> ファイルが選択されます。
-i	ユーザーのインデックス番号。有効な値は 1~16 です。

`usercertupload` コマンドはアップロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

制限

`usercertupload` サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できません。


例

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM

usercertview

 **メモ:** このコマンドを使うには、**IDRAC の設定** 権限が必要です。

[表 A-52](#) に、`usercertview` サブコマンドを示します。

表 A-52 `usercertview`

サブコマンド	説明
<code>usercertview</code>	IDRAC6 上にあるユーザー証明書またはユーザー CA 証明書を表示します。

概要

```
racadm sslcertview -t <type> [-A] -i <インデックス>
```

オプション

[表 A-53](#) に、`sslcertview` サブコマンドオプションについて説明します。

表 A-53 `sslcertview` サブコマンドオプション

オプション	説明
-t	表示する証明書の種類が ユーザー証明書かユーザー CA 証明書を指定します。 1 = ユーザー証明書 2 = ユーザー CA 証明書
-A	ヘッダー / ラベルを印刷しません。
-i	ユーザーのインデックス番号。有効な値は 1~16 です。

対応インターフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
 - 1 telnet/ssh/シリアル RACADM
-

localConRedirDisable

 **メモ:** このコマンドはローカル RACADM ユーザーしか実行できません。

[表 A-54](#) に、localConRedirDisable サブコマンドを示します。

表 A-54 localConRedirDisable

サブコマンド	説明
localConRedirDisable	管理ステーションへのコンソールリダイレクトを無効にします。

概要

```
racadm localConRedirDisable <オプション>
```

<オプション> を 1 に設定すると、コンソールリダイレクトが無効になります。

<オプション> を 0 に設定すると、コンソールリダイレクトが有効になります。

対応インターフェース

- 1 ローカル RACADM
-

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 プロパティデータベースグループとオブジェクト定義

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [表示可能な文字](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgRemoteHosts](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgOobSnmp](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgStandardSchema](#)
- [cfgIpmiSoj](#)
- [cfgIpmiLan](#)
- [cfgIpmiPetIpv6](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)
- [cfgUserDomain](#)
- [cfgServerPower](#)
- [cfgIPv6LanNetworking](#)
- [cfgIPv6URL](#)
- [cfgIpmiSerial](#)
- [cfgSmartCard](#)
- [cfgNetTuning](#)

iDRAC6 プロパティデータベースには iDRAC6 の設定情報が含まれています。データは関連オブジェクト別に整理され、オブジェクトはオブジェクトグループ別に整理されています。本項には、プロパティデータベースでサポートされているグループとオブジェクトの ID のリストが掲載されています。

RACADM ユーティリティでこれらのグループとオブジェクト ID を使って iDRAC6 を設定します。以下の各項で、それぞれのオブジェクトについて説明し、オブジェクトが読み取り可能か、書き込み可能か、またはその両方が可能であるかを示します。

文字列の値は、特に記載のない限り、表示可能な ASCII 文字のみとします。

表示可能な文字

表示可能な文字には以下の文字セットが含まれます。

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#\$%^&*()_+={}|~\:'<>.,?/

idRacInfo

このグループにはクエリされる iDRAC6 の特定の情報を提供するための表示パラメータが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

idRacProductInfo (読み取り専用)

有効値

最大 63 文字の ASCII 文字列。

デフォルト

iDRAC (Integrated Dell Remote Access Controller)

説明

製品を識別するテキスト文字列。

idRacDescriptionInfo (読み取り専用)

有効値

最大 255 文字の ASCII 文字列。

デフォルト

このシステムコンポーネントは Dell PowerEdge サーバー用のリモート管理機能一式をすべて提供します。

説明

iDRAC のタイプを説明するテキスト。

idRacVersionInfo (読み取り専用)

有効値

最大 63 文字の ASCII 文字列。

デフォルト

<現在のバージョン番号>

説明

現在の製品ファームウェアバージョンを示す文字列。

idRacBuildInfo (読み取り専用)

有効値

最大 16 文字の ASCII 文字列。

デフォルト

現在の iDRAC6 ファームウェアビルドバージョン。

説明

現在の製品ビルドバージョンを示す文字列。

idRacName (読み取り専用)

有効値

最大 15 文字の ASCII 文字列。

デフォルト

iDRAC

説明

このコントローラを識別するためにユーザーが割り当てた名前。

idRacType (読み取り専用)

有効値

プロダクト ID

デフォルト

10

説明

リモート アクセス コントローラーのタイプを iDRAC6 と識別します。

cfgLanNetworking

このグループには iDRAC6 NIC を設定するためのパラメータが格納されています。

このグループでは 1 つのインスタンスが使用できます。このグループのいくつかのオブジェクトで iDRAC6 NIC がリセットされる必要があり、このため接続が一時的に途絶える場合があります。iDRAC6 NIC IP アドレス設定を変更するオブジェクトによってすべてのアクティブなユーザーセッションが閉じられるので、ユーザーはアップデートされた IP アドレス設定を使って再接続する必要があります。

cfgNicIPv4Enable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC6 IPv4 スタックを有効または無効にします。

cfgNicSelection (読み取り / 書き込み)

有効値

0 = 共有

1 = フェイルオーバー LOM2 で共有

2 = 専用

3 = すべてのフェイルオーバー LOM で共有 (iDRAC6 Enterprise のみ)

デフォルト

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

説明

RAC ネットワークインタフェースコントローラ (NIC) の現在の動作モードを指定します。 [表 B-1](#) にサポートされているモードを示します。

表 B-1 cfgNicSelection でサポートされているモード

モード	説明
共有	ホストサーバー組み込み NIC がホストサーバー上で RAC と共有されている場合に使います。このモードでは、ネットワーク上でホストサーバーと RAC に共通してアクセスできるように同一の IP アドレスを使用できます。
フェイルオーバーで共有: LOM 2	ホストサーバー LOM2 組み込みネットワークインタフェースコントローラ間でのチーム機能を有効にします。
専用	RAC NIC をリモートアクセシビリティ専用 NIC として使うことを指定します。
すべてのフェイルオーバー LOM で共有	ホストサーバー内蔵ネットワークインタフェースコントローラ上のすべての LOM 間でチーム機能を有効にします。 リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムが NIC チューニング用に設定されている場合完全に機能します。リモートアクセスデバイスは NIC 1 と NIC 2 を通じてデータを受信しますが、データの送信は NIC 1 を通じてのみ行います。フェイルオーバーは、NIC 2 から NIC 3 へ、次に NIC 4 へと発生します。NIC 4 が故障した場合、リモート アクセス デバイスはすべての伝送を NIC 1 へ戻します。ただし、これは最初の NIC 1 の障害が修復済みである場合のみです。

cfgNicVlanEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC/BMC の VLAN 機能を有効または無効にします。

cfgNicVlanId (読み取り / 書き込み)

有効値

1~4094

デフォルト

1

説明

ネットワーク VLAN 設定用に VLAN ID を指定します。このプロパティは、cfgNicVlanEnable が 1 (有効) に設定されている場合にのみ有効です。

cfgNicVlanPriority (読み取り / 書き込み)

有効値

0~7

デフォルト

0

説明

ネットワーク VLAN 設定用に VLAN の優先順位を指定します。このプロパティは、cfgNicVlanEnable が 1 (有効) に設定されている場合にのみ有効です。

cfgDNSDomainNameFromDHCP (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0


説明

iDRAC6 DNS ドメイン名をネットワークの DHCP サーバーから割り当てる必要があることを指定します。

cfgDNSDomainName (読み取り / 書き込み)

有効値

最大 254 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。文字は英数字、「-」 および 「.」に制限されています。

 **メモ:** Microsoft® Active Directory® は、64 バイト以下の完全修飾ドメイン名 (FQDN) しかサポートしていません。

デフォルト

<空白>


説明

これは DNS ドメイン名です。

cfgDNSRacName (読み取り / 書き込み)

有効値

最大 63 文字の ASCII 文字列。少なくとも 1 文字は英字でなければなりません。

 **メモ:** 一部の DNS サーバーは 31 文字以内の名前しか登録しません。

デフォルト

idrac-<サービスタグ>

説明

デフォルトの iDRAC6 名 rac-サービスタグ が表示されます。このパラメータは、cfgDNSRegisterRac が 1 (TRUE) に設定されているときにのみ有効です。

cfgDNSRegisterRac (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバーに iDRAC6 の名前を登録します。

cfgTrapsSnmpFromDHCP (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバーの IPv4 アドレスをネットワーク上の DHCP サーバーから割り当てることを指定します。

cfgDNSServer1 (読み取り / 書き込み)

有効値

有効な IPv4 アドレスを表す文字列。例: 192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 1 の IPv4 アドレスを指定します。

cfgDNSServer2 (読み取り / 書き込み)

有効値

有効な IPv4 アドレスを表す文字列。例: 192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 2 の IPv4 アドレスを取得します。

cfgNicEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)


デフォルト

1

説明

iDRAC6 ネットワークインタフェースコントローラを有効または無効にします。NIC を無効にした場合、iDRAC6 へのリモートネットワークインタフェースはアクセスできません。

cfgNicIpAddress (読み取り / 書き込み)

 **メモ:** このパラメータは、cfgNicUseDhcp パラメータが 0 (FALSE) に設定されているときのみ設定できます。

有効値

有効な IPv4 アドレスを表す文字列。例: 192.168.0.20


デフォルト

192.168.0.120

説明

iDRAC6 に割り当てた IPv4 アドレスを指定します。

cfgNicNetmask (読み取り / 書き込み)

 **メモ:** このパラメータは、`cfgNicUseDhcp` パラメータが 0 (FALSE) に設定されているときにのみ設定できます。

有効値

有効なサブネットマスクを表す文字列。例: 255.255.255.0


デフォルト

255.255.255.0

説明

iDRAC6 IP アドレスに使用するサブネットマスク

cfgNicGateway (読み取り / 書き込み)

 **メモ:** このパラメータは、`cfgNicUseDhcp` パラメータが 0 (FALSE) に設定されているときにのみ設定できます。

有効値

有効な ゲートウェイ IPv4 アドレスを表す文字列。例: 192.168.0.1

デフォルト

192.168.0.1

説明

iDRAC6 ゲートウェイ IPv4 アドレス

cfgNicUseDhcp (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC の IPv4 アドレスの割り当てに DHCP を使用するかどうかを指定します。このプロパティを 1 (TRUE) に設定すると、iDRAC の IPv4 アドレス、サブネットマスク、ゲートウェイがネットワーク上の DHCP サーバーから割り当てられます。このプロパティを 0 (FALSE) に設定すると、ユーザーは `cfgNicIpAddress`、`cfgNicNetmask`、および `cfgNicGateway` プロパティを設定できます。

cfgNicMacAddress (読み取り専用)

有効値

iDRAC6 NIC MAC アドレスを表す文字列。

デフォルト

iDRAC6 NIC の現在の MAC アドレス。例: 00:12:67:52:51:A3

説明

iDRAC6 NIC の MAC アドレス。

cfgRemoteHosts

このグループは、電子メール警告用の SMTP サーバーの設定を可能にするプロパティを提供します。

cfgRhostsFwUpdateTftpEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

ネットワーク TFTP サーバーからの iDRAC6 ファームウェアのアップデートを有効または無効にします。

cfgRhostsFwUpdateIpAddr (読み取り / 書き込み)

有効値

有効な IPv4 アドレスを表す文字列。例: 192.168.0.61

デフォルト

0.0.0.0

説明

TFTP iDRAC6 ファームウェアのアップデートに使うネットワーク TFTP サーバー IPv4 アドレスを指定します。

cfgRhostsFwUpdatePath (読み取り / 書き込み)

有効値


最大 255 文字の ASCII 文字列。

デフォルト

<空白>

説明

TFTP サーバー上の iDRAC6 ファームウェアイメージファイルの TFTP パスを指定します。TFTP パスは、TFTP サーバー上の TFTP ルートパスの相対パスです。

 **メモ:** それでもドライブを指定する必要があることがあります (例: C:)。

cfgRhostsSmtServerIpAddr (読み取り / 書き込み)

有効値

有効なSMTP サーバー IPv4 アドレスを表す文字列。例: 192.168.0.55

デフォルト

0.0.0.0

説明

ネットワーク SMTP サーバーまたは TFTP サーバーの IPv4 アドレス。SMTP サーバーは、警告が設定されて有効になっていれば、iDRAC6 から電子メール警告を送信します。TFTP サーバーはファイルを iDRAC6 に対して送受信します。

cfgUserAdmin

このグループは、使用可能なリモートインタフェース経由で iDRAC6 へのアクセスが許可されているユーザーについての設定情報を提供します。

最大 16 のユーザーグループのインスタンスを使用できます。各インスタンスは各ユーザーの設定を表します。

cfgUserAdminIndex (読み取り専用)

有効値

1 ~ 16

デフォルト

インスタンス

説明

この数値はユーザーインスタンスを表します。

cfgUserAdminIpmiLanPrivilege (読み取り / 書き込み)

有効値

2 (ユーザー)

3 (オペレータ)

4 (Administrator: システム管理者)

15 (アクセスなし)

デフォルト

4 (ユーザー 2)

15 (その他すべて)

説明

IPMI LAN チャネル上での最大権限。

cfgUserAdminPrivilege (読み取り / 書き込み)

有効値

0x00000000 ~ 0x000001ff、および 0x0

デフォルト

0x00000000

説明

このプロパティは、ユーザーのロール（役割）ベースの権限を指定します。値は、権限の値を自由に組み合わせることのできるビットマスクとして表します。表 B-2 に、組み合わせてビットマスクを作成できるユーザー権限ビット値について説明します。

表 B-2 ユーザー権限に応じたビットマスク

ユーザー権限	権限ビットマスク
iDRAC へのログイン	0x00000001
iDRAC の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100


例

表 B-3 に、1 つまたは複数の権限を持つユーザーの権限ビットマスクの例を示します。

表 B-3 ユーザー権限ビットマスクの例

ユーザー権限	権限ビットマスク
ユーザーは iDRAC にアクセスできません。	0x00000000
ユーザーは iDRAC にログインして iDRAC とサーバーの設定情報を表示することのみできます。	0x00000001
ユーザーは iDRAC にログインして設定を変更できます。	0x00000001 + 0x00000002 = 0x00000003
ユーザーは iDRAC にログインして、仮想メディアにアクセスし、コンソールリダイレクトにアクセスできます。	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (読み取り / 書き込み)

 **メモ:** このプロパティ値は、ユーザー名で固有の値でなくてはなりません。

有効値

最大 16 文字の ASCII 文字列。


デフォルト

root (ユーザー 2)

<空白> (他のすべてのユーザー)

説明

この索引のユーザーの名前。索引に何も入っていない場合は、文字列をこの名前フィールドに書き込むとユーザー索引が作成されます。二重引用符 (“”) の文字列を書き込むと、その索引のユーザーが削除されます。文字列に / (フォワードスラッシュ)、\ (バックスラッシュ)、. (ピリオド)、@ (アット記号) および引用符を含めることはできません。

 **メモ:** このプロパティ値は、ユーザー名で固有の値でなくてはなりません。

cfgUserAdminPassword (書き込み専用)

有効値

最大 20 文字の ASCII 文字列。

デフォルト

説明

このユーザーのパスワード。ユーザーパスワードは暗号化され、プロパティに書き込んだ後は参照や表示ができなくなります。

cfgUserAdminEnable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1 (ユーザー 2)

0 (他のすべてのユーザー)

説明

ユーザーを個別に有効または無効にします。

cfgUserAdminSolEnable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

ユーザー用のシリアルオーバー LAN (SOL) ユーザーアクセスを有効または無効にします。

cfgUserAdminIpmiSerialPrivilege (読み取り / 書き込み)

有効値

2 (ユーザー)

3 (オペレータ)

4 (Administrator: システム管理者)

15 (アクセスなし)

デフォルト

4 (ユーザー 2)

15 (その他すべて)

説明

IPMI LAN チャンネル上での最大権限。

cfgEmailAlert

このグループには、iDRAC6 電子メール警告機能を設定するためのパラメータが入っています。

以下の各項では、このグループの各オブジェクトについて説明します。このグループは 4 つのインスタンスまで使用できます。

cfgEmailAlertIndex (読み取り専用)

有効値

1~4

デフォルト

<インスタンス>

説明

警告インスタンスの固有の索引。

cfgEmailAlertEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

警告インスタンスを有効または無効にします。

cfgEmailAlertAddress (読み取り/書き込み)

有効値

電子メールアドレス形式、最大 64 文字の ASCII 文字列。

デフォルト

<空白>

説明

電子メール用送信先電子メールアドレスを指定します。例: user1@company.com

cfgEmailAlertCustomMsg (読み取り/書き込み)

有効値

最大 32 文字の ASCII 文字列。

デフォルト

<空白>

説明

警告の件名を示すカスタムメッセージを指定します。

cfgSessionManagement

このグループには、iDRAC6 に接続できるセッション数を設定するパラメータが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgSsnMgtRacadmTimeout（読み取り / 書き込み）

有効値

10~1920

デフォルト

60

説明

リモート RACADM インタフェースの無動作タイムアウト待ち時間（秒）を定義します。リモート RACADM セッションで指定した秒数以上無動作状態が続いた場合、そのセッションは閉じられます。

cfgSsnMgtConsRedirMaxSessions（読み取り / 書き込み）

有効値

1~4

デフォルト

2

説明

iDRAC6 で許可されるコンソールリダイレクトセッションの最大数を指定します。

cfgSsnMgtWebserverTimeout（読み取り / 書き込み）

有効値

60 ~ 10800

デフォルト

1800

説明

ウェブサーバーの無動作時間を定義します。このプロパティでは、接続がアイドル（ユーザー入力なし）な状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、セッションはキャンセルされます。この設定を変更しても現在のセッションには影響はありません（新しい設定を有効にするには、ログアウトしてからログインし直す必要があります）。

cfgSsnMgtSshIdleTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60~1920

デフォルト

300

説明

セキュアシェルのアイドルタイムアウトを定義します。このプロパティでは、接続がアイドル（ユーザー入力なし）な状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、セッションはキャンセルされます。この設定を変更しても現在のセッションには影響はありません（新しい設定を有効にするには、ログアウトしてからログインし直す必要があります）。

期限の切れたセキュアシェルセッションは次のエラーメッセージを表示します。

```
Connection timed out (接続タイムアウト)
```

メッセージが表示された後、セキュアシェルセッションを生成したシェルに戻ります。

cfgSsnMgtTelnetTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60～1920

デフォルト

300

説明

telnet アイドルタイムアウトを定義します。このプロパティでは、接続がアイドル（ユーザー入力なし）な状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、セッションはキャンセルされます。この設定を変更しても、現在のセッションには影響しません（新しい設定を有効にするには、ログアウトしてログインする必要があります）。

期限の切れたセキュアシェルセッションは次のエラーメッセージを表示します。

```
Connection timed out (接続タイムアウト)
```

メッセージが表示された後、Telnet セッションを生成したシェルに戻ります。

cfgSerial

このグループには、iDRAC6 サービスの設定パラメータが含まれます。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgSerialBaudRate（読み取り / 書き込み）

有効値

9600、28800、57600、115200

デフォルト

57600

説明

iDRAC6 シリアルポートのボーレートを設定します。

cfgSerialConsoleEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC シリアルコンソールインタフェースを有効または無効にします。


cfgSerialConsoleQuitKey (読み取り / 書き込み)

有効値

最大 4 文字の文字列。

デフォルト

^^ (<Ctrl><^>)

 **メモ:** 「^」は <Ctrl> キーを示します。

説明

connect com2 コマンドを使用しているときに、このキーまたはキーの組み合わせによってテキストコンソールリダイレクトを終了できます。cfgSerialConsoleQuitKey の値は、次のいずれかで表すことができます。

- 1 10 進数 - 例: 95
- 1 16 進数 - 例: 0x12
- 1 8 進数 - 例: 007
- 1 ASCII 値 - 例: ^a

ASCII 値は次のエスケープキーコードを使って表すことができます。

- (a) ^ と任意の英字 (a-z, A-Z)
- (b) ^ と特殊文字 [] \ ^ _

cfgSerialConsoleIdleTimeout (読み取り / 書き込み)

有効値

0 = タイムアウトなし

60~1920

デフォルト

300

説明

無動作状態のシリアルセッションを切断するまでの最大待ち時間を秒で指定します。

cfgSerialConsoleNoAuth（読み取り / 書き込み）

有効値

0（シリアルログイン認証を有効にする）

1（シリアルログイン認証を無効にする）

デフォルト

0

説明

RAC シリアルコンソールログイン認証を有効または無効にします。

cfgSerialConsoleCommand（読み取り / 書き込み）

有効値

最大 128 文字の文字列。

デフォルト

<空白>

説明

ユーザーがシリアルコンソールインタフェースにログインした後実行するシリアルコマンドを指定します。

cfgSerialHistorySize（読み取り / 書き込み）

有効値

0~8192

デフォルト

8192

説明

シリアル履歴バッファの最大サイズを指定します。

cfgSerialCom2RedirEnable (読み取り / 書き込み)

デフォルト

1

有効値

1 (TRUE)

0 (FALSE)

説明

COM 2 ポートリダイレクト用のコンソールを有効または無効にします。

cfgSerialSshEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC6 の セキュアシェル (SSH) インタフェースを有効または無効にします。

cfgSerialTelnetEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の Telnet コンソールインタフェースを有効または無効にします。

cfgOobSnmp

このグループは、iDRAC6 の SNMP エージェントとトラップ機能を設定するパラメータを持っています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgOobSnmpAgentCommunity (読み取り / 書き込み)

有効値

最大 31 文字の文字列。

デフォルト

public

説明

SNMP トラップに使う SNMP コミュニティ名を指定します。

cfgOobSnmpAgentEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の SNMP エージェントを有効または無効にします。

cfgRacTuning

このグループは、有効なポートやセキュリティポート制限など、iDRAC6 の各種設定プロパティの設定に使用します。

cfgRacTuneConRedirPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

5900

説明

RAC へのキーボード、マウス、ビデオ、および仮想メディアのトラフィックに使用するポートを指定します。

cfgRacTuneRemoteRacadmEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC のリモート RACADM インタフェースを有効または無効にします。

cfgRacTuneCtrlEConfigDisable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

ローカルユーザーが BIOS POST オプション ROM から iDRAC を設定できる機能を無効にする機能を有効または無効にします。

cfgRacTuneHttpPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

80

説明

iDRAC6 との HTTP ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneHttpsPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

443

説明

iDRAC6 との HTTPS ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneIpRangeEnable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の IPv4 アドレス範囲の検証機能を有効または無効にします。

cfgRacTuneIpRangeAddr (読み取り/書き込み)

有効値

IPv4 アドレスフォーマット済み文字列、例: 192.168.0.44

デフォルト

192.168.1.1

説明

範囲マスクプロパティ (cfgRacTuneIpRangeMask) で 1 で決定される IPv4 アドレスビットパターンの可能な位置を指定します。

cfgRacTuneIpRangeMask (読み取り/書き込み)

有効値

IPv4 アドレスフォーマット済み文字列、例: 255.255.255.0

デフォルト

255.255.255.0

説明

左寄せビットを使用した標準的な IP マスク値 例: 255.255.255.0

cfgRacTuneIpBlkEnable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の IPv4 アドレスブロック機能を有効または無効にします。

cfgRacTuneIpBlkFailCount (読み取り/書き込み)

有効値

2~16

デフォルト

5

説明

ウィンドウ (cfgRacTuneIpBlkFailWindow) 内で何回ログインに失敗したら、この IP アドレスからのログイン試行が拒否されるかを指定します。

cfgRacTuneIpBlkFailWindow (読み取り/書き込み)

有効値

10~65535

デフォルト

60

説明

ログインの失敗を数える時間枠を秒で定義します。ログイン試行がこの制限時間に達すると、失敗回数カウントはゼロにリセットされます。

cfgRacTuneIpBlkPenaltyTime (読み取り/書き込み)

有効値

10~65535

デフォルト

300

説明

失敗回数が制限値を超えた IP アドレスからのセッション要求を拒否する時間枠を秒で定義します。

cfgRacTuneSshPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

22

説明

iDRAC の SSH インタフェースに使用するポート番号を指定します。

cfgRacTuneTelnetPort (読み取り / 書き込み)

有効値

1~65535

デフォルト

23

説明

iDRAC6 の telnet インタフェースに使用するポート番号を指定します。

cfgRacTuneConRedirEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

コンソールリダイレクトを有効にします。

cfgRacTuneConRedirEncryptEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)


デフォルト

1

説明

コンソールリダイレクトのセッションでビデオを暗号化します。

cfgRacTuneAsrEnable (読み取り / 書き込み)

 **メモ:** このオブジェクトは、アクティブになる前に iDRAC6 をリセットする必要があります。

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の前回クラッシュ画面キャプチャ機能を有効または無効にします。

cfgRacTuneLocalServerVideo (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

ローカルサーバービデオを有効 (スイッチオン) または無効 (スイッチオフ) にします。

cfgRacTuneLocalConfigDisable (読み取り/書き込み)

有効値

0 (TRUE)

1 (FALSE)

デフォルト

0

説明

1 に設定することにより、iDRAC6 設定データへの書き込みアクセスを無効にします。

cfgRacTuneWebserverEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC6 ウェブサーバーを有効または無効にします。このプロパティを無効にすると、クライアントのウェブブラウザを使用して iDRAC6 にアクセスできなくなります。このプロパティは Telnet/SSH またはローカル RACADM インタフェースには影響しません。

ifcRacManagedNodeOs

このグループには、管理下サーバーのオペレーティングシステムを記述するプロパティが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

ifcRacMnOsHostname (読み取り専用)

有効値

最大 255 文字の文字列。

デフォルト

<空白>

説明

管理下サーバーのホスト名。

ifcRacMnOsOsName (読み取り専用)

有効値

最大 255 文字の文字列。

デフォルト

<空白>

説明

管理下サーバーのオペレーティングシステム名。

cfgRacSecurity

このグループは、iDRAC6 SSL 証明書署名要求 (CSR) 機能に関連するオプションを設定するために使用します。このグループのプロパティは、iDRAC6 から CSR を生成する前に設定する必要があります。

証明書署名要求の生成の詳細については、RACADM [sslcsrgen](#) サブコマンドを参照してください。

cfgRacSecCsrCommonName (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

証明書に示してある IP または iDRAC 名である必要のある CSR 共通名 (CN) を指定します。

cfgRacSecCsrOrganizationName (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 組織名 (O) を指定します。

cfgRacSecCsrOrganizationUnit (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 部門名 (OU) を指定します。

cfgRacSecCsrLocalityName (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 地域 (L) を指定します。

cfgRacSecCsrStateName (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 都道府県名 (S) を指定します。

cfgRacSecCsrCountryCode (読み取り / 書き込み)

有効値

最大 2 文字の文字列。

デフォルト

<空白>

説明

CSR 国番号 (CC) を指定します。

cfgRacSecCsrEmailAddr (読み取り / 書き込み)

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR の電子メールアドレスを指定します。

cfgRacSecCsrKeySize (読み取り / 書き込み)

有効値

1024

2048

4096

デフォルト

1024

説明

CSR の非対称キーサイズを指定します。

cfgRacVirtual

このグループには iDRAC6 仮想メディア機能を設定するためのパラメータが含まれています。このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgVirMediaAttached (読み取り / 書き込み)

有効値

0 = 分離

1 = 連結

2 = 自動連結

デフォルト

0

説明

このオブジェクトは、USB バスを介して仮想デバイスをシステムに接続するために使用されます。デバイスを接続すると、サーバーは、システムに接続された有効な USB 大容量記憶装置を認識します。これは、ローカル USB CD-ROM/ フロッピードライブをシステムの USB ポートに接続する場合と同じです。デバイスが接続されると、iDRAC6 の ウェブインタフェースまたは CLI を使用してこれらの仮想デバイスにリモート接続できるようになります。このオブジェクトを 0 に設定すると、デバイスは USB バスから切断されます。

cfgVirtualBootOnce (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)


デフォルト

0

説明

iDRAC6 の仮想メディアのブートワンス機能を有効または無効にします。

cfgVirMediaFloppyEmulation (読み取り/書き込み)

 **メモ:** この変更を有効にするには、(VirMediaAttached を使用して) 仮想メディアを再連結する必要があります。

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

0 に設定されている場合、仮想フロッピードライブは Windows オペレーティングシステムにより、リムーバブルディスクとして認識されます。Windows オペレーティングシステムは列挙中に C: 以降のドライブ文字を割り当てます。1 に設定されている場合、仮想フロッピードライブは Windows オペレーティングシステムにより、フロッピードライブとして認識されます。Windows オペレーティングシステムは A: または B: のドライブ文字を割り当てます。

cfgVirMediaKeyEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の仮想メディアキー機能を有効または無効にします。

cfgActiveDirectory

このグループには iDRAC6 Active Directory 機能を設定するためのパラメータが格納されています。

cfgADracDomain (読み取り / 書き込み)

有効値

空白スペースなしの最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

iDRAC6 が置かれている Active Directory ドメイン。

cfgADracName (読み取り / 書き込み)

有効値

空白スペースなしの最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

Active Directory フォレストに記録された iDRAC6 名。

cfgADenable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 で Active Directory によるユーザー認証を有効または無効にします。このプロパティを無効にすると、ユーザーログインにローカルの iDRAC6 認証のみが使用されます。

cfgADDomainController1 (読み取り/書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDRAC6 は指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADDomainController2 (読み取り/書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDRAC6 は指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADDomainController3 (読み取り/書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDRAC6 は指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADAuthTimeout (読み取り / 書き込み)

有効値

15 ~ 300 秒

デフォルト

120

説明

Active Directory 認証要求の完了がタイムアウトになるまでの時間を秒で指定します。

cfgADType (読み取り / 書き込み)

有効値

1 (拡張スキーマ)

2 (標準スキーマ)

デフォルト

1

説明

Active Directory と併用するスキーマタイプを指定します。

cfgADGlobalCatalog1 (読み取り/書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDDRAC6 は指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADGlobalCatalog2 (読み取り/書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDDRAC6 は指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADGlobalCatalog3 (読み取り/書き込み)

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDDRAC6 は指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADCertValidationEnable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

Active Directory 設定プロセスの一部として Active Directory 証明書検証を有効または無効にします。

cfgStandardSchema

このグループには Active Directory 標準スキーマ設定を行うためのパラメータが格納されています。

cfgSSADRoleGroupIndex (読み取り専用)

有効値

1 ~ 5 の整数。

デフォルト

<インスタンス>

説明

Active Directory で記録したロール (役割) グループの索引。

cfgSSADRoleGroupName（読み取り / 書き込み）

有効値

空白スペースなしの最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

Active Directory フォレストで記録したロール（役割）グループの名前。

cfgSSADRoleGroupDomain（読み取り / 書き込み）

有効値

空白スペースなしの最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

ロール（役割）グループが置かれている Active Directory ドメイン。

cfgSSADRoleGroupPrivilege（読み取り / 書き込み）

有効値

0x00000000~0x000001ff

デフォルト

<空白>

説明

[表 B-4](#) のビットマスク番号を使って、ロール（役割）グループのロール（役割）ベースの権限を設定します。

表 B-4 ロール（役割）グループの権限のビットマスク

ロールグループの権限	ビットマスク
IDRAC へのログイン	0x00000001
IDRAC の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020

仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100

cfgIpmiSol

このグループは、システムのシリアルオーバー LAN (SOL) 機能の設定に使用されます。

cfgIpmiSolEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

SOL を有効または無効にします。

cfgIpmiSolBaudRate (読み取り / 書き込み)

有効値

9600、19200、57600、115200

デフォルト

115200

説明

シリアルオーバー LAN 通信のボーレート。

cfgIpmiSolMinPrivilege (読み取り / 書き込み)

有効値

2 (ユーザー)

3 (オペレータ)

4 (Administrator: システム管理者)

デフォルト

4

説明

SOL アクセスに必要な最小権限レベルを指定します。

cfgIpmiSolAccumulateInterval (読み取り / 書き込み)

有効値

1~255

デフォルト

10

説明

SOL 文字データパケットの一部を送信する前に通常 iDRAC6 が待機する時間を指定します。この値は 1 を基準に 5 ms 間隔で増分されます。

cfgIpmiSolSendThreshold (読み取り / 書き込み)

有効値

1~255

デフォルト

255

説明

SOL しきい値の限界値。SOL データパケット送信前にバッファする最大バイト数を指定します。

cfgIpmiLan

このグループは、システムの IPMI オーバー LAN 機能の設定に使用されます。

cfgIpmiLanEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

IPMI オーバー LAN インタフェースを有効または無効にします。

cfgIpmiLanPrivilegeLimit (読み取り/書き込み)

有効値

- 2 (ユーザー)
- 3 (オペレータ)
- 4 (Administrator: システム管理者)

デフォルト

4

説明

IPMI オーバー LAN アクセスに許可される最大権限レベルを指定します。

cfgIpmiLanAlertEnable (読み取り / 書き込み)

有効値

- 1 (TRUE)
- 0 (FALSE)

デフォルト

0

説明

グローバル電子メール警告を有効または無効にします。このプロパティは個々の電子メール警告の有効 / 無効プロパティすべてに優先されます。

cfgIpmiEncryptionKey (読み取り / 書き込み)

有効値

空白文字を含まない 0~40 文字の 16 進数文字列。偶数の桁数のみが許可されます。

デフォルト

00000000000000000000

説明

IPMI 暗号化キー。

cfgIpmiPetCommunityName (読み取り / 書き込み)

有効値

最大 18 文字の文字列。

デフォルト

public

説明

トラップの SNMP コミュニティ名。

cfgIpmiPetIpv6

このグループは、管理下サーバーの IPv6 プラットフォームイベントトラップの設定に使用します。

cfgIpmiPetIPv6Index (読み取り専用)

有効値

1~4

デフォルト

<索引値>

説明

トラップに対応する索引の固有の識別子。

cfgIpmiPetIPv6AlertDestIpAddr

有効値

IPv6 アドレス

デフォルト

<空白>

説明

トラップの IPv6 警告送信先 IP アドレスを設定します。

cfgIpmiPetIPv6AlertEnable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

トラップの IPv6 警告送信先を有効または無効にします。

cfgIpmiPef

このグループは、管理下サーバーで使用可能なプラットフォームイベントフィルタの設定に使用されます。

イベントフィルタは、管理下サーバーで重大なイベントが発生したときにトリガされる処置に関するポリシーを制御するために使用できます。

cfgIpmiPefName (読み取り専用)

有効値

最大 255 文字の文字列。

デフォルト

索引フィルタの名前。

説明

プラットフォームイベントフィルタの名前を指定します。

cfgIpmiPefIndex (読み取り/書き込み)

有効値

1 ~ 19

デフォルト

プラットフォームイベントフィルタオブジェクトの索引値。

説明

特定のプラットフォームイベントフィルタの索引を指定します。

cfgIpmiPefAction (読み取り / 書き込み)

有効値

0 (なし)

1 (電源を切る)

2 (リセット)

3 (電源を入れ直す)

デフォルト

0

説明

警告がトリガされたときに管理下サーバーで実行される処置を指定します。

cfgIpmiPefEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

特定のプラットフォームイベントフィルタを有効または無効にします。

cfgIpmiPet

このグループは、管理下サーバーのプラットフォームイベントトラップの設定に使用します。

cfgIpmiPetIndex (読み取り専用)

有効値

1~4

デフォルト

特定のプラットフォームイベントトラップの索引値。

説明

トラップに対応する索引の固有の識別子。

cfgIpmiPetAlertDestIpAddr (読み取り / 書き込み)

有効値

有効な IPv4 アドレスを表す文字列。例: 192.168.0.67

デフォルト

0.0.0.0

説明

ネットワーク上でのトラップレシーバの送信先 IPv4 アドレスを指定します。トラップレシーバは、管理下サーバーでイベントがトリガされたときに SNMP トラップを受信します。

cfgIpmiPetAlertEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

特定のトラップを有効または無効にします。

cfgUserDomain

このグループは、Active Directory のユーザードメイン名を設定するために使用されます。任意の時点で最大 40 個のドメイン名を指定できます。

cfgUserDomainIndex (読み取り専用)

有効値

1 ~ 40

デフォルト

索引値

説明

特定のドメインを表します。

cfgUserDomainName (読み取り専用)

有効値

最大 255 文字の ASCII 文字列。

デフォルト

<空白>

説明

Active Directory ユーザードメイン名を指定します。

cfgServerPower

このグループはいくつかの電源管理機能を提供します。

cfgServerPowerStatus (読み取り専用)

有効値

1 (ON)

0 (OFF)

デフォルト

<現在のサーバー電源状態>

説明

サーバー電源状態を ON または OFF で表します。

cfgServerPowerAllocation (読み取り専用)

 **メモ:** 複数の電源がある場合、このプロパティは最小容量電源の増加を保持します。

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

サーバーが使用できる割り当てられた電源を表します。

cfgServerActualPowerConsumption (読み取り専用)

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

現在サーバーにより消費される電力を表します。

cfgServerMinPowerCapacity (読み取り専用)

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

サーバーの最小電力容量を表します。

cfgServerMaxPowerCapacity (読み取り専用)

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

サーバーの最小電力容量を表します。

cfgServerPeakPowerConsumption (読み取り専用)

有効値

最大 32 文字の文字列。

デフォルト

<現在のサーバーのピーク電力消費>

説明

現在までにサーバーにより消費された最大電力を表します。

cfgServerPeakPowerConsumptionTimestamp (読み取り専用)

有効値

最大 32 文字の文字列。

デフォルト

最大電力消費タイムスタンプ

説明

最大電力消費が記録された時刻。

cfgServerPowerConsumptionClear (書き込み専用)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

説明

cfgServerPeakPowerConsumption (読み取り/書き込み) プロパティを 0 に、 cfgServerPeakPowerConsumptionTimestamp プロパティを現在の iDRAC 時刻にリセットします。

cfgServerPowerCapWatts (読み取り/書き込み)

有効値

最大 32 文字の文字列。

デフォルト

サーバー電源しきい値のワット数。

説明

サーバー電源しきい値のワット数を表します。

cfgServerPowerCapBtuhr (読み取り/書き込み)

有効値

最大 32 文字の文字列。

デフォルト

サーバー電源しきい値 (BTU/時)。

説明

サーバー電源しきい値 (BTU/時) を表します。

cfgServerPowerCapPercent (読み取り/書き込み)

有効値

最大 32 文字の文字列。

デフォルト

サーバー電源しきい値のワット数。

説明

サーバー電源しきい値のワット数を表します。

cfgIPv6LanNetworking

このグループは、IPv6 オーバー LAN ネットワーク接続機能の設定に使用します。

cfgIPv6Enable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 IPv6 スタックを有効または無効にします。

cfgIPv6Address1 (読み取り/書き込み)

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

iDRAC6 IPv6 アドレス。

cfgIPv6Gateway (読み取り/書き込み)

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

iDRAC6 ゲートウェイ IPv6 アドレス

cfgIPv6PrefixLength (読み取り/書き込み)

有効値

1~128

デフォルト

64

説明

iDRAC6 IPv6 アドレス 1 のプレフィクス長。

cfgIPv6AutoConfig (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

IPv6 自動設定オプションを有効または無効にします。

cfgIPv6LinkLocalAddress (読み取り専用)

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

iDRAC6 IPv6 リンクのローカルアドレス

cfgIPv6Address2 (読み取り専用)

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

iDRAC6 IPv6 アドレス。

cfgIPv6DNSServersFromDHCP6 (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

cfgIPv6DNSServer1 および cfgIPv6DNSServer2 が静的または DHCP IPv6 アドレスのいずれであるかを指定します。

cfgIPv6DNSServer1 (読み取り/書き込み)

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

IPv6 DNS サーバーアドレス

cfgIPv6DNSServer2 (読み取り/書き込み)

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

IPv6 DNS サーバーアドレス

cfgIPv6URL

このグループは、iDRAC6 IPv6 URL の設定に使用するプロパティを指定します。

cfgIPv6URLstring (読み取り専用)

有効値

最大 80 文字の文字列。

デフォルト

<空白>

説明

iDRAC6 IPv6 の URL アドレス。

cfgIpmiSerial

このグループは、BMC の IPMI シリアルインタフェースの設定に使用されるプロパティを指定します。

cfgIpmiSerialConnectionMode (読み取り / 書き込み)

有効値

0 (ターミナル)

1 (基本)

デフォルト

1

説明

iDRAC6 `cfgSerialConsoleEnable` プロパティを 0 (無効) に設定すると、iDRAC6 のシリアルポートが IPMI のシリアルポートになります。このプロパティによって、IPMI 定義のシリアルポートのモードが決まります。

基本モードの場合、ポートはシリアルクライアントのアプリケーションプログラムと通信するためにバイナリデータを使用します。ターミナルモードでは、ポートは非プログラム式 ASCII 端末が接続していると想定し、ごく単純なコマンドの入力を許可します。

cfgIpmiSerialBaudRate (読み取り / 書き込み)

有効値

9600、19200、57600、115200

デフォルト

57600

説明

IPMI を介したシリアル接続のボーレートを指定します。

cfgIpmiSerialChanPrivLimit (読み取り / 書き込み)

有効値

2 (ユーザー)

3 (オペレータ)

4 (Administrator: システム管理者)

デフォルト

4

説明

IPMI シリアルチャネルで許可される最大権限レベルを指定します。

cfgIpmiSerialFlowControl (読み取り / 書き込み)

有効値

- 0 (なし)
- 1 (CTS/RTS)
- 2 (XON/XOFF)

デフォルト

1

説明

IPMI シリアルポートのフロー制御の設定を指定します。

cfgIpmiSerialHandshakeControl (読み取り / 書き込み)

有効値

- 0 (FALSE)
- 1 (TRUE)

デフォルト

1

説明

IPMI ターミナルモードのハンドシェイク制御を有効または無効にします。

cfgIpmiSerialLineEdit (読み取り / 書き込み)

有効値

- 0 (FALSE)
- 1 (TRUE)

デフォルト

1

説明

IPMI シリアルインタフェースのライン編集を有効または無効にします。

cfgIpmiSerialEchoControl (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI シリアルインタフェースのエコー制御を有効または無効にします。

cfgIpmiSerialDeleteControl (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

デフォルト

0

説明

IPMI シリアルインタフェースの削除制御を有効または無効にします。

cfgIpmiSerialNewLineSequence (読み取り / 書き込み)

有効値

0 (なし)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

デフォルト

1

説明

IPMI シリアルインタフェースの改行シーケンスの仕様を指定します。

cfgIpmiSerialInputNewLineSequence (読み取り / 書き込み)

有効値

0 (<ENTER>)

1 (NULL)

デフォルト

1

説明

IPMI シリアルインタフェースの入力改行シーケンスの仕様を指定します。

cfgSmartCard

このグループは、スマートカードを使用した iDRAC6 へのアクセスのサポートに使用するプロパティを指定します。

cfgSmartCardLogonEnable (読み取り/書き込み)

有効値

0 (無効)

1 (有効)

2 (リモート RACADM により有効)

デフォルト

0

説明

スマートカードを使用した iDRAC6 へのアクセスのサポートを有効または無効にするか、リモート RACADM で有効にします。

cfgSmartCardCRLEnable (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

証明書取り消しリスト (CRL) を有効または無効にします。

cfgNetTuning

このグループを使うと、RAC NIC 用のアドバンスネットワークインタフェースパラメータを設定できます。新しい設定が有効になるまで 1 分までかかることがあります。

△ 注意: このグループのプロパティを変更する際は特別な注意が必要です。このグループのプロパティを不当に変更すると、RAC NIC が動作できなくなることがあります。

cfgNetTuningNicAutoneg (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

物理リンクの速度とデュプレックスのオートネゴシエーションを有効にします。有効にした場合、オートネゴシエーションは `cfgNetTuningNic100MB` および `cfgNetTuningNicFullDuplex` オブジェクトに設定された値より優先されます。

cfgNetTuningNic100MB (読み取り / 書き込み)

有効値

0 (10 メガビット)

1 (100 メガビット)

デフォルト

1

説明

RAC NIC で使う速度を指定します。このプロパティは、`cfgNetTuningNicAutoNeg` が 1 (有効) に設定されている場合には使用できません。

cfgNetTuningNicFullDuplex (読み取り / 書き込み)

有効値

0 (半二重)

1 (全二重)

デフォルト

1

説明

RAC NIC のデュプレックス設定を指定します。このプロパティは、`cfgNetTuningNicAutoNeg` が 1 (有効) に設定されている場合には使用できません。

cfgNetTuningNicMtu (読み取り / 書き込み)

有効値

576~1500

デフォルト

1500

説明

iDRAC6 NIC で使用する最大送信単位のバイトサイズ。

[目次ページに戻る](#)

[目次ページに戻る](#)

サポートされている RACADM インタフェース

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

以下の表に、RACADM サブコマンドとそれに対応するインタフェースのサポートについての概要を示します。

表 C-1 RACADM サブコマンドのインタフェースサポート

サブコマンド	Telnet/SSH/シリアル	ローカル RACADM	リモート RACADM
arp	✓	✗	✓
clearscreen	✓	✓	✓
clrraclog	✓	✓	✓
clrsel	✓	✓	✓
coredump	✓	✗	✓
coredumpdelete	✓	✓	✓
fwupdate	✓	✓	✓
getconfig	✓	✓	✓
getniccfg	✓	✓	✓
getraclog	✓	✓	✓
getractime	✓	✓	✓
getsel	✓	✓	✓
getssninfo	✓	✓	✓
getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
netstat	✓	✗	✓
ping	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✗	✓	✓
sslkeyupload	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓
usercontentupload	✗	✓	✓

usercertview	✔	✔	✔
localConRedirDisable	✘	✔	✘
✔ = サポートされている ✘ = サポートされていない			

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 の概要

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [iDRAC6 Express の管理機能](#)
- [iDRAC6 Enterprise](#)
- [iDRAC6 のセキュリティ機能](#)
- [対応プラットフォーム](#)
- [対応 OS](#)
- [対応ウェブブラウザ](#)
- [対応リモートアクセス接続](#)
- [iDRAC6 のポート](#)
- [その他のマニュアル](#)

Integrated Dell™ Remote Access Controller (iDRAC6) はシステム管理ハードウェアおよびソフトウェアのソリューションで、Dell PowerEdge™ システムのリモート管理機能、クラッシュしたシステムのリカバリ機能、電源制御機能などを提供します。

iDRAC6 は、リモート監視 / 制御システムに、システムオンチップの内蔵マイクロプロセッサを採用しています。iDRAC6 は、管理下 PowerEdge サーバーとシステム基板上で共存します。サーバーオペレーティングシステムはアプリケーションの実行に関係し、iDRAC6 はサーバー環境およびオペレーティングシステム外の状態の監視と管理に関係します。

警告やエラーが発生したときに、電子メールまたは 簡易ネットワーク管理プロトコル (SNMP) のトラップ警告を送信するように iDRAC6 を設定できます。システムクラッシュの原因を診断する際の手助けとして、iDRAC6 はシステムクラッシュを検出すると、イベントデータをログに記録し、画面イメージをキャプチャできます。

iDRAC6 ネットワークインタフェースはデフォルトで、静的 IP アドレス 192.168.0.120 で有効になります。これを設定しなければ、iDRAC6 にアクセスできません。iDRAC6 をネットワーク上で設定すると、iDRAC6 ウェブインタフェース、Telnet、Secure Shell (SSH) や、Intelligent Platform Management Interface (IPMI) などの対応するネットワーク管理プロトコルを使用して、割り当てられた IP アドレスにアクセスできるようになります。

iDRAC6 Express の管理機能

iDRAC6 には次の管理機能があります。

- 1 ダイナミックドメイン名システム (DDNS) の登録
- 1 ウェブインタフェース、およびシリアル、Telnet、または SSH 接続経由での SM-CLP コマンドラインを使用したリモートシステム管理と監視
- 1 Microsoft® Active Directory® 認証のサポート - 標準スキーマまたは拡張スキーマを使用して iDRAC6 のユーザー ID とパスワードを Active Directory で集約化
- 1 監視 (モニター) - システム情報やコンポーネントのステータスにアクセス可能
- 1 システムログへのアクセス - システムイベントログ、iDRAC6 のログ、およびオペレーティングシステムの状態とは関係なく、クラッシュしたシステムや応答しないシステムの前回クラッシュ画面にアクセス可能
- 1 Dell OpenManage™ ソフトウェアの統合 - Dell OpenManage Server Administrator または IT Assistant から iDRAC6 ウェブインタフェースの起動が可能
- 1 iDRAC6 警告 - 電子メールメッセージまたは SNMP トラップによって管理下ノードの不具合を警告
- 1 リモート電源管理 - シャットダウンやリセットなどのリモート電源管理機能を管理コンソールから提供
- 1 Intelligent Platform Management Interface (IPMI) のサポート
- 1 Secure Sockets Layer (SSL) 暗号化 - ウェブインタフェースからセキュアリモートシステム管理を提供
- 1 パスワードレベルのセキュリティ管理 - リモートシステムへの無許可のアクセスを防止
- 1 役割 (ロール) ベースの権限 - さまざまなシステム管理タスクに応じて割り当て可能な権限
- 1 IPv6 のサポート - IPv6 アドレスを使った iDRAC6 ウェブインタフェースへのアクセス、iDRAC NIC の IPv6 アドレスの指定、IPv6 SNMP 警告送信先を設定するための送信先番号の指定など、IPv6 のサポートを追加します。
- 1 WS-MAN のサポート - Provides network accessible management using the Web Services for Management (WS-MAN) プロトコルを使ったネットワークアクセス管理を提供します。
- 1 SM-CLP のサポート - Server Management-Command Line Protocol (SM-CLP) のサポートを追加します。これによって、Systems Management CLI 導入の標準が提供されます。
- 1 ファームウェアのロールバックとリカバリ - 選択したファームウェアイメージから起動、または選択したファームウェアイメージへロールバックできます。

iDRAC6 Express の詳細については、support.dell.com/manuals にある『ハードウェアオーナーズマニュアル』を参照してください。

iDRAC6 Enterprise


RACADM、仮想 KVM、仮想メディア機能、専用 NIC、仮想フラッシュ、(およびオプションで Dell vFlash Media カード) のサポートを追加します。iDRAC6 Enterprise の詳細については、support.dell.com/manuals にある『ハードウェアオーナーズマニュアル』を参照してください。

iDRAC6 のセキュリティ機能

iDRAC6 には次のセキュリティ機能があります。

- 1 Microsoft Active Directory (オプション) またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証

- 1 システム管理者が各ユーザーに特定の権限を設定できる役割(ロール)ベースの権限
- 1 ウェブインタフェースまたは SM-CLP を使用したユーザー ID とパスワードの設定
- 1 SM-CLP とウェブインタフェースは SSL 3.0 標準を使って 128 ビットおよび 40 ビット(128 ビットが認められていない国の場合)暗号化をサポートします。
- 1 ウェブインターフェースまたは SM-CLP を使用したセッションタイムアウトの設定(秒単位)
- 1 設定可能な IP ポート(該当する場合)

 **メモ:** Telnet は SSL 暗号化をサポートしていません。

- 1 暗号化トランスポート層を使用してセキュリティを強化するSSH
- 1 IP アドレスごとのログイン失敗制限により制限を越えた IP アドレスのログインを阻止
- 1 に接続するクライアントの IP アドレス範囲を制限する機能
- 1 スマートカードの認証

対応プラットフォーム

iDRAC6 は以下の PowerEdge システムに対応しています。

- 1 PowerEdge R710
- 1 PowerEdge R610
- 1 PowerEdge T610

対応プラットフォームの最新情報は、support.dell.com/manuals またはシステムに同梱の『Dell Systems Management Tools and Documentation DVD』にある iDRAC6 Readme ファイルと『Dell OpenManage Server Administrator 互換性ガイド』を参照してください。

対応 OS

表 1-1 は、iDRAC6 対応オペレーティングシステムのリストです。

最新情報は、support.dell.com/manuals またはシステムに同梱の『Dell Systems Management Tools and Documentation DVD』にある『Dell OpenManage Server Administrator 互換性ガイド』をご覧ください。

表 1-1 対応管理下サーバーオペレーティングシステム

オペレーティングシステムファミリー	オペレーティングシステム
Microsoft Windows	<p>以下を含む Windows Server® 2003 ファミリ。</p> <p>Microsoft Windows Server 2003 R2 Standard/Enterprise(x86)エディション SP2</p> <p>Microsoft Windows Server 2003 R2 Standard, Enterprise, Datacenter x64 の各エディション SP2</p> <p>Windows Server 2003 (SBS, Standard, Premium の各エディション) SP2</p> <p>メモ: Windows Server 2003 SP1 をインストールする場合は、DCOM のセキュリティ設定に注意してください。詳細については、Microsoft のサポートウェブサイト support.microsoft.com/kb/903220 で記事番号 903220 を参照してください。</p> <p>Windows Server 2008 とコア (Web, Standard, Enterprise の各エディション) (x86)</p> <p>Windows Server 2008 とコア (Standard, Enterprise, DataCenter の各エディション) (x64)</p> <p>Windows Server 2008 SBS, EBS, Standard, Premium の各エディション</p>
SUSE® Linux	Enterprise Server 10 SP2
Red Hat® Linux®	<p>Enterprise Linux 4.7 (x86_32, x86_64)</p> <p>Enterprise Linux 5 (x86_32, x86_64)</p>
VMware®	<p>ESX 3.5 U4</p> <p>ESXi 3.5 U4 Flash</p>

対応ウェブブラウザ

表 1-2 は、iDRAC6 のクライアントとしてサポートされているウェブブラウザのリストです。

最新の対応プラットフォームについては、デルサポートサイト support.dell.com にある iDRAC6 の Readme ファイルと『Dell OpenManage 互換性ガイド』を参照してください。


 **メモ:** セキュリティに重大な欠陥があるため、SSL 2.0 のサポートは中止になりました。ブラウザを正しく動作させるには、SSL 3.0 対応に設定する必要があります。

表 1-2 対応ウェブブラウザ

対応ウェブブラウザ
Microsoft Internet Explorer 6.0 SP2 for Windows XP, Windows 2000 Server, Windows 2000 Pro, Windows 2003 Server Gold, Windows 2003 Server SP1, Windows 2003 Server SP2
Microsoft Internet Explorer 7.0 for Windows 2003 Server Gold, Windows 2003 Server SP1, Windows 2003 Server SP2, Windows Server 2008, Windows Vista
Mozilla Firefox 2.0 on SUSE Linux Enterprise Server (SLES) 10 SP1
Mozilla Firefox 3.0 on Windows 2003 Server Gold, Windows 2003 Server SP1, Windows 2003 Server SP2, Windows 2000 Pro, Windows XP, Windows Server 2008, Windows Vista, Red Hat Enterprise Linux 4 と 5, SLES 9 と 10, SLES 10 SP1

対応リモートアクセス接続

表 1-3 は接続機能のリストです。

表 1-3 対応リモートアクセス接続

接続	機能
iDRAC6 NIC	<ul style="list-style-type: none">1 10Mbps/100Mbps/Ethernet1 DHCP のサポート1 SNMP トラップと電子メールによるイベント通知1 iDRAC6 設定、システム起動、リセット、電源投入、シャットダウンコマンドなどの操作に使用する SM-CLP (Telnet または SSH) コマンドシェルのサポート1 IPMITool や ipmishell などの IPMI ユーティリティのサポート1 シリアル接続

iDRAC6 のポート

表 1-4 は、iDRAC6 が接続を待ち受けるポートのリストです。表 1-5 は、iDRAC6 がクライアントとして使用するポートです。この情報は、ファイアウォールを開いて iDRAC6 にリモートからアクセスする場合に必要です。

表 1-4 iDRAC6 サーバリスニングポート

ポート番号	機能
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	コンソールリダイレクトキーボード/マウス、仮想メディアサービス、仮想メディアセキュアサービス、コンソールリダイレクトビデオ
* 設定可能なポート	

表 1-5 iDRAC6 クライアントポート


ポート番号	機能
25	SMTP
53	DNS
68	DHCP で割り当てた IP アドレス
69	TFTP
162	SNMP トラップ
636	LDAPS
3269	グローバルカタログ(GC)用 LDAPS

その他のマニュアル

この『ユーザーズガイド』のほかに、次の文書にもシステム内の iDRAC6 のセットアップと操作に関する追加情報が含まれています。これらのドキュメントは、デルサポートサイト support.dell.com/manuals から入手可能です。

- 1 iDRAC6 オンラインヘルプでは、ウェブインタフェースの使用方法について詳しく説明されています。
- 1 iDRAC ハードウェアとシステムサービスの設定の詳細については、『Dell Unified Server Configurator ユーザーズガイド』を参照してください。
- 1 IT Assistant の使用方法については、『Dell OpenManage IT Assistant ユーザーズガイド』を参照してください。
- 1 iDRAC6 のインストールについては、『ハードウェアオーナーズマニュアル』を参照してください。
- 1 、Server Administrator のインストールと使用方法については、『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。
- 1 対応プラットフォームの最新情報は、iDRAC6 Readme ファイルと『Dell OpenManage Server Administrator 互換性ガイド』を参照してください。
- 1 システムアップデート対策としての Dell Update Packages の入手とその使用方法については、『Dell Update Packages ユーザーズガイド』を参照してください。
- 1 iDRAC6 と IPMI インタフェースについては、『Dell OpenManage Baseboard Management Controller ユーティリティユーザーズガイド』を参照してください。

次のシステム文書にも、iDRAC6 をインストールするシステムに関する詳細が記載されています。

- 1 ラックソリューションに付属の『ラック取り付けガイド』では、システムをラックに取り付ける方法について説明しています。
 - 1 『はじめに』では、システムの機能、システムのセットアップ、および技術仕様の概要を説明しています。
 - 1 『ハードウェアオーナーズマニュアル』では、システムの機能、トラブルシューティングの方法、およびコンポーネントの取り付け方や交換方法について説明しています。
 - 1 システム管理ソフトウェアのマニュアルでは、ソフトウェアの機能、動作条件、インストール、および基本操作について説明しています。
 - 1 OS のマニュアルでは、OS ソフトウェアのインストール手順(必要な場合)や設定方法、および使い方について説明しています。
 - 1 別途購入されたコンポーネントのマニュアルでは、これらのオプション装置の取り付けや設定について説明しています。
 - 1 システム、ソフトウェア、またはマニュアルの変更について記載されたアップデート情報がシステムに付属していることがあります。
-  **メモ:** このアップデート情報には他の文書の内容を差し替える情報が含まれていることがあるので、必ず最初にお読みください。
- 1 リリースノートまたは readme ファイルには、システムやマニュアルに加えられたアップデートの情報や、上級ユーザーや技術者のための高度な技術情報が記載されています。

[目次ページに戻る](#)

仮想メディアの設定と使用法

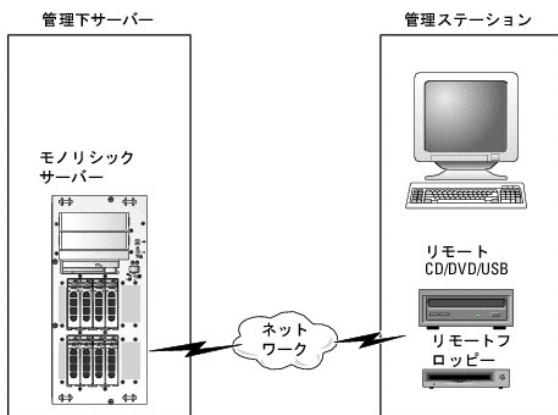
Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

- [概要](#)
- [仮想メディアの設定](#)
- [仮想メディアの実行](#)
- [よくあるお問い合わせ\(FAQ\)](#)

概要

コンソールリダイレクトビューアからアクセスする **仮想メディア** 機能は、ネットワーク上のリモートシステムに接続しているメディアへのアクセスを管理下サーバーに提供します。図 10-1 は、**仮想メディア** の全体的なアーキテクチャを示します。

図 10-1 仮想メディアの全体的なアーキテクチャ



仮想メディア を使用すると、管理下サーバーの起動から、アプリケーションのインストール、ドライバのアップデート、新しいオペレーティングシステムのインストールまで、仮想 CD/DVD およびディスクドライブからリモートで実行できます。

メモ: **仮想メディア** は 128 Kbps 以上のネットワーク帯域幅を必要とします。

仮想メディア は、管理下サーバーのオペレーティングシステムと BIOS に 2 つのデバイス(フロッピーディスクデバイスとオプティカルディスクデバイス)を定義します。

管理ステーションは、物理的なメディアまたはイメージファイルをネットワークを介して提供します。**仮想メディア** が連結または自動連結されている場合、管理下サーバーからのすべての仮想 CD/ フロッピードライブのアクセス要求がネットワーク経由で管理ステーションに転送されます。**仮想メディア** への接続は、物理デバイスへのメディアの挿入と同様に表示されます。仮想メディアが連結されていない場合、仮想デバイスは管理下サーバー上で表示されません。

表 10-1 に、仮想フロッピーと仮想オプティカルドライブにサポートされているドライブ接続をリストします。

メモ: 接続中に **仮想メディア** を変更すると、システムの起動シーケンスが停止する可能性があります。

表 10-1 サポートされているドライブ接続

サポートされている仮想フロッピードライブ接続	サポートされている仮想オプティカルドライブ接続
レガシー 1.44 フロッピードライブ(1.44 フロッピーディスク)	CD-ROM、DVD、CDRW、CD-ROM メディアとのコンボドライブ
USB フロッピードライブ(1.44 フロッピーディスク)	ISO9660 フォーマットの CD-ROM/DVD イメージファイル
1.44 フロッピーイメージ	CD-ROM メディアのある USB CD-ROM ドライブ
USB リムーバブルディスク	

Windows ベースの管理ステーション

Microsoft® Windows® オペレーティングシステムが稼動する管理ステーションで **仮想メディア** 機能を実行するには、対応バージョンの Internet Explorer または Firefox と Java ランタイム環境(JRE)をインストールします。詳細については、「[対応ウェブブラウザ](#)」を参照してください。

Linux ベースの管理ステーション

Linux オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Firefox の対応バージョンをインストールします。詳細については、「[対応ウェブブラウザ](#)」を参照してください。

コンソールリダイレクトプラグインを実行するには、Java ランタイム環境(JRE)が必要です。JRE は、java.sun.com からダウンロードできます。JRE バージョン 1.6 以降が推奨されます。

仮想メディアの設定

- iDRAC6 ウェブインタフェースにログインします。
- システム→コンソール/メディアの順で選択します。
- 設定→仮想メディアの順にクリックして仮想メディアを設定します。
[表 10-2](#) は 仮想メディア の設定値の説明です。
- 設定が終了したら、適用 をクリックします。
- 適切な ボタンをクリックして続行します。[表 10-3](#) を参照してください。

表 10-2 仮想メディアの設定プロパティ


Attribute(属性)	値
リモートメディアの連結状態	連結 - 瞬時に 仮想メディア をサーバーに連結します。 分離 - 瞬時に 仮想メディア からサーバーを分離します。 自動連結 - 仮想メディアセッションが開始している場合のみ、仮想メディア をサーバーに連結します。
最大セッション数	最大仮想メディアセッション数が表示されます。これは、常に 1 です。
アクティブセッション数	仮想メディアの現在のセッション数を表示します。
仮想メディア暗号化の有効	チェックボックスを選択または選択解除して、仮想メディア 接続の暗号化を有効または無効にします。選択すると暗号化は有効になり、選択解除すると暗号化は無効になります。
フロッピーのエミュレーション	仮想メディア がサーバーにフロッピードライブとして表示されるか USB キーとして表示されるかを示します。フロッピーのエミュレーション のチェックボックスがオンの場合、仮想メディア デバイスはサーバーでフロッピーデバイスとして表示されます。オフの場合は、USB キードライブとして表示されます。
ブートワンスを有効にする	ブートワンスオプションを有効にするには、このボックスをオンにします。このオプションは、サーバーが 1 度起動した後で 仮想メディア セッションを終了します。このオプションは、自動展開の際に便利です。


表 10-3 設定ページのボタン

ボタン	説明
印刷	画面に表示されている 設定 ページの値を印刷します。
更新	設定 ページを再ロードします。
変更の適用	設定 ページ上の新しい設定を保存します。

仮想メディアの実行

 **注意:** 仮想メディアセッションの実行中は、`racreset` コマンドを使用しないでください。使用すると、データ損失などの不測の結果が生じます。

 **メモ:** 仮想メディアにアクセス中、[コンソールビューア] ウィンドウアプリケーションはアクティブなままである必要があります。

 **メモ:** Red Hat® Enterprise Linux® (バージョン 4) がマルチ論理ユニット(LUN)の SCSI デバイスを認識できるようにするには、次の手順を実行します。

- `/ect/modprobe` に次の行を追加します。


```
options scsi_mod max_luns=256
```

```
cd /boot
```

```
mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
```
- サーバーを再起動します。

3. 仮想 CD/DVD または仮想フロッピーを表示するには、次のコマンドを実行します。

```
cat /proc/scsi/scsi
```

 **メモ:** 仮想メディアを使用する際、管理下サーバー上で(仮想)ドライブとして使用できるのは、管理ステーションのフロッピー/USB ドライブ/イメージ/キーが 1 つ、そしてオプティカルドライブが 1 台に限られています。

サポートされている仮想メディア設定

フロッピードライブと光ドライブ 1 台ずつの仮想メディアを有効にできます。1 度に仮想化できるのは各メディアタイプのドライブ 1 台のみです。


サポートされているフロッピードライブには 1 つのフロッピーイメージまたは 1 つの空きフロッピードライブがあります。サポートされている光ドライブには、最大 1 台の空き光ドライブまたは 1 つの ISO イメージファイルがあります。


仮想メディアの接続


仮想メディアを実行するには、次の手順を実施します。

1. 管理ステーションで対応ウェブブラウザを開きます。詳細については、「[対応ウェブブラウザ](#)」を参照してください。
2. iDRAC6 ウェブインタフェースを開始します。詳細については、「[ウェブインタフェースへのアクセス](#)」を参照してください。
3. **システム→コンソール/メディア** の順で選択します。


コンソールリダイレクトおよび仮想メディア ページが表示されます。表示されている属性値を変更する場合は、「[仮想メディアの設定](#)」を参照してください。

 **メモ:** このデバイスは仮想フロッピーとして仮想化できるので、**フロッピーイメージファイル** が **フロッピードライブ** (該当する場合)の下に表示されることがあります。同時に仮想化できるのは、オプティカルドライブが 1 台、そしてフロッピー/USB フラッシュドライブが 1 台です。

 **メモ:** 管理下サーバー上の仮想デバイスドライブ文字は、管理ステーション上の物理ドライブ文字とは一致しません。

 **メモ:** Internet Explorer の 拡張セキュリティが設定されている Windows オペレーティングシステムクライアントでは、**仮想メディア** が正しく機能しないことがあります。この問題を解決するには、Microsoft オペレーティングシステムのマニュアルを参照するか、システム管理者にお問い合わせください。


4. **ビューアの起動** をクリックします。

 **メモ:** Linux では、ファイル `jviewer.jnlp` がデスクトップにダウンロードされ、ファイルの処置について尋ねるダイアログボックスが表示されます。**プログラムを指定して開く** オプションを選択し、JRE インストールディレクトリの `bin` サブディレクトリにある `Javaws` アプリケーションを選択します。

iDRAC KVM エージェントアプリケーションが別のウィンドウで起動します。

5. **ツール→仮想メディアの起動** の順でクリックします。

[メディアリダイレクト] ウィザードが開きます。

 **メモ:** 仮想メディアセッションを終了したい場合を除き、このウィザードを閉じないでください。

6. メディアが接続している場合は、別のメディアソースに接続する前に切断してください。切断したい場合は、メディアの左のチェックボックスを選択解除します。

7. 接続したいメディアの種類隣のボックスを選択します。

フロッピーイメージまたは ISO イメージを接続する場合は、(ローカルコンピュータ上の)イメージのパスを入力するか、**イメージの追加...** ボタンでイメージを参照します。

メディアが接続され、**ステータス** ウィンドウが更新します。

仮想メディアの切断

1. **ツール→仮想メディアの起動** の順でクリックします。

2. 切断したいメディア隣のボックスを選択解除します。

メディアが切断し、**ステータス** ウィンドウが更新されます。

3. **メディアリダイレクト ウィザードを終了するには、終了** をクリックします。

仮想メディアからの起動

システム BIOS を使用すると、仮想オプティカルドライブまたは仮想フロッピードライブから起動できるようになります。POST 中、BIOS セットアップウィンドウを開き、仮想ドライブが有効になっており、正しい順序で表示されていることを確認します。

BIOS 設定を変更するには、次の手順を実行してください。

1. 管理下サーバーを起動します。
2. <F2> を押して BIOS 設定ウィンドウを開きます。
3. 起動順序をスクロールして、<Enter> キーを押します。
ポップアップウィンドウに、仮想オプティカルデバイスと仮想フロッピードライブのリストがその他の標準起動デバイスと共に表示されます。
4. 仮想ドライブが有効で、ブータブルメディア(起動メディア)の最初のデバイスとして表示されていることを確認してください。必要に応じて、画面の指示に従って起動順序を変更します。
5. 変更を保存して終了します。

管理下サーバーが再起動します。

管理下サーバーは起動順序に従って、ブータブル(起動)デバイスからの起動を試みます。仮想デバイスが接続済みでブータブルメディアが存在している場合、システムはこの仮想デバイスで起動します。起動メディアがない場合は、ブータブルメディアのない物理デバイスの場合と同様にデバイスを無視します。

仮想メディアを使用したオペレーティングシステムのインストール

本項では、管理ステーションに手動でインタラクティブにオペレーティングシステムをインストールする方法について説明します。完了までに数時間かかる場合があります。**仮想メディア**を使用してスクリーンでオペレーティングシステムをインストールする手順では 15 分以内で完了します。詳細については、「[オペレーティングシステムの導入](#)」を参照してください。



1. 次の点を確認します。
 - 1 管理ステーションの CD ドライブにオペレーティングシステムのインストール CD が挿入されている。
 - 1 ローカルの CD ドライブが選択されている。
 - 1 仮想ドライブに接続している。
2. 「[仮想メディアからの起動](#)」の仮想メディアからの起動手順に従って、BIOS がインストール元の CD ドライブから起動するように設定されていることを確認してください。
3. 画面の指示に従ってセットアップを完了します。

マルチディスクのインストールの場合、次の手順に従うことが重要です。

1. 仮想メディアコンソールから仮想化(リダイレクトされた) CD/DVD をマップ解除します。
2. リモートオプティカルドライブに次の CD/DVD を挿入します。
3. 仮想メディアコンソールからこの CD/DVD をマッピング(リダイレクト)します。
再マッピングすることなく、リモートオプティカルドライブに新しい CD/DVD を挿入しても、正常に動作しない可能性があります。

ブートワンス機能

ブートワンス機能は、リモートの仮想メディアデバイスから起動できるように、一時的に起動順序を変更できるようにします。この機能は、一般的にオペレーティングシステムのインストール時に仮想メディアと併用されます。

-  **メモ:** この機能を使用するには、iDRAC6 の **設定** 権限が必要となります。
-  **メモ:** リモートデバイスでこの機能を使用するには、仮想メディアでリダイレクトする必要があります。

ブートワンス機能の使用

1. サーバーに電源を投入し、BIOS 起動マネージャを立ち上げます。
2. リモートの仮想メディアデバイスから起動するように、起動順序を変更します。
3. ウェブインタフェースを介して iDRAC6 にログインし、**システム**→**コンソール/メディア**→**設定** の順でクリックします。
4. 仮想メディアの下の**ブートワンスを有効にする**オプションを選択します。
5. サーバーの電源をオフにし、再びオンにします。

サーバーは、リモートの仮想メディアデバイスから起動します。次のサーバーの起動時には、リモートの仮想メディア接続は分離された状態になります。

サーバーのオペレーティングシステムが実行しているときの仮想メディアの使用

Windows ベースシステム

Windows システムでは、仮想メディアドライブは接続されると自動的にマウントされ、ドライブ文字が設定されます。

Windows からの仮想ドライブの使い方は、物理ドライブの場合とほぼ同じです。仮想メディアウィザードを使用してメディアに接続し、ドライブをクリックしてその内容を参照すると、そのシステムでメディアが使用できるようになります。

Linux ベースのシステム

システムのソフトウェア構成によっては、仮想メディアドライブが自動的にマウントされない場合があります。ドライブが自動的にマウントされない場合は、Linux の `mount` コマンドを使ってドライブを手動でマウントします。

よくあるお問い合わせ (FAQ)

[表 10-4](#) は、よくあるお問い合わせとその回答です。

表 10-4 仮想メディアの使い方: よくあるお問い合わせ (FAQ)

質問	回答
仮想メディアのクライアントの接続が時々切断されます。どうしてでしょうか。	ネットワークのタイムアウトが発生した場合、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。 仮想メディアの設定を iDRAC6 ウェブインタフェースまたはローカル RACADM コマンドで変更した場合、設定変更が適用されると、接続しているすべてのメディアが切断されます。 仮想ドライブに再接続するには、仮想メディアウィザードを使用します。
どのオペレーティングシステムが iDRAC6 をサポートしていますか。	対応オペレーティングシステムについては、「 対応 OS 」のリストを参照してください。
どのウェブブラウザが iDRAC6 をサポートしていますか。	対応ウェブブラウザのリストは、「 対応ウェブブラウザ 」を参照してください。
時々クライアントの接続が切れるのはなぜですか。	<ol style="list-style-type: none">1 ネットワークが低速であるか、クライアントシステムの CD ドライブで CD を交換した場合は、クライアントの接続が途切れることがあります。たとえば、クライアントシステムの CD ドライブで CD を交換した場合、新しい CD には自動開始機能が備わっている可能性があります。この場合、クライアントシステムが CD の読み込み準備に時間が掛かりすぎて、ファームウェアがタイムアウトになり、接続が途切れることがあります。接続が途切れた場合は、GUI から再接続して、その前の操作を続けることができます。1 ネットワークのタイムアウトが発生した場合、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。また、ウェブインタフェースまたは RADACM コマンドの入力によって、他の人が仮想メディアの設定を変更した可能性があります。仮想ドライブに再接続するには、仮想メディア 機能を使用します。
Windows オペレーティングシステムのインストールに時間が掛かりすぎるようです。どうしてでしょうか。	『Dell Systems Management Tools and Documentation DVD』を使用して Windows オペレーティングシステムをインストールするときにネットワーク接続が低速な場合は、ネットワークの遅延により iDRAC6 ウェブベースインタフェースへのアクセスに時間が掛かることがあります。インストールウィンドウにインストールプロセスが表示されていないのに、インストールが進行しています。
仮想デバイスをブータブル(起動)デバイスとして設定するにはどうしますか。	管理下サーバーの [BIOS セットアップ] にアクセスして起動メニューに進みます。仮想 CD、仮想フロッピー、または仮想フラッシュを見つけ、必要に応じてデバイスの起動順序を変更します。たとえば、CD ドライブから起動するには、その CD ドライブを起動順序の最初のドライブとして設定してください。
どのタイプのメディアから起動できますか。	iDRAC6 では、以下のブータブルメディアから起動できます。 <ol style="list-style-type: none">1 CDROM/DVD データメディア1 ISO 9660 イメージ1 1.44 フロッピーディスクまたはフロッピーイメージ1 オペレーティングシステムがリムーバブルディスクとして認識した USB キー1 USB キーイメージ
USB キーをブータブルにするには、どうしますか。	support.dell.com で、Dell USB キーをブータブルにするための Windows プログラム、Dell 起動ユーティリティを検索してください。 Windows 98 起動ディスクでの起動、および起動ディスクから USB キーへのシステムファイルのコピーも可能です。たとえば、DOS プロンプトで次のコマンドを入力します。 <pre>sys a: x: /s</pre> x: は、ブータブルにする USB キーです。
Red Hat Enterprise Linux または SUSE® Linux オペレーティングシステムが稼動するシステム上で仮想フロッピーデバイスを見つけることができません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。	一部の Linux バージョンは仮想フロッピードライブと仮想 CD ドライブを同じ方法で自動マウントしません。仮想フロッピードライブをマウントするには、Linux が仮想フロッピードライブに割り当てたデバイスノードを検索します。仮想フロッピードライブを正しく見つけてマウントするには、次の手順を実行してください。 <ol style="list-style-type: none">1. Linux コマンドプロンプトウィンドウを開き、次のコマンドを入力します。 <pre>grep "Virtual Floppy" /var/log/messages</pre>

	<p>2. そのメッセージの最後のエントリを探し、その時刻を書きとめます。</p> <p>3. Linux のプロンプトで次のコマンドを入力します。</p> <pre>grep "hh:mm:ss" /var/log/messages</pre> <p>このコマンドで、</p> <p>hh:mm:ss は、手順 1 で grep から返されたメッセージのタイムスタンプです。</p> <p>4. 手順 3 で、grep コマンドの結果を読み、DELL 仮想フロッピー のデバイス名を探します。</p> <p>5. 仮想フロッピードライブに接続していることを確認します。</p> <p>6. Linux のプロンプトで次のコマンドを入力します。</p> <pre>mount /dev/sdx /mnt/floppy</pre> <p>このコマンドで、</p> <p>/dev/sdxはステップ 4 で見つけたデバイス名です。</p> <p>/mnt/floppy はマウントポイントです。</p>
<p>Red Hat® Enterprise Linux® または SUSE® Linux オペレーティングシステムが稼動するシステム上で仮想フロッピー/仮想 CD デバイスを見つけることができません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。</p>	<p>(回答の続き)</p> <p>仮想 CD ドライブをマウントするには、Linux が仮想 CD ドライブに割り当てるデバイスノードを検索します。仮想 CD ドライブを見つけ、マウントするには、次の手順に従います。</p> <p>1. Linux コマンドプロンプトウィンドウを開き、次のコマンドを入力します。</p> <pre>grep "Virtual CD" /var/log/messages</pre> <p>2. そのメッセージの最後のエントリを探し、その時刻を書きとめます。</p> <p>3. Linux のプロンプトで次のコマンドを入力します。</p> <pre>grep "hh:mm:ss" /var/log/messages</pre> <p>パラメータ</p> <p>hh:mm:ss は、ステップ 1 で grep から返されたメッセージのタイムスタンプです。</p> <p>4. ステップ 3 で、grep コマンドの結果を読み込んで、「Dell Virtual CD」に与えられたデバイス名を特定します。</p> <p>5. 仮想 CD ドライブに連結し、接続していることを確認します。</p> <p>6. Linux のプロンプトで次のコマンドを入力します。</p> <pre>mount /dev/sdx /mnt/CD</pre> <p>このコマンドで、</p> <p>/dev/sdxはステップ 4 で見つけたデバイス名です。</p> <p>/mnt/floppy はマウントポイントです。</p>
<p>IDRAC6 ウェブインタフェースを使用してファームウェアのアップデートをリモートで実行すると、サーバーで仮想ドライブが削除されました。どうしてでしょうか。</p>	<p>ファームウェアのアップデートによって IDRAC6 がリセットされ、リモート接続が切断して仮想ドライブがアンマウントされます。</p>
<p>USB デバイスを接続すると、すべての USB デバイスが分離されるのはなぜですか。</p>	<p>仮想メディアデバイスおよび仮想フラッシュデバイスは、複合 USB デバイスとしてホスト USB バスに接続しているため、共通の USB ポートを共有しています。仮想メディアまたは仮想フラッシュ USB デバイスがホスト USB バスに接続、または切断されると、すべての仮想メディアおよび仮想フラッシュデバイスは、一時的にホスト USB バスから切断され、再接続します。ホストオペレーティングシステムで仮想メディアデバイスが使用されている場合、1 つまたは複数の仮想メディアまたは仮想フラッシュデバイスを連結したり、分離することを避ける必要があります。ご利用になる前に、必要な USB デバイスをすべて接続することを推奨します。</p>
<p>USB リセットボタンの機能は何ですか。</p>	<p>サーバーに接続されたリモートおよびローカル USB デバイスをリセットします。</p>

[目次ページに戻る](#)

WS-MAN インタフェースの使用

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

● 対応 CIM プロファイル

iDRAC6 ファームウェアでは、ウェブサービスの管理 (WS-MAN) プロトコルを使って、ネットワークアクセス可能管理が可能です。WS-MAN は、情報交換用のトランスポートメカニズムです。管理が簡単になるよう、WS-MAN はデバイスがデータを共有するよう汎用言語を提供します。WS-MAN は、リモートシステム管理ソリューションの主要となる部分ですが、大切なのはここだけではありません。

WS-MAN では HTTPS を使用して、管理トラフィックセキュリティを維持しています。クライアントはローカルか Microsoft® Active Directory® ユーザー特権でログインして、セッションを認証する必要があります。HTTPS は IP ポート 443 のセキュアソケットレイヤー (SSL) を使用して、セキュリティを保護します。

WS-MAN で使用できるデータは、次の分散管理タスクフォース (DMTF) プロファイルと Dell の拡張子にマップされている iDRAC6 計装インタフェースによって提供されるデータのサブセットです。

WS-MAN を使用して DMTF CIM ベースの管理情報を伝えるには、WS-MAN を利用するのが最も一般的です。CIM は、管理下システムで操作される管理情報の種類を定義します。ここでは、ワイヤに関するクライアントとサービスの対話オブジェクトを提供します。WS-MAN は、管理オブジェクトで実行される標準的な処理をいくつか定義します。たとえば、WS-MAN を使用すると、クライアントシステムは管理オブジェクトの集まりを見つけ出し、管理オブジェクトのコンテンツを取得し、そのコンテンツを新しい値に設定することができます。WS-MAN は、管理会話のパーブを提供します。CIM クラスおよびプロパティがナウンで、パーブによってオブジェクトが機能します。

DMTF and Dell further specify a standard minimum vocabulary of CIM classes, properties, and behaviors that all parties must understand. クライアントとサービス間の相互運用性を確認するには、DMTF および Dell の CIM クラス、プロパティ、およびビヘイビアの最小要件 ポキヤプリ をさらに指定し、当事者全員が理解する必要があります。こうした DMTF や Dell 特有のプロファイルでは、規格準拠のサービスにのって実行される表記規則を定義します。したがって、正しく機能するかどうかはすべてのクライアントが表記規則に従っているかどうかによります。

対応 CIM プロファイル

表 11-1 対応 CIM プロファイル

標準 DMTF
1. ベースサーバー ホストサーバーを表す CIM クラスを定義します。
2. サービスプロセッサ: iDRAC6 を表す CIM クラスの定義が記載されています。
メモ: ベースサーバープロファイル(上記)およびサービスプロセッサプロファイルは、ある意味では自律的なもので、コンポーネントプロファイルで定義されているその他すべての CIM オブジェクトを総合的に説明するオブジェクトです。
3. 物理アセット 管理要素の物理アセットを表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して物理トポロジだけでなく、ホストサーバーとそのコンポーネントの FRU 情報、を表します。
4. SM CLP 管理者ドメイン CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して自らの CLP を実行します
5. 電源状況管理 電源制御操作の CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーの電源制御操作を実行します。
6. 電源ユニット (バージョン 1.1) 電源ユニットを表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーの電源ユニットを表し、消費電力の高い低いを示す電力消費を説明します。
7. CLP サービス CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して自らの CLP を実行します
8. IP インタフェース 9. DHCP Client(DHCP クライアント) 10. DNS Client(DHCP クライアント) 11. イーサネットポート 上記のプロファイルは、ネットワークを表す CIM クラスを定義します。iDRAC6 は、こうしたプロファイルを使用して iDRAC6 NIC の構成を表します。
12. レコードログ 異なるログの種類を表す CIM を定義します。iDRAC6 は、このプロファイルを使用してシステムイベントログ (SEL) と iDRAC6 RAC ログを表します。
13. ソフトウェアインベントリ インストールしたもの、または利用可能なインベントリの CIM クラスを定義します。iDRAC6 は、TFTP プロコルを通じて現在インストールしている iDRAC6 ファームウェアバージョンに、このプロファイルを使用します。
14. ロールベース認証 ロールを表す CIM を定義します。iDRAC6 は、このプロファイルを使用して iDRAC6 のアカウント特権を定義します。

15. ソフトウェアのアップデート 利用可能なソフトウェアアップデートのインベントリの CIM クラスを定義します。iDRAC6 は、.TFTP プロコルを通じてファームウェアのアップデートのインベントリに、このプロファイルを使用します。
16. SMASH コレクション CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して自らの CLP を実行します
17. プロファイル登録 プロファイルの実行アダプタイズする CIM を定義します。iDRAC6 は、このプロファイルを使用してこの表で説明しているように、自らの実行済みプロファイルをアダプタイズします。
18. ベースメトリック メトリックを表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーのメトリックを表し、消費電力の高い低いを示す電力消費を説明します。
19. 簡易 ID 管理 ID を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して iDRAC6 のアカウントを定義します。
20. USB リダイレクト ローカル USB ポートのリモートリダイレクトを表す CIM を定義します。iDRAC6 は、仮想メディアプロファイルと併せてこのプロファイルを使用して、仮想メディアを定義します。
Dell 拡張
1. Dell® Active Directory Client Version 2.0.0 iDRAC6 Active Directory クライアントおよび Active Directory グループのローカル権限を設定する CIM と Dell 拡張クラスを定義します。
2. Dell 仮想メディア iDRAC6 仮想メディアを設定する CIM と Dell 拡張クラスを定義します。USB リダイレクトプロファイルを拡張します。
3. Dell イーサネットポート iDRAC6 NIC 用 NIC サイドバンド(帯域)インターフェースを設定する CIM と Dell 拡張クラスを定義します。イーサネットポートプロファイルを拡張します。
4. Dell 電力使用制御 ホストサーバーの電力バジェットを表したり、ホストサーバーの電力を設定/監視する CIM と Dell 拡張クラスを定義します。

詳細については、www.dmtf.org/standards/profiles/ を参照してください。プロファイルのリストの最新版や最新情報については、WS-MAN のリリースノートまたは readme ファイルを参照してください。

WS-MAN システムは、DMTF ウェブサービスの管理仕様バージョン 1.0.0 に準拠しています。WS-Management プロトコルに対応しているツールには、Microsoft Windows® Remote Management (WinRM) と open wsman、wsmancli ツールがありますが、これらに限定されません。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 SM-CLP コマンドラインインタフェースの使用

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [iDRAC6 SM-CLP のサポート](#)
- [SM-CLP の機能](#)

本項では、iDRAC6 に組み込まれている Distributed Management Task Force (DMTF) Server Management-Command Line Protocol (SM-CLP) について説明します。

メモ: ここでは、ユーザーが Systems Management Architecture for Server Hardware (SMASH) イニシアチブおよび SMWG SM-CLP 仕様に精通していることを前提としています。これらの仕様の詳細については、DMTF のウェブサイト www.dmtf.org を参照してください。

iDRAC6 SM-CLP は、システム管理 CLI 実装の標準となっているプロトコルです。SM-CLP は、複数のプラットフォームでサーバー管理を主導する DMTF SMASH イニシアチブのサブコンポーネントです。Managed Element Addressing Specification (管理下エレメントアドレス指定仕様書) および SM-CLP マッピング仕様に対する多くのプロファイルに関連する SM-CLP 仕様書は、さまざまなタスク実行用の標準化されたパーブとターゲットについて説明しています。

iDRAC6 SM-CLP のサポート

SM-CLP は iDRAC6 コントローラのファームウェアからホストされ、telnet、SSH、およびシリアルベースのインタフェースをサポートしています。iDRAC6 SM-CLP インタフェースは DMTF 組織が提供する SM-CLP 仕様バージョン 1.0 に基づいています。iDRAC6 SM-CLP では、[表 11-1](#)「サポートされる CIM プロファイル」で説明したすべてのプロファイルがサポートされます。

以下の項では、iDRAC6 からホストされる SM-CLP 機能の概要を述べます。

SM-CLP の機能

SM-CLP はパーブとターゲットの概念を打ち出し、CLI を通じたシステム管理を提供します。パーブは実行する処理を指し、ターゲットはその処理を実行するエンティティ(またはオブジェクト)を決定します。

次は SM-CLP コマンドライン構文の例です。

<パーブ> [<オプション>] [<ターゲット>] [<プロパティ>]

通常の SM-CLP セッション中、[表 12-1](#)にあるパーブを使って操作を実行できます。

表 12-1 システムでサポートされている CLI パーブ

パーブ	定義
CD	シェルを使用して MAP を移動します。
set	特定の値に対してプロパティを設定します。
help	特定のターゲットのヘルプを表示します。
reset	ターゲットをリセットします。
show	ターゲットのプロパティ、パーブ、およびサブターゲットを表示します。
start	ターゲットをオンにします。
stop	ターゲットをシャットダウンします。
exit	SM-CLP シェルのセッションを終了します。
version	ターゲットのバージョン属性を表示します。
load	バイナリイメージを URL から指定されたターゲットアドレスに移動します。

SM-CLP の使用

正しい資格情報を使用して SSH(または telnet)で iDRAC6 に接続します。

SMCLP プロンプト(/admin1->)が表示されます。

SM-CLP のターゲット

[表 12-2](#)に、上記の[表 12-1](#)で説明した操作をサポートするために SM-CLP から提供されるターゲットをリストにします。

表 12-2 SM-CLP のターゲット

ターゲット	定義
-------	----

ターゲット	定義
admin1	admin domain
admin1/profiles1	iDRAC6 の登録プロファイル
admin1/hdwr1	ハードウェア
admin1/system1	管理下システムターゲット
admin1/system1/redundancys1	電源ユニット
admin1/system1/redundancys1/pwrsupply*	管理下システムの電源ユニット
admin1/system1/sensors1	管理下システムセンサー
admin1/system1/capabilities1	管理下システム SMASH 収集機能
admin1/system1/capabilities1/pwrcap1	管理下システムの電力使用機能
admin1/system1/capabilities1/elec1	管理下システムターゲット機能
admin1/system1/logs1	レコードログ収集ターゲット
admin1/system1/logs1/log1	システム イベント ログ (SEL) のレコードエントリ
admin1/system1/logs1/log1/ レコード*	管理下システムの SEL レコードの個々のインスタンス
admin1/system1/settings1	管理下システム SMASH 収集設定
admin1/system1/settings1/pwrmaxsetting1	管理下システム最大電源割り当て設定
admin1/system1/settings1/pwrminsetting1	管理下システム最小電源割り当て設定
admin1/system1/capacities1	管理下システム機能 SMASH 収集
admin1/system1/consoles1	管理下システムコンソール SMASH 収集
admin1/system1/usbredirectsap1	仮想メディア USB リダイレクト SAP
admin1/system1/usbredirectsap1/remotesap1	仮想メディア送信先 USB リダイレクト SAP
admin1/system1/sp1	サービスプロセス
admin1/system1/sp1/timesvc1	サービスプロセス時間サービス
admin1/system1/sp1/capabilities1	サービスプロセス機能 SMASH 収集
admin1/system1/sp1/capabilities1/clpcap1	CLP サービス機能
admin1/system1/sp1/capabilities1/pwrmgtcap1	システムの電源状態管理サービス機能
admin1/system1/sp1/capabilities1/ipcap1	IP インタフェース機能
admin1/system1/sp1/capabilities1/dhccap1	DHCP クライアント機能
admin1/system1/sp1/capabilities1/NetPortCfgcap1	ネットワークポート構成機能
admin1/system1/sp1/capabilities1/usbredirectcap1	仮想メディア機能 USB リダイレクト SAP
admin1/system1/sp1/capabilities1/vmsapcap1	仮想メディア SAP 機能
admin1/system1/sp1/capabilities1/swinstallsvc1	ソフトウェアインストールサービス機能
admin1/system1/sp1/capabilities1/acctmgtcap*	アカウント管理サービス機能
admin1/system1/sp1/capabilities1/adcap1	Active Directory 機能
admin1/system1/sp1/capabilities1/rolemgtcap*	ローカルロールベースの管理機能
admin1/system1/sp1/capabilities/PwrtlmgtCap1	電力使用管理機能
admin1/system1/sp1/capabilities/metriccap1	メトリックサービス機能
admin1/system1/sp1/capabilities/elec1	複数要素認証機能
admin1/system1/sp1/capabilities1/lanendptcap1	LAN (Ethernet ポート) エンドポイント機能
admin1/system1/sp1/logs1	サービスプロセスログ収集
admin1/system1/sp1/logs1/log1	システムレコードログ
admin1/system1/sp1/logs1/log1/record*	システムログエントリ
admin1/system1/sp1/settings1	サービスプロセス設定収集
admin1/system1/sp1/settings1/clpsetting1	CLP サービス設定データ
admin1/system1/sp1/settings1/ipsettings1	IP インタフェース割り当て設定データ (静的)
admin1/system1/sp1/settings1/ipsettings1/staticipsettings1	静的 IP インタフェース割り当て設定データ
admin1/system1/sp1/settings1/ipsettings1/dnssettings1	DNS クライアント設定データ
admin1/system1/sp1/settings1/ipsettings2	IP インタフェース割り当て設定データ (DHCP)
admin1/system1/sp1/settings1/ipsettings2/dhcpsettings1	DHCP クライアント設定データ
admin1/system1/sp1/clpsvc1	CLP サーバプロトコルサービス
admin1/system1/sp1/clpsvc1/clpendpt*	CLP サーバプロトコルエンドポイント
admin1/system1/sp1/clpsvc1/tcpndpt*	CLP サーバプロトコル TCP エンドポイント
admin1/system1/sp1/jobq1	CLP サーバプロトコルジョブキュー
admin1/system1/sp1/jobq1/job*	CLP サーバプロトコルジョブ
admin1/system1/sp1/pwrmtgsvc1	電源状況管理サービス
admin1/system1/sp1/ipcfsvc1	IP インタフェース設定サービス
admin1/system1/sp1/ipendpt1	IP インタフェースプロトコルエンドポイント

admin1/system1/sp1/ipendpt1/gateway1	IP インタフェースゲートウェイ
admin1/system1/sp1/ipendpt1/dhccpendpt1	DHCP クライアントプロトコルエンドポイント
admin1/system1/sp1/ipendpt1/dnsendpt1	DNS クライアントプロトコルエンドポイント
admin1/system1/sp1/ipendpt1/dnsendpt1/dnsserver*	DNS クライアントサーバー
admin1/system1/sp1/NetPortCfgsvc1	ネットワークポート構成サービス
admin1/system1/sp1/lanendpt1	LAN エンドポイント
admin1/system1/sp1/lanendpt1/enetport1	Ethernet ポート
admin1/system1/sp1/VMediaSvc1	仮想メディアサービス
admin1/system1/sp1/VMediaSvc1/tcpendpt1	仮想メディア TCP プロトコルエンドポイント
admin1/system1/sp1/swid1	ソフトウェア識別
admin1/system1/sp1/swinstallsvc1	ソフトウェアインストールサービス
admin1/system1/sp1/account1-16	複数要素認証 (MFA) アカウント
admin1/system1/sp1/account1-16/identity1	ローカルユーザー識別アカウント
admin1/system1/sp1/account1-16/identity2	IPMI 識別 (LAN) アカウント
admin1/system1/sp1/account1-16/identity3	IPMI 識別 (シリアル) アカウント
admin1/system1/sp1/account1-16/identity4	CLP 識別アカウント
admin1/system1/sp1/acctsvc1	MFA アカウント管理サービス
admin1/system1/sp1/acctsvc2	IPMI アカウント管理サービス
admin1/system1/sp1/acctsvc3	CLP アカウント管理サービス
admin1/system1/sp1/group1-5	Active Directory グループ
admin1/system1/sp1/group1-5/identity1	Active Directory 識別
admin1/system1/sp1/ADSvc1	Active Directory サービス
admin1/system1/sp1/rolesvc1	ローカルロールベース認証 (RBA) サービス
admin1/system1/sp1/rolesvc1/Role1-16	ローカルロール
admin1/system1/sp1/rolesvc1/Role1-16/privilege1	ローカルロール権限
admin1/system1/sp1/rolesvc1/Role17-21/	Active Directory ロール
admin1/system1/sp1/rolesvc1/Role17-21/privilege1	Active Directory 権限
admin1/system1/sp1/rolesvc2	IPMI RBA サービス
admin1/system1/sp1/rolesvc2/Role1-3	IPMI ロール
admin1/system1/sp1/rolesvc2/Role4	IPMI シリアルオーバー LAN (SOL) ロール
admin1/system1/sp1/rolesvc3	CLP RBA サービス
admin1/system1/sp1/rolesvc3/Role1-3	CLP ロール
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	CLP ロール権限
admin1/system1/sp1/pwrutilmgtsvc1	電源使用管理サービス
admin1/system1/sp1/pwrutilmgtsvc1/pwrcurr1	電源使用管理サービスの電力設定割り当て設定データ
admin1/system1/sp1/metricsvc1	メトリックサービス
/admin1/system1/sp1/metricsvc1/cumbmd1	累積ベースメトリック定義
/admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1	累積ベースメトリック値
/admin1/system1/sp1/metricsvc1/cumwattamd1	累積ワット集約メトリック定義
/admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1	累積ワット集約メトリック値
/admin1/system1/sp1/metricsvc1/cumampamd1	累積アンペア集約メトリック定義
/admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1	累積ワット集約メトリック値
/admin1/system1/sp1/metricsvc1/loamd1	低累積メトリック定義
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	低累積メトリック値
/admin1/system1/sp1/metricsvc1/hiamd1	高累積メトリック定義
/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*	高累積メトリック値
/admin1/system1/sp1/metricsvc1/avgamd1	平均累積メトリック定義
/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*	平均累積メトリック値

[目次ページに戻る](#)

[目次ページに戻る](#)

VMCLI を使ってオペレーティングシステムを導入する

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [作業を開始する前に](#)
- [起動イメージファイルの作成](#)
- [導入の準備](#)
- [オペレーティングシステムの導入](#)
- [VMCLI ユーティリティの使用](#)

仮想メディアコマンドラインインタフェース (VMCLI) ユーティリティは、管理ステーションからリモートシステムの iDRAC6 に仮想メディアの機能を提供するコマンドラインインタフェースです。VMCLI とスクリプトメソッドの使用によって、オペレーティングシステムをネットワーク上の複数のリモートシステムに導入できます。

ここでは、VMCLI ユーティリティを会社のネットワークに組み込む方法について説明します。

作業を開始する前に

VMCLI ユーティリティを使う前に、対象となるリモートシステムと会社のネットワークが以下の項に記載する要件を満たしていることを確認してください。

リモートシステム要件

各リモートシステムで iDRAC6 が設定されている。

ネットワーク要件

ネットワーク共有に以下のコンポーネントが含まれている。

- 1 オペレーティングシステムファイル
- 1 必要なドライバ
- 1 オペレーティングシステムの起動イメージファイル

イメージファイルは、業界標準のブータブルフォーマットのオペレーティングシステム CD か CD/DVD ISO イメージである必要があります。

起動イメージファイルの作成

イメージファイルをリモートシステムに導入する前に、サポートされているシステムがそのファイルから起動できることを確認してください。イメージファイルをテストするには、iDRAC6 ウェブユーザーインターフェースを使用してイメージファイルをテストシステムに転送してから、システムを再起動します。

以下の項では、Linux と Microsoft® Windows® システム用のイメージファイルの作成方法について説明します。

Linux システム用のイメージファイルの作成

Linux システム用にブータブルイメージファイルを作成するには、データ複製ユーティリティ (dd) を使用します。

ユーティリティを実行するには、コマンドプロンプトを開いて次のように入力します。

```
dd if=<入力デバイス> of=<出力ファイル>
```

例:

```
dd if=/dev/sdc0 of=mycd.img
```

Windows システム用のイメージファイルの作成

Windows イメージファイル用のデータ複製ユーティリティを選択する際、イメージファイルと CD/DVD ブートセクターをコピーするユーティリティを選択してください。

導入の準備

リモートシステムの設定

1. 管理ステーションからアクセスできるネットワーク共有フォルダを作成します。
2. オペレーティングシステムファイルをネットワーク共有フォルダにコピーします。
3. オペレーティングシステムをリモートシステムに導入するためのブータブルな設定済み展開イメージファイルがある場合は、このステップをスキップしてください。

設定済みのブータブルな展開イメージファイルがない場合は、このファイルを作成します。オペレーティングシステムの導入手順に使用されるプログラムやスクリプトをすべて含めます。

たとえば、Windows オペレーティングシステムを導入する場合、イメージファイルには Microsoft Systems Management Server (SMS) で使用する導入方法に類似したプログラムを含むことができます。

イメージファイルを作成するときは、以下の操作を行ってください。

- 1 標準的なネットワークベースのインストール手順に従う
 - 1 対象システムのそれぞれが同じ導入プロセスを起動して実行するように、導入イメージを「読み取り専用」とマークする
- 1 次のいずれかの手順を実行してください。
 - 1 既存のオペレーティングシステム導入アプリケーションに IPMI tool と VMCLI を組み込みます。ユーティリティを使用する際の手引きとして `vm6deploy` サンプルスクリプトを使用します。
 - 1 オペレーティングシステムの導入には、既存の `vm6deploy` スクリプトを使用します。

オペレーティングシステムの導入

VMCLI ユーティリティとそのユーティリティに含まれている `vm6deploy` スクリプトを使って、リモートシステムにオペレーティングシステムを導入します。

始める前に、VMCLI ユーティリティに含まれているサンプル `vm6deploy` スクリプトを見直してください。このスクリプトは、ネットワーク内のリモートシステムにオペレーティングシステムを導入するために必要な詳しい手順を説明しています。

以下の手順は、ターゲットのリモートシステムにオペレーティングシステムを導入するための概要です。

1. `ip.txt` テキストファイルに、導入するリモートシステムの iDRAC6 IPv4 アドレス(1 行に 1 つの IPv4 アドレス)を入力します。
2. ブータブルオペレーティングシステム CD または DVD をクライアントメディアドライブに挿入します。
3. コマンドラインで `vm6deploy` を実行します。

`vm6deploy` スクリプトを実行するには、コマンドプロンプトで次のコマンドを入力します。

```
vm6deploy -r ip.txt -u <iDRAC-user> -p <iDRAC-passwd> -c {<iso9660-img> | <path>} -f {<111128899.590floppy-img> | <path>}
```

このコマンドで、


- 1 <iDRAC6 ユーザー> は iDRAC ユーザー名です(例:`root`)。
- 1 <iDRAC6 パスワード> は iDRAC ユーザーのパスワードです(例:`calvin`)。
- 1 <iso9660-img> は、オペレーティングシステムインストール CD または DVD の ISO9660 イメージのパスです。
- 1 <パス> は、オペレーティングシステムインストール CD、DVD、またはフロッピーに含まれるデバイスのパスです。
- 1 <フロッピーイメージ> は有効なフロッピーイメージのパスです。

`vm6deploy` スクリプトは、コマンドラインオプションを VMCLI ユーティリティに渡します。これらのオプションの詳細については、「[コマンドラインオプション](#)」を参照してください。このスクリプトの `-r` オプションの処理方法は、`vmcli -r` オプションとは若干異なります。`-r` オプションの引数が既存のファイル名である場合、スクリプトは指定したファイルから iDRAC6 IPv4 アドレスを読み取り、各行で VMCLI ユーティリティを一度実行します。`-r` オプションの引数が既存のファイル名でない場合は、単独の iDRAC6 のアドレスになります。この場合、`-r` は VMCLI ユーティリティの説明通りに機能します。

VMCLI ユーティリティの使用

VMCLI ユーティリティは、管理ステーションから iDRAC6 に仮想メディアの機能を提供するスクリプト可能なコマンドラインインタフェースです。

VMCLI ユーティリティは次の機能を持ちます。

 **メモ:** 読み取り専用のイメージファイルを仮想化するとき、複数セッションで同一イメージメディアを共有できる。物理ドライブを仮想化するとき、1 度に 1 つのセッションが指定の物理ドライブにアクセスできる。

- 1 仮想メディアプラグインに対応したリムーバブルデバイスまたはイメージファイル
- 1 iDRAC6 ファームウェアのブートワンスオプションが有効の場合の自動終了

- 1 セキュアソケットレイヤ(SSL)を使用した iDRAC6 へのセキュアな通信

ユーティリティを実行する前に、iDRAC6 に対し仮想メディアのユーザー権限があることを確認してください。

オペレーティングシステムが管理者権限、オペレーティングシステム固有の権限、またはグループメンバーシップをサポートしている場合、VMCLI コマンドを実行するためには管理者権限も必要です。

クライアントシステムの管理者(Administrator)は、ユーザーグループと権限を制御するので、このユーティリティを実行できるユーザーも制御することになります。

Windows システムでは、VMCLI ユーティリティを実行するためにはパワーユーザー権限が必要です。


Linux システムでは、**sudo** コマンドを使うことで管理者権限なしで VMCLI コマンドにアクセスできます。このコマンドは、Administrator(システム管理者)以外のアクセス権を一元的に与える手段となり、すべてのユーザーコマンドをログに記録します。VMCLI グループへのユーザーの追加や編集を行う場合、システム管理者は **visudo** コマンドを使用します。管理者権限を持たないユーザーは、**sudo** コマンドを VMCLI コマンドライン(または VMCLI スクリプト)のプレフィックスとして追加することでリモートシステムの iDRAC6 へのアクセス権を取得し、このユーティリティを実行できます。

VMCLI ユーティリティのインストール

VMCLI ユーティリティは、Dell OpenManage システム管理ソフトウェアキットに含まれている『Dell Systems Management Tools and Documentation DVD』に収録されています。このユーティリティをインストールするには、『Dell Systems Management Tools and Documentation DVD』をシステムの DVD ドライブに挿入して画面に表示される指示に従ってください。

『Dell Systems Management Tools and Documentation DVD』には、診断、ストレージ管理、リモートアクセスサービス、IPMI tool ユーティリティなど最新のシステム管理ソフトウェア製品が含まれています。この DVD には、システム管理ソフトウェアの最新の製品情報が含まれた Readme ファイルも入っています。

『Dell Systems Management Tools and Documentation DVD』にはまた、iMCLI と IPMI tool ユーティリティを使ってソフトウェアを複数のリモートシステムに導入する方法を示す **vm6deploy** と呼ばれるサンプルスクリプトも収録されています。

 **メモ:** **vm6deploy** スクリプトは、インストール時にディレクトリに存在する他のファイルに依存しています。別のディレクトリからスクリプトを使用する場合は、一緒にすべてのファイルをコピーする必要があります。IPMI tool ユーティリティがインストールされていない場合は、これもコピーする必要があります。

コマンドラインオプション

VMCLI インタフェースは Windows と Linux システムで全く同じです。

VMCLI コマンド形式は次のとおりです。

```
VMCLI [parameter] [operating_system_shell_options]
```

コマンドライン構文では、大文字と小文字が区別されます。詳細については、「[VMCLI パラメータ](#)」を参照してください。

リモートシステムでコマンドが受け入れられ、iDRAC6 が接続を許可した場合は、次のどちらかが発生するまでコマンドの実行が続行します。

- 1 何らかの理由で VMCLI 接続が切られた場合。
- 1 オペレーティングシステムのコントロールを使用して処理が手動で中止された場合。たとえば、Windows でタスク マネージャを使うと処理を終了できます。

VMCLI パラメータ

iDRAC6 IP アドレス

```
-e <iDRAC IP アドレス>[:<iDRAC SSL ポート>]
```

このパラメータは、iDRAC6 の IPv4 アドレスと SSL ポートを提供します。これらは、ユーティリティがターゲット iDRAC6 と仮想メディア接続を確立するために必要です。無効な IPv4 アドレスまたは DDNS 名を入力すると、エラーメッセージが表示されてコマンドは終了します。

<iDRAC -IP- アドレス> は有効な固有の IPv4 アドレスまたは iDRAC6 動的ドメインネームシステム(DDNS)名です(サポートしている場合)。<iDRAC SSL ポート> を省くと、ポート 443(デフォルトポート)が使用されます。iDRAC6 のデフォルト SSL ポートを変更していない限り、オプションの SSL ポートは不要です。

iDRAC6 ユーザー名

```
-u <iDRAC ユーザー名>
```

このパラメータは仮想メディアを実行する iDRAC6 ユーザー名を提供します。

<iDRAC ユーザー名> には、次の属性が必要です。

- 1 有効なユーザー名
- 1 iDRAC6 仮想メディアユーザー権限

iDRAC6 の認証に失敗した場合は、エラーメッセージが表示されてコマンドが終了します。

iDRAC6 ユーザーパスワード

-p <iDRAC ユーザーパスワード>


このパラメータは、指定した iDRAC6 ユーザーのパスワードを提供します。

iDRAC6 の認証に失敗した場合は、エラーメッセージが表示されてコマンドが終了します。

フロッピー / ディスクデバイスまたはイメージファイル

-f {<device-name> | <イメージファイル>}

ここで、<デバイス名> は有効なドライブ文字 (Windows システム) または有効なデバイスファイル名 (Linux システム) です。<イメージファイル> は有効なイメージファイルのファイル名とパスです。

 **メモ:** VMCLI ではマウントポイントはサポートされていません。

このパラメータは、仮想フロッピー / ディスクメディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

-f c:\temp\myfloppy.img (Windows システム)


-f /tmp/myfloppy.img (Linux システム)

イメージファイルが書き込み保護されていない場合、仮想メディアはそのファイルに書き込むことができます。上書きしてはならないフロッピーイメージファイルへの書き込みを保護するようにオペレーティングシステムで設定します。

たとえば、デバイスは次のように指定します。

-f a:\ (Windows システム)

-f /dev/sdb4 # デバイス上の 4 番目のパーティション /dev/sdb (Linux システム)

 **メモ:** Red Hat® Enterprise Linux® バージョン 4 では、複数 LUN はサポートされておらず、サポートされる予定也没有ありません。カーネルはこの機能をサポートしますが、次の手順で Red Hat Enterprise Linux バージョン 4 が複数 LUN を持つ SCSI デバイスを認識するようにする必要があります。

1. /etc/modprobe.conf を編集して、次の行を追加します。
options scsi_mod max_luns=8
(LUN の数としては 8 だけでなく、2 以上の任意の数を指定することができます。)
2. コマンドラインで次のコマンドを入力することで、カーネルイメージの名前を取得します。

uname -r
3. /boot ディレクトリに移動し、ステップ 2 で取得した名前を持つカーネルイメージファイルを削除します。

mkinitrd /boot/initrd-`uname -r`.img `uname -r`
4. サーバーを再起動します。
5. 次のコマンドを実行して、ステップ 1 で指定した LUN 数だけの複数 LUN のサポートが追加されたことを確認します。

```
cat /sys/modules/scsi_mod/max_luns
```

デバイスに書き込み保護機能がある場合は、その機能を使用して仮想メディアがメディアに書き込めないようにしてください。

フロッピーメディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出されたら、エラーメッセージが表示されてコマンドが終了します。

CD/DVD デバイスまたはイメージファイル

-c {<デバイス名> | <イメージファイル>}

<デバイス名> は有効な CD/DVD ドライブ文字 (Windows システム) または有効な CD/DVD デバイスファイル名 (Linux システム) で、<イメージファイル> は有効な ISO-9660 イメージファイルのファイル名とパスです。

このパラメータは、仮想 CD/DVD-ROM メディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

-c c:\temp\mydvd.img (Windows システム)

-c /tmp/mydvd.img (Linux システム)

たとえば、デバイスは次のように指定します。

-c d:\ (Microsoft® Windows® システム)

-c /dev/cdrom (Linux システム)

CD/DVD メディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出されたら、エラーメッセージが表示されてコマンドが終了します。

スイッチオプションしかない場合を除き、このコマンドを使って少なくとも 1 つのメディアタイプ(フロッピーまたは CD/DVD ドライブ)を指定します。指定しないと、エラーメッセージが表示されてコマンドが終了します。

バージョン表示

-v

このパラメータは VMCLI ユーティリティのバージョンを表示するために使用します。その他の非スイッチオプションが提供されていない場合、コマンドはエラーメッセージなしで終了します。

ヘルプの表示

-h

このパラメータは、VMCLI ユーティリティパラメータの概要を示します。その他の非スイッチオプションが提供されていない場合、コマンドはエラーなしで終了します。

暗号化データ

-e

このパラメータがコマンドラインに含まれていると、VMCLI は SSL-暗号化チャネルを使用して、管理ステーションとリモートシステムの iDRAC6 間でデータを転送します。このパラメータがコマンドラインに含まれていない場合は、データ転送が暗号化されません。


 **メモ:** このオプションを使用しても、RACADM やウェブインタフェースなどその他の iDRAC6 設定インタフェースに表示されている仮想メディアの暗号化状態は 有効 には変更されません。

VMCLI オペレーティングシステムシェルオプション

VMCLI コマンドラインでは次のオペレーティングシステム機能が使用できます。

- 1 stderr/stdout redirection - 印刷されたユーティリティの出力をファイルにリダイレクトします。

たとえば、「より大」の不等号 (>)にファイル名を続けると、指定したファイルが VMCLI ユーティリティの印刷出力で上書きされます。

 **メモ:** VMCLI ユーティリティは標準入力 (stdin) からは読み込みません。このため、stdin リダイレクションは不要です。

- 1 バックグラウンドでの実行- デフォルトで VMCLI ユーティリティはフォアグラウンドで実行されます。オペレーティングシステムのコマンドシェル機能を使用すると、ユーティリティをバックグラウンドで実行できます。たとえば、Linux オペレーティングシステムでは、コマンドに続いてアンパサンド(&)を指定すると、プログラムから新しいバックグラウンドプロセスが生成されます。

後者の方法はスクリプトプログラムの場合に便利です。VMCLI コマンドの新しいプロセスが開始した後、スクリプトを継続できます(そうでない場合は、VMCLI プログラムが終了するまでスクリプトがロックされます)。VMCLI の複数のインスタンスがこの方法で開始し、コマンドインスタンスの 1 つ以上を手動で終了しなければならない場合は、オペレーティングシステムに固有の機能を使用して、プロセスをリストにして終了します。

VMCLI 戻りコード

エラーが発生した場合は、標準エラー出力に英語のみのテキストメッセージも表示されます。

[目次ページに戻る](#)

[目次ページに戻る](#)

Intelligent Platform Management Interface (IPMI) の設定

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

- [IPMI の設定](#)
- [ウェブベースのインタフェースによる Serial Over LAN の設定](#)

IPMI の設定

ここでは、iDRAC6 IPMI インタフェースの設定と使用について説明します。インタフェースには以下が含まれます。

- 1 LAN 上の IPMI
- 1 IPMI オーバーシリアル
- 1 シリアルオーバー LAN

iDRAC6 は完全に IPMI 2.0 対応です。以下を使用して iDRAC6 IPMI を設定できます。

- 1 お使いのブラウザからの iDRAC6 GUI
- 1 IPMITool などのオープンソースユーティリティ
- 1 Dell® OpenManage® IPMI シェル、**ipmish**
- 1 RACADM

IPMI シェル、ipmish の使い方の詳細については、support.dell.com/manualsにある『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

RACADM の使い方の詳細については、[「RACADM のリモート使用」](#)を参照してください。

ウェブベースインタフェースを使った IPMI の設定

詳細については、[「IPMI の設定」](#)を参照してください。

RACADM CLI を使った IPMI の設定

1. RACADM インタフェースを使ったリモートシステムへのログイン「[RACADM のリモート使用](#)を参照してください。
2. IPMI オーバー LAN を設定します。

コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

 **メモ:** この設定によって、IPMI オーバー LAN インタフェースから実行できる IPMI コマンドが決まります。詳細については、IPMI 2.0 の仕様を参照してください。

- a. IPMI チャネル権限を更新します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <レベル>
```


<レベル> は次のいずれかです。

- 2 (ユーザー)
- 3 (オペレータ)
- 4 (管理者)

たとえば、IPMI LAN チャネル権限を 2(ユーザー) に設定するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

- b. 必要なら IPMI LAN チャネルの暗号キーを設定します。

 **メモ:** iDRAC6 IPMI は RMCP+ プロトコルに対応しています。詳細については、IPMI 2.0 仕様を参照してください。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <キー>
```


<キー> は有効な 16 進数 形式の 20 文字からなる暗号キーです。

3. IPMI シリアルオーバー LAN (SOL)を設定します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

- a. IPMI SOL の最低権限レベルを更新します。

 **メモ:** IPMI SOL 最低権限レベルは、IPMI SOL をアクティブにするために最低限必要な権限を決定します。詳細については、IPMI 2.0 の仕様を参照してください。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <レベル>
```


<レベル> は次のいずれかです。

- o 2 (ユーザー)
- o 3 (オペレータ)
- o 4 (管理者)

たとえば、IPMI 権限を 2 (ユーザー) に設定するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

- b. IPMI SOL ボーレートをアップデートします。

 **メモ:** シリアルコンソールを LAN 経由でリダイレクトする場合、SOL ボーレートが管理下システムのボーレートと同等であることを確認してください。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。


```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <ボーレート>
```

ここで、<ボーレート> は 9600、19200、57600、または 115200 bps です。

例:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

- c. 個々のユーザーに対して SOL 有効にします。

 **メモ:** SOL は個々のユーザーに対して有効または無効にできます。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

<ID> はユーザーの固有の ID です。

4. IPMI シリアルを設定します。

- a. IPMI シリアル接続モードを適切な設定に変更します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

- b. IPMI シリアルボーレートを設定します。

コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <ボーレート>
```

ここで、<ボーレート> は 9600、19200、57600、または 115200 bps です。

例:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

- c. IPMI シリアルハードウェアフロー制御を有効にします。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

- d. IPMI シリアルチャネルの最低権限レベルを設定します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <レベル>
```

<レベル> は次のいずれかです。

- o 2 (ユーザー)
- o 3 (オペレータ)
- o 4 (管理者)

たとえば、IPMI シリアルチャネル権限を 2 (ユーザー) に設定するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

- e. BIOS セットアッププログラムでシリアル MUX が正しく設定されていることを確認します。

- o システムを再起動します。
- o POST 中に F2 を押して BIOS セットアッププログラムを起動します。
- o **シリアル通信** に移動します。
- o **シリアル接続** メニューで **外部シリアルコネクタ** が **リモートアクセスデバイス** に設定されていることを確認します。
- o 保存して BIOS セットアッププログラムを終了します。
- o システムを再起動します。

IPMI の設定が完了しました。

IPMI シリアルが端末モードの場合は、`racadm config cfgIpmiSerial` コマンドを使って次の設定を追加できます。

- o 削除制御
- o エコー制御
- o Line edit
- o New line sequences
- o Input new line sequences

For more information about these properties, see the IPMI 2.0 specification.

IPMI リモートアクセスシリアルインタフェースの使用

IPMI シリアルインタフェースでは、次のモードが使用できます。

- 1 **IPMI 端末モード** - シリアル端末から送信された ASCII コマンドをサポートします。コマンドセット内のコマンド(電源制御を含む)の数は限られていますが、16 進形式の ASCII 文字で入力された生の IPMI コマンドをサポートしています。
- 1 **IPMI 基本モード** - プログラムへのアクセス用に、Baseboard Management Utility (BMU) に含まれている IPMI シェル (IPMISH) など、バイナリインタフェースをサポートしていません。

RACADM を使って IPMI モードを設定するには:

1. RAC シリアルインタフェースを無効にします。

コマンドプロンプトで、次のコマンドを入力します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

2. 適切な IPMI モードを有効にします。


たとえば、コマンドプロンプトで次のコマンドを入力します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 or 1>
```

詳細については、「[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)」を参照してください。

ウェブベースのインタフェースによる Serial Over LAN の設定

詳細については、「[IPMI の設定](#)」を参照してください。

 **メモ:** Serial Over LAN は、次の Dell OpenManage ツールで使用することができます: SOLProxy および IPMItool。詳細については、support.dell.com/manualsにある『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC 設定ユーティリティの使用

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [概要](#)
- [iDRAC 設定ユーティリティの起動](#)
- [iDRAC 設定ユーティリティの使用](#)

概要


iDRAC 設定ユーティリティは、iDRAC6 および管理下サーバーのパラメータを表示および設定できる起動前の設定環境です。具体的には、以下のことが可能です。

- 1 iDRAC6 および一次バックプレーンのファームウェアリビジョン番号を表示する
- 1 iDRAC6 ローカルエリアネットワークを設定する、有効または無効にする
- 1 IPMI オーバー LAN の有効または無効にする
- 1 LAN パラメータの設定
- 1 仮想メディアの設定
- 1 スマートカードの設定
- 1 システム管理者のユーザー名およびパスワードを変更する
- 1 iDRAC 設定を出荷時のデフォルトに戻す
- 1 システムイベントログ (SEL) メッセージを表示する、またはログからメッセージをクリアする
- 1 LCD の設定
- 1 システムデバイスの設定

iDRAC 設定ユーティリティを使用して実施できるタスクは、SM-CLP コマンドラインインタフェースやローカル RACADM コマンドラインインタフェースなどの iDRAC または Dell™ OpenManage™ ソフトウェアで提供されるその他のユーティリティを使用して行うことも可能です。

iDRAC 設定ユーティリティの起動

1. サーバーの前面にある電源ボタンを押してサーバーの電源を入れるか、再起動します。
2. <Ctrl-E> を押し、5 秒以内にリモートアクセスのセットアップを というメッセージが表示されたら、すぐに <Ctrl><E> を押します。

 **メモ:** <Ctrl><E> キーを押す前にオペレーティングシステムがロードを開始した場合は、起動が完了するのを待ってからシステムを再起動して、もう一度やり直してください。

iDRAC 設定ユーティリティが表示されます。最初の 2 行に、iDRAC6 ファームウェアと一次バックプレーンファームウェアのリビジョンに関する情報が表示されます。リビジョンレベルは、ファームウェアアップグレードが必要かどうかを決定するのに役立ちます。

iDRAC6 ファームウェアは、ウェブインタフェース、SM-CLP など、外部インタフェースに関連するファームウェアの一部です。一次バックプレーンファームウェアは、サーバーのハードウェア環境とインタフェースし、それを監視するファームウェアの一部です。

iDRAC 設定ユーティリティの使用

ファームウェアのリビジョンメッセージの下の iDRAC 設定ユーティリティの残りの部分は、上向き矢印キーと下向き矢印キーを使用してアクセスできるメニューアイテムです。

- 1 メニュー項目からサブメニューまたは編集可能なテキストフィールドが表示されたら、Enter キーを押してその項目にアクセスし、設定が終了したら Esc キーを押します。
- 1 項目には / いいえ、有効 / 無効 など選択可能な値がある場合は、左向き矢印 キーまたは右向き矢印キー、スペース キーを押して値を選択します。
- 1 編集不可能な項目は青色で表示されます。項目によっては、他の選択内容によって編集可能になるものがあります。
- 1 画面の下部に現在の項目の操作手順が表示されます。F1 キーを押すと現在の項目のヘルプを表示できます。
- 1 iDRAC 設定ユーティリティの使用を終えたら、Esc キーを押して 終了 メニューを表示します。このメニューでは、変更の保存または無視を選択できるほか、ユーティリティに戻ることもできます。

次の項では、iDRAC 設定ユーティリティのメニュー項目について説明します。

iDRAC6 LAN

左矢印、右矢印、スペースキーを使用して **オン** または **オフ** を選択します。

iDRAC6 LAN は、デフォルト設定では有効になっています。LAN は、ウェブインタフェース、SM-CLP コマンドラインインタフェースへの Telnet/SSH および RAC シリアルアクセス、コンソールリダイレクト、仮想メディアなど iDRAC6 機能の使用を許可するために有効にする必要があります。

LAN を無効にすると、次の警告が表示されます。

LAN チャンネルがオフの場合、iDRAC6 帯域外インタフェースは無効になります。

任意のキーを押してメッセージをクリアし、続行します。

このメッセージでは、LAN が無効になっていると、iDRAC6 HTTP、HTTPS、Telnet、または SSH ポートに直接接続されている装置にアクセスできないだけでなく、管理ステーションから iDRAC6 に送信される IPMI メッセージなどの帯域外管理ネットワークトラフィックも受信できないことが通知されます。ただし、ローカル RACADM インタフェースは使用可能で、iDRAC6 LAN の再設定に使用できます。

IPMI オーバー LAN

<左矢印>、<右矢印>、およびスペースキーを押して **オン** または **オフ** を選択します。**オフ** を選択すると、iDRAC6 は LAN インタフェース経由での IPMI メッセージを受け入れられません。

オフ を選択すると、次の警告が表示されます。

iDRAC IPMI Over LAN Out-of-Band interface will be disabled if the LAN Channel is OFF.

(LAN チャンネルがオフの場合、iDRAC IPMI オーバー LAN 帯域外インタフェースは無効になります。)

任意のキーを押してメッセージをクリアし、続行します。メッセージの説明は、「[iDRAC6 LAN](#)」を参照してください。

LAN パラメータ

LAN パラメータのサブメニューを表示するには、Enter キーを押します。LAN パラメータの設定を終えた後、Esc キーを押すと前のメニューに戻ります。

表 15-1 LAN パラメータ

項目	説明
共通設定	
NIC の選択	<右矢印>、<左矢印> およびスペースキーを押して、モードを切り替えます。 専用、共有、Shared with Failover LOM2 (LOM2 へのフェールオーバーありで共有) および Shared with Failover All LOMs (すべての LOM へのフェールオーバーありで共有) のモードから選択できます。 これらのモードは、iDRAC と外界との通信に該当するインタフェースを使用できるようにします。
MAC Address	これは、iDRAC6 ネットワークインタフェースの編集不可能な MAC アドレスです。
VLAN の有効化	iDRAC6 の仮想 LAN フィルタを有効にするには、 オン を選択します。
VLAN ID	VLAN を有効にする が オン に設定する場合、VLAN ID を 1 から 4094 の範囲で入力します。
VLAN	VLAN を有効にする が オン に設定する場合、VLAN の優先度を 0 から 7 の範囲で選択します。
iDRAC6 名の登録	オン を選択すると DNS サービスに iDRAC6 名を登録できます。ユーザーが DNS 内で iDRAC6 名を見えないようにするには、 オフ を選択します。
iDRAC6 名	iDRAC 名の登録を オン に設定すると、Enter キーを押して 現在の DNS iDRAC 名 テキストフィールドを編集できます。iDRAC6 名の編集が終了したら <Enter> キーを押します。前のメニューに戻るには、<Esc> キーを押します。iDRAC6 名は有効な DNS ホスト名でなければなりません。
DHCP からのドメイン名	ネットワーク上の DHCP サービスからドメイン名を取得するには、 オン を選択します。ドメイン名を指定するには、 オフ を選択します。
ドメイン名	DHCP からのドメイン名が オフ の場合、<Enter> キーを押して、 現在のドメイン名 テキストフィールドを編集します。編集を終えたら Enter キーを押します。前のメニューに戻るには、<Esc> キーを押します。ドメイン名は、有効な DNS ドメイン (例: mycompany.com) でなければなりません。
ホスト名文字列	Enter キーを押して編集します。プラットフォームイベントトラップ (PET) 警告を有効にするホスト名を入力します。
LAN 警告有効	PET LAN 警告を有効にするには、 オン を選択します。
警告ポリシーエントリ 1	有効 または 無効 を選択すると、最初の送信先がアクティブになります。
警告送信先 1	LAN 警告を有効にする が オン に設定されている場合、PET LAN 警告の転送先となる IP アドレスを入力します。
IPv4 設定	IPv4 接続に対するサポートを有効または無効にします。
IPv4	IPv4 プロトコルのサポートに対して、 有効 または 無効 を選択します。
RMCP+ 暗号化キー	<Enter> キーを押して値を編集し、終了したら <Esc> キーを押します。RMCP+ 暗号化キーは、40 文字の 16 進法の文字列 (文字 0 ~ 9、a ~ f、A ~ F) です。RMCP+ は認証および暗号化を IPMI に追加する IPMI のエクステンションです。デフォルト値は 0 (ゼロ) を 40 個連ねたものです。
IP アドレスソース	DHCP または 静的 を選択します。DHCP を選択すると、DHCP サーバーから Ethernet IP アドレス、サブネットマスク、デフォルトゲートウェイ フィールドが取得されます。ネットワーク上に DHCP が見つからない場合、フィールドはゼロに設定されます。 静的 を選択すると、 Ethernet IP アドレス、サブネットマスク、デフォルトゲートウェイ アイテムは編集可能になります。
Ethernet IP アドレス	IP アドレスソース を DHCP に設定すると、このフィールドには DHCP から取得された IP アドレスが表示されます。 IP アドレスソース を 静的 に設定する場合、iDRAC6 に割り当てる IP アドレスを入力します。


	デフォルトは 192.168.0.120 です。
サブネットマスク	IP アドレスソースを DHCP に設定すると、このフィールドには DHCP から取得したサブネットマスクアドレスが表示されます。 IP アドレスソースを 静的 に設定する場合は、iDRAC6 のサブネットマスクを入力します。デフォルトは 255.255.255.0 です。
デフォルトゲートウェイ	IP アドレスソースを DHCP に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイのアドレスが表示されます。 IP アドレスソースを 静的 に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。デフォルトは 192.168.0.1 です。
DHCP からの DNS サーバー	オン を選択するとネットワーク上の DHCP サービスから DNS サーバーアドレスが取得されます。 オフ を選択すると以下の DNS サーバーアドレスを指定できます。
DNS サーバー 1	DHCP からの DNS サーバーが オフ の場合、最初の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	DHCP からの DNS サーバーが オフ の場合、2 番目の DNS サーバーの IP アドレスを入力します。
IPv6 の設定	IPv6 接続に対するサポートを有効または無効にします。
IP アドレスソース	AutoConfig(自動設定) または 静的 のいずれかを選択します。AutoConfig(自動設定) を選択すると、IPv6 アドレス 1、プレフィックス長、およびデフォルトゲートウェイフィールドの値は DHCP から取得されます。 静的 を選択すると、IPv6 アドレス 1、プレフィックス長、デフォルトゲートウェイフィールドは編集可能になります。
IPv6 アドレス 1	IP アドレスソースを AutoConfig(自動設定) に設定すると、このフィールドには DHCP から取得された IP アドレスが表示されます。 IP アドレスソースを 静的 に設定する場合、iDRAC6 に割り当てる IP アドレスを入力します。
プレフィックス長	IPv6 アドレスのプレフィックス長を設定します。この値は、1 ~ 128 です。
デフォルトゲートウェイ	IP アドレスソースを AutoConfig(自動設定) に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイの IP アドレスが表示されます。 IP アドレスソースを 静的 に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。
IPv6 リンクローカルアドレス	これは、iDRAC ネットワークインタフェースの編集不可能な IPv6 リンクローカルアドレスです。
IPv6 アドレス 2	これは、iDRAC ネットワークインタフェースの編集不可能な IPv6 アドレス 2 です。
DHCP からの DNS サーバー	オン を選択するとネットワーク上の DHCP サービスから DNS サーバーアドレスが取得されます。 オフ を選択すると以下の DNS サーバーアドレスを指定できます。
DNS サーバー 1	DHCP からの DNS サーバーが オフ の場合、最初の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	DHCP からの DNS サーバーが オフ の場合、最初の DNS サーバーの IP アドレスを入力します。
LAN 詳細設定	
オートネゴシエート	NIC の選択が 専用 に設定する場合、 有効 または 無効 のいずれかを選択します。 有効 を選択する場合、LAN スピード設定 および LAN デュプレックス設定は自動的に設定されます。
LAN の速度設定	オートネゴシエート を 無効 に設定する場合、10Mbps または 100Mbps のいずれかを選択します。
LAN の二重設定	オートネゴシエート を 無効 に設定する場合、 半二重 または 全二重 のいずれかを選択します。

仮想メディアの設定

仮想メディア

<Enter> キーを押して、**分離**、**連絡**、または**自動連絡**を選択します。**連絡**を選択すると、仮想メディアデバイスが USB バスに接続され、**コンソールリダイレクト**セッション中に使用可能になります。

分離を選択すると、ユーザーは **コンソールリダイレクト**セッション中に仮想メディアデバイスにアクセスできません。


 **メモ:** 仮想メディア機能で USB フラッシュドライブを使用するには、BIOS 設定ユーティリティで **USB フラッシュドライブのエミュレーションタイプ**を **ハードディスク**に設定してください。BIOS 設定ユーティリティへは、サーバー起動中に F2 キーを押すとアクセスできます。USB フラッシュドライブのエミュレーションタイプが **自動**に設定されていると、フラッシュドライブはシステムでフロッピードライブとして表示されます。

仮想フラッシュ

<Enter> キーを押して、**無効**または**有効**を選択します。


有効 / **無効** に選択することにより、すべての仮想メディアデバイスが USB バスから **分離**または**連絡**されます。

無効にすると、仮想フラッシュが取り外され使用できなくなります。

 **メモ:** 256 MB 以上の容量を持つ SD カードが iDRAC6 Express カードスロットに存在しない場合は、このフィールドは読み取り専用になります。

スマートカードのログイン


<Enter> キーを押して、**無効**または**有効**を選択します。このオプションは、スマートカードログイン機能を設定します。**有効**、**無効** および **Enabled with RACADM(RACADM で有効)** のオプションから選択できます。

 **メモ:** **有効**を選択する場合、IPMI オーバー LAN はオフになり、編集できなくなります。

システムサービス設定

システムサービス

<Enter> キーを押して、**無効** または **有効** を選択します。詳細については、デルサポートサイト support.dell.com/manuals にある『Dell Unified Server Configurator ユーザーズガイド』を参照してください。

 **メモ:** このオプションを変更し、新しい設定を適用するために**保存**して、**終了**すると、サーバーが再起動します。

システムサービスのキャンセル

<Enter> キーを押して、**いいえ** または **はい** を選択します。

はい を選択した場合は、新しい設定を適用するために **保存** して、**終了** すると、すべての Unified Server Configurator セッションが閉じ、サーバーが再起動します。

LCD の設定

LCD 設定 サブメニューを表示するには、<Enter> キーを押します。LCD パラメータの設定を終えた後、<Esc> キーを押すと前のメニューに戻ります。

表 15-2 LCD ユーザー設定

LCD ライン 1	<右矢印>、<左矢印> およびスペースキーを押して、オプションを切り替えます。 この機能は、LCD 上の ホーム 表示を次のいずれかのオプションに設定します。 周辺温度 、 管理タグ 、 ホスト名 、 iDRAC6 IPv4 アドレス 、 iDRAC6 IPv6 アドレス 、 iDRAC6 MAC アドレス 、 モデル番号 、 なし 、 サービスタグ 、 システム電源 、 ユーザー定義の文字列 。
LCD ユーザー定義の文字列	LCD ライン 1 を ユーザー定義の文字列 に設定する場合、LCD に表示する文字列を入力します。 文字列は、最大 62 文字まで入力できます。
LCD システム電力単位	LCD ライン 1 を システム電源 に設定する場合、LCD に表示する単位を ワット または BTU/時 から選択します。
LCD 周辺温度単位	LCD ライン 1 を 周辺温度 に設定する場合、LCD に表示する単位を 摂氏 または 華氏 から選択します。
LCD エラー表示	Simple (簡易) または SEL (システムイベントログ) を選択します。 この機能は、次のいずれかの形式で LCD にエラーメッセージを表示させることができます。 簡易フォーマットは、イベントの説明を英語で表示します。 SEL フォーマットは、システムイベントログのテキスト文字列を表示します。
LCD のリモート KVM 表示	装置上で仮想 KVM がアクティブの間、テキスト KVM を表示させるには、 有効 を選択します。
LCD フロントパネルアクセス	<右矢印>、<左矢印> およびスペースキーを押して、 無効 、 表示/変更 、および 表示のみ のオプションを切り替えます。 この設定は、LCD におけるユーザーのアクセスレベルを設定します。

LAN ユーザー設定

LAN ユーザーは iDRAC の Administrator (システム管理者) アカウント (デフォルトで **root** [ルート]) です。LAN ユーザー設定のサブメニューを表示するには、Enter キーを押します。LAN ユーザーの設定を終えて、Esc キーを押すと前のメニューに戻ります。

表 15-3 LAN ユーザー設定

項目	説明
アカウントアクセス	有効 を選択すると Administrator (システム管理者) アカウントが有効になります。 無効 を選択すると Administrator (システム管理者) アカウントが無効になります。
アカウント権限	システム管理者 (Admin) 、 ユーザー 、 オペレータ 、 アクセスなし のいずれかを選択します。
アカウントユーザー名	Enter キーを押してユーザー名を編集し、終了したら Esc キーを押します。デフォルトのユーザー名は root (ルート) です。
パスワードを入力する	Administrator (システム管理者) アカウントの新しいパスワードを入力します。入力時に、文字は表示されません。
パスワードの確認	Administrator (システム管理者) アカウントの新しいパスワードを再入力します。入力した文字が パスワードを入力する フィールドに入力した文字と一致しない場合はメッセージが表示され、パスワードを再度入力する必要があります。

デフォルトに戻す

デフォルトに戻す メニュー項目を使用すると、iDRAC6 設定項目がすべて出荷時のデフォルトにリセットされます。これは、システム管理者のユーザーパスワードを忘れた場合や iDRAC6 をデフォルト設定から再設定する場合に必要な可能性があります。

Enter キーを押して項目を選択します。次の警告メッセージが表示されます。

```
Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?
```

```
< NO (Cancel) >
```

```
< YES (Continue) >
```

(出荷時のデフォルト設定に戻すとリモートの非揮発性ユーザー設定が復元されます。続行しますか？)

```
<いいえ (キャンセル) ...>
```

```
<はい (続行) >
```

はい を選択し、Enter キーを押すと iDRAC はデフォルト設定に戻ります。

システムイベントログメニュー

システムイベントログ メニューでは、システムイベントログ (SEL) メッセージを表示したり、ログメッセージをクリアできます。Enter キーを押すと **システムイベントログメニュー** が表示されます。システムはログエントリをカウントし、レコード総数と最新のメッセージを表示します。SEL は、最大 512 のメッセージを保持します。

SEL メッセージを表示するには、**システムイベントログの表示** を選択して Enter キーを押します。左向き矢印 キーを使用すると前の (古い) メッセージに移動し、右向き矢印 キーを押すと次の (新しい) メッセージに移動します。レコード番号を入力するとそのレコードに移動します。SEL メッセージの表示を終了するには Esc キーを押します。

SEL メッセージをクリアするには、**システムイベントログのクリア** を選択して Enter キーを押します。

SEL メニューの使用を終えて、Esc キーを押すと前のメニューに戻ります。

iDRAC 設定ユーティリティの終了

iDRAC 設定の変更が終了し、Esc キーを押すと Exit (終了) メニューが表示されます。

変更を保存して終了 を選択して Enter キーを押すと変更が保存されます。

変更を保存せずに終了 を選択して Enter キーを押すと変更は保存されません。

セットアップに戻る を選択して Enter キーを押すと iDRAC 設定ユーティリティに戻ります。

[目次ページに戻る](#)

[目次ページに戻る](#)

監視と警告管理

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [管理下システムが前回クラッシュ画面を取り込むように設定する](#)
- [Windows の自動再起動オプションを無効にする](#)
- [プラットフォームイベントの設定](#)
- [よくあるお問い合わせ\(FAQ\)](#)

ここでは、iDRAC6 の監視方法と、システムと iDRAC6 が警告を受け取るように設定する手順を説明します。

管理下システムが前回クラッシュ画面を取り込むように設定する

iDRAC6 が前回クラッシュ画面を取り込めるようにするには、管理下システムの次の必須項目を設定する必要があります。

1. 管理下システムソフトウェアをインストールします。管理下システムソフトウェアのインストールについては、『Server Administrator ユーザーズガイド』を参照してください。
2. **Windows の起動と回復設定** で Windows の「自動再起動」機能を選択解除した対応 Microsoft® Windows® オペレーティングシステムを実行します。
3. 前回クラッシュ画面を有効にする(デフォルト=無効)。

ローカル RACADM を使って前回クラッシュ画面機能を有効にするには、コマンドプロンプトで次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
```

4. 自動回復タイマーを有効にして、**自動回復動作をリセット**、**電源を切る**、または**電源を入れ直す** に設定します。**自動回復** タイマーを設定するには、Server Administrator または IT Assistant を使用する必要があります。

自動リカバリ の設定手順の詳細については、『Server Administrator ユーザーズガイド』を参照してください。前回のクラッシュ画面を取り込めるように、**自動回復** タイマーを 60 秒以上に設定してください。デフォルト設定は 480 秒です。

自動回復動作 が **シャットダウン** または **電源の入れ直し** に設定されている場合は、管理下システムがクラッシュしたときに前回のクラッシュ画面は使用できません。

Windows の自動再起動オプションを無効にする

iDRAC6 のウェブインタフェースの前回クラッシュ画面機能を正しく動作させるには、Microsoft Windows Server® 2008 および Windows Server 2003 オペレーティングシステムを実行している管理下システムで、**自動再起動** オプションを無効にしてください。

Windows 2008 Server の自動再起動オプションを無効にする

1. Windows **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. 左側の **タスク** の下にある **詳細システム設定** をクリックします。
3. **詳細** タブをクリックします。
4. **起動と回復** で **設定** をクリックします。
5. **自動再起動** チェックボックスを選択解除します。
6. **OK** を 2 度クリックします。

Windows Server 2003 の自動再起動オプションを無効にする

1. Windows **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. **詳細** タブをクリックします。
3. **起動と回復** で **設定** をクリックします。

4. **自動再起動** チェックボックスを選択解除します。
5. **OK** を 2 度クリックします。

プラットフォームイベントの設定

プラットフォームイベントの設定によって、リモートアクセスデバイスが特定のイベントメッセージに応答して選択された動作を行うように設定することができます。これらの動作には、再起動、電源の入れ直し、電源オフ、警告のトリガー(プラットフォームイベントトラップ [PET] または電子メール)。

フィルタ可能なプラットフォームイベントには次のようなイベントがあります。

- 1 ファン重要アサートフィルタ
- 1 バッテリー警告アサートフィルタ
- 1 バッテリー重要アサートフィルタ
- 1 低電圧重要アサートフィルタ
- 1 温度警告アサートフィルタ
- 1 温度重要アサートフィルタ
- 1 インタルージョン重要アサートフィルタ
- 1 冗長性低下フィルタ
- 1 冗長性喪失フィルタ
- 1 プロセッサ警告アサートフィルタ
- 1 プロセッサ重要アサートフィルタ
- 1 プロセッサ不在フィルタ
- 1 プロセッサ供給警告アサートフィルタ
- 1 プロセッサ供給重要アサートフィルタ
- 1 プロセッサ供給不在アサートフィルタ
- 1 イベントログ重要アサートフィルタ
- 1 ウォッチドッグ重要アサートフィルタ
- 1 システム電源警告アサートフィルタ
- 1 システム電源重要アサートフィルタ

プラットフォームイベントが発生すると(ファンブローブエラーなど)、システムイベントが生成されてシステムイベントログ (SEL) に記録されます。このイベントがウェブベースインタフェースのプラットフォームイベントフィルタリストにあるプラットフォームイベントフィルタ (PEF) に一致し、このフィルタが警告 (PET または 電子メール) を生成するように設定されていると、PET または電子メール警告が 1 つまたは複数の宛先に送信されます。

同じプラットフォームイベントフィルタで別の動作(システムの再起動など)を実行するように設定すると、その動作が行われます。

プラットフォームイベントフィルタ (PEF) の設定

プラットフォームイベントトラップまたは電子メール警告設定を行う前にプラットフォームイベントとフィルタを設定してください。

ウェブベースインタフェースを使った PEF の設定

詳細については、「[プラットフォームイベントフィルタ \(PEF\) の設定](#)」を参照してください。

RACADM CLI を使った PEF の設定

1. PEF を有効にします。

コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
```

ここで、1 と 1 はそれぞれ PEF インデックスと有効 / 無効の選択です。

PEF インデックス値は 1~19 です。有効 / 無効の選択は 1 (有効) または 0 (無効) です。

たとえば、PEF をインデックス 5 で有効にするには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
```

2. PEF の動作を設定します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <動作>
```

ここで、<動作> のビット値は次の通りです。

- 1 0 = 警告処置なし
- 1 1 = サーバーの電源を切る
- 1 2 = サーバーを再起動する
- 1 3 = サーバーの電源を入れなおす

たとえば、PEF でサーバーを再起動するには次のコマンドを入力します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
```

ここで、1 は PEF インデックス、2 は PEF 動作を再起動に設定します。

PET の設定

ウェブユーザーインターフェースを使った PET の設定

詳細については、「[プラットフォームイベントラップ\(PET\)の設定](#)」を参照してください。

RACADM CLI を使った PET の設定

1. グローバル警告を有効にします。

コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. PET を有効にします。

コマンドプロンプトで以下のコマンドを入力し、各コマンドの後で <Enter> を押します。

```
IPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
```

```
IPv6:racadm config -g cfgIpmiPetIPv6 -o cfgIpmiPetIPv6PetAlertEnable -i 1 1
```

ここで、1 と 1 はそれぞれ PET の宛先と有効 / 無効の選択です。

PET の宛先値は 1~4 です。有効 / 無効の選択は 1 (有効) または 0 (無効) です。

たとえば、PET を索引 4 で有効にするには、次のコマンドを入力します。

```
IPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```

```
IPv6:racadm config -g cfgIpmiPetIPv6 -o cfgIpmiPetIPv6PetAlertEnable -i 4 1
```

3. PET ポリシーを設定します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
IPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IPv4_address>
```

```
IPv6:racadm config -g cfgIpmiPetIPv6 -o cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6_address>
```

ここで、1 は PET の宛先インデックスで <IPv4_address> および <IPv6_address> はプラットフォームイベント警告の宛先の IP アドレスです。

4. コミュニティ名の文字列を設定します。

コマンドプロンプトで、次のコマンドを入力します。

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名前>
```


電子メール警告の設定

ウェブユーザーインターフェースを使った電子メール警告の設定

詳細については、「[電子メール警告の設定](#)」を参照してください。

RACADM CLI を使った電子メール警告の設定

1. グローバル警告を有効にします。

コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. 電子メール警告を有効にします。

コマンドプロンプトで以下のコマンドを入力し、各コマンドの後に <Enter> を押します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
```

ここで、1 と 1 はそれぞれ電子メールの宛先と有効 / 無効の選択です。

電子メールの送信先索引は 1~4 の値が可能です。有効 / 無効の選択は 1 (有効) または 0 (無効) です。

たとえば、PET を索引 4 で有効にするには、次のコマンドを入力します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

3. 電子メール設定を指定します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <電子メールアドレス>
```

ここで、1 は電子メールの宛先インデックスで <電子メールアドレス> はプラットフォームイベント警告の宛先の電子メールアドレスです。

カスタムメッセージを設定するには、コマンドプロンプトに次の内容を入力し、Enter を押します。


```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <カスタムメッセージ>
```

ここで、1 は電子メール宛先インデックスで <custom_message> は電子メール警告に表示されるメッセージです。

電子メール警告のテスト

RAC 電子メール警告機能を使うと、ユーザーは管理下システムで重大イベントが発生したときに電子メール警告を受信できます。次に、RAC がネットワーク経由で正しく電子メール警告を送信できることを確認するために電子メール警告機能のテストを行う例を示します。

```
racadm testemail -i 2
```

 **メモ:** 電子メール警告機能のテストを行う前に、SMTP と電子メール警告設定が指定されていることを確認してください。詳細については、「[電子メール警告の設定](#)」を参照してください。

RAC SNMP トラップ警告機能のテスト

RAC SNMP トラップ警告機能を使用すると、管理下システム上で発生したシステムイベントのトラップを SNMP トラップリスナー設定で受信できます。

次の例では、ユーザーが RAC のトラップ警告機能进行测试する例を示します。

```
racadm testtrap -i 2
```


RAC SNMP トラップ警告機能进行测试する前に、SNMP とトラップの設定が正しく設定されていることを確認してください。これらの設定の指定方法については、「[testtrap](#)」と「[sskeyupload](#)」のサブコマンドの説明を参照してください。

よくあるお問い合わせ(FAQ)

どうして次のメッセージが表示されるのでしょうか？

リモートアクセス : SNMP 認証エラー

検出作業の一部として、IT Assistant はデバイスの get と set コミュニティ名の確認を試みます。IT Assistantには、get community name = public と set community name = private があります。iDRAC6 エージェントのデフォルトコミュニティ名は public です。IT Assistant が set リクエストを送信すると、iDRAC6 エージェントはコミュニティ = publicからのリクエストしか受け入れないため、SNMP 認証エラーが生成されます。

 **メモ:** これは、検出に使う SNMP エージェントコミュニティです。

RACADM を使用して、iDRAC6 のコミュニティ名を変更できます。

iDRAC6 コミュニティ名を表示するには、次のコマンドを使用します。

```
racadm getconfig -g cfgOobSnmpp
```

iDRAC6 コミュニティ名を設定するには、次のコマンドを使用します。

```
racadm config -g cfgOobSnmpp -o cfgOobSnmppAgentCommunity <コミュニティ名>
```

ウェブインタフェースを使って iDRAC6 SNMP エージェントコミュニティ名にアクセス/設定するには、リモートアクセス → **設定** → **サービス** に進み、**SNMP エージェント** をクリックします。

SNMP 認証エラーの生成を防止するには、エージェントに受け入れられるコミュニティ名を入力する必要があります。iDRAC6 では 1 つしかコミュニティ名を許可しないので、同じ get と set コミュニティ名を IT Assistant の検出設定用に使用しなければなりません。

[目次ページに戻る](#)

[目次ページに戻る](#)

管理下システムの回復とトラブルシューティング

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [リモートシステムのトラブルシューティングで最初に行うこと](#)
- [リモートシステムの電源管理](#)
- [システム情報の表示](#)
- [システムイベントログ \(SEL\) の使用](#)
- [POST 起動ログの使用](#)
- [前回のシステムクラッシュ画面の表示](#)

本項では、iDRAC6 ウェブインタフェースを使って、クラッシュしたリモートシステムの回復とトラブルシューティングに関連したタスクの実行方法について説明します。

- 1 「[リモートシステムのトラブルシューティングで最初に行うこと](#)」
- 1 「[リモートシステムの電源管理](#)」
- 1 「[IPv6 情報](#)」
- 1 「[前回のシステムクラッシュ画面の表示](#)」

リモートシステムのトラブルシューティングで最初に行うこと

以下は、管理下システムで発生する複雑な問題をトラブルシューティングする際に確認すべき事項です。

- 1 システムの電源はオンになっていますか、オフになっていますか？
- 2 電源がオンの場合は、オペレーティングシステムが正しく機能していますか、それともクラッシュまたはフリーズしていますか？
- 3 電源がオフの場合は、突然オフになりましたか？

システムがクラッシュした場合は、前回のクラッシュ画面を確認し（「[前回のシステムクラッシュ画面の表示](#)」を参照）、コンソールリダイレクトとリモート電源管理（「[リモートシステムの電源管理](#)」を参照）を使用してシステムを再起動し、その過程を確認します。

リモートシステムの電源管理

iDRAC6 では、管理下システムでシステムクラッシュ、またはその他のシステムイベントが発生した後、リモートで電源管理処置を実行して回復することができます。

iDRAC6 ウェブインタフェースからの電源制御処置の選択

ウェブインタフェースを使用して電源管理処置を実施するには、「[サーバーに対する電源制御操作の実行](#)」を参照してください。

iDRAC6 CLI からの電源制御処置の選択

racadm serveraction サブコマンドを使うと、ホストシステムの電源管理を行うことができます。

racadm serveraction <動作>

<処置> の文字列のオプションは以下のとおりです。

- 1 **powerdown** - 管理下システムの電源を切ります。
- 1 **powerup** - 管理下システムの電源を入れます。
- 1 **powercycle** - 管理下システムの電源を入れ直します。これは、システムのフロントパネルの電源ボタンを押してシステムの電源を切ってから入れ直す操作に似ています。
- 1 **powerstatus** - サーバーの現在の電源状態を表示します（「オン」または「オフ」）。
- 1 **hardreset** - 管理下システムのリセット（再起動）を行います。

システム情報の表示

システム概要 ページには、次のシステムコンポーネントに関する情報が表示されます。

- 1 メインシステムシャーシ
- 1 Integrated Dell Remote Access Controller 6 - Enterprise

システム情報にアクセスするには、**システム** ツリーを展開して **プロパティ** をクリックします。

メインシステムシャーシ

表 17-1 と 表 17-2 に、システムシャーシのプロパティを示します。

 **メモ:** ホスト名 と OS 名 の情報を受け取るには、管理下システムに iDRAC6 サービスをインストールしておく必要があります。

表 17-1 システム情報フィールド

フィールド	説明
説明	システムの説明
BIOS バージョン	システム BIOS バージョン
サービスタグ	システムのサービスタグナンバー
ホスト名	ホストシステム名
OS 名	システムで実行しているオペレーティングシステム

表 17-2 自動回復のフィールド

フィールド	説明
リカバリ処置	「システムハング」が検知されたときに、iDRAC6 に次の処置を行うように設定できます: 処置なし、ハードリセット、電源を切る、電源を入れ直す。
初期カウントダウン	「システムハング」が検知されてから iDRAC6 がリカバリ処置を実行するまでの秒数。
現在のカウントダウン	カウントダウンタイマーの現在の値(秒)。

Integrated Dell Remote Access Controller 6 Enterprise

表 17-3 では、iDRAC6 Enterprise のプロパティを説明しています。

表 17-3 iDRAC6 Enterprise の情報フィールド

フィールド	説明
日時	現在の時刻(以下の形式で表記): 日 月 DD HH:MM:SS:YYYY
ファームウェアバージョン	iDRAC ファームウェアバージョン。
ファームウェアアップデート	ファームウェアが最後にフラッシュされた日付(以下のフォーマットで表記): 日 月 DD HH:MM:SS:YYYY
ハードウェアバージョン	リモートアクセスコントローラのバージョン。
MAC Address	ネットワークの各ノードを固有に識別するメディアアクセスコントロール(MAC)アドレス

IPv4 情報

表 17-4 は、IPv4 プロパティについて説明しています。

表 17-4 IPv4 の情報フィールド

フィールド	説明
有効	はいまたは いいえ
IP アドレス	ホストとネットワークインタフェースカード(NIC)を結びつける 32 ビットアドレス。値は、143.166.154.127 のようなドット区切りのフォーマットで表示されます。
サブネットマスク	サブネットマスクは、IP アドレスを構成する拡張ネットワークプレフィックスとホスト番号の部分を示します。値は、255.255.0.0 のようなドット区切りのフォーマットで表示されます。
ゲートウェイ	ルーターまたはスイッチのアドレス。値は、143.166.154.1 のようなドット区切りのフォーマットで表示されます。
DHCP 有効	はいまたは いいえ 動的ホスト構成プロトコル(DHCP)が有効であるかを示します。

IPv6 情報

表 17-5 は、IPv6 プロパティについて説明しています。

表 17-5 IPv6 の情報フィールド

フィールド	説明
有効	IPv6 スタックが有効であることを示します。
IP アドレス 1	iDRAC NIC の IPv6 アドレスを指定します。
プレフィックス長	IPv6 アドレスのプレフィックス長を指定する整数。この値は、1 ~ 128 です。
IP ゲートウェイ	iDRAC NIC のゲートウェイを指定します。
リンクのローカルアドレス	iDRAC NIC の IPv6 アドレスを指定します。
IP アドレス 2	利用可能な場合、iDRAC NIC の追加 IPv6 アドレスを指定します。
Auto Config (自動設定)	AutoConfig(自動設定)は、Server Administrator が動的ホスト構成プロトコル(DHCPv6)サーバーから iDRAC NIC の IPv6 アドレスを取得できるようにします。また、静的 IP アドレス、プレフィックス長および静的ゲートウェイの値を無効にし、フラッシュします。

システムイベントログ(SEL)の使用

SEL ログ ページには、管理下システム上で発生するシステムの重要イベントが表示されます。

システムイベントログを表示するには、次の手順を実行してください。

1. システム ツリーの **システム** をクリックします。
2. **ログ** タブをクリックしてから **システムイベントログ** をクリックします
システムイベントログ ページにイベントの重大度が表示され、その他表 17-6 に示すような情報も提供されます。
3. **システムイベントログ** ページの適切なボタンをクリックして続行します(「表 17-6」を参照)。

表 17-6 状態インジケータのアイコン





アイコン / カテゴリ	説明
	緑のチェックマークは、正常(平常)ステータスを示します。
	感嘆符の入った黄色の三角形は、警告(非重要)ステータスを示します。
	赤い X は、重要(エラー)ステータスを示します。
	疑問符のアイコンは、不明なステータスを示します。
日時	イベントが発生した日時。日付が空白の場合は、システム起動時にイベントが実行されます。24 時間制 mm/dd/yyyy hh:mm:ss の形式です。
説明	イベントの短い説明

表 17-7 SEL ページのボタン


ボタン	動作
印刷	ウィンドウに表示される並び順に SEL を印刷します。
更新	SEL ページを再ロードします。
ログのクリア	SEL をクリアします。 メモ: ログのクリア ボタンは、ログのクリア 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、選択したディレクトリに SEL を保存できます。 メモ: Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト support.microsoft.com から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。


コマンドラインを使ってシステムログを表示する

```
racadm getsel -i
```

getsel -i コマンドは SEL 内のエントリ数を表示します。

racadm getsel <オプション>


 **メモ:** 引数を何も指定しないと、ログ全体が表示されます。

 **メモ:** 使用できるオプションの詳細については、「[getsel](#)」を参照してください。

clrset コマンドは SEL から既存のレコードをすべて削除します。

racadm clrset

POST 起動ログの使用


 **メモ:** iDRAC6 を再起動すると、すべてのログはクリアされます。

iDRAC6 のこの機能を使用すると、BIOS POST 起動の最後の 3 つのインスタンスとオペレーティングシステム起動のストップモーションビデオを再生できます。

POST 起動のキャプチャログを表示するには:


1. システム ツリーの **システム** をクリックします。
2. **ログ** タブをクリックしてから、**起動キャプチャ** タブをクリックします。
3. POST 起動キャプチャログのログ番号を選択し、**再生** をクリックします。

新しい画面にログのビデオが再生されます。

 **メモ:** 他のビデオを再生するには、開かれている POST 起動ログのビデオを閉じる必要があります。2 つのログを同時に再生することはできません。

4. POST キャプチャログのビデオを再生するには、**Playback(プレイバック)** → **Play(再生)** の順でクリックします。
5. ビデオを停止するには、**終了** をクリックします。

前回のシステムクラッシュ画面の表示

 **メモ:** 前回クラッシュ画面の機能を使用するには、管理下システムの Server Administrator に **自動回復** 機能が設定されている必要があります。さらに、DRAC を使った **自動システムリカバリ** 機能が有効になっていることを確認します。この機能は、**リモートアクセス** セクションの **設定** タブにある **サービス** ページで有効にします。

前回のクラッシュ画面 ページには、システムクラッシュ前に発生したイベントに関する情報を含む最新クラッシュ画面が表示されます。前回システムクラッシュ情報は、iDRAC6 メモリに保存され、リモートからアクセスが可能です。


前回のクラッシュ画面 ページを表示するには、次の手順を実行してください。

1. システム ツリーの **システム** をクリックします。
2. **ログ** タブをクリックして、**前回のクラッシュ画面** をクリックします。

前回のクラッシュ画面 ページの右上に次のボタンがあります ([表 17-8](#) を参照)。

表 17-8 前回のクラッシュ画面ページのボタン

ボタン	動作
印刷	前回のクラッシュ画面 ページを印刷します。
更新	前回のクラッシュ画面 ページを再ロードします。

 **メモ:** 自動回復タイマーの変動により、システムリセットタイマーの値が 30 秒未満に設定されている場合は、**前回のクラッシュ画面** を取り込めないことがあります。Server Administrator と IT Assistant でシステムリセットタイマーを 30 秒以上に設定して、**前回のクラッシュ画面** が正しく機能することを確認します。詳細については、「[管理下システムが前回クラッシュ画面を取り込むように設定する](#)」を参照してください。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 のリカバリとトラブルシューティング

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [RAC ログの使用](#)
- [コマンドラインの使用](#)
- [診断コンソールの使用](#)
- [トレースログの使用](#)
- [racdump の使用](#)
- [coredump の使用](#)

ここでは、クラッシュした iDRAC6 の回復とトラブルシューティングに関連するタスクを実行する方法を説明します。

iDRAC6 のトラブルシューティングには、以下のいずれかのツールを使用できます。

- 1 RAC ログからすべてのエントリをクリアします。
- 1 診断コンソール
- 1 トレースログ
- 1 racdump
- 1 coredump

RAC ログの使用

RAC ログ は持続的なログで、iDRAC6 ファームウェアに保管されています。ログにはユーザーの処置 (ログイン、ログアウト、セキュリティポリシーの変更など) と iDRAC6 が発行する警告のリストが格納されています。ログがいっぱいになると、最も古いエントリから上書きされます。

iDRAC6 ユーザーインタフェース (UI) から RAC ログにアクセスするには、次の手順を行います。

1. システム ツリーの **リモートアクセス** をクリックします。
2. **ログ** タブをクリックして、**RAC ログ** をクリックします。

RAC ログには、[表 18-1](#) に示す情報が記録されています。

表 18-1 RAC ログページ情報

フィールド	説明
日時	日付と時刻 (Dec 19 16:55:47 など)。 iDRAC6 を最初に起動したときにまだ管理下システムと通信 できない間は、時刻にはシステムの起動と表示されます。
ソース	イベントを引き起こしたインタフェース
説明	イベントの概要と iDRAC6 にログインしたユーザー名。

RAC ログページのボタンの使用

RAC ログ ページには、[表 18-2](#) に示すボタンがあります。

表 18-2 RAC ログのボタン

ボタン	動作
印刷	RAC ログ ページを印刷します。
ログのクリア	RAC ログ のエントリを消去します。 メモ: ログのクリア ボタンは、ログのクリア 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、選択したディレクトリに RAC ログ を保存できます。 メモ: Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト support.microsoft.com から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。

更新 | RAC ログ ページを再ロードします。


コマンドラインの使用

RAC ログのエントリを表示するには、`getraclog` コマンドを使用します。

```
racadm getraclog -i
```

`getraclog -i` コマンドは、iDRAC ログ内のエントリ数を表示します。

```
racadm getraclog [オプション]
```

 **メモ:** 詳細については、「[getraclog](#)」を参照してください。

RAC ログからすべてのエントリをクリアするには、`clrtraclog` コマンドを使用します。

```
racadm clrtraclog
```

診断コンソールの使用

iDRAC6 には、Microsoft® Windows® や Linux システムに含まれているのと同様なネットワーク診断ツールが標準装備されています(「[表 18-3](#)」を参照)。iDRAC6 ウェブインタフェースを使用して、ネットワークのデバッグツールにアクセスできます。

診断コンソール ページにアクセスするには、次の手順を行います。

1. システム ツリーの **リモートアクセス** をクリックします。
2. **診断** タブをクリックします。

[表 18-3](#) に、**診断コンソール** ページで使用できるオプションを示します。コマンドを入力して **送信** をクリックします。デバッグの結果が **診断コンソール** ページに表示されます。

診断コンソール ページを更新するには、**更新** をクリックします。別のコマンドを実行するには、**診断ページに戻る** をクリックします。

表 18-3 診断コマンド


コマンド	説明
arp	ARP (Address Resolution Protocol) テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を印刷します。netstat オプションの右のテキストフィールドにインタフェース番号をオプションで入力すると、インタフェース、パッファの使用率、その他のネットワークインタフェースに関する情報が印刷されます。
ping <IP アドレス>	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。宛先 IP アドレスをこのオプションの右にあるフィールドに入力してください。ICMP(インターネットコントロールメッセージプロトコル)エコーパケットが現在のルーティングテーブルの内容に基づいて宛先 IP アドレスに送信されます。
gettracelog	iDRAC6 トレースログを表示します。詳細については、「 gettracelog 」を参照してください。

トレースログの使用

iDRAC6 の内部トレースログは、システム管理者が iDRAC6 の警告およびネットワークに関する問題をデバッグするために使用します。

iDRAC6 ウェブベースユーザーインタフェースからトレースログにアクセスするには、次の手順を行います。


1. システム ツリーの **リモートアクセス** をクリックします。
2. **診断** タブをクリックします。
3. `gettracelog` コマンドまたは `racadm gettracelog` コマンドを **コマンド** フィールドに入力します。

 **メモ:** このコマンドはコマンドラインインタフェースからも使用できます。詳細については、「[gettracelog](#)」を参照してください。

トレースログは次の情報を追跡します。


1. DHCP - DHCP サーバーから送受信したパケットを追跡します。
1. IP - 送受信した IP パケットを追跡します。

トレースログには、管理下システムのオペレーティングシステムではなく、iDRAC6 の内部ファームウェアに関連する iDRAC6 ファームウェア固有のエラーコードが含まれている場合もあります。

 **メモ:** iDRAC6 は、1500 バイトより大きいパケットサイズの ICMP(Ping)には応答しません。

racdump の使用

`racadm racdump` コマンドは単一コマンドで、ダンプ、状態、iDRAC6 ボードの一般情報を取得します。

 **メモ:** このコマンドは Telnet と SSH のインタフェースでのみ使用できます。詳細については、[racdump](#) コマンドを参照してください。

coredump の使用

`racadm coredump` コマンドは、RAC で最近発生した重要な問題に関する詳細情報を表示します。coredump 情報はこれらの重要な問題の診断に使用できます。

使用可能な場合、coredump 情報は RAC の電源を切った後も次の状態が発生するまで保持されます。

- 1 `coredumpdelete` サブコマンドを使って coredump 情報がクリアされた
- 1 RAC で別の重要問題が発生した この場合、coredump 情報は最後に発生した重要エラーに関するものです。

`racadm coredumpdelete` コマンドは、現在 RAC に保存されている coredump データをクリアするために使用できます。

詳細については、「[coredump](#)」および「[coredumpdelete](#)」サブコマンドを参照してください。

[目次ページに戻る](#)

[目次ページに戻る](#)

センサー

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド


- [バッテリープローブ](#)
- [ファンプローブ](#)
- [シャーシインテリジェントプローブ](#)
- [電源装置プローブ](#)
- [電力監視プローブ](#)
- [温度プローブ](#)
- [電圧プローブ](#)

ハードウェアセンサーまたはプローブを使用すると、不安定なシステムや損傷などの障害に対して適切な処置を講じることができるため、ネットワーク上のシステムをさらに効率的に監視できます。

iDRAC6 を使用して、ハードウェアセンサーのバッテリー、ファンプローブ、シャーシインテリジェント、電源装置、消費電力、温度、電圧を監視できます。

バッテリープローブ

バッテリープローブは、システム基板 CMOS とストレージ ROMB (RAM on Motherboard) のバッテリーに関する情報を提供します。

 **メモ:** ストレージ ROMB のバッテリー設定は、システムに ROMB がある場合にのみ使用可能です。

ファンプローブ

ファンプローブセンサーは以下についての情報を提供します。

- 1 ファン の冗長性 - プライマリファンが事前に設定された速度で熱を放散しなくなると、セカンダリファンが取って代わる機能。
- 1 ファンプローブリスト - システムのすべてのファンのファン速度についての情報を提供します。


シャーシインテリジェントプローブ

シャーシインテリジェントプローブは、シャーシが開いているか閉じているかというシャーシの状態を表示します。

電源装置プローブ

電源装置プローブは以下についての情報を提供します。

- 1 電源装置の状態
- 1 電源装置の冗長性 (プライマリ電源が故障した場合に冗長電源が取って代わる機能)。

 **メモ:** システムに電源装置が1個しかない場合、電源の冗長性は **無効** に設定されます。

電力監視プローブ

電力監視プローブは、リアルタイムの消費電力に関する情報をワットとアンペアで表示します。

iDRAC6 で設定した現在の日時から数えて最後の 1 時間、1 日、1 週間の消費電力をグラフで表示することもできます。

温度プローブ

温度センサーは、システム基板の周辺温度についての情報を提供します。温度プローブは、プローブの状態が事前に設定された警告値と重要なしきい値の範囲内にあるかどうかを示します。

電圧プローブ

以下は一般的な電圧プローブです。ご使用のシステムにこれら以外も付いている可能性があります。

- 1 CPU [n] VCORE

- 1 システム基板 0.9V PG
- 1 システム基板 1.5V ESB2
- 1 システム基板 1.5V PG
- 1 システム基板 1.8V PG
- 1 システム基板 3.3V PG
- 1 システム基板 1.5V PG
- 1 システム基板バックプレーン PG
- 1 システム基板 CPU VTT
- 1 システム基板リニア PG

電圧プローブは、プローブの状態が事前に設定された警告値と重要なしきい値の範囲内にあるかどうかを示します。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 を始めるにあたって


Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

iDRAC6 を使用することで、システムがダウンしていても Dell システムのリモート監視、トラブルシューティング、修復を行うことができます。iDRAC6 には、コンソールリダイレクト、仮想メディア、仮想 KVM、スマートカード認証を始め、豊富な機能が揃っています。

管理ステーションとは、システム管理者がリモートから iDRAC6 を備えた Dell システムを管理するシステムのことを指します。このように監視されるシステムのことを、管理下システム と称します。

また、管理ステーションに加え、管理下システム上に Dell™ OpenManage™ ソフトウェアをインストールすることも可能です。管理下システムソフトウェアなしでは RACADM をローカルで使用できず、iDRAC6 は前回のクラッシュ画面をキャプチャできません。

iDRAC6 をセットアップするには、次の一般的な手順に従います。

 **メモ:** この手順はシステムによって異なります。ご利用のシステムにおける正確な手順については、デルサポートサイト support.dell.com/manuals で該当する『ハードウェア取扱説明書』を参照してください。

1. iDRAC6 のプロパティ、ネットワーク、ユーザーを設定します - iDRAC6 の設定には、iDRAC6 設定ユーティリティ、ウェブインタフェース、または RACADM を使用できます。
2. Windows システムを使用している場合、iDRAC6 へのアクセスを提供し、Active Directory ソフトウェアの既存ユーザーに iDRAC6 ユーザー権限の追加および制御が行えるように Microsoft® Active Directory® を設定します。
3. スマートカード認証を設定します - スマートカードは企業のセキュリティを強化します。
4. コンソールリダイレクトや仮想メディアなどのリモートアクセスポイントを設定します。
5. セキュリティ設定を行います。
6. システム管理機能を効率化するための警告を設定します。
7. 標準ベースの IPMI ツールを使用してネットワーク上のシステムを管理するには、iDRAC6 Intelligent Platform Management Interface (IPMI) を設定します。

[目次ページに戻る](#)

[目次ページに戻る](#)

電源モニタおよび電源管理

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

- [電力インベントリ、電力バジェット、電力制限](#)
- [電源モニター](#)
- [電源の設定と管理](#)
- [電源装置の正常性状態を表示する](#)
- [電力バジェットの表示](#)
- [電力バジェットのしきい値](#)
- [電源モニタの表示](#)
- [サーバーに対する電源制御操作の実行](#)

Dell™ PowerEdge™ システムでは、新しい強化された電源管理機能が搭載されています。ハードウェアからファームウェア、そしてシステム管理ソフトウェアのプラットフォーム全体が、電源効率、電源モニタおよび電源管理に焦点を当てた設計となっています。

基本的なハードウェア設計は、電源の観点から最適化されました。

- 1 高効率電源装置と電圧レギュレータが組み込まれました。
- 1 該当する場合、最下位の電源コンポーネントが選択されていました。
- 1 シャーシの設計によりシステムを通るエアフローが最適化され、ファンの電力消費量が最小化されるようになりました。

PowerEdge システムは電源を制御、管理する多数の機能を提供します。

- 1 **電力バジェット**: 起動時に、システムインベントリにより、現在の設定のシステム電力バジェットが算出されます。
- 1 **電力制限**: 指定された電力制限を維持するように、システムが減速されます。
- 1 **電源モニタ**: iDRAC6 は電源装置をポーリングして電力測定値を収集します。iDRAC6 は電力測定履歴を収集して、移動平均とピーク値を計算します。iDRAC6 のウェブベースのインタフェースを使用することで、[電源モニタ](#) ページ上でこれら情報を閲覧することができます。

電力インベントリ、電力バジェット、電力制限

使用上、ラックレベルでの冷却量が制限されることがあります。ユーザー定義の電力制限の使用により、パフォーマンスの要件を満たすために必要に応じて電力を割り当てることができます。

iDRAC6 は電力消費量を監視し、指定された電力制限レベルに合わせて動的にプロセッサを減速することで、電源要件に適合しながらパフォーマンスを最大化できます。

電源モニター

iDRAC6 は、継続的に PowerEdge サーバーの消費電力を監視します。iDRAC6 は、下記の電力値を算出し、ウェブインタフェースまたは RACADM CLI を介して、情報を提供します。

- 1 累積電力
- 1 平均、最小および最大電力
- 1 電力ヘッドルーム値
- 1 電力消費量 (ウェブインタフェースでグラフとしても表示)

電源の設定と管理

iDRAC6 ウェブインタフェースおよび RACADM コマンドラインインタフェース (CLI) を使用して、PowerEdge システム上の電源制御の管理および設定ができます。具体的には、以下のことが可能です。

- 1 サーバーの電源状態を表示できます。
- 1 サーバーの電源制御操作 (例: 電源オン、電源オフ、システムリセット、電源サイクル) を実行できます。
- 1 サーバーとインストールされている電源装置の電力バジェット情報 (設定可能な最大および最小電力消費量) を表示します。
- 1 サーバーの電力バジェットのしきい値を表示、設定できます。


電源装置の正常性状態を表示する

電源装置 ページに、インストールされているサーバー内の電源装置の状態と定格が表示されます。

ウェブインタフェースの使用

ファン装置の正常性状態を表示するには

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. システムツリーで **電源装置** を選択します。電源装置 ページが開いて、次の情報が表示されます。
 1. **電源装置冗長性状態**: 次のような値があります。
 - **完全**: 電源装置 PS1 と PS2 は同一タイプで、正しく機能しています。
 - **喪失**: 電源装置 PS1 と PS2 は異なるタイプで、どちらか一方が正しく機能していません。冗長性なし。
 - **無効**: 2 台の電源装置のうち 1 台しか使用できません。冗長性なし。
 1. **個々の電源装置**: 次のような値があります。
 - **状態** には以下が表示されます。
 - **OK**: 電源装置があり、サーバーと通信していることを示します。
 - **警告**: 警告のみが発行され、システム管理者が設定した時間内に修正処置が必要であることを示します。システム管理者が設定した時間内に対応処置を取らなかった場合は、シャーシの安全性に影響するような重要または重大なエラーを引き起こす可能性があります。
 - **重大**: 少なくとも 1 つのエラー警告が発行されたことを示します。エラーステータスは、シャーシの電源エラーを示し、直ちに対応処置を取る必要があります。
 - **場所**: 電源装置ユニットの名前 PS-n を表示します。n は電源装置番号です。
 - **タイプ**: 電源装置のタイプを表示します (AC または DC、AC-DC または DC-DC 電圧変換)。
 - **入力ワット数**: 電源装置の入力ワット数。これは、システムがデータセンターにかけられることのできる最大 AC 電力負荷です。
 - **最大ワット数**: 電源装置の最大ワット数。これは、システムで使用できる DC 電力です。この値は、システム構成に対して十分な電源容量があることを示すために使用されます。
 - **オンライン状態**: 電源装置の電源状況 (存在し OK、入力の喪失、不在、予測エラー) を示します。
 - **ファームウェアバージョン**: 電源装置のファームウェアバージョンを表示します。

 **メモ**: 電源装置の効率が関わるため、最大ワット数は入力ワット数とは異なります。たとえば、電源装置の効率が 89% である場合に最大ワット数が 717W であれば、入力ワット数は 797W と推定されます。

RACADM の使用


CMC への Telnet/SSH テキストコンソールを開いて、ログイン後、以下を入力します。

```
racadm getconfig -g cfgServerPower
```

電力バジェットの表示

サーバーは、**電力バジェット情報** ページに電源サブシステムの電力バジェット状態の概要を提供します。

ウェブインタフェースの使用

 **メモ**: 電源管理操作を行うには、**システム管理者** 権限が必要となります。

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. **Power Management** (電力の管理) タブをクリックします。
3. **電力バジェット** オプションを選択します。
4. **電力バジェット状態** ページが表示されます。

最初のテーブルには、現在のシステム構成でのユーザー指定の最大と最小の電源制限しきい値が表示されます。これらは、システム制限として設定できる AC 電力消費量の範囲を表します。選択されたシステム制限は、システムがデータセンターにかけられることのできる最大 AC 電力負荷となります。


設定可能な最小電力消費量 には、指定できる電力バジェット下限のしきい値が表示されます。

設定可能な最大電力消費量 には、指定できる電力バジェット上限のしきい値が表示されます。この値は、現在のシステム設定の絶対的な最大電力消費量でもあります。

RACADM の使用

CMC への Telnet/SSH テキストコンソールを開いて、ログイン後、以下を入力します。

```
racadm getconfig -g cfgServerPower
```

 **メモ:** 出力の詳細を含む `cfgServerPower` の詳細については、「[cfgServerPower](#)」を参照してください。


電力バジェットのしきい値

電力バジェットのしきい値を有効にすると、システムの電力制限の範囲を設定できます。指定したしきい値近く消費電力を維持するために、システムパフォーマンスが動的に調整されます。低負荷環境においては、実際の電力消費量は少なくなり、パフォーマンスの調整が完了するまで、一時的にしきい値を下回る場合もあります。

電力バジェットのしきい値の **有効** を選択すると、システムはユーザー指定のしきい値を強制的に適用します。電力バジェットのしきい値の**選択を解除**すると、電力制限は適用されません。たとえば、あるシステム構成での設定可能な最大電力消費量が 700W で、設定可能な最小電力消費量が 500W であるとして、電力バジェットのしきい値を現在の 650W から 525W に下げて有効にすることができます。以降、システムのパフォーマンスはユーザー指定のしきい値 525W を超えないように電力消費量を維持すべく動的に調整されます。

ウェブインターフェースの使用

1. iDRAC6 のウェブベースのインターフェースにログインします。
2. **Power Management** (電力の管理) タブをクリックします。
3. **電力バジェット** オプションを選択します。**電力バジェット情報** ページが表示されます。
4. **電力バジェットのしきい値** テーブルに値をワット、BTU/時、またはパーセント単位で入力します。ワットまたは BTU/時 単位は、電力バジェットのしきい値の上限値の入力に使用します。パーセント単位は、設定可能な最大と最小電力消費量範囲内のパーセントで指定する場合に使用します。たとえば、100% しきい値は設定可能な最大電力消費量を示し、0% は最小電力消費量を示します。

 **メモ:** 電力バジェットのしきい値は設定可能な最大電力消費量を上回ったり、設定可能な最小電力消費量を下回ることはできません。


5. しきい値を有効にする場合は **有効** を選択し、有効にしない場合は選択しないままにします。**有効** を選択すると、システムはユーザー指定のしきい値を強制的に適用します。**を選択しないと**、システムは電力制限されません。
6. **変更の適用** をクリックします。

RACADM の使用

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts <ワット単位の電力制限値>
```

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr <BTU/時の電力制限値>
```

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent <電力制限値のパーセント>
```

 **メモ:** 電力バジェットのしきい値を BTU/時で設定するときは、ワットに変換すると最も近い整数値に丸められます。電力バジェットのしきい値をワットから BTU/時に読み戻すときにも、これと同じく最も近い整数値に丸められます。このため、書き込まれた値は読み込まれたものとはわずかに異なる場合があります。たとえば、600 BTU/時のしきい値は 601 BTU/時として読み返されます。

電源モニタの表示

ウェブインターフェースの使用

電源モニタデータを表示するには:

1. iDRAC6 ウェブインターフェースにログインします。
2. システムツリーで **電源モニタ** を選択します。**電源モニタ** ページが表示されます。

電源モニタ ページに表示される情報は次のとおりです。


電源モニター

1. **状態:** OK は、電源装置ユニットがあり、現在サーバーと通信していることを示し、**警告** は警告が発行されたこと、**重大** はエラーが発行されたことを示します。
1. **プローブ名:** システム基板のシステムレベル この説明は、システムにおける場所に基づいて、プローブが監視されていることを示します。
1. **読み取り値:** ワット単位または BTU/時の現在の消費電力量。


アンペア数

- 1 **場所**：電源装置ユニットの名前 PS-n を表示します。n は電源装置番号です。
- 1 **読み取り値**：アンペア単位の現在の消費電力量。

電源トラッキング統計

 **メモ**：現在の時間とピーク時間のリストに未解決のエラーがあります。現在時間の下に表示されている値は実際はピーク時間の値で、ピーク時間の下の値は現在時間の値です。

- 1 **累積** 電源装置の入力側から測定したサーバーの現在の累積エネルギー消費量を示します。値は KWh で表示される累積値で、システムによって使用された総エネルギー量です。この値は、**累積のリセット** ボタンを使ってリセットできます。
- 1 **最大ピーク アンペア数** は、開始と現在時間ので指定された間隔内のピーク現在値です。この値は、**最大ピークのリセット** ボタンを使ってリセットできます。
- 1 **最大ピーク ワット数** は、開始と現在時間ので指定された間隔内のピーク現在値です。この値は、**最大ピークのリセット** ボタンを使ってリセットできます。
- 1 **測定開始時間** はシステムエネルギー消費量の値が最後にクリアされ、新しい測定サイクルが開始された日時を表示します。**累積** では、この値は **累積のリセット** ボタンを使ってリセットできますが、システムリセットまたはフェールオーバー時まで持続します。**最大ピーク アンペア数** と **最大ピーク ワット数** では、この値は **最大ピークのリセット** ボタンを使ってリセットできませんが、システムリセットまたはフェールオーバー時まで持続します。
- 1 **累積** の **測定終了時刻** は、システムエネルギー消費量が算出された現在の日付と時刻を表示します。**最大ピーク アンペア数** と **最大ピーク ワット数** では、**測定終了時刻** イールドにはこれらのピークが発生した時刻が表示されます。

 **メモ**：電源追跡統計値は、システムがリセットされても維持されるため、測定開始から終了までの期間のすべてのアクティビティを反映しています。**最大ピークのリセット** ボタンをクリックすることで、各フィールドがゼロにリセットされます。次の表の電力消費量のデータは、システムのリセット後に失われるため、ゼロにリセットされます。表示される電力値は、特定の時間間隔(過去 1 分、1 時間、1 日 および 1 週間)にわたって測定された累積平均値です。開始から終了までの間隔が電源追跡統計値と異なる場合もあるため、ピーク電力値(最大ピークワット数 対 最大電力消費量)も異なる可能性があります。

電力消費

- 1 過去 1 分、1 時間、1 日、1 週間の平均、最大、および最小電力消費量が表示されます。
- 1 平均電力消費量：過去 1 分、過去 1 時間、過去 1 日および過去 1 週間の平均値。
- 1 最大電力消費量 および 最小電力消費量：特定の時間間隔において測定された最大および最小電力消費量。
- 1 最大電力消費時間 および 最小電力消費時間：電力消費量が最大であった時間および 最小であった時間。


ヘッドルーム

システムの即時ヘッドルームには電源装置ユニットで使用可能な電力とシステムの現在の電力消費量間の差を表示します。


システムのピークヘッドルームには電源装置ユニットで使用可能な電力とシステムのピーク電力消費量間の差を表示します。

グラフの表示

このボタンをクリックすると、過去 1 時間の iDRAC6 の電力および電流消費量がそれぞれワットとアンペア単位で表示されます。これらの統計値は、グラフの上方にあるドロップダウンメニューを使って 1 週間前まで表示できます。

 **メモ**：グラフに描かれた各データポイントは、読み取り値の 5 分間平均を表します。このため、電力または電流消費量の短時間の変動がグラフに反映されない場合もあります。

サーバーに対する電源制御操作の実行

 **メモ**：電源の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

iDRAC6 では、正常なシャットダウンなど、いくつかの電源管理処置をリモートで実行できます。

ウェブインタフェースの使用

1. iDRAC6 ウェブインタフェースにログインします。
2. Power Management (電力の管理) タブをクリックします。**電力制御** ページが表示されます。
3. ラジオボタンをクリックして、**電源制御操作** のいずれかを選択します。
 - **システムの電源を入れる** は、サーバーの電源をオンにします(サーバーの電源がオフのときに電源ボタンを押す操作と同じ)。サーバーの電源がすでにオンの場合は、このオプションが無効になっています。
 - **システムの電源を切る** は、サーバーの電源をオフにします。サーバーの電源がすでにオフの場合、このオプションは無効になっています。

- **NMI (マスク不能な割り込み)** は、NMI を生成し、システム動作を一時停止させます。
 - **正常なシャットダウン** は、システムをシャットダウンします。
 - **システムをリセットする** (ウォームブート) は、電源をオフにすることなく、システムをリセットします。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
 - **システムの電源サイクル** (コールドブート) はサーバーの電源を切ってから再起動します。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
4. **適用** をクリックします。確認を求めるダイアログボックスが表示されます。
 5. **OK** をクリックして、電力管理の操作(システムのリセットなど)を行います。

RACADM の使用

サーバーへの Telnet/SSH テキストコンソールを開いて、ログイン後、以下を入力します。

```
racadm serveraction <動作>
```

ここで、<動作> は、powerup(電源投入)、powerdown(電源切断)、powercycle(電源サイクル)、hardreset(ハードリセット)または powerstatus(電源状態)を指します。

[目次ページに戻る](#)

[目次ページに戻る](#)

セキュリティ機能の設定

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [iDRAC6 システム管理者用のセキュリティオプション](#)
- [SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保](#)
- [Secure Shell \(SSH\) の使用](#)
- [サービスの設定](#)
- [iDRAC6 の追加のセキュリティオプションを有効にする](#)

iDRAC6 には次のセキュリティ機能があります。

- 1 iDRAC6 管理者用の高度なセキュリティオプション
 - 1 コンソールリダイレクトを無効にするオプションを使用すると、ローカルシステムユーザーは iDRAC6 コンソールリダイレクト機能によるコンソールリダイレクトを無効にできません。
 - 1 ローカル設定を無効にする機能を使用すると、リモート iDRAC6 管理者は以下からの iDRAC6 の設定能力を無効にすることができます。
 - BIOS POST オプション ROM
 - ローカル racadm と Dell OpenManage Server Administrator ユーティリティを使用するオペレーティングシステム
 - 1 128 ビット SSL 暗号化と 40 ビット SSL 暗号化(128 ビットが許可されていない国)をサポートする RACADM CLI とウェブベースインタフェース操作による
 - 📌 **メモ:** Telnet は SSL 暗号化をサポートしていません。
- 1 ウェブベースのインタフェースまたは RACADM CLI を使用したセッションタイムアウトの設定(分単位)
 - 1 設定可能な IP ポート(該当する場合)
 - 1 暗号化トランスポート層を使用してセキュリティを強化するセキュアシェル (SSH)
 - 1 IP アドレスごとのログイン失敗数の制限により制限を超えた IP アドレスのログインを阻止
 - 1 iDRAC6 に接続するクライアントの IP アドレス範囲を制限

iDRAC6 システム管理者用のセキュリティオプション

iDRAC6 ローカル設定を無効にする

システム管理者は、**リモートアクセス**→**設定**→**サービス**を選択することで、iDRAC6 グラフィカルユーザーインタフェース (GUI) を介したローカル設定を無効にできます。**オプションの ROM を使用した iDRAC のローカル設定を無効にする** チェックボックスを選択すると、リモートアクセス設定ユーティリティ(システム起動時に Ctrl+E を押してアクセス)は読み取り専用モードで起動し、ローカルユーザーがデバイスを設定できないようにします。システム管理者が **RACADM を使用した iDRAC のローカル設定を無効にする** チェックボックスを選択すると、ローカルユーザーは iDRAC6 の設定を読み取ることはできますが、RACADM ユーティリティや Dell OpenManage Server Administrator を使用して設定を変更できなくなります。

システム管理者はこれらのオプションのいずれか一方、または両方を同時に有効にできます。ウェブインタフェースを介して有効にするほかに、ローカル RACADM コマンドを使って有効にすることもできます。

システム再起動中のローカル設定を無効にする

この機能は、システムの再起動中に管理下システムのユーザーが iDRAC6 を設定できないようにします。

```
racadm config -g cfgRacTuning -o
```

```
cfgRacTuneCtrlEConfigDisable 1
```

📌 **メモ:** このオプションは、iDRAC6 設定ユーティリティでのみサポートされています。このバージョンにアップグレードするには、デルサポートサイト support.dell.com から BIOS アップデートパッケージを使用して BIOS をアップグレードしてください。

ローカル RACADM からローカル設定を無効にする

この機能は、管理下システムのユーザーがローカル RACADM または Dell OpenManage Server 管理ユーティリティを使って iDRAC6 を設定する機能を無効にします。

```
racadm config -g cfgRacTuning -o cfgRacTuneLocalConfigDisable 1
```

⚠ **注意:** これらの機能は、ローカルユーザーがローカルシステムから iDRAC6 を設定する能力(デフォルト設定に戻す能力も含む)を著しく制限します。デルでは、これらの機能を慎重に使用し、一度に 1 つのインタフェースのみを無効にして、ログイン権限を完全に失うことを避けることをお勧めします。

📌 **メモ:** 詳細については、デルサポートサイト support.dell.com にあるホワイトペーパー「DRAC 上のローカル設定とリモート仮想 KVM を無効にする」をお読みください。

システム管理者はローカル RACADM コマンドを使ってローカル設定オプションを設定できますが、セキュリティ上の理由で、リセットは帯域外の iDRAC6 ウェブインタフェース またはコマンドライン

ターフェイスからのみできるようになっています。システムの電源投入時自己診断テストが完了し、オペレーティングシステムが起動したら、`cfgRacTuneLocalConfigDisable` オプションが適用されます。オペレーティングシステムとしては、ローカル RACADM コマンドを実行できる Microsoft® Windows Server® または Enterprise Linux、あるいは Dell OpenManage Deployment Toolkit のローカル RACADM コマンドを実行するために限定的に使用される Microsoft Windows® Preinstallation Environment や vmlinix などが挙げられます。

次のような場合には、システム管理者がローカル設定を無効にする必要があります。たとえば、サーバーおよびリモートアクセスデバイスの管理者が複数人いるデータセンターでは、サーバースタックの保守担当者はリモートアクセスデバイスへの管理者権限を必要としない場合があります。同様に、技術者はシステムの定期保守作業中、サーバーへの物理的なアクセス権限を持ちます。この間、システムを再起動し、パスワード保護されている BIOS にアクセスできますが、リモートアクセスデバイスの設定は許可されるべきではありません。このような状況下では、リモートアクセスデバイスの管理者はローカル設定を無効にします。

管理者は、ローカル設定を無効にすると、iDRAC6 をデフォルト設定に戻す能力を含めてローカル設定権限が著しく制限されるため、これらのオプションは必要なときのみ使用すべきで、通常一度に 1 つだけのインターフェイスを無効にし、ログイン権限を完全に失わないようにすべきです。たとえば、管理者がローカル iDRAC6 ユーザー全員を無効にし、Microsoft Active Directory® ディレクトリサービスのユーザーだけが iDRAC6 にログインできるようにした後、Active Directory の認証インフラストラクチャにエラーが発生すると、管理者がログインできなくなる可能性があります。同様に、管理者がすべてのローカル設定を無効にし、動的ホスト構成プロトコル (DHCP) サーバーを含むネットワークに静的 IP アドレスを使って iDRAC6 を配置した後、DHCP サーバーが iDRAC6 の IP アドレスをネットワーク上の別のデバイスに割り当てた場合、その競合によって DRAC の帯域外の接続が無効になり、管理者がシリアル接続を通してファームウェアをデフォルト設定に戻すことが必要になります。

iDRAC6 リモート仮想 KVM を無効にする

管理者は iDRAC6 リモート KVM を選択的に無効にすることで、コンソールリダイレクトを通して他のユーザーから見られることなくローカルユーザーがシステムを操作するための柔軟でセキュアなメカニズムを提供できます。この機能を使用するには、サーバーに iDRAC 管理下ノードソフトウェアをインストールする必要があります。管理者は次のコマンドを使って、リモート vKVM を無効にできます。

```
racadm LocalConRedirDisable 1
```

LocalConRedirDisable コマンドは、引数 1 を使って実行すると既存のリモート vKVM セッションウィンドウを無効にします。

リモートユーザーがローカルユーザーの設定を上書きするのを防ぐために、このコマンドはローカル RACADM でのみ使用可能です。管理者は、Microsoft Windows Server 2003 および SUSE Linux Enterprise Server 10 など、ローカル RACADM 対応のオペレーティングシステムで使用できます。このコマンドはシステム再起動後も有効であるため、リモート vKVM を再度有効にするためには管理者がこのコマンドを無効にする必要があります。これには、次のように引数 0 を使用します。

```
racadm LocalConRedirDisable 0
```

次のように、iDRAC6 リモート vKVM を無効にする必要が生じる状態がいくつかあります。たとえば、管理者は自分が設定した BIOS 設定をリモート iDRAC6 ユーザーに見られたくない場合、LocalConRedirDisable コマンドを使ってシステム POST 中にリモート vKVM を無効にできます。また、管理者がシステムにログインするたびにリモート vKVM を自動的に無効にすることでセキュリティを強化できます。これには、ユーザーログオンスクリプトから LocalConRedirDisable コマンドを実行します。



メモ: 詳細については、デルサポートサイト support.dell.com にあるホワイトペーパー「DRAC 上のローカル設定とリモート仮想 KVM を無効にする」をお読みください。

ログオンスクリプトの詳細については、technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx を参照してください。

SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保

ここでは、iDRAC6 に組み込まれているデータセキュリティの機能について説明します。

- 1 [「SSL \(Secure Sockets Layer\)」](#)
- 1 [「証明書署名要求 \(CSR\)」](#)
- 1 [「SSL メインメニューへのアクセス」](#)
- 1 [「証明書署名要求の生成」](#)

SSL (Secure Sockets Layer)

iDRAC6 には、業界標準の SSL セキュリティプロトコルを使用してインターネットで暗号化データを送信するように設定されたウェブサーバーが含まれています。公開鍵と秘密鍵の暗号技術に基づく SSL は、クライアントとサーバー間の認証済みの暗号化された通信により、ネットワーク上での盗聴を防止する広く受け入れられているセキュリティ方式です。

SSL 対応システム:

- 1 SSL 対応のクライアントに対して認証する
- 1 クライアントがサーバーに対して認証できるようにする
- 1 両システムが暗号化された接続を確立できるようにする

この暗号処理は高度なデータ保護を提供します。iDRAC6 では、北米のインターネットブラウザで一般的に使用されている最も安全な暗号化方式である 128 ビットの SSL 暗号化標準を採用しています。

iDRAC6 ウェブサーバーには、デルが署名をした SSL デジタル証明書 (サーバー ID) が含まれています。インターネットで高度なセキュリティを確保するには、新しい証明書署名要求 (CSR) を生成する要求を iDRAC6 に送信して、ウェブサーバー SSL 証明書を置き換えてください。

証明書署名要求 (CSR)

CSR は、認証局 (CA) に対してセキュアサーバー証明書の発行を求めるデジタル要求です。セキュアサーバー証明書は、リモートシステムの身元を保護して、リモートシステムとやり取りする情報を他のユーザーが閲覧または変更できないようにします。DRAC のセキュリティを確保するため、CSR を生成して CSR を CA に送信し、CA から返された証明書をアップロードすることをお勧めします。

CA は、信頼性の高いスクリーニング、身分証明、その他の重要なセキュリティ条件を満たすことが IT 業界で認められた事業者です。CA には、Thawte や VeriSign などがあります。CA は CSR を受け取ると、CSR に含まれている情報を確認します。応募者が CA のセキュリティ標準を満たしていると、CA はネットワークおよびインターネットを介したトランザクションに対して、応募者を一意に識別する証明書を発行します。

CA が CSR を承認して証明書を送信したら、証明書を iDRAC6 ファームウェアにアップロードする必要があります。iDRAC6 ファームウェアに保管されている CSR 情報は、証明書に記載されている情報と一致する必要があります。

SSL メインメニューへのアクセス

1. システム ツリーを拡張し、リモートアクセスをクリックします。
2. 設定 タブをクリックし、SSL をクリックします。

CSR を生成、既存サーバー証明書をアップロード、または既存サーバー証明書を閲覧するには、SSL メインメニュー(「表 21-1」を参照)を使用します。CSR 情報は iDRAC6 ファームウェアに保存されています。表 21-2 では、SSL メインメニュー ページ上で利用できるボタンについて説明しています。


表 21-1 SSL メインメニュー

フィールド	説明
証明書署名要求 (CSR) の生成	次へ をクリックして、証明書署名要求の生成 ページを開くと、CSR を生成して CA に送信し、安全な ウェブ証明書を要求できます。
サーバー証明書のアップロード	次へ をクリックし、iDRAC6 へのアクセス制御に使用する会社が保有する既存の証明書をアップロードします。 メモ: iDRAC6 で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER によって符号化された証明書は受け入れられません。新しい証明書をアップロードし、iDRAC6 を使って受信したデフォルトの証明書と置き換えます。
サーバー証明書の表示	次へ をクリックして、既存のサーバー証明書を表示します。

表 21-2 SSL メインメニューボタン

ボタン	説明
印刷	SSL メインメニュー ページを印刷します。
更新	SSL メインメニュー ページを再ロードします。
次へ	次のページに移動します。

証明書署名要求の生成

 **メモ:** 新しい CSR は、ファームウェアにある古い CSR を上書きします。iDRAC が署名済み CSR を受け入れるには、ファームウェア内の CSR が CA から返される証明書と一致する必要があります。

1. SSL メインメニュー ページで、証明書署名要求 (CSR) の生成 を選択して、次へ をクリックします。
2. 証明書署名要求 (CSR) の生成 ページで、各 CSR 属性の値を入力します。
[表 21-3](#) に、証明書署名要求 (CSR) の生成 ページのオプションを示します。
3. CSR を開くまたは保存するには、生成 をクリックします。
4. 証明書署名要求 (CSR) の生成 ページで適切なボタンをクリックして続行します。[表 21-4](#) では、証明書署名要求 (CSR) の生成 で使用できるボタンについて説明しています。

表 21-3 証明書署名要求 (CSR) の生成 ページのオプション

フィールド	説明
コモンネーム	証明する名前(通常は www.xyzcompany.com のようなウェブサーバーのドメイン名)。英数字、ハイフン、下線、ピリオドのみが有効です。スペースは使用できません。
組織名	この組織に関連付けられた名前(たとえば「XYZ Corporation」)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
組織単位	部門など組織単位に関連付けられた名前(たとえば「エンタープライズグループ」)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
地域	証明する会社が所在する都市や地域(たとえば「Minatoku」)。英数字とスペースのみが有効です。下線やその他の文字で単語を区切らないでください。
都道府県名	証明書を申請している組織がある都道府県(たとえば「Tokyo」)。英数字とスペースのみが有効です。略語は使用しないでください。
国番号	証明書を申請している組織が所在する国の名前。国を選択するには、ドロップダウンメニューを使用します。
電子メール	CSR に関連付けられている電子メールアドレス。会社の電子メールアドレスや、CSR に関連付けたいその他の電子メールアドレスを入力できます。このフィールドは任意選択です。

表 21-4 証明書署名要求 (CSR) の生成 ページのボタン

ボタン	説明
印刷	証明書署名要求 (CSR) の生成 ページを印刷します。
更新	証明書署名要求 (CSR) の生成 ページを再ロードします。
SSL メインメニューに戻る	SSL メインメニュー ページに戻ります。
生成	CSR を生成します。

サーバー証明書の表示

1. SSL メインメニュー ページで **サーバー証明書の表示** を選択して、**次へ** をクリックします。

[表 21-5](#) に、証明書 ウィンドウに表示されるフィールドと説明を示します。

2. **サーバー証明書の表示** ページの適切なボタンを押して続行します。


表 21-5 証明書情報

フィールド	説明
シリアルナンバー	証明書のシリアル番号
タイトル情報	タイトルによって入力された証明書の属性
発行者情報	発行者によって返された証明書の属性
有効期間の開始	証明書の発行日
有効期間の終了	証明書の失効日

Secure Shell (SSH) の使用

SSH の使用方法の詳細については、「[Secure Shell \(SSH\) の使用](#)」を参照してください。

サービスの設定

 **メモ:** これらの設定を変更するには、iDRAC の **設定** 権限が必要です。また、リモート RACADM コマンドラインユーティリティは、ユーザーが **root** としてログインしているときにのみ有効になります。

1. **システム ツリー** を展開し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**サービス** をクリックします。
3. 必要に応じて次のサービスを設定します。
 - 1 ローカル設定 ([表 21-6](#))
 - 1 ウェブサーバー ([表 21-7](#))
 - 1 SSH ([表 21-8](#))
 - 1 Telnet ([表 21-9](#))
 - 1 リモート RACADM ([表 21-10](#))
 - 1 SNMP エージェント ([表 21-11](#))
 - 1 自動システムリカバリエージェント ([表 21-12](#))

自動システムリカバリエージェントを使用して、iDRAC6 の **前回のクラッシュ画面** 機能を有効にします。

 **メモ:** iDRAC6 で **前回クラッシュ画面** が機能するためには、Server Administrator をインストールするときに **処置** を **システムの再起動**、**システムの電源を切る**、または **システムの電源を入れ直す** に設定して **自動回復** 機能をアクティブにする必要があります。

4. **変更の適用** をクリックします。

5. サービス ページの適切なボタンをクリックして続行します。表 21-13 を参照してください。

表 21-6 ローカル設定

設定	説明
オプション ROM を使って iDRAC ローカル設定を無効にする	オプション ROM を使って iDRAC のローカル設定を無効にします。システム再起動中に <Ctrl+E> を押してセットアップモジュールに入るようにプロンプトされます。
RACADM を使って iDRAC ローカル設定を無効にする	ローカル RACADM を使って iDRAC のローカル設定を無効にします。

表 21-7 ウェブサーバーの設定

設定	説明
有効	ウェブサーバーを有効または無効にします。オン=有効、オフ=無効
最大セッション数	システムで許可される同時セッションの最大数。
アクティブセッション数	システムの現在のセッション数(最大セッション数 以下)。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定への変更はすぐに適用され、現在のウェブインタフェースセッションが終了します。また、ウェブサーバーもリセットされます。新しいウェブインタフェースセッションが始まるまで数分お待ちください。タイムアウト範囲は 60 ~ 10800 秒です。デフォルトは 1800 秒です。
HTTP ポート番号	iDRAC がサーバー接続に使用するポート。デフォルト設定は 80 秒です。
HTTPS ポート番号	iDRAC がサーバー接続に使用するポート。デフォルト設定は 443 秒です。

表 21-8 SSH の設定

設定	説明
有効	SSH を有効または無効にします。チェックボックスが選択されている場合、SSH は有効であることを示します。
タイムアウト	セキュアシェルのアイドルタイムアウト(秒)。タイムアウト範囲は 60 ~ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは 300 です。
ポート番号	SSH 接続で iDRAC6 が通信するポート。デフォルトは 22 です。

表 21-9 Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。選択されている場合、Telnet は有効です。
タイムアウト	telnet のアイドルタイムアウト(秒)。タイムアウト時間の範囲は 60~1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは 300 です。
ポート番号	Telnet 接続で iDRAC6 が通信するポート。デフォルトは 23 です。

表 21-10 リモート RACADM の設定

設定	説明
有効	リモート RACADM を有効または無効にします。選択した場合、リモート RACADM が有効になります。
アクティブセッション数	システムの現在のセッション数。
アクティブセッション数	システムの現在のセッション数(最大セッション数 以下)。

表 21-11 SNMP エージェントの設定

設定	説明
有効	SNMPエージェントを有効または無効にします。オン=有効、オフ=無効
コミュニティ名	SNMP 警告の送信先 IP アドレスを含むコミュニティ名。コミュニティ名は、空白文字を含まずに最大 31 文字まで使用できます。デフォルト設定は public です。

表 21-12 自動システムリカバリエージェントの設定

設定	説明
有効	自動システムリカバリエージェントを有効にします。

表 21-13 サービスページのボタン

ボタン	説明
印刷	サービス ページを印刷します。
更新	サービス ページを更新します。
変更の適用	サービス ページの設定を適用します。

iDRAC6 の追加のセキュリティオプションを有効にする

リモートシステムへの不正アクセスを防ぐため、iDRAC6 では次の機能を提供しています。

- 1 IP アドレスフィルタ (IPRange) - iDRAC6 にアクセスできる特定の IP アドレス範囲を定義します。
- 1 IP アドレスのブロック - 特定の IP アドレスからのログイン試行の失敗回数を制限します。

これらの機能は iDRAC6 のデフォルト設定では無効になっています。次のサブコマンドまたはウェブインタフェースを使用して、これらの機能を有効にしてください。

```
racadm config -g cfgRacTuning -o <オブジェクト名> <値>
```

これらの機能はまた、セッションのアイドルタイムアウト値や、ネットワークに定義済みのセキュリティプランと一緒に使用できます。

以下の各項で、これらの機能について詳しく説明します。

IP フィルタ (IpRange)

IP アドレスフィルタ(または IP 範囲チェック)を使用すると、ユーザーが特定した範囲内にある IP アドレスのクライアントワークステーションや管理ワークステーションからのみ iDRAC6 へのアクセスを許可します。その他のログインはすべて拒否されます。

IP フィルタは着信ログインの IP アドレスを、次の `cfgRacTuning` プロパティで指定する IP アドレス範囲と比較します。

- 1 `cfgRacTuneIpRangeAddr`
- 1 `cfgRacTuneIpRangeMask`

`cfgRacTuneIpRangeMask` プロパティは着信 IP アドレスと `cfgRacTuneIpRangeAddr` プロパティの両方に適用されます。両方のプロパティの結果が同じであれば、受信ログイン要求の iDRAC6 へのアクセスが許可されます。この範囲外の IP アドレスからのログイン要求にはエラーが返されます。

次の式の値がゼロに等しい場合は、ログインに進みます。

```
cfgRacTuneIpRangeMask & (<着信 IP アドレス> ^ cfgRacTuneIpRangeAddr)
```

& は数量のビットワイズ AND で ^ はビットワイズ XOR です。

`cfgRacTuning` プロパティの完全なリストは、「[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)」に掲載されています。

表 21-14 IP アドレスフィルタ (IpRange) のプロパティ

プロパティ	説明
<code>cfgRacTuneIpRangeEnable</code>	IP アドレスのチェック機能を有効にします。
<code>cfgRacTuneIpRangeAddr</code>	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。 このプロパティと <code>cfgRacTuneIpRangeMask</code> とのビットワイズ ANDIによって、許可する IP アドレスの上位部分が決定されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0~192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
<code>cfgRacTuneIpRangeMask</code>	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。

IP フィルタを有効にする

以下に、IP フィルタ設定のコマンド例を示します。

RACADM と RACADM コマンドの詳細については、「[RACADM のリモート使用](#)」を参照してください。

 **メモ:** 次の RACADM コマンドは 192.168.0.57 以外のすべての IP アドレスをブロックします。

ログインを 1 つの IP アドレスに限定するには(たとえば 192.168.0.57)、次のようにフルマスクを使用してください。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

ログインを4つの連続するIPアドレスに限定するには(192.168.0.212~192.168.0.215)、次のようにマスクの最下位の2ビットを除くすべてを選択します。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

IPフィルタのガイドライン

IPフィルタを有効にする場合は、次のガイドラインに従ってください。

- 1 `cfgRacTuneIpRangeMask` は必ずネットマスク形式で設定してください。最上位ビットがすべて1で(これがマスクのサブネットを定義)、下位ビットはすべてゼロにします。
- 1 必要な範囲の基底アドレスを `cfgRacTuneIpRangeAddr` の値として使用します。このアドレスの32ビットのバイナリ値は、マスクにゼロがある下位ビットがすべてゼロになります。


IPブロック

IPブロックは、事前に選択した時間内に特定のIPアドレスからのログイン失敗回数が過剰になったのを自動的に判断し、そのアドレスがiDRAC6にログインできないようにブロックします。

IPブロックのパラメータは、次のような `cfgRacTuning` グループ機能を使用します。

- 1 許可するログイン失敗回数
- 1 これらの失敗を数える時間枠(秒)
- 1 ログイン失敗数が失敗の合計許容回数を超えたIPアドレスからのセッション確立が防止される時間(秒)

特定のIPアドレスからのログイン失敗が累積すると、それらは内部カウンタによって計数されます。ユーザーがログインに成功すると、失敗履歴がクリアされて、内部カウンタがリセットされます。

 **メモ:** クライアントIPアドレスからのログイン試行が拒否されると、SSHクライアントに「ssh exchange identification: Connection closed by remote host(SSH ID: リモートホストが接続を閉じました)」というメッセージが表示される場合があります。

`cfgRacTuning` プロパティの完全なリストは、「[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)」に掲載されています。

[表 21-15](#) に、ユーザー定義のパラメータを示します。

表 21-15 ログイン再試行制限のプロパティ

プロパティ	定義
<code>cfgRacTuneIpBlkEnable</code>	IPブロック機能を有効にします。 一定時間内に(<code>cfgRacTuneIpBlkFailCount</code>)1つのIPアドレスからの失敗が連続すると(<code>cfgRacTuneIpBlkFailWindow</code>)、以降そのアドレスからのセッション確立試行がすべて一定の時間(<code>cfgRacTuneIpBlkPenaltyTime</code>)拒否されます。
<code>cfgRacTuneIpBlkFailCount</code>	ログイン試行を拒否するまでのIPアドレスのログイン失敗回数を設定します。
<code>cfgRacTuneIpBlkFailWindow</code>	失敗回数を数える時間枠を秒で指定します。失敗回数がこの制限値を超えると、カウンタはリセットされます。
<code>cfgRacTuneIpBlkPenaltyTime</code>	失敗回数が制限値を超えたIPアドレスからのセッションをすべて拒否する時間枠を秒で定義します。

IPブロックを有効にする

次の例では、クライアントが1分間に5回ログイン試行に失敗した場合に、5分間このクライアントIPアドレスのセッション確立を防止します。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

次の例は、1分以内に失敗が3回を超えた場合に、1時間ログイン試行を阻止します。


```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```


iDRAC6 GUI を使ったネットワークセキュリティの設定

 **メモ:** 次の手順を実行するには、iDRAC6 の設定 権限が必要です。

1. システム ツリーの **リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**ネットワーク** をクリックします。
3. **ネットワークの設定** ページで **詳細設定** をクリックします。
4. **ネットワークセキュリティ** ページで属性値を設定してから **変更の適用** をクリックします。

[表 21-16](#) に、**ネットワークセキュリティ** ページの設定を示します。

5. **ネットワークセキュリティ** ページの適切なボタンをクリックして続行します。**ネットワークセキュリティ** ページのボタンについては、[表 21-17](#) を参照してください。

表 21-16 ネットワークセキュリティページの設定

設定	説明
IP 範囲を有効にする	IP 範囲のチェック機能を有効にします。この設定により、iDRAC6 にアクセスできる IP アドレスの範囲を定義できます。
IP 範囲のアドレス	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。可能な IP アドレスの上位部分を決定するため、この値は IP 範囲サブネットマスクとビット単位で AND されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0~192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。 例: 255.255.255.0
IP ブロックを有効にする	事前に選択した時間枠で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。
IP ブロックエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。
IP ブロックエラー時間枠	IP ブロックペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間枠を秒で指定します。
IP ブロックペナルティ時間	失敗回数が制限値を超えた IP アドレスからのセッションをすべて拒否する時間を秒で指定します。

表 21-17 ネットワークセキュリティページのボタン

ボタン	説明
印刷	ネットワークセキュリティ ページを印刷します。
更新	ネットワークセキュリティ ページを再ロードします。
変更の適用	ネットワークセキュリティ ページに加えた変更を保存します。
ネットワーク設定ページに戻る	ネットワーク設定 ページに戻ります。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 の基本インストール

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

- [作業を開始する前に](#)
- [iDRAC6 Express/Enterprise ハードウェアの取り付け](#)
- [iDRAC 6 を使用するためのシステムの設定](#)
- [ソフトウェアのインストールと設定の概要](#)
- [ソフトウェアを管理下システムにインストールする](#)
- [ソフトウェアを管理ステーションにインストールする](#)
- [iDRAC6 ファームウェアのアップデート](#)
- [対応ウェブブラウザの設定](#)


ここでは、iDRAC6 のハードウェアの取り付けとソフトウェアのインストールおよび設定方法について説明します。

作業を開始する前に

iDRAC6 ソフトウェアをインストールして設定する前に、システムに付随する以下のアイテムを用意してください。

- 1 iDRAC6 ハードウェア (組み込みかまたはオプションキットに同梱)
- 1 iDRAC6 インストール手順 (本章で記載)
- 1 『Dell Systems Management Tools and Documentation DVD』

iDRAC6 Express/Enterprise ハードウェアの取り付け

 **メモ:** iDRAC6 接続は USB キーボード接続をエミュレートします。このため、システムを再起動したとき、キーボードが接続されていなくてもそのことを通知しません。

iDRAC6 Express/Enterprise は、事前にシステムに取り付けられているか、個別に取り付けることができます。システムに取り付けられている iDRAC6 の利用を開始するには、「[ソフトウェアのインストールと設定の概要](#)」を参照してください。

iDRAC6 Express/Enterprise がシステムに取り付けられていない場合は、ご利用プラットフォームの『ハードウェアオーナーズマニュアル』でハードウェアの取り付け方法を参照してください。

iDRAC 6 を使用するためのシステムの設定

iDRAC6 を使用するようにシステムを設定するには、iDRAC6 設定ユーティリティを使用します。

iDRAC6 設定ユーティリティを実行するには:

1. システムの電源を入れるか、再起動します。
2. POST 中に画面の指示に従って <Ctrl><E> を押します。
<Ctrl><E> キーを押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、もう一度システムを再起動し、この手順を実行してください。
3. LOM を設定します。
 - a. 矢印キーを使用して LAN パラメータを選択し、<Enter> を押します。NIC の選択 が表示されます。
 - b. 矢印キーを使用して、次のいずれかの NIC モードを選択します。
 - **専用** - このオプションは、リモートアクセスデバイスから iDRAC Enterprise 上で使用可能な専用ネットワークインタフェースを使用できるようにする場合に選択します。このインタフェースは、ホストオペレーティングシステムと共有されず、管理トラフィックを別の物理ネットワークに経路することでアプリケーショントラフィックから分離します。このオプションは、システムに iDRAC6 Enterprise が搭載されている場合にのみ、利用可能です。
 - **共有** - このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムが NIC チューニング用に設定されている場合に完全に機能します。リモートアクセスデバイスは NIC 1 と NIC 2 を通じてデータを受信しますが、データの送信は NIC 1 を通じてのみ行います。NIC 1 が故障した場合、リモートアクセスデバイスはすべてのデータ送信を NIC 2 にフェールオーバーします。リモートアクセスデバイスはデータの送信に NIC 2 を引き続き使用します。NIC 2 が故障した場合、リモートアクセス デバイスはすべての送受信を NIC 1 へ戻します。ただし、これは最初の NIC 1 の障害が修復されている場合に限ります。
 - **Shared with failover LOM2 (LOM2 へのフェールオーバーありで共有)** - このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムが NIC チューニング用に設定されている場合に完全に機能します。リモートアクセスデバイスは、NIC 1、NIC 2、NIC 3 および NIC 4 からデータを受信しますが、NIC 1 からのみデータを送信します。NIC 1 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 2 にフェールオーバーします。NIC 2 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 3 にフェールオーバーします。NIC 3 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 4 にフェールオーバーします。NIC 4 が故障した場合、リモートアクセス デバイスはすべての送受信を NIC 1 へ戻します。ただし、これは最初の NIC 1 の障害が修復されている場合に限ります。
 - **Shared with failover All LOMs (すべての LOM へのフェールオーバーありで共有)** - このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムが NIC チューニング用に設定されている場合に完全に機能します。リモートアクセスデバイスは、NIC 1、NIC 2、NIC 3 および NIC 4 からデータを受信しますが、NIC 1 からのみデータを送信します。NIC 1 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 2 にフェールオーバーします。NIC 2 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 3 にフェールオーバーします。NIC 3 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 4 にフェールオーバーします。NIC 4 が故障した場合、リモートアクセス デバイスはすべての送受信を NIC 1 へ戻します。ただし、これは最初の NIC 1 の障害が修復されている場合に限ります。
4. DHCPまたは静的 IP アドレスソースを使用するようにネットワークコントローラ LAN パラメータを設定します。

- a. 下向きキーを使って、LAN パラメータを選択し、<Enter> を押します。
 - b. 上下の矢印キーを使って、IP アドレスソースを選択します。
 - c. 左右の矢印キーを使って、DHCP、Auto Config(自動設定)または 静的 を選択します。
 - d. 静的 を選択した場合は、イーサネット IP アドレス、サブネットマスク、デフォルトゲートウェイ 設定を選択します。
 - e. <Esc> を押します。
5. <Esc> を押します。
6. 変更を保存して終了 を選択します。

ソフトウェアのインストールと設定の概要

ここでは、iDRAC6 ソフトウェアのインストールと設定について概説します。iDRAC6 のソフトウェアコンポーネントの詳細については、「[ソフトウェアを管理下システムにインストールする](#)」を参照してください。


iDRAC6 ソフトウェアのインストール

iDRAC6 ソフトウェアをインストールするには:

1. ソフトウェアを管理下システムにインストールします。「[ソフトウェアを管理下システムにインストールする](#)」を参照してください。
2. ソフトウェアを管理ステーションにインストールします。「[ソフトウェアを管理下システムにインストールする](#)」を参照してください。

iDRAC6 の設定

iDRAC6 を設定するには:


1. 次のいずれかの設定ツールを選択します。
 - 1 ウェブインタフェース(「[ウェブインタフェースを使用した iDRAC6 の設定](#)」を参照)
 - 1 RACADM CLI(「[iDRAC6 SM-CLP コマンドラインインタフェースの使用](#)」を参照)
 - 1 Telnet コンソール(「[Telnet コンソールの使用](#)」を参照)
-  **メモ:** 複数の iDRAC6 設定ツールを同時に使用すると、不測の結果が生じることがあります。
2. iDRAC6 ネットワークを設定します。「[iDRAC6 のネットワーク設定](#)」を参照してください。
 3. iDRAC6 ユーザーを追加および設定します。「[iDRAC6 ユーザーの追加と設定](#)」を参照してください。
 4. ウェブベースのインタフェースにアクセスするために ウェブブラウザを設定します。「[対応ウェブブラウザの設定](#)」を参照してください。
 5. Microsoft® Windows® の自動再起動オプションを無効にします。「[Windows の自動再起動オプションを無効にする](#)」を参照してください。
 6. iDRAC6 ファームウェアをアップデートします。「[iDRAC6 ファームウェアのアップデート](#)」を参照してください。

ソフトウェアを管理下システムにインストールする

管理下システムへのソフトウェアのインストールは任意選択です。管理下システムソフトウェアなしでは、RACADM をローカルで使用できず、iDRAC6 は前回のクラッシュ画面をキャプチャできません。

管理下システムソフトウェアをインストールするには、『Dell Systems Management Tools and Documentation DVD』で管理下システムにソフトウェアをインストールします。本ソフトウェアのインストール手順については、デルサポートサイト support.dell.com/manuals の『クイックインストールガイド』を参照してください。

管理下システムソフトウェアは、Dell™ OpenManage™ Server Administrator の適切なバージョンからユーザーが選択したコンポーネントを管理下システムにインストールします。

 **メモ:** iDRAC6 管理ステーションソフトウェアと iDRAC6 管理下システムソフトウェアを同じシステムにインストールしないでください。

管理下システムに Server Administrator がインストールされていない場合は、システムの前回クラッシュ画面の表示や自動回復機能の使用はできません。

前回クラッシュ画面の詳細については、「[前回のシステムクラッシュ画面の表示](#)」を参照してください。

ソフトウェアを管理ステーションにインストールする


システムには、『Dell Systems Management Tools and Documentation DVD』が同梱されています。この DVD には、以下のコンポーネントが入っています。

- ・ DVD root - サーバーセットアップおよびシステムインストール情報を提供する Dell Systems Build and Update Utility が含まれます。
- ・ SYSGMT - Dell OpenManage Server Administrator を含むシステム管理ソフトウェアの製品が含まれます。
- ・ Docs - システム、システム管理ソフトウェア製品、周辺機器および RAID コントローラのマニュアルが入っています。
- ・ SERVICE - システムを設定するために必要なツールやシステムの最新の診断および Dell 最適化ドライバが含まれます。

Server Administrator、IT Assistant および Unified Server Configurator の詳細については、デルサポートサイト support.dell.com/manuals の『Server Administrator ユーザーズガイド』、『IT Assistant ユーザーズガイド』および『Unified Server Configurator ユーザーズガイド』を参照してください。

Linux 管理ステーションでの RACADM のインストールと削除

リモート RACADM 機能を使用するには、Linux を実行している管理ステーションに RACADM をインストールします。

 **メモ:** 『Dell Systems Management Tools and Documentation DVD』で**Setup(セットアップ)**を実行すると、サポートされているすべてのオペレーティングシステム用の RACADM ユーティリティが管理ステーションにインストールされます。

RACADM のインストール

1. 管理ステーションコンポーネントをインストールするシステムにルート権限でログオンします。
2. 必要に応じて、次のコマンドまたは同等のコマンドを使って、『Dell Systems Management Tools and Documentation DVD』をマウントします。

```
mount /media/cdrom
```

3. `/linux/rac` ディレクトリに移動して、次のコマンドを実行します。

```
rpm -ivh *.rpm
```

RACADM コマンドに関するヘルプは、コマンドを入力した後「`racadm help`」と入力してください。

RACADM のアンインストール

RACADM をアンインストールするには、コマンドプロンプトを開いて次のように入力します。

```
rpm -e <racadm パッケージ名>
```

ここで、<racadm/パッケージ名> は RAC ソフトウェアのインストールに使用する rpm パッケージです。

たとえば、rpm パッケージ名が `srvadmin-racadm5` であれば、次のように入力します。

```
rpm -e srvadmin-racadm5
```

iDRAC6 ファームウェアのアップデート

iDRAC6 ファームウェアをアップデートするには、次のいずれかの方法を使用します。


1. ウェブインタフェース (『[ウェブベースのインタフェースを使用した iDRAC6 ファームウェアのアップデート](#)』を参照)
1. RACADM CLI (『[RACADM を使用した iDRAC6 ファームウェアのアップデート](#)』を参照)
1. Dell Update Packages (『[Windows および Linux 対応オペレーティングシステム用の Dell Update Packages を使用した iDRAC6 ファームウェアのアップデート](#)』を参照)

作業を開始する前に

ローカル RACADM または Dell Update Packages を使って iDRAC6 ファームウェアをアップデートする前に、次の手順を実行してください。この手順を実行しないと、アップデートに失敗することがあります。

1. 適切な IPMI と管理下ノードのドライバをインストールして有効にします。

2. システムで Windows オペレーティングシステムが実行されている場合は、Windows Management Instrumentation (WMI) サービスを有効にして起動します。
3. iDRAC6 Enterprise を使用し、システム上で SUSE® Linux Enterprise Server (バージョン 10) for Intel® EM64T が稼働している場合は、Raw サービスを開始します。
4. 仮想メディアを切断してマウント解除します。

 **メモ:** iDRAC6 ファームウェアのアップデートが何らかの理由で中断されると、ファームウェアアップデートを再び行うまでに最長 30 分間待たなければならない場合があります。

5. USB が有効になっていることを確認してください。

iDRAC6 ファームウェアのダウンロード

iDRAC6 ファームウェアをアップデートするには、デルサポートサイト support.dell.com から最新ファームウェアをダウンロードしてローカルシステムに保存します。

iDRAC6 ファームウェアパッケージには、次のソフトウェアコンポーネントが含まれています。

- 1 コンパイルされた iDRAC6 ファームウェアコードとデータ
- 1 ウェブベースのインタフェース、JPEG、およびその他のユーザーインタフェースのデータファイル
- 1 デフォルト構成ファイル

ウェブベースのインタフェースを使用した iDRAC6 ファームウェアのアップデート

詳細については、「[iDRAC6 ファームウェア/システムサービスリカバリイメージのアップデート](#)」を参照してください。

RACADM を使用した iDRAC6 ファームウェアのアップデート

CLI ベースの RACADM ツールを使用して iDRAC6 ファームウェアをアップデートできます。管理下システムに Server Administrator をインストールしている場合は、ローカル RACADM を使用してファームウェアをアップデートしてください。

1. デルのサポートサイト support.dell.com から iDRAC6 のファームウェアイメージを管理下システムにダウンロードします。

例:

```
C:\downloads\firmimg.d6
```

2. 次の RACADM コマンドを実行します。

```
racadm fwupdate -pud c:\downloads\
```

リモート RACADM および TFTP サーバーを使用して、ファームウェアをアップデートすることも可能です。


例:

```
racadm -r <iDRAC6 IP アドレス> -u <ユーザー名> -p <パスワード> fwupdate -g -u -a <パス>
```

ここでパスは、firmimg.d6 が保管されている TFTP サーバー上の場所です。

Windows および Linux 対応オペレーティングシステム用の Dell Update Packages を使用した iDRAC6 ファームウェアのアップデート

Windows および Linux の対応オペレーティングシステム用の Dell Update Package をデルのサポートサイト support.dell.com からダウンロードして実行します。詳細については、デルサポートサイト support.dell.com/manuals の『Dell Update Package ユーザーズガイド』を参照してください。

 **メモ:** Linux で Dell Update Package ユーティリティを使用して iDRAC6 ファームウェアをアップデートする際は、コンソール上に次のメッセージが表示される場合があります。

```
usb 5-2: device descriptor read/64, error -71
```

```
usb 5-2: device descriptor not accepting address 2, error -71
```

これらのエラーは表面的なものであり、無視しても構いません。これらのメッセージは、ファームウェアのアップデート処理中に USB デバイスがリセットされるために生成されるものであり、安全性に問題はありません。

ブラウザキャッシュのクリア

ファームウェアアップグレード後、ウェブベースブラウザのキャッシュをクリアします。

詳細については、ウェブブラウザのオンラインヘルプを参照してください。

対応ウェブブラウザの設定

次に、対応ウェブブラウザの設定手順を説明します。

iDRAC6 ウェブインタフェースに接続するためのウェブブラウザの設定

プロキシサーバー経由でインターネットに接続している管理ステーションから iDRAC6 のウェブインタフェースに接続する場合は、このサーバーからインターネットにアクセスするようにウェブブラウザを設定する必要があります。

Internet Explorer ウェブブラウザをプロキシサーバーにアクセスするように設定するには：

1. ウェブブラウザのウィンドウを開きます。
2. **ツール** をクリックして、**インターネットオプション** をクリックします。
3. **インターネットオプション** ウィンドウで **接続** タブをクリックします。
4. **ローカルエリアネットワーク(LAN) 設定** で **LAN 設定** をクリックします。
5. **プロキシサーバーを使用** ボックスが選択されている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** ボックスを選択します。
6. **OK** を 2 度クリックします。

信頼されているドメインのリスト

ウェブブラウザを使って iDRAC6 ウェブインタフェースにアクセスする際、iDRAC6 の IP アドレスが信用するドメインのリストにない場合は、IP アドレスをリストに加えるように要求されることがあります。追加し終えたら、**更新** をクリックするかウェブブラウザを再起動して、iDRAC6 ウェブインタフェースへの接続を再確立します。

32 ビットと 64 ビットのウェブブラウザ

iDRAC6 ウェブインタフェースは、64 ビットウェブブラウザではサポートされていません。64 ビットブラウザを開いた後、コンソールリダイレクトページにアクセスしてプラグインをインストールすると、インストールに失敗します。このエラーを確認しないでこの手順を繰り返すと、最初の試みでプラグインのインストールに失敗したにも関わらず、コンソールリダイレクトページがロードされます。これは、プラグインのインストールに失敗しても、ウェブブラウザがプロファイルディレクトリにプラグイン情報を保存するからです。この不具合を修正するには、32 ビットの対応ウェブブラウザをインストールして起動し、iDRAC6 にログインします。

ウェブインタフェースの日本語版の表示

Windows

iDRAC6 ウェブインタフェースは、次の Windows オペレーティングシステム言語でサポートされています。

- 1 英語
- 1 フランス語
- 1 ドイツ語
- 1 スペイン語
- 1 日本語
- 1 簡体字中国語

Internet Explorer で iDRAC6 ウェブインタフェースのローカライズバージョンを表示するには、次の手順に従います。

1. **ツール** をクリックして、**インターネットオプション** を選択します。
2. **インターネットオプション** ウィンドウで **言語** をクリックします。
3. **言語設定 ウィンドウ** で **追加** をクリックします。

4. **言語の追加** ウィンドウでサポートされている言語を選択します。
複数の言語を選択するには、<Ctrl> を押しながら選択します。
5. 優先言語を選択して **上に移動** をクリックし、その言語をリストの先頭に移動します。
6. **OK** をクリックします。
7. **言語設定** ウィンドウで **OK** をクリックします。

Linux

Red Hat® Enterprise Linux® (バージョン 4) クライアントで簡体字中国語の GUI を使ってコンソールリダイレクトを実行している場合は、ビューアのメニューとタイトルが文字化けすることがあります。この問題は、Red Hat Enterprise Linux (バージョン 4) 簡体字中国語オペレーティングシステムでのエンコードエラーによるものです。この問題を解決するには、次の手順で現在のエンコード設定にアクセスして変更してください。

1. コマンド端末を開きます。
2. 「ローカル」を入力して、<Enter> を押します。次の出力メッセージが表示されます。

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. 値に「zh_CN.UTF-8」が含まれる場合は変更は必要ありません。値に「zh_CN.UTF-8」が含まれない場合は、ステップ 4 に進みます。
4. /etc/sysconfig/i18n ファイルに移動します。
5. ファイルに次の変更を加えます。

現在のエントリ:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CN.GB2312:zh_CN:zh"
```

アップデート後のエントリ:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CN.GB2312:zh_CN:zh"
```

6. ログアウトしてから、オペレーティングシステムにログインします。
7. iDRAC6 を再起動します。

他の言語から簡体字中国語に切り替える場合、この修正が有効になっていることを確認してください。有効になっていない場合は、この手順を繰り返します。

iDRAC6 の詳細設定については、[「iDRAC6 の詳細設定」](#)を参照してください。

[目次ページに戻る](#)

[目次ページに戻る](#)

ウェブインタフェースを使用した iDRAC6 の設定

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [ウェブインタフェースへのアクセス](#)
- [iDRAC6 NIC の設定](#)
- [プラットフォームイベントの設定](#)
- [iDRAC6 ユーザーの設定](#)
- [SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保](#)
- [Active Directory 証明書の設定と管理](#)
- [iDRAC6 サービスの設定](#)
- [iDRAC6 ファームウェア/システムサービスリカバリーイメージのアップデート](#)

iDRAC6 は、iDRAC6 プロパティとユーザーの設定、リモート管理タスクの実行、障害に対してリモート(管理下)システムのトラブルシューティングを可能にするウェブインタフェースを提供します。日常のシステム管理に、iDRAC6 ウェブインタフェースを使用してください。この章では、iDRAC6 のウェブインタフェースを使って一般的なシステム管理タスクを実行する方法について説明し、関連情報へのリンクも掲載しています。

ほとんどのウェブインタフェースの設定タスクは、RACADM コマンドまたは SM-CLP (サーバー管理コマンドラインプロトコル) を使用して実施することも可能です。

ローカル RACADM コマンドは、管理下サーバーから実行できます。

SM-CLP および SSH/Telnet RACADM コマンドは、Telnet または SSH 接続によってリモートアクセス可能なシェルにて実行されます。SM-CLP の詳細については、「[iDRAC6 SM-CLP コマンドラインインタフェースの使用](#)」を参照してください。RACADM コマンドの詳細については、「[RACADM サブコマンドの概要](#)」および「[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)」を参照してください。

ウェブインタフェースへのアクセス

iDRAC6 ウェブインタフェースにアクセスするには、次の手順を実行します。

1. サポートされているウェブブラウザのウィンドウを開きます。
詳細については、「[対応ウェブブラウザ](#)」を参照してください。
IPv4 アドレスを使用してウェブインタフェースにアクセスする場合は、ステップ 2 へ進みます。
IPv6 アドレスを使用してウェブインタフェースにアクセスする場合は、ステップ 3 へ進みます。
2. IPv4 アドレスを使用してウェブインタフェースにアクセスするには、IPv4 が有効になっている必要があります。
ブラウザのアドレスバーに、次のように入力します。
`https://<iDRAC IPv4 アドレス>`
次に、<Enter> キーを押します。
3. IPv6 アドレスを使用してウェブインタフェースにアクセスするには、IPv6 が有効になっている必要があります。
ブラウザのアドレスバーに、次のように入力します。
`https://[<iDRAC IPv6 アドレス>]`
次に、<Enter> キーを押します。
4. デフォルトの HTTPS ポート番号(ポート 443)が変更されている場合は、次のように入力します。
`https://<iDRAC IP アドレス>:<ポート番号>`
iDRAC IP アドレスは iDRAC6 用の IP アドレスで、ポート番号は HTTPS ポート番号です。
5. アドレスフィールドに、`https://<iDRAC IP アドレス>` を入力し、Enter キーを押します。
デフォルトの HTTPS ポート番号(ポート 443)が変更されている場合は、次のように入力します。
`https://<iDRAC IP アドレス>:<ポート番号>`
iDRAC IP アドレスは iDRAC6 用の IP アドレスで、ポート番号は HTTPS ポート番号です。

iDRAC6 ログインウィンドウが表示されます。

ログイン

iDRAC6 ユーザーまたは Microsoft® Active Directory® ユーザーとしてログインできます。iDRAC6 ユーザーのデフォルトのユーザー名とパスワードは、それぞれ root および calvin です。

iDRAC6 にログインするには、システム管理者から iDRAC へのログイン権限が与えられている必要があります。

ログインするには、次の手順に従ってください。

1. **ユーザー名** フィールドで、以下のいずれかを入力します。


- 1 あなたの iDRAC6 ユーザー名。

ローカルユーザーのユーザー名は大文字と小文字が区別されます。たとえば、root、it_user、john_doe などです。

- 1 Active Directory ユーザー名。

Active Directory 名は、<ユーザー名>、<ドメイン>\<ユーザー名>、<ドメイン>/<ユーザー名>、<ユーザー>@<ドメイン> のいずれかの形式で入力できます。大文字と小文字の区別はありません。たとえば、dell.com\john_doe または JOHN_DOE@DELL.COM などです。


2. **パスワード** フィールドに、iDRAC6 のユーザーパスワードまたは Active Directory のユーザーパスワードを入力します。パスワードでは大文字と小文字が区別されます。
3. **ドメイン** ドロップダウンボックスから、This iDRAC を選択して iDRAC6 ユーザーとしてログインするか、利用可能ないずれかのドメインを選択して Active Directory ユーザーとしてログインします。


 **メモ:** Active Directory ユーザーの場合、ユーザー名の一部としてドメイン名を指定した場合は、ドロップダウンメニューから This iDRAC を選択します。


4. **OK** をクリックするか、Enter キーを押します。

ログアウト

1. セッションを閉じるには、メインウィンドウの右上にある **ログアウト** をクリックします。
2. ブラウザウィンドウを閉じます。

 **メモ:** ログインするまで **ログアウト** ボタンは表示されません。


 **メモ:** 正常にログアウトせずにブラウザを閉じると、セッションはタイムアウトになるまで開いたままになることがあります。ログアウトボタンをクリックしてセッションを終了することをお勧めします。この手順でログアウトしない場合、タイムアウトになるまでセッションがアクティブなままになることがあります。


 **メモ:** Microsoft Internet Explorer で、ウィンドウの右上隅の閉じるボタン("x")を使用して iDRAC6 ウェブインタフェースを閉じると、アプリケーションエラーが発生する可能性があります。この不具合を修正するには、Microsoft サポートウェブサイト support.microsoft.com から、最新の Internet Explorer 用累積セキュリティアップデートをダウンロードしてください。


iDRAC6 NIC の設定

ここでは、iDRAC6 がすでに設定され、ネットワーク上でアクセス可能である状態を想定しています。初期 iDRAC6 ネットワークの設定に関しては、「[iDRAC6 の設定](#)」を参照してください。

ネットワークおよび IPMI LAN の設定


 **メモ:** 次の手順を実行するには、iDRAC の **設定** 権限が必要です。

 **メモ:** ほとんどの DHCP サーバーは、予約テーブルにクライアントの ID トークンを保存するためのサーバーを必要とします。このトークンはクライアント(例:iDRAC)が DHCP ネゴシエーション中に提供します。iDRAC6 は、1 バイトのインタフェース 番号(0)とそれに続く 6 バイトの MAC アドレスを使用して、クライアント ID オプションを提供します。

 **メモ:** スパニングツリープロトコル (STP) を有効にした状態で実行している場合、PortFast または類似テクノロジーが次の通り有効になっていることも確認してください。

n iDRAC6 に接続されたスイッチ用のポート上

n iDRAC KVM セッションを実行中の管理ステーションに接続されたポート上

 **メモ:** POST 中にシステムが停止した場合、次のメッセージが表示されることがあります。Strike the F1 key to continue, F2 to run the system setup program(続行するには F1 キーを押してください。システム設定プログラムを実行するには F2 を押してください)
エラーについて考えられる 1 つの理由に、iDRAC6 との通信が失われるネットワークストームイベントが挙げられます。ネットワークストームが収まった後、システムを再起動します。

1. **リモートアクセス** → **設定** → **ネットワーク** の順でクリックします。
2. **ネットワーク** ページで、ネットワークインタフェースカードの設定、共通 iDRAC 設定、IPv4 設定、IPv6 設定、IPMI 設定、および VLAN 設定を入力できます。これら設定の説明については、[表 4-1](#)、[表 4-2](#)、[表 4-3](#)、[表 4-4](#)、[表 4-5](#) および [表 4-6](#) を参照してください。
3. 必要な設定を入力したら、**変更の適用** をクリックします。
4. 適切な ボタンをクリックして続行します。[表 4-7](#) を参照してください。

表 4-1 ネットワークインタフェースカードの設定

--	--

設定	説明
NIC の選択	次の 4 つのモードから現在のモードを設定します。 <ul style="list-style-type: none"> ・ 専用 (iDRAC NIC) <p>メモ: このオプションは iDRAC6 Enterprise でのみ利用可能です。</p> <ul style="list-style-type: none"> ・ 共有 (LOM1) ・ Shared with Failover LOM2 (LOM2 へのフェールオーバーありで共有) ・ Shared with Failover All LOMs (すべての LOM へのフェールオーバーありで共有)
MAC Address	ネットワークの各ノードを固有に識別するメディアアクセスコントロール (MAC) アドレスを表示します。
NIC を有効にする	選択すると、NIC が有効になり、このグループの残りのコントロールがアクティブになることを示します。NIC が無効になっている場合、ネットワーク経由の iDRAC6 とのすべての通信はブロックされます。 デフォルトは、オンです。
オートネゴシエーション	オンに設定した場合、最も近いルーターまたはハブと通信することによりネットワーク速度およびモードを表示します。オフに設定した場合、ネットワーク速度とデュプレックスモードを手動で設定できます (オフ)。 NIC の選択 が 専用 に設定されていない場合、オートネゴシエーションは常に有効になります (オン)。
ネットワーク速度	ネットワーク環境に合わせて、ネットワーク速度を 100 Mb または 10 Mb に設定することができます。このオプションは、オートネゴシエーションが オン に設定されているときは使用できません。
デュプレックスモード	ネットワーク環境に合わせて、デュプレックスモードを全二重または半二重に設定することができます。オートネゴシエーション が オン の場合、このオプションは使用できません。

表 4-2 共通 iDRAC 設定

設定	説明
DNS に iDRAC を登録	DNS サーバーに iDRAC6 の名前を登録します。 デフォルトは 無効 です。
DNS iDRAC 名	DNS に iDRAC を登録 が選択されている場合にのみ、iDRAC6 名を表示します。デフォルト名は idrac-サービス_タグで、サービス_タグは Dell サーバーのサービスタグ番号を示します。例: idrac-00002
DNS ドメイン名に DHCP を使用	デフォルトの DNS ドメイン名を使用します。このチェックボックスが選択されておらず、DNS に iDRAC を登録 オプションが選択されている場合は、DNS ドメイン名 フィールドで DNS ドメイン名を変更します。 デフォルトは 無効 です。 <p>メモ: DNS ドメイン名に DHCP を使用 チェックボックスを選択する場合は、DHCP の使用 (NIC IP アドレス用) チェックボックスが選択されている必要があります。</p>
DNS ドメイン名	デフォルトの DNS ドメイン名は空白です。DNS ドメイン名に DHCP を使用 チェックボックスが選択されている場合、このオプションはグレー表示になり、フィールドを変更できません。

表 4-3 IPv4 設定

設定	説明
有効	NIC を有効にすると、IPv4 プロトコルサポートが選択され、このセクションの他のフィールドが有効に設定されます。
NIC IP アドレスに DHCP を使用	iDRAC6 に動的ホスト構成プロトコル (DHCP) サーバーから NIC 用の IP アドレスを取得するように指示します。デフォルトは オフ です。
IP アドレス	iDRAC NIC の IP アドレスを指定します。
サブネットマスク	iDRAC6 NIC の静的 IP アドレスを入力または編集できます。この設定を変更するには、DHCP を使用 (NIC IP アドレス用) チェックボックスを選択解除します。
ゲートウェイ	ルーターまたはスイッチのアドレス。この値は「ドット区切り」の形式です。例: 192.168.0.1
DHCP を使用して DNS サーバーアドレスを取得する	DHCP を使用して DNS サーバーアドレスを取得する チェックボックスを選択し、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合、優先 DNS サーバーおよび代替 DNS サーバーフィールドに IP アドレスを入力します。 デフォルトは オフ です。 <p>メモ: DHCP を使用して DNS サーバーアドレスを取得する チェックボックスが選択されている場合、IP アドレスを 優先 DNS サーバー および 代替 DNS サーバー フィールドに入力することはできません。</p>
優先 DNS サーバー	DNS サーバーの IP アドレス
代替 DNS サーバー	代替 IP アドレス

表 4-4 IPv6 の設定

--	--

設定	説明
有効	チェックボックスを選択した場合、IPv6 が有効になります。チェックボックスを選択しなかった場合、IPv6 が無効になります。デフォルトは 無効 です。
Auto Config (自動設定)	このボックスをチェックすると、iDRAC6 は動的ホスト設定 (DHCPv6) サーバーから iDRAC6 NIC の IPv6 アドレスを取得できます。Auto Config(自動設定) を有効にすると、IP アドレス、プレフィックス長、および IP ゲートウェイの静的な値を非アクティブにし、削除します。
IP アドレス 1	iDRAC NIC の IPv6 アドレスを設定します。この設定を変更するには、まず関連チェックボックスを選択解除することにより AutoConfig(自動設定) を無効にする必要があります。
プレフィックス長	IPv6 アドレスのプレフィックス長を設定します。この値は、1 ~ 128 です。この設定を変更するには、まず関連チェックボックスを選択解除することにより AutoConfig(自動設定) を無効にする必要があります。
IP ゲートウェイ	iDRAC NIC の静的ゲートウェイを設定します。この設定を変更するには、まず関連チェックボックスを選択解除することにより AutoConfig(自動設定) を無効にする必要があります。
リンクのローカルアドレス	iDRAC NIC の IPv6 アドレスを指定します。
IP アドレス 2	利用可能な場合、iDRAC NIC の追加 IPv6 アドレスを指定します。
DHCP を使用して DNS サーバーアドレスを取得する	DHCP を使用して DNS サーバーアドレスを取得する チェックボックスを選択し、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合、 優先 DNS サーバー および 代替 DNS サーバー フィールドに IP アドレスを入力します。 デフォルトは オフ です。見直しコピーを確認します。 メモ: DHCP を使用して DNS サーバーアドレスを取得する チェックボックスが選択されている場合、IP アドレスを 優先 DNS サーバー および 代替 DNS サーバー フィールドに入力することはできません。
優先 DNS サーバー	優先 DNS サーバーの静的 IPv6 アドレスを設定します。この設定を変更するには、まず DHCP を使用して DNS サーバーアドレスを取得する を選択解除する必要があります。
代替 DNS サーバー	代替 DNS サーバーの静的 IPv6 アドレスを設定します。この設定を変更するには、まず DHCP を使用して DNS サーバーアドレスを取得する を選択解除する必要があります。

表 4-5 IPMI 設定

設定	説明
IPMI オーバー LAN を有効にする	選択されている場合、IPMI LAN チャネルが有効であることを示します。デフォルトは オフ です。
チャネル権限レベルの制限	LAN チャネル上で許可されるユーザーの最小権限レベルを設定します。 システム管理者 (Administrator) 、 オペレータ 、 ユーザー のオプションから 1 つを選択します。デフォルトは システム管理者 (Administrator) です。
暗号キー	暗号キーの文字形式の設定では、0 ~ 20 の 16進法の文字を使用します(空白は使用できません)。デフォルトは空白です。


表 4-6 VLAN 設定

設定	説明
VLAN ID を有効にする	有効である場合、一致する仮想 LAN (VLAN) ID トラフィックのみが受け入れられます。
VLAN ID	802.1g フィールドの VLAN ID フィールド。VLAN ID の有効値を入力します (1 ~ 4094 の値である必要があります)。
優先順位	802.1g フィールドの 優先度 フィールド。0 ~ 7 の値を入力して、VLAN ID の優先度を設定します。

表 4-7 ネットワーク設定ページのボタン

ボタン	説明
印刷	画面に表示されている ネットワーク設定 ページの値を印刷します。
更新	ネットワーク設定 ページを再ロードします。
詳細設定	ネットワークセキュリティ ページを開いて、IP 範囲と IP ブロックの属性を入力できます。
変更の適用	ネットワーク設定ページに追加された新規設定を保存します。 メモ: NIC の IP アドレス設定を変更すると、すべてのユーザーセッションが終了します。ユーザーは、更新後の IP アドレス設定を使って iDRAC6 ウェブインタフェースに再接続する必要があります。その他の変更では NIC をリセットする必要があり、このため接続が一時的に途絶える場合があります。

IP フィルタおよびIP ブロックの設定

 **メモ:** 次の手順を実行するには、iDRAC の **設定** 権限が必要です。

1. **リモートアクセス** → **設定** をクリックし、次に **ネットワークタブ** をクリックして **ネットワーク** ページを開きます。
2. **詳細設定** をクリックして、ネットワークセキュリティ設定を行います。

表 4-8 では、ネットワークセキュリティページ設定が説明されています。設定が終了したら、適用 をクリックします。

- 適切な ボタンをクリックして続行します。表 4-9 を参照してください。

表 4-8 ネットワークセキュリティページの設定

設定	説明
IP 範囲を有効にする	IP 範囲のチェック機能を有効します。これにより、iDRAC にアクセスできる IP アドレスの範囲を定義できます。デフォルトは オフ です。
IP 範囲のアドレス	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。可能な IP アドレスの上位部分を決定するため、この値は IP 範囲サブネットマスクとビット単位で AND されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0~192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。デフォルトは 255.255.255.0 です。
IP ブロックを有効にする	事前に選択した時間枠で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。デフォルトは オフ です。
IP ブロックエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。デフォルトは 10 です。
IP ブロックエラー時間枠	IP ブロックペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間枠を秒で指定します。デフォルトは 3600 です。
IP ブロックペナルティ時間	ログイン失敗回数が制限値を超えた IP アドレスからのログインを拒否する時間を秒で指定します。デフォルトは 3600 です。

表 4-9 ネットワークセキュリティページのボタン

ボタン	説明
印刷	画面に表示中の ネットワークセキュリティ ページのデータを印刷します。
更新	ネットワークセキュリティ ページを再ロードします。
変更の適用	ネットワークセキュリティ ページに追加された新規設定を保存します。
ネットワーク設定 ページに戻ります。	ネットワーク設定 ページに戻ります。

プラットフォームイベントの設定

プラットフォームイベントの設定では、特定のイベントメッセージに対して iDRAC6 が選択した処置を実行するように設定します。処置には、処置の必要なし、システムの再起動、システムの電源を入れ直す、システムの電源を切る、警告の生成(プラットフォームイベントトラップ [PET]、電子メール)があります。

表 4-10 に、フィルタ可能なプラットフォームイベントを示します。

表 4-10 プラットフォームイベントフィルタ


索引	プラットフォームイベント
1	ファン重要アサート
2	バッテリー警告アサート
3	バッテリー重要アサート
4	低電圧重要アサート
5	温度警告アサート
6	温度重要アサート
7	侵入重要アサート
8	ファン冗長性低下
9	ファン冗長性喪失
10	プロセッサ警告アサート
11	プロセッサ重要アサート
12	プロセッサがありません
13	電源供給警告アサート
14	電源供給重要アサート
15	電源装置がありません
16	イベントログ重要アサート

17	ウォッチドッグ重要アサート
18	システム電源警告アサート
19	システム電源重要アサート


プラットフォームイベント(例、バッテリー警告アサート)が発生すると、システムイベントが生成され、システムイベントログ(SEL)に記録されます。このイベントが有効にされているプラットフォームイベントフィルタ(PEF)と一致し、警告(PET または電子メール)を生成するようにフィルタを設定している場合、1 つまたは複数の設定されている送信先に PET または電子メール警告が送信されます。

同じプラットフォームイベントフィルタで別の動作(システムの再起動など)を実行するように設定すると、その動作が行われます。


プラットフォームイベントフィルタ (PEF) の設定

 **メモ:** プラットフォームイベントトラップまたは電子メール警告設定を行う前に、プラットフォームイベントフィルタを設定してください。

1. 対応ウェブブラウザを使ってリモートシステムにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. システム → 警告管理 → プラットフォームイベント の順でクリックします。
3. 最初のテーブルで、プラットフォームイベントフィルタ警告を有効にするチェックボックスを選択し、変更の適用をクリックします。

 **メモ:** 設定されている有効な送信先(PET または電子メール)に警告を送信するためには、プラットフォームイベントフィルタ警告を有効にするを有効にする必要があります。

4. 次の表の プラットフォームイベントフィルタリストで、設定するフィルタをクリックします。
5. プラットフォームイベント設定 ページで、適切な シャットダウン動作 または なし を選択します。
6. 警告の生成 を選択または選択解除して、この処置を有効または無効にします。


 **メモ:** 設定されている有効な宛先(PET または電子メール)に警告を送信するためには、警告の生成 を有効にする必要があります。

7. 変更の適用 をクリックします。


プラットフォームイベント ページが再表示され、実行した変更がプラットフォームイベントフィルタリストに表示されます。

8. ステップ 4 ~ 7 を繰り返して追加のプラットフォームイベントフィルタを設定します。

プラットフォームイベントトラップ(PET)の設定

 **メモ:** SNMP 警告を追加したり有効 / 無効にするには、iDRAC の設定 権限が必要です。iDRAC の設定 権限がない場合、次のオプションは使用できません。

1. 対応ウェブブラウザを使ってリモートシステムにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. 「[プラットフォームイベントフィルタ \(PEF\) の設定](#)」の手順に必ず従ってください。
3. システム → 警告管理 → トラップ設定 の順でクリックします。
4. IPv4 送信先リスト または IPv6 送信先リスト で、送信先番号をクリックして IPv4 または IPv6 SNMP 警告送信先を設定します。
5. プラットフォームイベント警告送信先の設定 ページで、送信先を有効にする を選択または選択解除します。チェック済みボックスは、警告を受信するために IP アドレスが有効になっていることを示しています。チェックされていないボックスは、警告受信用に IP アドレスが無効になっていることを示しています。
6. 有効なプラットフォームイベントトラップ送信先 IP アドレスを入力し、変更の適用 をクリックします。
7. テストトラップを送信 をクリックして設定済み警告をテストするか、プラットフォームイベント送信先ページへ戻る をクリックします。

 **メモ:** ユーザーアカウントは、テストトラップを送信するためテスト警告の権限を持っている必要があります。詳細については、「[表 6-6](#)」の「iDRAC グループ権限」を参照してください。

プラットフォームイベント警告送信先 ページで、適用された変更が IPv4 または IPv6 送信先リストに表示されます。

8. コミュニティ文字列フィールドで、適切な iDRAC SNMP コミュニティ名を入力します。変更の適用 をクリックします。


 **メモ:** 送信先コミュニティ文字列は iDRAC6 コミュニティ文字列と同じである必要があります。

9. ステップ 4 ~ 7 を繰り返して、追加の IPv4 または IPv6 送信先番号を設定します。

電子メール警告の設定

 **メモ:** 電子メール警告は IPv4 および IPv6 の両方のアドレスをサポートしています。

1. 対応ウェブブラウザを使ってリモートシステムにログインします。
2. 「[プラットフォームイベントフィルタ \(PEF\) の設定](#)」の手順に必ず従ってください。
3. システム → 警告管理 → 電子メール警告の設定 の順でクリックします。
4. 送信先電子メールアドレス の表で、送信先アドレスを設定する対象の 電子メール警告番号 をクリックします。
5. 電子メール警告の設定 ページで、電子メール警告を有効にする を選択または選択解除します。チェック済みボックスは、警告を受信するために電子メールアドレスが有効になっていることを示しています。チェックされていないボックスは、警告受信用に電子メールアドレスが無効になっていることを示しています。
6. 送信先電子メールアドレス フィールドに有効な電子メールアドレスを入力します。
7. 電子メールの説明 フィールドで、電子メールに表示する簡単な説明を入力します。
8. 変更の適用 をクリックします。
9. 設定済みの電子メール警告をテストする場合、テスト電子メールの送信 をクリックします。テストしない場合、電子メール警告送信先ページへ戻る をクリックします。
10. 電子メール警告送信先ページへ戻る をクリックし、SMTP (電子メール) サーバー IP アドレス フィールドに有効な SMTP IP アドレスを入力します。

 **メモ:** テスト電子メールの送信に成功するには、SMTP (電子メール) サーバー IP アドレスは、電子メール警告設定ページで設定する必要があります。SMTP サーバーは設定した IP アドレスを使用して iDRAC6 と通信し、プラットフォームイベントが発生したときに電子メール警告を送信します。

11. 変更の適用 をクリックします。
12. ステップ 4 ~ 9 を繰り返して、追加の電子メール警告送信先を設定します。

IPMI の設定

1. 対応ウェブブラウザを使ってリモートシステムにログインします。
2. IPMI オーバー LAN を設定します。
 - a. システム ツリーの リモートアクセス をクリックします。
 - b. 設定 タブをクリックし、ネットワーク をクリックします。
 - c. ネットワーク設定 ページの IPMI LAN 設定 で IPMI オーバー LAN を有効にする を選択して 変更の適用 をクリックします。
 - d. 必要なら IPMI LAN チャネル権限を更新します。


 **メモ:** この設定によって、IPMI オーバー LAN インタフェースから実行できる IPMI コマンドが決まります。詳細については、IPMI 2.0 の仕様を参照してください。

IPMI LAN 設定でチャネル権限レベルの制限 ドロップダウンメニューをクリックし、管理者、オペレータ、または ユーザー を選択して、変更の適用 をクリックします。

- e. 必要なら IPMI LAN チャネルの暗号キーを設定します。


 **メモ:** iDRAC6 IPMI は RMCP+ プロトコルに対応しています。

暗号鍵 フィールドの IPMI LAN 設定 に暗号鍵を入力して、変更の適用 をクリックします。

 **メモ:** 暗号鍵は 40 文字までの偶数の 16 進数で指定します。

3. IPMI シリアルオーバー LAN (SOL)を設定します。
 - a. システム ツリーの リモートアクセス をクリックします。
 - b. 設定 タブでシリアルオーバー LAN をクリックします。
 - c. シリアルオーバー LAN の設定 ページでシリアルオーバー LAN を有効にする を選択します。

- d. IPMI SOL ボーレートをアップデートします。

 **メモ:** シリアルコンソールを LAN 経由でダイレクトする場合、SOL ボーレートが管理下システムのボーレートと同等であることを確認してください。

- e. **ボーレート** ドロップダウンメニューで、適切なボーレートを選択して **変更の適用** をクリックします。
- f. **最低限必要な権限 を更新します。** このプロパティは、**シリアルオーバー LAN** 機能を使うために最低限必要な権限を定義します。

チャンネル権限レベルの制限 ドロップダウンメニューで、**ユーザー**、**オペレータ**、または **管理者** を選択します。

- g. **変更の適用** をクリックします。

4. IPMI シリアルを設定します。

- a. **設定** タブで **シリアル** をクリックします。
- b. **シリアルの設定** メニューで、IPMI シリアル接続モードを適切な設定に変更します。

IPMI シリアルの 接続モードの設定 ドロップダウンメニューで適切なモードを選択します。

- c. IPMI シリアルボーレートを設定します。

ボーレート ドロップダウンメニューをクリックして、適切なボーレートを選択し、**変更の適用** をクリックします。

- d. チャンネル権限レベルの制限を設定します。

チャンネル権限レベルの制限 ドロップダウンメニューで **管理者**、**オペレータ**、または **ユーザー** を選択します。

- e. **変更の適用** をクリックします。

- f. 管理下システムの BIOS セットアッププログラムでシリアル MUX が正しく設定されていることを確認します。

- o システムを再起動します。
- o POST 中に F2 を押して BIOS セットアッププログラムを起動します。
- o **シリアル通信** に移動します。
- o **シリアル接続** メニューで **外部シリアルコネクタ** が **リモートアクセスデバイス** に設定されていることを確認します。
- o 保存して BIOS セットアッププログラムを終了します。
- o システムを再起動します。

IPMI シリアルが端末モードの場合は、次の設定を追加できます。

- 1 削除制御
- 1 エコー制御
- 1 Line edit
- 1 New line sequences
- 1 Input new line sequences

For more information about these properties, see the IPMI 2.0 specification. ターミナルモードコマンドの詳細については、support.dell.com/manuals/ の『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

iDRAC6 ユーザーの設定

詳細については、「[iDRAC6 ユーザーの追加と設定](#)」を参照してください。

SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保

ここでは、iDRAC に組み込まれているデータセキュリティ機能について説明します。

- 1 SSL (Secure Sockets Layer)
- 1 証明書署名要求 (CSR)
- 1 ウェブインタフェースを介した SSL へのアクセス
- 1 CSR の生成
- 1 サーバー証明書のアップロード
- 1 サーバー証明書の表示

SSL (Secure Sockets Layer)

iDRAC6 には、業界標準の SSL セキュリティプロトコルを使用してネットワーク上で暗号化データを送信するように設定されたウェブサーバーが含まれています。公開キーと秘密キーの暗号化技術を基礎とする SSL は、ネットワークでの盗聴を防ぐためにクライアントとサーバー間に認証された暗号化通信を提供する技術として広く普及しています。

SSL 対応システムは、次のタスクを実行できます。

- 1 SSL 対応クライアントに自らを認証する
- 1 クライアントがサーバーに対して自らを認証できるようにする
- 1 両システムが暗号化接続を確立できるようにする

暗号化プロセスは高度なデータ保護を提供します。iDRAC6 では、北米のインターネットブラウザで一般的に使用されている最も安全な暗号化方式である 128 ビットの SSL 暗号化標準を採用しています。

iDRAC6 のウェブサーバーは、デフォルトで Dell の署名入り SSL デジタル証明書 (サーバー ID) を提供します。インターネット上で高いセキュリティを確保するには、ウェブサーバーの SSL 証明書を、有名な認証局によって署名された証明書と交換してください。署名された証明書を取得するには、まず、iDRAC6 ウェブインタフェースを使用して企業情報を掲載した証明書署名要求 (CSR) を生成します。生成した CSR を VeriSign や Thawte などの認証局 (CA) に送信します。

証明書署名要求 (CSR)

CSR は、セキュアサーバー証明書の CA へのデジタル要求です。セキュアなサーバー証明書によって、サーバーのクライアントは接続しているサーバーの身元を信用できるほか、サーバーとの暗号化セッションをネゴシエートできます。

認証局は、IT 業界で認められたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を満たしています。CA には、Thawte や VeriSign などがあります。CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ基準を満たしていれば、ネットワークおよびインターネットを介したトランザクションを行う申請者を固有に識別するデジタル署名済みの証明書を発行します。

CA が CSR を承認して証明書を送信したら、それを iDRAC6 ファームウェアにアップロードします。iDRAC6 ファームウェアに保管されている CSR 情報は、証明書に記載されている情報と一致する必要があります。

ウェブインタフェースを介した SSL へのアクセス

- 1 **リモートアクセス** → **設定** をクリックします。
- 2 **SSL** をクリックして **SSL ページ** を開きます。

SSL ページを使用して次のいずれかのオプションを実行します。

- 1 CA に送信する証明書署名要求 (CSR) を生成する。CSR 情報は iDRAC6 ファームウェアに保存されています。
- 1 サーバー証明書をアップロードする。
- 1 サーバー証明書を表示する

表 4-11 では、上記の SSL ページのオプションについて説明しています。

表 4-11

フィールド	説明
証明書署名要求 (CSR) の生成	このオプションにより、CA に送信する安全なウェブ証明書を要求するための CSR を生成できます。 メモ: 新しい CSR は、ファームウェアにある古い CSR を上書きします。CA が CSR を受け入れるためには、ファームウェアにある CSR が CA から返された証明書と一致する必要があります。
サーバー証明書のアップロード	このオプションにより、会社が保有する既存の証明書をアップロードし、iDRAC6 へのアクセス制御に利用できます。 メモ: iDRAC6 で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER でエンコードされた証明書は受け入れられません。新しい証明書をアップロードすると、iDRAC6 を使って受信したデフォルトの証明書と置き換えられます。
サーバー証明書の表示	このオプションにより、既存のサーバー証明書を表示できます。

SSL ページのオプション

証明書署名要求の生成

 **メモ:** 新しい CSR はファームウェアに保存されている古い CSR データを上書きします。iDRAC が署名済み CSR を受け入れる前に、ファームウェア内の CSR が CA から返される証明書と一致する必要があります。

- 1 SSL ページで、**証明書署名要求 (CSR) の生成** を選択し、**次へ** をクリックします。

2. **証明書署名要求 (CSR) の生成** ページで、各 CSR 属性の値を入力します。[表 4-12](#) では、CSR 属性について説明しています。
3. **生成** をクリックして CSR を生成し、ローカルコンピュータへダウンロードします。
4. 適切なボタンをクリックして続行します。[表 4-13](#) を参照してください。

表 4-12 証明書署名要求 (CSR) 属性の生成

フィールド	説明
コモンネーム	証明する名前 (通常は <code>www.xyzcompany.com</code> のような iDRAC のドメイン名)。英数字、ハイフン、下線、ピリオドのみが有効です。スペースは使用できません。
組織名	この組織に関連付けられた名前 (たとえば「XYZ Corporation」)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
組織単位	部門など組織単位に関連付ける名前 (例、Information Technology)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
地域	証明する会社が所在する都市または地域 (たとえば「Minatoku」)。英数字とスペースのみが有効です。下線や他の文字で単語を区切らないでください。
都道府県名	証明書を申請している組織が所在する都道府県 (たとえば「Tokyo」)。英数字とスペースのみが有効です。略語は使用しないでください。
国番号	証明書を申請している組織が所在する国の名前。
電子メール	CSR に関連付けられている電子メールアドレス。組織の電子メールアドレスまたは CSR に関連付ける電子メールアドレスを入力します。このフィールドは任意選択です。

表 4-13 証明書署名要求 (CSR) の生成 ページのボタン

ボタン	説明
印刷	画面に表示中の 証明書署名要求の生成 ページのデータを印刷します。
更新	証明書署名要求の生成 ページを再ロードします。
生成	CSR を生成し、指定のディレクトリに保存するようユーザーに指示します。
SSL メインメニューに戻る	SSL ページに戻ります。

サーバー証明書のアップロード

1. SSL ページで **サーバー証明書のアップロード** を選択して **次へ** をクリックします。

サーバー証明書のアップロード ページが表示されます。

2. **ファイルパス** フィールドの **値** フィールドに証明書のパスを入力するか、**参照** をクリックして証明書ファイルに移動します。

 **メモ:** アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパス、完全なファイル名、ファイル拡張子を含む絶対ファイルパスを入力する必要があります。

3. **適用** をクリックします。
4. 適切なボタンをクリックして続行します。[表 4-14](#) を参照してください。

表 4-14 証明書のアップロードページのボタン

ボタン	説明
印刷	証明書のアップロード ページを印刷します。
SSL メインメニューに戻る	SSL メインメニュー ページに戻ります。
適用	証明書を iDRAC6 ファームウェアに適用します。

サーバー証明書の表示

1. SSL ページで **サーバー証明書の表示** を選択して **次へ** をクリックします。

サーバー証明書の表示 ページは、iDRAC へアップロードしたサーバー証明書を表示します。

[表 4-15](#) に、**証明書** テーブルに表示されるフィールドと関連する説明を示します。

2. 適切なボタンをクリックして続行します。[表 4-16](#) を参照してください。

表 4-15 証明書情報




フィールド	説明
シリアルナンバー	証明書のシリアル番号
タイトル情報	タイトルによって入力された証明書の属性
発行者情報	発行者によって返された証明書の属性
有効期間の開始	証明書の発行日
有効期間の終了	証明書の失効日

表 4-16 サーバー証明書の表示ページのボタン

ボタン	説明
印刷	画面に表示中の サーバー証明書の表示 ページのデータを印刷します。
更新	サーバー証明書の表示 ページを再ロードします。
SSL メインメニューに戻る	SSL ページに戻ります。

Active Directory 証明書の設定と管理

このページでは、Active Directory 設定の設定と管理ができます。

-  **メモ:** Active Directory を使用または設定するには、iDRAC の設定権限が必要です。
-  **メモ:** Active Directory の機能を設定または使用する前に、Active Directory サーバーと iDRAC6 が通信できるように設定されていることを確認してください。
-  **メモ:** Active Directory 設定の詳細および拡張スキーマまたは標準スキーマによる Active Directory の設定方法については、「[Microsoft Active Directory での iDRAC6 の使用](#)」を参照してください。

Active Directory の設定と管理 ページにアクセスするには:

1. リモートアクセス → 設定 の順でクリックします。
2. Active Directory をクリックして Active Directory の設定と管理 ページを開きます。
[表 4-17](#) に、Active Directory の設定と管理 ページのオプションを示します。
3. 適切なボタンをクリックして続行します。[表 4-18](#) を参照してください。

表 4-17 Active Directory の設定と管理 ページのオプション


Attribute(属性)	説明
共通設定	
Active Directory が有効	Active Directory が有効か無効かを指定します。
スキーマの選択	Active Directory で標準スキーマまたは拡張スキーマのいずれを使用するかを指定します。
ユーザードメイン名	この値は最大 40 個のユーザードメインエントリを保持します。設定した場合、ログインユーザーが選択できるユーザードメイン名のリストがログインページのプルダウンメニューに表示されます。設定しなかった場合、Active Directory ユーザーは ユーザー名@ドメイン名、ドメイン名/ユーザー名、またはドメイン名\ユーザー名の形式でユーザー名を入力することにより、ログインできます。
タイムアウト	Active Directory クエリが完了するまで待つ時間(秒)を指定します。デフォルト値は 120 秒です。
ドメインコントローラーサーバーアドレス 1-3 (FQDN または IP)	ドメインコントローラーの完全修飾ドメイン名 (FQDN) または IP アドレスを指定します。3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。拡張スキーマを選択した場合、これらは iDRAC デバイスオブジェクトと関連オブジェクトが存在するドメインコントローラーのアドレスです。標準スキーマでは、ユーザーアカウントとロールグループが存在するドメインコントローラーのアドレスとなります。
証明書検証が有効	iDRAC は Active Directory への接続時に、常に SSL (セキュリティソケットレイヤ) 経由で LDAP (Lightweight Directory Access Protocol) を使用します。デフォルト設定では、iDRAC は SSL (セキュリティソケットレイヤ) のハンドシェイク時に、iDRAC にロードされた CA 証明書を使用して、ドメインコントローラーの SSL (セキュリティソケットレイヤ) サーバー証明書を検証するため、強度なセキュリティを提供します。テスト目的の場合、あるいはシステム管理者が SSL (セキュリティソケットレイヤ) 証明書を検証せずにセキュリティ境界内のドメインコントローラーを信頼することにした場合、証明書の検証は無効にできます。このオプションは、証明書の検証を有効にするか、無効にするかを指定します。
Active Directory CA 証明書	
証明書	すべてのドメインコントローラーの SSL (セキュリティソケットレイヤ) サーバー証明書に署名する認証局の証明書。
拡張スキーマの設定	iDRAC 名: Active Directory 内の iDRAC を一意に識別する名前を指定します。この値はデフォルトで NULL になっています。 iDRAC ドメイン名: Active Directory iDRAC オブジェクトが存在するドメインの DNS 名(文字列)。この値はデフォルトで NULL になっています。

標準スキーマ設定	<p>グローバルカタログサーバーアドレス 1-3 (FQDN または IP) :グローバルカタログサーバーの完全修飾ドメイン名 (FQDN) または IP アドレスを指定します。3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。ユーザーアカウントと役割グループが異なるドメインにある場合、グローバルカタログサーバーは標準スキーマのみに必要です。</p> <p>役割グループ :iDRAC6 に関連する役割グループのリストを指定します。</p> <p>グループ名 - iDRAC6 に関連付けられている Active Directory の役割グループを識別する名前を指定します。</p> <p>グループドメイン :グループのドメインを指定します。</p> <p>グループ権限 - グループの権限レベルを指定します。</p>

表 4-18 Active Directory の設定と管理 ページのボタン

ボタン	定義
印刷	Active Directory の設定と管理ページに表示される値を印刷します。
更新	Active Directory の設定と管理 ページを再ロードします。
Active Directory の設定	Active Directory を設定できます。設定情報の詳細については、「 Microsoft Active Directory での iDRAC6 の使用 」を参照してください。
テスト設定	指定した設定を使用して Active Directory の設定をテストできます。 テスト設定 オプションの使用方法については、「 Microsoft Active Directory での iDRAC6 の使用 」を参照してください。

iDRAC6 サービスの設定

 **メモ**: これらの設定を変更するには、iDRAC の**設定** 権限が必要です。

1. リモートアクセス→ **設定** の順でクリックします。次に、**サービス** タブをクリックして **サービス**設定 ページを表示します。
2. 必要に応じて、次のサービスを設定します。
 1. ローカル設定 - 「[表 4-19](#)」を参照
 1. ウェブサーバー - ウェブサーバーの設定については「[表 4-20](#)」を参照
 1. SSH - SSH 設定については「[表 4-21](#)」を参照
 1. Telnet - Telnet 設定については「[表 4-22](#)」を参照
 1. リモート RACADM - リモート RACADM 設定については「[表 4-23](#)」を参照
 1. SNMP - SNMP 設定については「[表](#)」を参照
 1. 自動システムリカバリ (ASR) エージェント - ASR エージェント設定については「[表 4-25](#)」を参照
3. **適用** をクリックします。
4. 適切なボタンをクリックして続行します。[表 4-26](#) を参照してください。

表 4-19 ローカル設定

設定	説明
オプションの ROM を使用した iDRAC ローカル設定を無効にする	オプションの ROM を使用した iDRAC のローカル設定を無効にします。オプションの ROM は BIOS 内にあり、BMC および iDRAC の設定を可能にするユーザーインタフェースエンジンを提供します。オプションの ROM は、<Ctrl+E> を押してセットアップモジュールを開始するよう指示します。
RACADM を使用した iDRAC ローカル設定を無効にする	ローカル RACADM を使用した iDRAC のローカル設定を無効にします。

表 4-20 ウェブサーバーの設定

設定	説明

有効	iDRAC ウェブサーバーを有効または無効にします。チェックボックスが選択されている場合、ウェブサーバーが有効であることを示します。デフォルトは 有効 です。
最大セッション数	システムで許可される同時セッションの最大数。このフィールドは編集できません。最大同時セッション数は 5 です。
アクティブセッション数	システムの現在のセッション数(最大セッション数 以下)。このフィールドは編集できません。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定への変更はすぐに適用され、現在のウェブインタフェースセッションを中止します。ウェブサーバーもリセットされます。新しいウェブインタフェースセッションが始まるまで数分お待ちください。タイムアウト範囲は 60 ~ 10800 秒です。デフォルト値は 1800 秒です。
HTTP ポート番号	ブラウザ接続で iDRAC6 が通信するポート。デフォルトは 80 です。
HTTPS ポート番号	セキュアブラウザ接続で iDRAC6 が通信するポート。デフォルトは 443 です。

表 4-21 SSH の設定

設定	説明
有効	SSH を有効または無効にします。チェックボックスが選択されている場合、SSH は有効であることを示します。
タイムアウト	セキュアシェルのアイドルタイムアウト(秒)。タイムアウト範囲は 60 ~ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは 300 です。
ポート番号	SSH 接続で iDRAC6 が通信するポート。デフォルトは 22 です。

表 4-22 Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。選択されている場合、Telnet は有効です。
タイムアウト	telnet のアイドルタイムアウト(秒)。タイムアウト時間の範囲は 60~1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは 300 です。
ポート番号	Telnet 接続で iDRAC6 が通信するポート。デフォルトは 23 です。

表 4-23 リモート RACADM の設定

設定	説明
有効	リモート RACADM を有効または無効にします。選択した場合、リモート RACADM が有効になります。
アクティブセッション数	システムの現在のセッション数。

表 4-24 SNMP 設定

設定	説明
有効	SNMP を有効または無効にします。選択した場合、SNMP が有効になります。
SNMP コミュニティ名	SNMP コミュニティ名を有効または無効にします。選択した場合、SNMP コミュニティ名が有効になります。SNMP 警告の送信先 IP アドレスを含むコミュニティ名。コミュニティ名は最大 31 文字まで指定できます。デフォルトは public です。


表 4-25 自動システムリカバリエージェントの設定


設定	説明
有効	自動システムリカバリエージェントを有効または無効にします。選択した場合、自動システムリカバリエージェントが有効になります。

表 4-26 サービスページのボタン


ボタン	説明
印刷	サービス ページを印刷します。
更新	サービス ページを更新します。
変更の適用	サービス ページの設定を適用します。

iDRAC6 ファームウェア/システムサービスリカバリエージョンのアップデート

 **メモ:** iDRAC6 ファームウェアのアップデートが完了する前に中断されるなどで、iDRAC6 ファームウェアが破損した場合、iDRAC6 ウェブインタフェースを使用して iDRAC6 を回復できます。

 **メモ:** ファームウェアアップデートは、デフォルトで現在の iDRAC6 設定を保持します。アップデートプロセス中、iDRAC6 設定を工場出荷時のデフォルト設定にリセットできるオプションが用意されています。設定を工場出荷時のデフォルト設定に設定する場合、iDRAC6 設定ユーティリティを使用してネットワークを設定する必要があります。

1. iDRAC6 ウェブインタフェースを開いてリモートシステムにログインします。
2. **リモートアクセス** をクリックし、次に **アップデート** タブをクリックします。
3. **アップロード/ロールバック (手順 1/ 3)** ページで **参照** をクリックするか、support.dell.com からダウンロードしたファームウェアイメージまたはシステムサービスリカバリイメージへのパスを入力します。

 **メモ:** Firefox を実行している場合は、**ファームウェアイメージ** フィールドにテキストカーソルは表示されません。

例:


C:\Updates\V1.0<イメージ名>

または


\\192.168.1.10\Updates\V1.0<イメージ名>

デフォルトのファームウェアイメージ名は **firmimg.d6** です。

4. **アップロード** をクリックします。
ファイルは iDRAC6 にアップロードされます。この処理には数分かかることがあります。
プロセスが完了するまで次のメッセージが表示されます。
File upload in progress... (ファイルアップロード中)
5. **ステータス (ページ 2/3)** ページで、アップロードしたイメージファイルに対する検証結果が表示されます。
 1. イメージファイルのアップロードに成功し、すべての検証チェックに合格した場合、イメージファイル名が表示されます。ファームウェアイメージをアップロードした場合、現在および新規のファームウェアバージョンが表示されます。
または
 1. イメージのアップロードに成功しなかった場合、あるいは検証チェックに合格しなかった場合、適切なエラーメッセージが表示され、アップデートが**アップロード/ロールバック (手順 1/ 3)** ページへ戻ります。iDRAC6 のアップグレードを再試行するか、**キャンセル** をクリックして iDRAC を通常の動作モードにリセットします。
1. ファームウェアイメージの場合、**設定の保存** は既存の iDRAC6 設定を保存または消去するオプションを提供します。このオプションは、デフォルトで選択されています。

 **メモ:** **設定の保存** チェックボックスを選択解除すると、iDRAC6 はデフォルト設定にリセットされます。デフォルト設定では LAN は無効になっています。iDRAC6 ウェブインタフェースにログインできない場合もあります。BIOS POST 時に iDRAC6 設定ユーティリティを使用して LAN 設定を再設定する必要があります。

7. **アップデート** をクリックして、アップデートプロセスを開始します。
8. **アップデート中 (手順 3/ 3)** ページに、アップデートの状況が表示されます。アップグレードの進行状況は、**進行状況** 列にパーセントで表示されます。

 **メモ:** アップデートモードでは、このページから別のページに移ってもアップデートプロセスはバックグラウンドで継続されます。


ファームウェアアップデートが成功した場合、iDRAC6 は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC6 に再接続する必要があります。エラーが発生した場合、該当するエラーメッセージが表示されます。

システムサービスリカバリアップデートが成功/失敗した場合、該当するステータスメッセージが表示されます。

iDRAC6 ファームウェアのロールバック


iDRAC6 は、2 つの同時ファームウェアイメージを保持することができます。任意のファームウェアイメージからの起動(または任意ファームウェアイメージへのロールバック)を選択できます。

1. iDRAC6 ウェブインタフェースを開いてリモートシステムにログインします。
システム → **リモートアクセス** をクリックし、次に **アップデート** タブをクリックします。
2. **アップロード/ロールバック (手順 1/ 3)** ページで、**ロールバック** をクリックします。現在およびロールバックのファームウェアバージョンが**ステータス (手順 2/ 3)** ページに表示されません。
設定の保存 により、既存の iDRAC6 設定を保存または消去できます。このオプションは、デフォルトで選択されています。

 **メモ:** **設定の保存** チェックボックスを選択解除すると、iDRAC6 はデフォルト設定にリセットされます。デフォルト設定では LAN は無効になっています。iDRAC6 ウェブインタフェースにログインできない場合もあります。BIOS POST 時に iDRAC6 設定ユーティリティを使用するか、racadm コマンド(ローカルサーバー上で利用可能)を使用して LAN 設定を再設定する必要があります。

3. **アップデート** をクリックして、ファームウェアアップデートプロセスを開始します。

アップデート中 (手順 3/ 3) ページに、ロールバック動作の状況が表示されます。進行度のパーセントが **進行状況** 列に表示されます。

 **メモ:** アップデートモードでは、このページから別のページに移ってもアップデートプロセスはバックグラウンドで継続されます。

ファームウェアアップデートが成功した場合、iDRAC6 は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC6 に再接続する必要があります。エラーが発生した場合、該当するエラーメッセージが表示されます。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 の詳細設定

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [作業を開始する前に](#)
- [リモート SSH/Telnet 経由でシリアル出力を表示するための iDRAC6 設定](#)
- [シリアル接続のための iDRAC6 の設定](#)
- [シリアルコンソールの DB-9 またはヌルモデムケーブルの接続](#)
- [管理ステーションのターミナルエミュレーションソフトウェアの設定](#)
- [シリアルと端末モードの設定](#)
- [iDRAC6 のネットワーク設定](#)
- [ネットワーク経由による iDRAC6 へのアクセス](#)
- [RACADM のリモート使用](#)
- [RACADM 権限概要](#)
- [racadm リモート機能の有効 / 無効化](#)
- [複数の iDRAC6 コントローラの設定](#)
- [よくあるお問い合わせ \(FAQ\)](#)

ここでは、iDRAC6 の詳細設定について説明します。システム管理の知識が豊富なユーザーや、特定のニーズに応じて iDRAC6 環境をカスタマイズしたいユーザーにお勧めします。

作業を開始する前に

iDRAC6 ハードウェアとソフトウェアの基本インストールと設定が完了していることを前提とします。詳細については、「[iDRAC6 の基本インストール](#)」を参照してください。

リモート SSH/Telnet 経由でシリアル出力を表示するための iDRAC6 設定

以下の手順を実行して、リモートシリアルコンソールリダイレクト用に iDRAC6 を設定できます。

まず、BIOS を設定して、シリアルコンソールリダイレクトを有効にします。

1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に <F2> を押します。

<F2> = System Setup

3. スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。
4. **シリアル通信** 画面のオプションを次のように設定します。

シリアル通信...com2 のシリアルリダイレクトでオン に設定



メモ: シリアルポートアドレス フィールドのシリアルデバイス2 も com1 に設定されている限り、シリアル通信 フィールドを **com1 のシリアルリダイレクトでオン** に設定することができます

シリアルポートアドレス...シリアルデバイス1 = com1、シリアルデバイス2 = com2

外部シリアルコネクタ...シリアルデバイス1

フェイルセーフポート...115200

リモートターミナルの種類...vt100/vt220

起動後のリダイレクト...有効

次に、**変更を保存** を選択します。

5. **セットアップユーティリティ** を終了してシステムセットアップ プログラムの設定を完了するには、<Esc> を押してください。

SSH/Telnet を有効にするための iDRAC6 設定

次に、ssh/telnet を有効にするために iDRAC6 を設定します。RACADM または iDRAC6 ウェブインタフェースでも有効にすることができます。

ssh/telnet を有効にするために RACADM を使用して iDRAC6 を設定するには、以下のコマンドを実行します。

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
```

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

リモートでも RACADM コマンドを実行できます。「[RACADM のリモート使用](#)」を参照してください。

ssh/telnet を有効にするために iDRAC6 ウェブインタフェースを使用して iDRAC6 を設定するには、次の手順を実行します。

1. システム ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**サービス** をクリックします。
3. SSH または Telnet セクションの下にある **有効** を選択します。
4. **変更の適用** をクリックします。

次に、Telnet または SSH 経由で iDRAC6 に接続します。

Telnet または SSH 経由でのテキストコンソールの起動

管理ステーションの端末ソフトウェアから telnet または SSH を使って iDRAC6 にログインした後、telnet/SSH である **console com2** を使って、管理下システムのテキストコンソールをリダイレクトできます。1 度に 1 つの **console com2** クライアントのみサポートされています。

管理下システムのテキストコンソールに接続するには、iDRAC6 コマンドプロンプトを開いて (telnet または SSH セッションを通して表示)、次のように入力します。

```
console com2
```

console -h com2 コマンドは、キーボードからの入力またはシリアルポートからの新しい文字を待つ前にシリアル履歴バッファの内容を表示します。

履歴バッファのデフォルト(最大)サイズは 8192 文字です。この値は、次のコマンドを使って小さくすることができます。

```
racadm config -g cfgSerial -o cfgSerialHistorySize <数値>
```

起動中に Linux をコンソールダイレクト用に設定するには、「[起動中に Linux をシリアルコンソールリダイレクト用に設定する](#)」を参照してください。

Telnet コンソールの使用

Microsoft® Windows® XP または Windows 2003 を使って Telnet を実行する

管理ステーションで Windows XP または Windows 2003 を実行している場合は、iDRAC6 の telnet セッションで文字の不具合が発生する可能性があります。リターンキーが応答しなかったり、パスワードプロンプトが表示されないなど、ログインのフリーズ状態が発生することがあります。

この問題を解決するには、hotfix 824810 を Microsoft サポートウェブサイト support.microsoft.com からダウンロードしてください。詳細については、Microsoft 技術情報の記事 824810 を参照してください。

Windows 2000 を使って Telnet を実行する

管理ステーションで Windows 2000 を実行している場合は、<F2> キーを押して BIOS セットアップにアクセスすることはできません。この問題は、Microsoft から無料でダウンロードできる UNIX® 3.5 の Windows サービスに同梱されている telnet クライアントを使用することで解決できます。www.microsoft.com/downloads/ に移動して「Windows Services for UNIX 3.5.」を検索します。

telnet コンソールリダイレクトのための Microsoft Telnet の有効指定

 **メモ:** Some telnet clients on Microsoft オペレーティングシステム上の一部の telnet クライアントでは、BIOS コンソールリダイレクトを VT100 エミュレーションに設定した場合に BISO セットアップ画面が正しく表示されないことがあります。この問題が起きた場合は、GLOS コンソールリダイレクトを ANSI モードに変更することで表示を更新してください。BIOS セットアップメニューでこの手順を実行するには、**Console Redirection** → **リモート端末タイプ** → **ANSI** を選択してください。

1. **Windows コンポーネントサービス** で Telnet を有効にします。
2. 管理ステーションの iDRAC6 に接続します。

コマンドプロンプトを開いて次のテキストを入力し、<Enter> を押します。

```
telnet <IP アドレス>:<ポート番号>
```

ここで、IP アドレス は iDRAC6 の IP アドレスで、ポート番号は telnet ポート番号です(新しいポートを使う場合)。

Telnet セッションのための Backspace キーの設定

一部の Telnet クライアントでは、<Backspace> キーを使用すると予想外の結果が生じることがあります。たとえば、セッションが ^h をエコーすることがあります。Microsoft と Linux の telnet クライアントではほとんどの場合、<Backspace> キーの使用を設定できます。

Microsoft telnet クライアントで <Backspace> キーを使用できるように設定するには:

1. コマンドプロンプトウィンドウを開きます(必要な場合)。
2. telnet セッションをまだ実行していない場合は、次のように入力します。

```
telnet
```

telnet セッションを実行している場合は、<Ctrl><]> を押します。

3. コマンドプロンプトで、次のコマンドを入力します。

```
set bsasdel
```

次のメッセージが表示されます。

Backspace will be sent as delete. (Backspace が Delete として送信されます。)

Linux telnet セッションで <Backspace> キーを使用できるように設定するには:

1. コマンドプロンプトを開いて、次を入力します。

```
stty erase ^h
```

2. コマンドプロンプトで、次のコマンドを入力します。


```
telnet
```

Secure Shell (SSH) の使用

システムのデバイスとデバイス管理がセキュアであることが不可欠です。組み込み接続デバイスは多くのビジネスプロセスの中核となっています。これらのデバイスが危険に曝されると、コマンドラインインタフェース (CLI) デバイス管理ソフトウェアの新しいセキュリティ要件を必要とするビジネスに支障が生じることになります。

Secure Shell (SSH) は telnet セッションと同じ機能を持つコマンドラインセッションですが、セキュリティ面で telnet より優れています。iDRAC6 は、パスワード認証付きの SSH バージョン 2 をサポートしています。iDRAC6 ファームウェアをインストールまたはアップデートすると、iDRAC6 上の SSH が有効になります。

管理ステーション上では、PuTTY または OpenSSH を使用して、管理下システムの iDRAC6 に接続できます。ログイン中にエラーが発生すると、セキュアシェルクライアントはエラーメッセージを表示します。メッセージのテキストはクライアントによって異なり、iDRAC6 で制御することはできません。

 **メモ:** OpenSSH は Windows の VT100 または ANSI 端末エミュレータから実行してください。Windows のコマンドプロンプトから OpenSSH を実行した場合は、一部の機能を使用できません(複数のキーが機能せず、グラフィックが表示されません)。

一度に 4 つの SSH セッションまでしかサポートされていません。セッションタイムアウトは、「[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)」に示した `cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。

iDRAC6 で SSH を有効にするには、次を入力します。

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

SSH ポートを変更するには、次を入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <ポート番号>
```


`cfgSerialSshEnable` と `cfgRacTuneSshPort` のプロパティについては、「[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)」を参照してください。

iDRAC6 SSH の実装では、[表 5-1](#)に示すように複数の暗号化スキームがサポートされています。

表 5-1 暗号化スキーム


スキーマの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024(ランダム)ビット(NIST 仕様)
対称暗号	1 AES256-CBC 1 RIJNDAEL256-CBC 1 AES192-CBC 1 RIJNDAEL192-CBC 1 AES128-CBC 1 RIJNDAEL128-CBC 1 BLOWFISH-128-CBC 1 3DES-192-CBC 1 ARCFOUR-128
メッセージの整合性	1 HMAC-SHA1-160 1 HMAC-SHA1-96 1 HMAC-MD5-128

	1 HMAC-MD5-96
認証	1 パスワード

 **メモ:** SSHv1 はサポートされていません。

起動中に Linux をシリアルコンソールリダイレクト用に設定する

以下は Linux GRand Unified Bootloader (GRUB) 固有の手順です。別のブートローダを使用する場合も、同様の変更が必要になる可能性があります。

 **メモ:** クライアント VT100 エミュレーションウィンドウを設定するとき、リダイレクトコンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定し、適切なテキスト表示を確保してください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

/etc/grub.conf ファイルを次のように編集します。

1. ファイルの 全般設定 セクションを見つけて、次の 2 行を追加します。

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2. カーネル行に次の 2 つにオプションを追加します。

```
kernel .....console=ttyS1,57600
```

3. /etc/grub.conf に splashimage ディレクティブがある場合はコメントアウトしてください。

[表 5-2](#) に、この手順で説明する変更を示すサンプル/etc/grub.conf ファイルを示します。

表 5-2 サンプルファイル: /etc/grub.conf

grub.conf (作成者: anaconda)
#
#このファイルに変更を加えた後 grub を再実行する
必要はありません。
通知: /boot パーティションがありません。これは
全てのカーネルと initrd バスが / に相対パスであることを意味します。例:
root (hd0,0)
kernel /boot/vmlinuz-version ro root=/dev/sdal
initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial
title Red Hat Linux Advanced Server (2.4.9-e.3smp)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sdal hda=ide-scsi console=ttyS0 console=ttyS1,57600
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sdal s
initrd /boot/initrd-2.4.9-e.3.im

/etc/grub.conf ファイルを編集するとき、次のガイドラインに従ってください。

1. GRUB のグラフィカルインタフェースを無効にして、テキストベースのインタフェースを使用してください。そしないと、RAC コンソールリダイレクトで GRUB 画面は表示されません。グラフィカルインタフェースを無効にするには、splashimage で始まる行をコメントアウトしてください。
2. RAC シリアル接続を介してコンソールセッションを開始する GRUB オプションを複数有効にするには、すべてのオプションに次の行を追加してください。

```
console=ttyS1,57600
```

[表 5-2](#) に、console=ttyS1,57600 を最初のオプションにのみ追加した例を示します。

ブート後のコンソールへのログインを有効にする

/etc/inittab ファイルを次のように編集します。

COM2 シリアルポートに agetty を設定する新しい行を追加します。

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

表 5-3 に、新しい行を追加したサンプルファイルを示します。

表 5-3 サンプルファイル: /etc/inittab

```
#
# inittab このファイルは INIT プロセスで特定ランレベルのシステムを
# セットアップする方法を記述します。
#
# 作成者: Miquel van Smoorenburg
#        RHS Linux 用に修正: Marc Ewing, Donnie Barnes
#
# デフォルトランレベル。RHS が使用するランレベル:
# 0 - 停止 (initdefault はこの値に設定しないでください)
# 1 - シングルユーザーモード
# 2 - マルチユーザー、NFS なし (ネットワークがない場合は
#   3 と同じ)
# 3 - フルマルチユーザーモード
# 4 - 未使用
# 5 - X11
# 6 - 再起動 (initdefault はこの値に設定しないでください)
#
id:3:initdefault:

# システムの初期化。
si:sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

# 各ランレベルで実行するもの。
ud:once:/sbin/update

# Trap CTRL-ALT-DELETE
ca:ctrlaltdel:/sbin/shutdown -t3 -r now

# UPS から停電が知らされたら、数分間の
# 電源が残っていることを仮定します。シャットダウンを 2 分後にスケジュールします。
# 電源が取り付けられており UPS が接続されて
# 正しく動作していることを前提とします。
pf:powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# シャットダウンの前に電源が復元した場合は、割り込んでキャンセルします。
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# gettys を標準ランレベルで実行します。
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# xdm をランレベル 5で実行します。
# xdm iが別のサービスになりました。
x:5:respawn:/etc/X11/prefdm -nodaemon
```

/etc/securetty ファイルを下記のように編集します。

Add a new line with the name of the serial tty for COM2 用のシリアル tty の名前の新しい行を追加します。

```
ttyS1
```

表 5-4 に、新しい行を追加したサンプルファイルを示します。

表 5-4 サンプルファイル: /etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
```

```
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

シリアル接続のための iDRAC6 の設定

シリアル接続経由での iDRAC6 への接続には、次のいずれかのインターフェースを使用できます。

- 1 iDRAC6 CLI
- 1 直接接続基本モード
- 1 直接接続端末モード

システムをセットアップして、これらいずれかのインターフェースを使用するには、以下の手順を実行します。

BIOS を設定して、シリアル接続を有効にします。

1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に <F2> を押します。

```
<F2> = System Setup
```

3. スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。
4. **シリアル通信** 画面を次のように設定します。

```
外部シリアルコネクタ .... リモートアクセスデバイス
```

次に、**変更を保存** を選択します。

5. **セットアップユーティリティ**を終了してシステムセットアッププログラムの設定を完了するには、<Esc> を押してください。

次に、DB-9 または nulモデムケーブルを管理ステーションから管理下ノードサーバーに接続します。「[シリアルコンソールの DB-9 または nulモデムケーブルの接続](#)」を参照してください。

次に、管理ステーションのターミナルエミュレーションソフトウェアが、シリアル接続できるよう設定されていることを確認してください。「[管理ステーションのターミナルエミュレーションソフトウェアの設定](#)」を参照してください。

最後に、シリアル接続を有効にするために iDRAC6 を設定します。RACADM または iDRAC6 ウェブインターフェースでも有効にすることができます。

シリアル接続を有効にするために RACADM を使用して iDRAC6 を設定するには、以下のコマンドを実行します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

シリアル接続を有効にするために iDRAC6 ウェブインターフェースを使用して iDRAC6 を設定するには、次の手順を実行します。

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. **RAC シリアル** セクションの下にある **有効** を選択します。
4. **変更の適用** をクリックします。

元の設定でシリアルに接続した場合は、ログインプロンプトが表示されます。iDRAC6 ユーザー名とパスワードを入力してください(デフォルト値では、ユーザー名は root、パスワードは calvin です)。

このインターフェースから、RACADM などの機能を実行できます。たとえば、システムイベントログを表示するには、次の RACADM コマンドを入力します。

```
racadm getsel
```

直接接続基本モードと直接接続端末モードの iDRAC の設定

RACADM を使用して次のコマンドを実行し、iDRAC6 コマンドラインインターフェースを無効にします。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

次に、以下の RACADM コマンドを実行し、直接接続基本モードを有効にします。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 1
```

または、以下の RACADM コマンドを実行し、直接接続端末モードを有効にします。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 0
```

iDRAC6 ウェブインタフェースを使用して同じ処置を実行できます。

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. **RAC シリアル** セクションの下にある **有効** を選択解除します。

直接接続基本モードの設定

IPMI シリアル セクションの下にある **接続モード設定** ドロップダウンメニューを **直接接続基本モード** に変更します。

直接接続端末モードの設定

IPMI シリアル セクションの下にある **接続モード設定** ドロップダウンメニューを **直接接続端末モード** に変更します。

4. **変更の適用** をクリックします。
直接接続基本モードと直接接続端末モードの詳細については、「[シリアルと端末モードの設定](#)」を参照してください。

直接接続基本モードでは、シリアル接続から直接 ipmish などのツールを使用できます。たとえば、IPMI 基本モードから ipmish を使用してシステムイベントログを印刷するには、次のコマンドを実行します。

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```

直接接続端末モードでは、iDRAC6 に ASCII コマンドを発行できます。たとえば、直接接続端末モードでサーバーの電源をオンまたはオフにするには、

1. ターミナルエミュレーションソフトウェアから iDRAC6 に接続します
2. 次のコマンドを入力し、ログインします。

```
[SYS PWD -U root calvin]
```

次の応答が表示されます。

```
[SYS]
```

```
[OK]
```

3. 次のコマンドを入力し、ログインが成功したことを確認します。

```
[SYS TMODE]
```

次の応答が表示されます。

```
[OK TMODE]
```

4. サーバーの電源をオフにするには(サーバーの電源はすぐに切れます)、次のコマンドを入力します。

```
[SYS POWER OFF]
```

5. サーバーの電源をオンにするには(サーバーの電源はすぐに入ります)、次のコマンドを入力します。

```
[SYS POWER ON]
```

直接接続端末モードとシリアルコンソールリダイレクトの切り替え

iDRAC6 は、直接接続端末モードとシリアルコンソールリダイレクトを切り替えることができる Esc キーシーケンスをサポートしています。

この切り替えを可能とするためのシステムセットアップは、次の手順に従ってください。


1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に <F2> を押します。

```
<F2> = System Setup
```

3. スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。

4. **シリアル通信** 画面を次のように設定します。

シリアル通信 -- com2 のシリアルリダイレクトでオン に設定

 **メモ:** シリアルポートアドレス フィールドの**シリアルデバイス2** も com1 に設定されている限り、**シリアル通信** フィールドを com1 の**シリアルリダイレクトでオン** に設定することができます。

シリアルポートアドレス -- シリアルデバイス1 = com1、シリアルデバイス2 = com2

外部シリアルコネクタ -- シリアルデバイス2

フェイルセーフ ポーレート... 115200

モーターミナルの種類... vt100/vt220

起動後のリダイレクト... 有効

次に、**変更を保存** を選択します。

5. **セットアップユーティリティ** を終了してシステムセットアップ プログラムの設定を完了するには、<Esc> を押してください。

直接接続端末モードのときにシリアルコンソールリダイレクトモードに切り替えるには、以下のEsc キーシーケンスを使用してください。

<Esc> + <Shift> <q>

シリアルコンソールリダイレクトモードのときに直接接続端末モードに切り替えるには、以下のEsc キーシーケンスを使用してください。

<Esc> + <Shift> <9>

シリアルコンソールの DB-9 またはヌルモデムケーブルの接続

シリアルテキストコンソールを使って DRAC/MC にアクセスするには、管理下システム上の COM ポートに DB-9 ヌルモデムケーブルを接続します。ヌルモデムケーブルで接続するには、対応するシリアル通信設定を CMOS セットアップで行う必要があります。DB-9 ケーブルのすべてがこの接続に必要なピン割り当て / 信号を用意しているわけではありません。この接続に使用する DB-9 ケーブルは、[表 5-5](#) の仕様に従っている必要があります。


 **メモ:** DB-9 ケーブルは BIOS テキストコンソールリダイレクトにも使用できます。

表 5-5 DB-9 ヌルモデムケーブルに必要なピン割り当て

信号名	DB-9 ピン (7 ピン)	DB-9 ピン (ワークステーションピン)
FG (Frame Ground)	-	-
TD (Transmit data)	3	2
RD (Receive Data)	2	3
RTS (Request To Send)	7	8
CTS (Clear To Send)	8	7
SG (Signal Ground)	5	5
DSR (Data Set Ready)	6	4
CD (Data Carrier Detect)	1	4
DTR (Data Terminal Ready)	4	1 と 6

管理ステーションのターミナルエミュレーションソフトウェアの設定

iDRAC6 は、次のいずれかの種類のターミナルエミュレーションソフトウェアを実行している管理ステーションからシリアルまたは telnet テキストコンソールをサポートしています。


- 1 Xterm の Linux Minicom
- 1 Hilgraeve の HyperTerminal Private Edition (バージョン 6.3)
- 1 Xterm の Linux Telnet
- 1 Microsoft Telnet

使用するターミナルソフトウェアを設定するには、以下の項の手順に従ってください。Microsoft Telnet を使う場合は、設定は必要ありません。

シリアルコンソール用の Linux Minicomの設定

Minicom は Linux 用のシリアルポートアクセスユーティリティです。次の手順は、Minicom のバージョン 2.0 に対して有効です。他のバージョンでは若干異なる場合がありますが、必要な基本設定は同じです。他のバージョンの Minicom の設定については、「[シリアルコンソールエミュレーションに必要な Minicom の設定](#)」を参照してください。


シリアルコンソールエミュレーションに使用する Minicom バージョン 2.0 の設定

 **メモ:** telnet コンソールを表示する場合は、テキストが正しく表示されるように、Linux のインストールによるデフォルトウィンドウでなく、Xterm ウィンドウの使用をお勧めします。

1. 新しい Xterm セッションを開始するには、コマンドプロンプトで `xterm &` と入力します。
2. Xterm ウィンドウで、矢印キーをウィンドウの右下隅に移動してウィンドウのサイズを 80 x 25 に変更します。
3. Minicom の設定ファイルがない場合には、次のステップに進んでください。

Minicom の設定ファイルがある場合は、`minicom <Minicom config file name>` と入力し、[手順 17](#) に進んでください。

4. Xterm コマンドプロンプトで、`minicom -s` と入力します。
5. **Serial Port Setup**(シリアルポートのセットアップ)を選択し、<Enter> を押します。
6. <a> を押して、該当するシリアルデバイスを選択します(例: `/dev/ttyS0`)。
7. <e> を押して、**Bps/Par/Bits** オプションを **57600 8N1** に設定します。
8. <f> を押して、**ハードウェアフロー制御** を **はい** に設定し、**ソフトウェアフロー制御** を **いいえ** に設定します。
9. **シリアルポートの設定** メニューを終了するには、<Enter> を押します。
10. **モデムとダイヤル** を選択して、<Enter> を押します。
11. **モデムダイヤルとパラメータのセットアップ** メニューで、<Backspace>を押して **初期化、リセット、接続、切断** 設定をクリアすると、設定が空白になります。
12. <Enter> を押して、各ブランク値を保存します。
13. 指定のフィールドをすべてクリアする場合には、<Enter >を押して **モデムダイヤルとパラメータのセットアップ** メニューを終了します。
14. **セットアップを config_name として保存** を選択して、<Enter> を押します。
15. **Minicom から終了** を選択して、<Enter> を押します。
16. コマンドシェルプロンプトで、`minicom <Minicom config file name>` と入力します。
17. Minicom ウィンドウを 80 x 25 に拡大するには、ウィンドウの隅をドラッグします。
18. <Ctrl+a>、<z>、<x> を押して、Minicom を終了します。

 **メモ:** シリアルテキストコンソールのリダイレクトに Minicom を使用して管理下システムの BIOS を設定する場合は、Minicom で色をオンにすると便利です。色をオンにするには、`minicom -c on` コマンドを入力します。

Minicom ウィンドウがコマンドプロンプトを表示するか確認します。コマンドプロンプトが表示されたら、接続が確立されて `connect` シリアルコマンドを使って管理下システムのコンソールに接続できることを意味します。

シリアルコンソールエミュレーションに必要な Minicom の設定

[表 5-6](#) を使って、Minicom を設定します。

表 5-6 シリアルコンソールエミュレーションに必要な Minicom の設定

設定の説明	必要な設定
Bps/Par/Bits	57600 8N1

ハードウェアフロー制御	○
ソフトウェアフロー制御	×
ターミナルエミュレーション	ANSI
モデムダイヤルとパラメータの設定	初期化、リセット、接続、切断 設定をクリアして空白にします。
ウィンドウのサイズ	80 x 25 (サイズ変更するには、ウィンドウの隅をドラッグする)

シリアルコンソールリダイレクト用ハイパーターミナルの設定

HyperTerminal は、Microsoft Windows のシリアルポートアクセスユーティリティです。コンソール画面のサイズを正しく設定するには、Hilgraeve の HyperTerminal Private Edition バージョン 6.3 を使用します。

シリアルコンソールリダイレクト用に HyperTerminal を設定するには:

1. HyperTerminal プログラムを起動します。
2. 新しい接続名を入力して、OK をクリックします。
3. **使用する接続方法**: の隣で、DB-9 スルモデムケーブルを接続した管理ステーション上の COM ポート (たとえば COM1) を選択し、OK をクリックします。
4. [表 5-7](#) に示す COM ポート設定を設定します。
5. OK をクリックします。
6. [ファイル] → **プロパティ** をクリックして、**設定** タブをクリックします。
7. Telnet **ターミナル ID**: を ANSI に設定します。
8. **ターミナル設定** をクリックして、**画面の行数** を 26 に設定します。
9. **列数** を 80 に設定して、OK をクリックします。

表 5-7 管理ステーション COM ポート設定

設定の説明	必要な設定
Bps	57600
データビット	8
パリティ	なし
停止ビット	1
フロー制御	ハードウェア

シリアルと端末モードの設定

IPMI と iDRAC6 シリアルの設定

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. IPMI のシリアル設定を指定します。
IPMI シリアル設定の説明は、[表 5-8](#) を参照してください。
4. iDRAC6 のシリアル設定
iDRAC6 シリアル設定の説明は、[表 5-9](#) を参照してください。
5. **変更の適用** をクリックします。

6. シリアル設定 ページの適切なボタンをクリックして続行します。シリアル設定ページの設定については、[表 5-10](#) を参照してください。

表 5-8 IPMI シリアル設定

設定	説明
接続モード設定	<ul style="list-style-type: none"> 1 直接接続基本モード - IPMI シリアル基本モード 1 直接接続端末モード - IPMI シリアル端末モード
ボーレート	<ul style="list-style-type: none"> 1 データ速度を設定します。9600 bps、19.2 kbps、57.6 kbps、または 115.2 kbps を選択します。
フロー制御	<ul style="list-style-type: none"> 1 なし - ハードウェアフロー制御オフ 1 RTS/CTS - ハードウェアフロー制御オン
チャンネル権限レベルの制限	<ul style="list-style-type: none"> 1 システム管理者 1 オペレータ 1 ユーザー

表 5-9 iDRAC6 シリアル設定

設定	説明
有効	iDRAC6 シリアルコンソールを有効または無効にします。オン=有効、オフ=無効
タイムアウト	回線が切断される前の最大アイドル時間(秒)。範囲は 60~1920 秒です。デフォルトは 300 秒です。タイムアウト機能を無効にするには、0 秒を使用します。
リダイレクト有効	コンソールリダイレクトを有効または無効にします。オン=有効、オフ=無効
ボーレート	外部シリアルポート上のデータ速度。値は9600 bps、28.8 kbps、57.6 kbps、または 115.2 kbps です。デフォルトは 57.6 kbps です。
Esc キー	<Esc> キーを指定します。デフォルトは ^\ です。
履歴バッファサイズ	コンソールに書き込まれた最後の文字を保持するシリアル履歴バッファのサイズ。最大値およびデフォルト値 = 8192 文字
ログインコマンド	有効なログイン後に実行する iDRAC6 コマンドライン。

表 5-10 シリアル設定ページの設定

ボタン	説明
印刷	シリアル設定 ページを印刷します。
更新	シリアル設定 ページを更新します。
変更の適用	IPMI と iDRAC6 シリアルの変更を適用します。
端末モードの設定	端末モード設定 ページを開きます。

端末モードの設定

1. システム ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. シリアル設定 ページで **端末モードの設定** をクリックします。

4. 端末モード設定を指定します。

端末モードの設定の説明は、[表 5-11](#) を参照してください。

5. **変更の適用** をクリックします。

6. **端末モードの設定** ページの適切なボタンをクリックして続行します。端末モードの設定 ページのボタンの説明は、[表 5-12](#) を参照してください。

表 5-11 端末モードの設定


設定	説明
ライン編集	ライン編集を有効または無効にします。
削除制御	次のいずれかを選択します。

	<ul style="list-style-type: none"> 1 iDRAC は、<bkspace> または を受け取ると、<bkspace><space><bkspace> 文字を出力します - 1 iDRAC は、<bkspace> または を受け取ると、 文字を出力します -
エコー制御	エコーを有効または無効にします。
ハンドシェイク制御	ハンドシェイクを有効または無効にします。
新しいラインシーケンス	None、<CR-LF>、<NULL>、<CR>、<LF-CR>、または <LF> を選択します。
新しいラインシーケンスの入力	<CR> または <NULL> を選択します。

表 5-12 端末モード設定ページのボタン


ボタン	説明
印刷	端末モード設定 ページを印刷します。
更新	端末モード設定 ページを更新します。
シリアルポート設定に戻る	シリアルポート設定 ページに戻ります。
変更の適用	端末モード設定の変更を適用します。

iDRAC6 のネットワーク設定

 **注意:** iDRAC6 のネットワーク設定を変更すると、現在のネットワーク接続が切断される可能性があります。

iDRAC6 のネットワーク設定には、次のいずれかのツールを使用します。

- 1 ウェブベースのインタフェース - 「[iDRAC6 NIC の設定](#)」を参照してください。
- 1 RACADM CLI - 「[cfgLanNetworking](#)」を参照してください。
- 1 iDRAC6 設定ユーティリティ - 「[iDRAC 6 を使用するためのシステムの設定](#)」を参照してください。

 **メモ:** Linux 環境で iDRAC6 を展開する場合は、「[RACADM のインストール](#)」を参照してください。

ネットワーク経路による iDRAC6 へのアクセス

iDRAC6 を設定した後、以下のいずれかのインタフェースを使って管理下システムにリモートアクセスできます。

- 1 ウェブインタフェース
- 1 RACADM
- 1 Telnet コンソール
- 1 SSH
- 1 IPMI

[表 5-13](#) に、各 iDRAC6 インタフェースを示します。。

表 5-13 iDRAC6 インタフェース

インタフェース	説明
ウェブインタフェース	<p>グラフィカルユーザーインタフェースを使って iDRAC6 へのリモートアクセスを提供します。ウェブベースのインタフェースは iDRAC6 ファームウェアに内蔵されており、管理ステーション上の対応ウェブブラウザから NIC インタフェースを通してアクセスします。</p> <p>対応ウェブブラウザのリストについては、「対応ウェブブラウザ」を参照してください。</p>
RACADM	<p>コマンドラインインタフェースを使って iDRAC6 にリモートアクセスできます。RACADM は iDRAC6 IP アドレスを使って RACADM コマンドを実行します</p> <p>メモ: racadm リモート機能オプションは、管理ステーションだけでサポートされています。詳細については、「RACADM のリモート使用」を参照してください。</p> <p>メモ: racadm リモート機能を使用する場合には、次に示すようなファイル操作で RACADM サブコマンドを使っているフォルダへの書き込み権限が必要になります。</p> <pre>racadm getconfig -f <ファイル名></pre> <p>または</p>

	racadm sslcertupload -t 1 -f c:\cert\cert.txt サブコマンド
Telnet コンソール	iDRAC6 へアクセスを提供し、 電源オフ 、 電源オン 、 パワーサイクル 、 ハードリセット などのコマンドを含んだシリアルおよび RACADM コマンドをサポートしています。 メモ: Telnet はすべてのデータ(パスワードも含めて)をテキスト形式で送信するプロトコルです。機密情報を送信する場合は、SSH インタフェースを使用してください。
SSH インタフェース	高度なセキュリティ用の暗号化トランスポート層を使った telnet コンソールと同じ機能を提供します。
IPMI インタフェース	iDRAC6 を通じてリモートシステムの基本管理機能にアクセスできます。このインタフェースには IPMI オーバー LAN、IPMI オーバーシリアル、シリアルオーバー LAN が含まれます。詳細については、 support.dell.com/manuals にある『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

メモ: iDRAC6 のデフォルトユーザー名は root、デフォルトパスワードは calvin です。

iDRAC6 NIC 経由で iDRAC6 のウェブインタフェースにアクセスするには、対応するウェブブラウザか、Server Administrator または IT Assistant を使用します。

対応ウェブブラウザのリストは、「[対応ウェブブラウザ](#)」を参照してください。

Server Administrator を使って iDRAC6 リモートアクセスインタフェースにアクセスするには、Server Administrator を起動します。Server Administrator ホームページの左ペインにあるシステムツリーで、**システム** → **メインシステムシャシー** → **リモートアクセスコントローラ** をクリックします。詳細については、『Server Administrator ユーザーズガイド』を参照してください。

RACADM のリモート使用

メモ: RACADM のリモート機能を使用する前に、iDRAC6 の IP アドレスを設定してください。詳細な iDRAC6 の設定方法および関連情報については、「[iDRAC6 の基本インストール](#)」を参照してください。

RACADM には、管理下システムに接続し、リモートコンソールまたは管理ステーションから RACADM サブコマンドを実行できるリモート機能オプション(-r)があります。リモート機能を使用するには、有効なユーザー名(-u オプション)、パスワード(-p オプション)、および iDRAC6 IP アドレスが必要です。

メモ: リモートシステムにアクセスしているシステムのデフォルト証明書ストアに iDRAC6 証明書がない場合は、RACADM コマンドを入力したときにメッセージが表示されます。iDRAC6 証明書の詳細については、「[SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保](#)」を参照してください。

セキュリティ警告: 証明書が無効です - 証明書の名前が無効かサイト名に一致しません

実行を続けます。証明書関連のエラーが発生したとき racadm に実行を停止させるには、-s オプションを使用します。

RACADM はコマンドの実行を続行します。ただし、-s オプションを使用した場合は、RACADM がコマンドの実行を停止し、次のメッセージを表示します。

セキュリティ警告: 証明書が無効です - 証明書の名前が無効かサイト名に一致しません

Racadm はコマンドの実行を続行しません。

エラー: 指定した IP アドレスで iDRAC6 に接続できません。

メモ: RACADM リモート機能は、管理ステーションだけでサポートされています。詳細については、デルサポートサイト support.dell.com/manuals にある Dell OpenManage ソフトウェアの『Dell システムソフトウェアサポートマトリックス』を参照してください。

メモ: RACADM リモート機能を使用する場合には、次に示すようなファイル操作で RACADM サブコマンドを使っているフォルダへの書き込み権限が必要になります。

```
racadm getconfig -f <ファイル名>
```

または

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt サブコマンド
```

RACADM 構文概要

```
racadm -r <iDRAC6 IP アドレス> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <iDRAC6 IP アドレス> <サブコマンド> <サブコマンドオプション>
```

例:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

iDRAC6 の HTTPS ポート番号をデフォルトポート(443)以外のカスタムポートに変更した場合は、次の構文を使用します。

```
racadm -r <iDRAC6 IP アドレス>:<ポート> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <iDRAC6 IP アドレス>:<ポート> <サブコマンド> <サブコマンドオプション>
```


RACADM オプション

表 5-14 に、RACADM コマンドのオプションを示します。

表 5-14 racadm コマンドオプション

オプション	説明
-r <racIpAddr>	コントローラのリモート IP アドレスを指定します。
-r <racIpAddr>:<ポート番号>	iDRAC6 のポート番号がデフォルトポート(443)と異なる場合は、<ポート番号> を使用します。
-i	インタラクティブにユーザーのユーザー名とパスワードを問い合わせるように RACADM に指示します。
-u <ユーザー名>	コマンドのトランザクションの認証に使用するユーザー名を指定します。-u オプションを使用すると、-pp オプションも必要になり、-i オプション(インタラクティブ)は使用できなくなります。
-p <パスワード>	コマンドのトランザクションを認証するパスワードを指定します。-p オプションを使用すると、-i オプションは使用できなくなります。
-S	RACADM が無効な証明書エラーをチェックするように指定します。RACADM は無効な証明書を検出した場合にコマンドの実行を停止して、エラーメッセージを表示します。

racadm リモート機能の有効 / 無効化

 **メモ:** これらのコマンドはローカルシステムで実行することをお勧めします。

RACADM リモート機能はデフォルトで有効になっています。無効になっている場合は、次の RACADM コマンドを入力して有効にします。

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1
```

リモート機能を無効にするには、次を入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

RACADM サブコマンド

表 5-15 は、RACADM で実行できる各 RACADM サブコマンドについて説明しています。構文と有効なエントリを含む RACADM サブコマンドの詳細リストは、「[RACADM サブコマンドの概要](#)」を参照してください。

RACADM サブコマンドを入力するときは、コマンドに racadm を前付けしてください。

```
racadm help
```

表 5-15 RACADM サブコマンド

コマンド	説明
help	iDRAC6 サブコマンドを一覧にします。
help <サブコマンド>	指定したサブコマンドの使用ステートメントを一覧にします。
arp	ARP テーブルの内容を表示します。ARP エントリの追加や削除はできません。
clearasrscreen	前回の ASR (クラッシュ) 画面をクリアします (前回の青色画面)。
clrriaclog	iDRAC6 のログをクリアします。ログがクリアされたときのユーザーと時間を示すエントリが 1 つ作成されます。
config	iDRAC6 を設定します。
getconfig	現在の iDRAC6 設定のプロパティを表示します。
coredump	前回の iDRAC6 コア ダンプを表示します。
coredumpdelete	iDRAC6 に保存されているコアダンプを削除します。
fwupdate	iDRAC6 ファームウェアアップデートを実行、または状態を表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsysinfo	iDRAC6 とシステムの一般情報を表示します。
getrtime	iDRAC6 の時刻を表示します。
ifconfig	現在の iDRAC6 の IP 設定を表示します。
netstat	ルーティングテーブルと現在の接続を表示します。
ping	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。
setniccfq	コントローラの IP 設定を指定します。
getniccfq	コントローラの現在の IP 設定を表示します。
getsvctag	サービスタグを表示します。

racdump	iDRAC6 のステータスと状態情報をデバッグ用にダンプします。
racreset	iDRAC6 をリセットします。
racresetcfg	iDRAC6 をデフォルト設定にリセットします。
serveraction	管理下システムの電源管理を行います。
getraclog	iDRAC6 のログを表示します。
clrsele	システムイベントログのエントリをクリアします。
gettracelog	iDRAC6 トレースログ を表示します。-i と共に使用すると、iDRAC6 のトレースログ内のエントリ数を表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
sslcertupload	CA 証明書またはサーバー証明書を iDRAC6 にアップロードします。
sslcertdownload	CA 証明書をダウンロードします。
sslcertview	iDRAC6 で CA 証明書またはサーバー証明書を表示します。
sslkeyupload	電子メールの設定をチェックするには、iDRAC6 に iDRAC6 NIC 経由でテスト電子メールを送信させます。
testtrap	トラップの設定をチェックするには、iDRAC6 に iDRAC6 NIC 経由でテスト SNMP トラップを送信させます。
vmdisconnect	仮想メディア接続を強制終了します。
vmkey	仮想フラッシュサイズをデフォルトサイズ(256 MB)に戻します。

RACADM エラーメッセージについてよくあるお問い合わせ

(racadm racreset コマンドを使用して) iDRAC6 リセットを実行した後、コマンドを発行すると次のメッセージが表示されます。

エラー: 指定した IP アドレスで RAC に接続できません。

このメッセージは何を意味しますか?

iDRAC6 のリセットが完了するまで待つてから、別のコマンドを発行してください。

racadm コマンドやサブコマンドを使用すると、原因不明のエラーが発生します。

RACADM コマンドやサブコマンドを使用するとき、次のようなエラーが 1 つまたは複数起きることがあります。


- 1 ローカル RACADM エラーメッセージ - 構文、入力ミス、名前の誤りなどの問題。
- 1 リモート RACADM エラーメッセージ - IP アドレスの誤り、ユーザー名の誤り、パスワードの誤りなどの問題。

システムから iDRAC6 IP アドレスを ping した後、iDRAC6 を専用と共有モード間で切り替えると、応答が返りません。

システムの ARP テーブルをクリアしてください。


複数の iDRAC6 コントローラの設定

RACADM を使用すると、同じプロパティで 1 つまたは複数の iDRAC6 コントローラを設定できます。グループ ID と オブジェクト ID を使って特定の iDRAC6 コントローラをクエリすると、RACADM は取得した情報から racadm.cfg 設定ファイルを作成します。ファイルを 1 つまたは複数の iDRAC6 カードにエクスポートして、同じプロパティのコントローラを最短の時間で設定できます。

 **メモ:** 一部の設定ファイルには、他の iDRAC6 カードにファイルをエクスポートする前に変更が必要な固有の iDRAC6 情報(静的 IP アドレスなど)が含まれています。


複数の iDRAC6 コントローラを設定するには、次の手順を実行します。

1. RACADM を使って、適切な設定を持つターゲット iDRAC6 をクエリします。

 **メモ:** 生成された .cfg ファイルにはユーザーパスワードは含まれません。

コマンドプロンプトを開いて、次を入力します。

```
racadm getconfig -f myfile.cfg
```

 **メモ:** getconfig -f を使った iDRAC6 設定のファイルへのリダイレクトは、ローカルまたはリモート RACADM インタフェースでのみサポートされています。

2. テキストエディタを使って設定ファイルに変更を加えます(任意選択)。
3. 新しい設定ファイルを使って、ターゲット iDRAC6 を変更します。

コマンドプロンプトで、次を入力します。

```
racadm getconfig -f myfile.cfg
```

4. 設定されたターゲット iDRAC6 をリセットします。

コマンドプロンプトで、次を入力します。

```
racadm racreset
```

`getconfig -f racadm.cfg` サブコマンドは iDRAC6 の設定を要求し、`racadm.cfg` ファイルを生成します。必要なら、ファイルに別の名前を付けることもできます。


`getconfig` コマンドを使って、次の操作を行うことができます。

- 1 グループのすべての設定プロパティを表示(グループ名とインデックスで指定)
- 1 ユーザーのすべての設定プロパティをユーザー名別に表示

`config` サブコマンドは、この情報を他の iDRAC6 カードにロードします。`config` を使用して、ユーザーとパスワードのデータベースを Server Administrator と同期させます。

初期設定ファイルの `rracadm.cfg` は、ユーザーが命名します。次の例では、設定ファイルの名前は `myfile.cfg` です。このファイルを作成するには、プロンプトが表示された時に次を入力します。

```
racadm getconfig -f myfile.cfg
```


 **注意:** このファイルはテキストエディタで編集することをお勧めします。RACADM ユーティリティは ASCII テキストの構文解析を使います。フォーマットすると、パーサーが混乱して RACADM データベースが破損する可能性があります。

iDRAC6 設定ファイルの作成

iDRAC6 設定ファイル <ファイル名>.cfg は、`racadm racadm config -f <ファイル名>.cfg` コマンドで使用されます。この設定ファイルを使って設定ファイルを作成し(.ini ファイルと同様)、このファイルから iDRAC6 を設定することができます。ファイル名は自由に指定可能で、最後に .cfg を付ける必要もありません(ただし、この項ではその命名法を用いています)。

.cfg ファイルの扱いは次のとおりです。

- 1 作成される
- 1 `racadm getconfig -f <ファイル名>.cfg` コマンドで取得する
- 1 `racadm getconfig -f <filename>.cfg` コマンドで取得した後、編集する

 **メモ:** `getconfig` コマンドの詳細については、「[getconfig](#)」を参照してください。

.cfg ファイルは、最初に解析が行われ、有効なグループとオブジェクト名があること、およびいくつかの単純な構文規則が守られていることが検証されます。エラーはエラーが検出された行番号でフラグ指定され、その問題を説明した簡単なメッセージがあります。ファイル全体の整合性についての解析が終わると、すべてのエラーが表示されます。エラーが .cfg ファイルで見つかった場合、iDRAC6 へ書き込みコマンドは送信されません。設定する前に、すべてのエラーを訂正する必要があります。-c オプションは `config` サブコマンドで使用できます。これは構文のみを検証し、iDRAC6 への書き込みを行いません。

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

- 1 パーサーが索引付けされたグループを見つけた場合、これはさまざまな索引との差を表すアンカー付きオブジェクトの値です。


パーサーは、iDRAC6 からそのグループのすべてのインデックスを読み取ります。グループ内のオブジェクトはすべて iDRAC6 が設定されたときに簡単な変更が加えられたものです。変更されたオブジェクトが新しいインデックスを表す場合、設定中にその iDRAC6 のインデックスが作成されます。

- 1 .cfg ファイルでは、インデックスを選択して指定することはできません。

索引は作成と削除が繰り返されるため、グループは次第に使用中の索引と未使用索引で断片化して行く可能性があります。索引が存在する場合は、変更されます。索引が存在しない場合は、最初に使用できる索引が使用されます。この方法では、管理されているすべての RAC 間で索引を正確に一致させる必要のない場合に、索引付きエントリを追加できるという柔軟性が得られます。新しいユーザーは、最初に使用可能な索引に追加されます。すべてのインデックスが一杯で新しいユーザーを追加しなければならない場合は、1 つの iDRAC6 で正しく解析および実行される .cfg ファイルが別の iDRAC6 で也正しく実行されるとは限りません。

- 1 まったく同じプロパティを持つすべての iDRAC6 カードの設定には、`racresetcfg` サブコマンドを使います。

`racresetcfg` サブコマンドを使って iDRAC6 を元のデフォルトに戻し、`racadm config -f <ファイル名>.cfg` コマンドを実行します。cfg ファイルにすべての必要オブジェクト、ユーザー、インデックス、およびその他のパラメータが入っていることを確認します。

 **注意:** `racresetcfg` サブコマンドを使用すると、データベースと C iDRAC6 NIC は元のデフォルトの設定にリセットされ、ユーザーとユーザー設定はすべて削除されます。root (ルート)ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。

構文解析規則

- 1 「#」で始まる行はすべてコメントとして扱われます。

コメント行は一列目から記述する必要があります。その他の列にある「#」の文字は単に # という文字として扱われます。

一部のモデムパラメータでは # をその文字列内に含むことができます。エスケープ文字は必要ありません。`racadm getconfig -f <ファイル名>.cfg` コマンドで .cfg を生成し、エスケープ文字を追加せずに、`racadm config -f <ファイル名>.cfg` コマンドを異なる iDRAC6 上で実行します。

例:

```
#
```

これはコメントです。

```
[cfgUserAdmin]
```

```
cfgUserAdminPageModemInitString=<モデムの初期文字列の # はコメントではありません>
```

- 1 すべてのグループエントリは「[]」の文字で囲む必要があります。

グループ名を示すときの開始の「[」文字は一列目になければなりません。このグループ名はそのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。設定データは「[iDRAC6 プロパティデータベースグループとオブジェクト定義](#)」で定義されているようにグループにまとめられます。

次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

例:

```
[cfgLanNetworking] -{グループ名}
```

```
cfgNicIpAddress=143.154.133.121 {オブジェクト名}
```

- 1 すべてのパラメータは、「object(オブジェクト)」、「=」、または「value(値)」の間に空白を入れずに「object=value」のペアとして指定されます。


値の後にあるスペースは無視されます。値の文字列内にあるスペースはそのままにされます。'=' の右側の文字はそのまま使用されます(例:2 番目の '='、または '#', '[', ']', など)。これらの文字はすべてモデムの設定に使われるチャットスクリプト文字です。

上記の例を参照してください。

- 1 .cfg パーサーはインデックスオブジェクトエントリを無視します。

ユーザーは使用する索引を指定できません。索引がすでに存在する場合は、それが使用されます。索引がない場合は、そのグループで最初に使用可能な索引に新しいエントリが作成されません。

racadm getconfig -f <ファイル名>.cfg コマンドは、インデックスオブジェクトの前にコメントを配置するため、ユーザーは使用されているコメントをここで参照できます。


 **メモ:** 次のコマンドを用いるとインデックスグループを手動で作成することができます。

```
racadm config -g <グループ名> -o <アンカー付きオブジェクト> -i <インデックス 1 ~ 16> <固有アンカー名>
```

- 1 インデックスグループの行は、.cfg ファイルからは削除できません。

次のコマンドを使用して、手動で索引オブジェクトを削除する必要があります。

```
racadm config -g <グループ名> -o <オブジェクト名> -i <インデックス 1~16> ""
```

 **メモ:** NULL 文字列(2 つの "" 文字)は、指定したグループのインデックスを削除するように iDRAC6 に命令します。

索引付きグループの内容を表示するには、次のコマンドを使用します。

```
racadm getconfig -g <グループ名> -i <インデックス 1~16>
```

- 1 インデックスグループの場合、オブジェクトアンカーは「[]」の組み合わせ後に現われる最初にオブジェクトでなければなりません。次は、現在の索引付きグループの例です。

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<ユーザー名>
```

racadm getconfig -f <myexample>.cfg と入力すると、現在の iDRAC6 設定用の .cfg ファイルが構築されます。この設定ファイルを固有の .cfg ファイルに向けた使用例または開始点として利用することができます。

iDRAC6 IP アドレスの変更

設定ファイルの iDRAC6 IP アドレスを変更する場合は、不要な <変数>=<値> のエントリをすべて削除します。IP アドレスの変更に関する <値>=<値> エントリを含む実際の変数グループのラベルと "[]" と "]" だけが残ります。

例:

```
#
```

```
# オブジェクトグループ"cfgLanNetworking"
```

```
#
```

```
[cfgLanNetworking]
```

```
cfgNicIpAddress=10.35.10.110
```

```
cfgNicGateway=10.35.10.1
```

このファイルは次のようにアップデートされます。


```
#
```

```
# オブジェクトグループ"cfgLanNetworking"
```

```
#
[ cfgLanNetworking ]
cfgNicIpAddress=10.35.9.143
# コメント、以下の行は無視されます
cfgNicGateway=10.35.9.1
```

racadm config -f myfile.cfg コマンドは、このファイルをパースし、行番号ごとにエラーを探します。ファイルが正しければ、その内容で該当するエントリをアップデートします。アップデートを確認するために前の例でも使用した **getconfig** コマンドを使用できます。

このファイルを使用して会社全体の変更をダウンロードしたり、ネットワークで新しいシステムを設定することができます。

 **メモ:** "Anchor" は内部用語です。ファイルには使用しないでください。

iDRAC6 ネットワークプロパティの設定

使用可能なネットワークプロパティのリストを生成するには、次のように入力します。

```
racadm getconfig -g cfgLanNetworking
```

DHCP を使用して IP アドレスを取得するには、次のコマンドを使って **cfgNicUseDhcp** オブジェクトを記述し、この機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

コマンドは、起動時に <Ctrl><E> の入力を求められたときの iDRAC6 設定ユーティリティと同じ設定機能を提供します。iDRAC6 設定ユーティリティを使用したネットワークプロパティ設定の詳細については、[「iDRAC 6 を使用するためのシステムの設定」](#)を参照してください。

次に、LAN ネットワークプロパティの設定に入力できるコマンドの例を示します。

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

 **メモ:** **cfgNicEnable** を 0 に設定すると、DHCP が有効の場合でも iDRAC6 LAN は無効になります。

iDRAC6 モード

iDRAC6 は、次の 4 つのモードのいずれかに設定できます。

- 1 専用
- 1 共有
- 1 フェイルオーバー LOM2 で共有
- 1 すべてのフェイルオーバー LOM で共有

[表 5-16](#) に、各モードを示します。

表 5-16 iDRAC6 NIC 設定

モード	説明
専用	iDRAC6 は、ネットワークトラフィックに対して独自の NIC (RJ-45 コネクタ) と iDRAC MAC アドレスを使用します。

共有	iDRAC6 はブレーナで LOM1 を使用します。
フェイルオーバー LOM2 で共有	iDRAC6 は LOM1 と LOM2 をフェイルオーバー用のチームとして使用します。チームは iDRAC MAC アドレスを使用します。
すべてのフェイルオーバー LOM で共有	iDRAC6 は LOM1、LOM2、LOM3、および LOM4 をフェイルオーバー用のチームとして使用します。チームは iDRAC MAC アドレスを使用します。

よくあるお問い合わせ(FAQ)

iDRAC6 ウェブインタフェースにアクセスすると、SSL 証明書が iDRAC6 のホスト名に一致しないというセキュリティ警告が表示されます。

iDRAC6 にはデフォルトの iDRAC6 サーバー証明書が含まれており、ウェブインタフェースのネットワークセキュリティとリモート RACADM 機能を確保します。この証明書を使用する場合には、ウェブブラウザにはセキュリティ警告が表示されます。これは、デフォルトの証明書が iDRAC6 のホスト名(たとえば IP アドレス)と一致しない **iDRAC6 デフォルト証明書** に対して発行されたためです。

このセキュリティ問題に対応するには、iDRAC6 の IP アドレスまたは iDRAC 名に発行された iDRAC6 サーバー証明書をアップロードします。証明書の発行に使用する証明書署名要求(CSR)を生成する場合には、CSR の共通名(CN)が **(証明書を IP に発行する場合)** iDRAC6 の IP アドレス(例:192.168.0.120)に、**(証明書を登録済み iDRAC 名に発行する場合)** 登録されている DNS iDRAC6 名と一致することを確認してください。

CSR が登録されている DNS iDRAC6 名に一致することを確認するには:

1. **システム ツリーの リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**ネットワーク** をクリックします。
3. **共通設定** テーブルで以下の操作を行います。
 - a. **DNS に iDRAC を登録** チェックボックスを選択します。
 - b. **DNS iDRAC 名** フィールドに iDRAC6 名を入力します。
4. **変更の適用** をクリックします。

CSR の生成と証明書の発行については、[SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保](#) を参照してください。

プロパティを変更すると、リモート RACADM とウェブベースのサービスを使用できなくなるのはなぜですか？

iDRAC6 ウェブサーバーがリセットした後、リモート RACADM サービスとウェブベースのインタフェースが使用できるようになるまでに幾分時間がかかることがあります。

iDRAC6 ウェブサーバーは次のような場合にリセットします。

- 1 iDRAC6 ウェブユーザーインタフェースを使ってネットワーク設定またはネットワークセキュリティのプロパティが変更された
- 1 `cfgRacTuneHttpsPort` プロパティが変更された(`config -f <設定ファイル>` によって変更された場合を含む)
- 1 `racresetcfg` が使われた
- 1 iDRAC6 がリセットされた
- 1 新しい SSL サーバー証明書がアップロードされた

DNS サーバーで iDRAC6 を登録できない理由は何ですか？

一部の DNS サーバーは 31 文字以内の名前しか登録しません。

iDRAC6 ウェブインタフェースにアクセスすると、SSL 証明書が信頼できない認証局(CA)から発行されたというセキュリティ警告が表示されます。

iDRAC6 にはデフォルトの iDRAC6 サーバー証明書が含まれており、ウェブインタフェースのネットワークセキュリティとリモート RACADM 機能を確保します。この証明書は信頼できる CA によって発行されませんでした。このセキュリティ問題に対処するには、信頼できる CA(たとえば Microsoft 認証局、Thawte または Verisign)から発行された iDRAC6 サーバー証明書をアップロードしてください。証明書の発行の詳細については、「」を参照してください。[SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保](#)

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 ユーザーの追加と設定

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [ウェブインタフェースを使用した iDRAC6 ユーザーの設定](#)
- [RACADM ユーティリティを使用した iDRAC6 ユーザーの設定](#)


iDRAC6 を使用してシステムを管理し、システムのセキュリティを維持するには、特定の管理者権限(または役割ベースの権限)を持つ固有のユーザーを作成します。セキュリティを強化するために、特定のシステムイベントが発生したときに特定のユーザーに電子メールで警告を送るように設定することもできます。

ウェブインタフェースを使用した iDRAC6 ユーザーの設定

iDRAC6 ユーザーの追加と設定


iDRAC6 を使用してシステムを管理し、システムのセキュリティを確保するには、特定の管理者権限(役割ベースの権限)を持つ固有のユーザーを作成します。

iDRAC6 のユーザーを追加して設定するには、次の手順を実行してください。

 **メモ:** iDRAC ユーザーを設定するには、**ユーザーの設定権限**が必要です。

1. **リモートアクセス** → **設定** → **ユーザー**の順でクリックします。

ユーザー ページは iDRAC ユーザーの次の情報を表示します。**ユーザー ID**、**状態 (有効/無効)**、**ユーザー名**、**RAC 権限**、**IPMI LAN 権限**、**IPMI シリアル権限**、および **シリアルオーバー LAN 状態 (有効/無効)**。**表** は、iDRAC ユーザー設定用のユーザー状態および権限を示しています。

 **メモ:** ユーザー 1 は IPMI の匿名ユーザー用に予約されており、変更できません。

2. **ユーザー ID** 列で、ユーザー ID をクリックします。

ユーザーメインメニュー ページで、ユーザーの設定、ユーザー証明書の表示、信頼される認証局 (CA) 証明書のアップロード、あるいは信頼される CA 証明書の表示ができます。

ユーザーの設定 を選択して **次へ** をクリックすると、**ユーザー設定** ページが表示されます。ステップ 4 へ進みます。

スマートカードの設定 でオプションを選択した場合、**表**を参照してください。

3. **ユーザー設定** ページで、次の項目を設定します。

- 1 新規または既存の iDRAC ユーザーのユーザー名、パスワード、およびアクセス権限。では、**一般ユーザー設定** について **表** 説明しています。
- 1 ユーザーの IPMI 権限。**表 6-4**では、ユーザーの LAN 権限を設定するための **IPMI ユーザー権限**を説明しています。
- 1 iDRAC ユーザー権限 **表 6-5**では、iDRAC **ユーザー権限**について説明しています。
- 1 iDRAC グループアクセス権限。**表 6-6**では、iDRAC **グループ権限**について説明しています。

4. 完了したら、**変更の適用** をクリックします。

5. 適切な ボタンをクリックして続行します。**表 6-7** を参照してください。

表 6-1 ユーザーの状態および権限

設定	説明
ユーザー ID	ユーザー ID 番号の一連のリストを表示します。 ユーザー ID の各フィールドには、事前設定された 16 個のユーザー ID 番号の 1 つが含まれています。このフィールドは、編集できません。
都道府県	ユーザーのログイン状態(有効または無効)を表示します。(デフォルトでは無効になっています。) メモ: ユーザー 2 はデフォルトで有効になっています。
ユーザー名	ユーザーのログイン名を表示します。iDRAC6 ユーザー名は、最大 16 文字で指定できます。各ユーザーは固有のユーザー名を持つ必要があります。 メモ: iDRAC6 のユーザー名に / (フォワードスラッシュ) や . (ピリオド) を含めることはできません。 メモ: ユーザー名を変更した場合は、新しい名前は次のユーザーログイン時までユーザーインタフェースに表示されません。

RAC 権限	ユーザー(管理者、オペレーター、読み取り専用、またはなし)を割り当てたグループ(権限レベル)を表示します。
IPMI LAN 権限	ユーザー(管理者、オペレーター、読み取り専用、またはなし)を割り当てた IPMI LAN 権限レベルを表示します。
IPMI シリアル権限	ユーザー(管理者、オペレーター、読み取り専用、またはなし)を割り当てた IPMI シリアルポート権限レベルを表示します。
シリアルオーバー LAN	IPMI シリアルオーバー LAN の使用を許可または拒否します。

表 6-2 スマートカード設定オプション

オプション	説明
ユーザー証明書の表示	iDRAC にアップロードされたユーザー証明書ページを表示します。
信頼される CA 証明書のアップロード	信頼される CA 証明書を iDRAC にアップロードしてユーザープロファイルにインポートできます。
信頼される CA 証明書の表示	iDRAC にアップロードされた信頼される CA 証明書を表示します。信頼される CA 証明書は、ユーザーに証明書を発行することを許可されている CA によって発行されます。

表 6-3 一般ユーザー設定

ユーザー ID	16 個ある設定済みユーザー ID 番号の 1 つです。
ユーザーを有効にする	選択されている場合、iDRAC6 へのユーザーのアクセスが有効であることを示します。選択解除されている場合、ユーザーアクセスは無効であることを示します。
ユーザー名	最大 16 文字のユーザー名。
パスワードの変更	新しいパスワードと新しいパスワードの確認 フィールドを有効にします。選択しないと、ユーザーのパスワードを変更することはできません。
新しいパスワード	20 文字以内でパスワードを入力します。文字は表示されません。
新しいパスワードの確認	確認のために iDRAC ユーザーのパスワードを再入力します。

表 6-4 IPMI ユーザー権限

プロパティ	説明
許可される最高 LAN ユーザー権限	IPMI LAN チャネル上でのユーザーの最高権限として、システム管理者、オペレータ、ユーザー、またはなしのユーザーグループのいずれかを指定します。
許可する最大シリアルポートユーザー権限	IPMI シリアルチャネル上でのユーザーの最高権限として、システム管理者、オペレータ、ユーザー、またはなしのユーザーグループのいずれかを指定します。
シリアルオーバー LAN を有効にする	IPMI シリアルオーバー LAN を使用できます。選択すると、権限が有効になります。

表 6-5 iDRAC ユーザー権限

プロパティ	説明
役割	iDRAC ユーザーの最高権限として、システム管理者、オペレータ、読み取り専用、またはなしのいずれかを指定します。iDRAC グループ 権限については、「表 6-6」を参照してください。
iDRAC へのログイン	iDRAC にログインできます。
iDRAC の設定	iDRAC を設定できます。
ユーザーの設定	特定ユーザーのシステムアクセスを許可できるようにします。
ログのクリア	iDRAC のログをクリアできます。
サーバーコントロールコマンドの実行	サーバー制御のコマンドを実行できるようにします。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告(電子メールと PET)を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。


表 6-6 iDRAC グループ権限

ユーザーグループ	許可する権限
システム管理者	iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバーコントロールコマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
オペレータ	次の権限を組み合わせて選択します。iDRAC へのログイン、iDRAC の設定、ユーザーの設定、ログのクリア、サーバー処置コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
読み取り専用	iDRAC へのログイン
なし	権限の割り当てなし

表 6-7 ユーザー設定ページのボタン

ボタン	動作
印刷	画面に表示されている ユーザー設定 ページの値を印刷します。
更新	ユーザー設定 ページを再ロードします。
ユーザー ページに戻る	ユーザーページに戻ります。
変更の適用	ユーザー設定に追加された新規設定を保存します。

RACADM ユーティリティを使用した iDRAC6 ユーザーの設定

 **メモ:** リモート Linux システム上で RACADM コマンドを実行するには、ユーザー `root` としてログインする必要があります。


iDRAC6 ユーザーを設定する方法として、iDRAC6 ウェブインタフェースを使用するのが最速となります。コマンドラインまたはスクリプトの設定を好む場合、または複数の iDRAC6 を設定する必要がある場合は、管理下システム上に iDRAC6 と共にインストールされている RACADM を使用してください。


まったく同じ設定を複数の iDRAC6 に対して指定する場合は、次のいずれかの手順を行ってください。

- 1 本項にある RACADM の例をガイドにして、RACADM コマンドのバッチファイルを作成し、各管理下システム上でこのバッチファイルを実行します。
- 1 「[RACADM サブコマンドの概要](#)」に記述されているとおりに iDRAC6 設定ファイルを作成し、各管理下システム上で同じ設定ファイルを使って `racadm config` サブコマンドを実行します。

作業を開始する前に

iDRAC6 のプロパティデータベースには、最大 16 のユーザーを設定できます。iDRAC6 ユーザーを手動で有効にする前に、現在のユーザーが既に存在するか確認します。新しい iDRAC6 を設定している場合や、`racadm racresetcfg` コマンドを実行した場合、現在のユーザーは `root` のみで、パスワードは `calvin` になります。`racresetcfg` サブコマンドは iDRAC6 をデフォルト値にリセットします。

 **注意:** `racresetcfg` コマンドを使用するときは十分に注意してください。すべての設定パラメータはデフォルト値に戻されます。それまでに行った変更がすべて失われます。

 **メモ:** ユーザーは経時的に有効にしたり、無効にしたりできます。その結果、ユーザーが各 iDRAC6 に異なる索引番号を持つ場合があります。


コマンドプロンプトで次のコマンドを入力すると、ユーザーが存在するかどうかわかります。

```
racadm getconfig -u <ユーザー名>
```

または

または、1~16 までの各インデックスに次のコマンドを 1 回ずつ入力することもできます。

```
racadm getconfig -g cfgUserAdmin -i <索引>
```


 **メモ:** `racadm getconfig -f <myfile.cfg>` と入力して、iDRAC6 設定パラメータが含まれる `myfile.cfg` ファイルを表示したり編集したりできます。

複数のパラメータとオブジェクト ID が現在値と共に表示されます。対象オブジェクトは次の 2 つです。

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

`cfgUserAdminUserName` オブジェクトに値がない場合は、`cfgUserAdminIndex` オブジェクトで示されるその索引番号は使用可能です。(等号)の後に名前が表示される場合は、インデックスがそのユーザーによって使用されています。

 **メモ:** `rracadm config` サブコマンドを使ってユーザーを手動で追加または削除する場合は、`-i` オプションでインデックスを指定する必要があります。前の例で示した `cfgUserAdminIndex` オブジェクトに '#' 文字が含まれていることに注目してください。グループ / オブジェクトを書き込むことを指定するために `racadm config -f racadm.cfg` コマンドを使用する場合は、インデックスは指定できません。新しいユーザーが最初に使用可能なインデックスに追加されます。この動作により、同じ設定を持つ複数の iDRAC6 を設定する柔軟性が得られます。

iDRAC6 ユーザーの追加

新しいユーザーを RAC 設定に追加するには、基本コマンドをいくつか使うことができます。通常は、次の手順を実行してください。

- 1 ユーザー名を設定します。
- 2 パスワードを設定します。
- 3 次のユーザー権限を設定します。

- 1 iDRAC 権限

- 1 IPMI LAN 権限
- 1 IPMI シリアル権限
- 1 シリアルオーバー LAN 権限

4. ユーザーを有効にします。

例

次の例ではパスワード "123456" と LOGIN 権限を持つ新しいユーザー名 "John" を RAC に追加します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmlanPrivilege 4
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmlSerialPrivilege 4
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminSolEnable 1
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

確認するには、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 2
```

iDRAC6 ユーザーの削除

RACADM を使用している場合は、ユーザーを手動で個別に無効にする必要があります。設定ファイルを使用してユーザーを削除することはできません。


次の例では、RAC ユーザーの削除に使用できるコマンド構文を示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス> ""
```

二重引用符の("")のヌル文字列は、指定した索引のユーザー設定を削除して、出荷時のデフォルトにリセットするように iDRAC6 に指示します。

権限のある iDRAC6 ユーザーを有効にする

ユーザーに特定の管理権限(ロールベースの権限)を与えるには、まず「[作業を開始する前に](#)」に記述されている手順で使用可能なユーザーインデックスを探します。その後、新しいユーザー名とパスワードを使って次のコマンドラインを入力します。

 **メモ:** 各ユーザー権限用に有効なビットマスク値のリストは、[表 B-2](#) を参照してください。デフォルト権限値は 0 で、これはユーザーにどの権限も与えられていないことを示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <インデックス> <ユーザー権限ビットマスク値>
```

[目次ページに戻る](#)

[目次ページに戻る](#)

Microsoft Active Directory での iDRAC6 の使用

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0 ユーザーズガイド

- [iDRAC6 用に Active Directory 認証を有効にするための必要条件](#)
- [サポートされている Active Directory の認証機構](#)
- [拡張スキーマ Active Directory の概要](#)
- [標準スキーマの Active Directory の概要](#)
- [設定のテスト](#)
- [ドメインコントローラの SSL を有効にする](#)
- [Active Directory を使用した iDRAC6 へのログイン](#)
- [よくあるお問い合わせ \(FAQ\)](#)

ディレクトリサービスは、ネットワーク上のユーザー、コンピュータ、プリンタなどを制御するのに必要な全情報に共通のデータベースを管理します。会社で Microsoft® Active Directory® サービスソフトウェアを既に使用している場合は、iDRAC6 にアクセスできるように設定し、Active Directory ソフトウェアの既存のユーザーに iDRAC6 のユーザー権限を追加して制御できます。


 **メモ:** Microsoft Windows® 2000、Windows Server® 2003、および Windows Server 2008 オペレーティングシステムでは、Active Directory を使用して DRAC 5 のユーザーを認識できます。

表 7-1 では、9 つの iDRAC6 Active Directory ユーザー権限を記載しています。

表 7-1 iDRAC6 ユーザー権限

権限	説明
iDRAC へのログイン	iDRAC6 にログインできます。
iDRAC の設定	iDRAC6 を設定できます。
ユーザーの設定	特定ユーザーのシステムアクセスを許可できるようにします。
ログのクリア	iDRAC6 のログをクリアできます。
サーバーコントロールコマンドの実行	RACADM コマンドを実行できます。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告 (電子メールと PET) を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

iDRAC6 用に Active Directory 認証を有効にするための必要条件

Active Directory で iDRAC6 を認証する機能を使用するには、Active Directory インフラストラクチャが既に展開されている必要があります。Active Directory インフラストラクチャがまだ構築されていない場合、その設定方法については、Microsoft のウェブサイト参照してください。

iDRAC6 は標準の公開鍵インフラストラクチャ (PKI) メカニズムを使用して Active Directory に対して安全に認証するため、Active Directory インフラストラクチャに PKI を統合させる必要があります。PKI の設定については、Microsoft のウェブサイト参照してください。

すべてのドメインコントローラに対して正しく認証するには、iDRAC6 に接続するすべてのドメインコントローラ上で Secure Socket Layer (SSL) を有効にする必要もあります。詳細については、「[ドメインコントローラの SSL を有効にする](#)」を参照してください。

サポートされている Active Directory の認証機構

Active Directory を使用して 2 つの方法で iDRAC6 へのユーザーアクセスを定義できます。1 つめは、デフォルトの Active Directory オブジェクトが追加された拡張スキーマソリューションの利用です。2 つめの方法は、Active Directory グループオブジェクトのみを使用する標準スキーマソリューションの利用です。これらソリューションについての詳細は、以降に続く該当するセクションを参照してください。

Active Directory を使用して iDRAC6 へのアクセスを設定する場合は、拡張スキーマソリューションまたは標準スキーマソリューションのどちらかを選択する必要があります。

拡張スキーマソリューションを使用する場合の長所は次のとおりです。

- 1 すべてのアクセスコントロールオブジェクトを Active Directory で管理可能。
- 1 さまざまな権限レベルで異なる iDRAC6 カードへのユーザーアクセスを設定するために、最大限の柔軟性が提供されています。

標準スキーマソリューションを利用する利点として、スキーマ拡張子が必要ないことが挙げられます。必要となるすべてのオブジェクトクラスは、Active Directory スキーマの Microsoft のデフォルト設定で提供されているためです。

拡張スキーマ Active Directory の概要

拡張スキーマソリューションを利用する場合は、下記の項で説明されるように、Active Directory のスキーマ拡張子が必要となります。

Active Directory スキーマの拡張

重要: 本製品のスキーマ拡張は、過去の Dell リモート管理製品のものとは異なります。新しいスキーマを拡張し、ディレクトリ上に新しい Active Directory ユーザーとコンピュータ Microsoft 管理コンソール (MMC) スナップインをインストールする必要があります。本製品では、古いスキーマに対応していません。

メモ: 新しいスキーマの拡張または Active Directory ユーザーとコンピュータ スナップインに新しい拡張子をインストールしても、製品の過去のバージョンに何の影響もありません。

スキーマエクステンダおよび Active Directory ユーザーとコンピュータ MMC スナップイン拡張子は、『Dell Systems Management Tools and Documentation DVD』に収録されています。詳細については、『Active Directory の拡張』および『Active Directory ユーザーとコンピュータ スナップインへの Dell 拡張子のインストール』を参照してください。iDRAC6 向けのスキーマ拡張および Active Directory ユーザーとコンピュータ MMC スナップインのインストールの詳細については、support.dell.com/manuals 上の『Dell OpenManage インストールとセキュリティ ユーザーズガイド』を参照してください。

メモ: iDRAC 関連オブジェクトまたは iDRAC デバイスオブジェクトを作成する際、**Dell リモート管理オブジェクトの詳細設定** を選択するようにしてください。

Active Directory スキーマ拡張

Active Directory データは、属性とクラスの分散データベースです。Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。ユーザークラスは、データベースに保存されるクラスの一例です。ユーザークラスの属性の例としては、ユーザーの名、姓、電話番号などがあります。会社は、自社環境に特有のニーズを満たすための固有の属性とクラスを追加することで、Active Directory データベースを拡張できます。デルでは、スキーマを拡張して、リモート管理の認証と許可をサポートするために必要な変更を含めました。

既存の Active Directory スキーマに追加した属性やクラスは、それぞれ固有の ID で定義する必要があります。業界を通じて一意な ID の維持を図るため、Microsoft が Active Directory オブジェクト識別子 (OID) のデータベースを管理して、会社がスキーマに拡張機能を追加する際、それが固有なもので互いに重複しないことが保証されています。デルでは、Microsoft の Active Directory のスキーマを拡張できるように、ディレクトリサービスに追加された属性とクラス用の固有の OID、固有の名前の拡張子、および固有のリンク属性 ID を受け取っています。

Dell の拡張子: dell

Dell ベースの OID: 1.2.840.113556.1.8000.1280

RAC LinkID の範囲: 12070 ~ 12079

iDRAC スキーマ拡張の概要

Dell では、さまざまな顧客環境に柔軟に対応できるように、ユーザーが達成したい成果に応じて設定できるプロパティを用意しています。Dell は、関連、デバイス、権限のプロパティを加えて、このスキーマを拡張しました。関連プロパティは、特定の権限セットを持つユーザーまたはグループを 1 台または複数台の iDRAC デバイスにリンクするために使用します。このモデルでは、ユーザー、iDRAC 権限、およびネットワーク上の iDRAC デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

Active Directory オブジェクトの概要

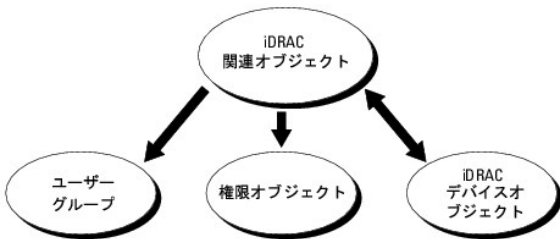
認証と許可のために Active Directory に統合するネットワーク上の物理 RAC の 1 台につき、少なくとも 1 個ずつ関連オブジェクトと RAC デバイスオブジェクトを作成しておきます。関連オブジェクトは必要な数だけ作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、iDRAC デバイスオブジェクトの数にも制限はありません。ユーザーと iDRAC デバイスオブジェクトは、企業内のどのドメインのメンバーでも構いません。

ただし、各関連オブジェクトは 1 つの権限オブジェクトにしかリンクできず、ユーザー、ユーザーグループ、iDRAC デバイスオブジェクトを 1 つの権限オブジェクトにしかリンクできません。この例では、Administrator (システム管理者) は特定の iDRAC で各ユーザーの権限を制御できます。

iDRAC デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための iDRAC ファームウェアへのリンクです。iDRAC をネットワークに追加した場合、システム管理者は iDRAC とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と許可を実行できるようにする必要があります。さらに、ユーザーが認証できるように、iDRAC を少なくとも 1 つの関連オブジェクトに追加する必要があります。

[図 7-1](#) は、関連オブジェクトがすべての認証と許可に必要な関連付けを提供する仕組みを示しています。

図 7-1 Active Directory オブジェクトの典型的なセットアップ



作成する関連オブジェクトの数に制限はありません。ただし、iDRAC で認証と許可を実行するには、関連オブジェクトを少なくとも 1 つ作成する必要があり、Active Directory と統合するネットワーク上の iDRAC デバイスごとに iDRAC デバイスオブジェクトが 1 つ必要となります。

関連オブジェクトに含むことができるユーザー、グループ、iDRAC デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる権限オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは、iDRACs デバイス上で「権限」を持つ「ユーザー」を接続します。

Active Directory ユーザーとコンピュータ MMC スナップインへの Dell 拡張子は、関連オブジェクトと同じドメインの権限オブジェクトおよび iDRAC オブジェクトのみと関連付けさせることができます。Dell 拡張子は、異なるドメインのグループまたは iDRAC オブジェクトを関連オブジェクトの製品メンバーとして追加することを許可していません。

いかなるドメインのユーザー、ユーザーグループまたはネストされたユーザーグループを関連オブジェクトに追加することができます。拡張スキーマソリューションは、Microsoft Active Directory に

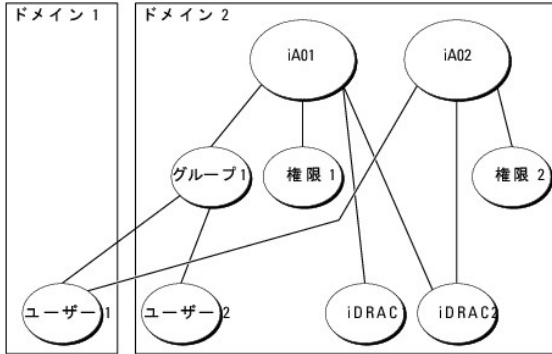
よって許可されている複数のドメインにわたってネストされるいかなるユーザーグループおよびユーザーグループの種類をサポートしています。

拡張スキーマを使った権限の蓄積

拡張スキーマ認証機構は、異なる関連オブジェクトを通して同じユーザーに関連付けられている異なるオブジェクトからの権限の蓄積をサポートしています。つまり、拡張スキーマ認証は権限を蓄積することで、同じユーザーに関連付けられている異なる権限オブジェクトに対応するすべての権限のスーパーセットを使用できるようにします。

図 7-2 に、拡張スキーマを使用した権限の蓄積例を示します。

図 7-2 ユーザーの権限の蓄積



この図には、A01 と A02 の 2 つの関連オブジェクトが示されています。ユーザー 1 は、両関連オブジェクトを介して、iDRAC2 と関連付けられています。したがって、ユーザー 1 には iDRAC2 上で権限 1 と権限 2 のオブジェクトに設定された両方の権限が付与されます。

たとえば、権限 1 には、ログイン、仮想メディアおよびログのクリアの権限が割り当てられ、権限 2 には、iDRAC へのログイン、テストおよびテスト警告の権限が割り当てられます。その結果、ユーザー 1 には、権限 1 と権限 2 の両方の権限を組み合わせた iDRAC へのログイン、仮想メディア、ログのクリア、iDRAC の設定、テスト警告の権限が付与されます。

拡張スキーマ認証は、同じユーザーに関連付けられている異なる権限オブジェクトに割り当てられている権限を考慮してこのように権限を蓄積することでユーザーに最大限の権限を与えます。

この設定では、ユーザー 1 は iDRAC2 において、権限 1 と権限 2 を保有しています。ユーザー 1 は、iDRAC1 において、権限 1 しか保有していません。ユーザー 2 は、iDRAC1 と iDRAC2 の両方において、権限 1 が付与されます。さらに、この図では、ユーザー 1 は異なるドメインに属していても、ネストされたグループに関連付けられることを示しています。

iDRAC にアクセスするための拡張スキーマ Active Directory の設定

Active Directory を使って iDRAC6 にアクセスする前に、次の手順を実行して、Active Directory ソフトウェアと iDRAC6 を設定する必要があります。

1. Active Directory スキーマを拡張します。(「[Active Directory スキーマの拡張](#)」を参照)
2. Active Directory ユーザーおよびコンピュータの Snap-in を拡張します。(「[Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール](#)」を参照)
3. iDRAC6 ユーザーとその権限を Active Directory に追加します(「[Active Directory への iDRAC ユーザーと権限の追加](#)」を参照)。
4. SSL を各ドメインコントローラで有効にします(「[ドメインコントローラの SSL を有効にする](#)」を参照)。
5. iDRAC6 ウェブインタフェースまたは RACADM を使用して、iDRAC6 Active Directory プロパティを設定します(「[iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定](#)」または「[RACADM を使用した拡張スキーマの Active Directory の設定](#)」を参照)。

Active Directory スキーマを拡張すると、Dell の組織単位、スキーマのクラスと属性、サンプル権限、および関連オブジェクトが Active Directory スキーマに追加されます。スキーマを拡張するには、ドメインフォレストのスキーママスター FSMO(Flexible Single Master Operation)ロール(役割)オーナーのスキーマ Administrator 権限が必要です。

次のいずれかの方法を使用してスキーマを拡張できます。

1. Dell Schema Extender ユーティリティ
1. LDIF スクリプトファイル

LDIF スクリプトファイルを使用すると、Dell の組織単位はスキーマに追加されません。

LDIF ファイルと Dell Schema Extender はそれぞれ『Dell Systems Management Tools and Documentation DVD』の次のディレクトリに入っています。

1. DVD ドライブ:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
1. <DVD ドライブ>:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender

LDIF ファイルを使用するには、LDIF_Files ディレクトリにある readme の説明を参照してください。Dell Schema Extender を使用して Active Directory スキーマを拡張するには、「[Dell Schema Extender の使用](#)」を参照してください。

Schema Extender または LDIF ファイルのコピーと実行はどの場所からでもできます。

Dell Schema Extender の使用

メモ: Dell Schema Extender (スキーマ拡張ユーティリティ) は、SchemaExtenderOem.ini ファイルを使用します。Dell Schema Extender ユーティリティが正しく機能するように、このファイルの名前と内容を変更しないでください。

1. ようこそ 画面で、次へ をクリックします。
2. 警告を読んでから、もう一度 次へ をクリックします。
3. 資格情報で現在のログの使用 を選択するか、スキーマ Administrator 権限でユーザー名とパスワードを入力します。
4. Dell Schema Extender を実行するには、次へ をクリックします。
5. 完了 をクリックします。

スキーマが拡張されます。スキーマ拡張子を確認するには、Microsoft 管理コンソール (MMC) と Active Directory スキーマスナップインを使用して、次のものがあることを確認します。

- 1 クラス(「表 7-2」～「表 7-7」を参照)。
- 1 属性(「表 7-8」)

MMC および Active Directory スキーマスナップインの使用の詳細については、Microsoft のマニュアルを参照してください。

表 7-2 Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられるオブジェクト識別番号(OID)
dellIDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
dellIDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellIRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 7-3 dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.1
説明	Dell iDRAC デバイスを表します。iDRAC デバイスは Active Directory では dellIDRACDevice として設定する必要があります。この設定を使って、iDRAC は Lightweight Directory Access Protocol(LDAP)クエリを Active Directory に送信できます。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 7-4 dellIDRACAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.2
説明	Dell 関連オブジェクトを表します。この関連オブジェクトはユーザーとデバイスを結び付けます。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	dellProductMembers dellPrivilegeMember

表 7-5 dellIRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	iDRAC デバイスの権限(許可権限)を定義します。
クラスの種類	補助クラス
SuperClasses	なし
属性	dellIsLoginUser

dellIsCardConfigAdmin
dellIsUserConfigAdmin
dellIsLogClearAdmin
dellIsServerResetUser
dellIsConsoleRedirectUser
dellIsVirtualMediaUser
dellIsTestAlertUser
dellIsDebugCommandAdmin

表 7-6 dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	Dell の権限 (許可権限) のコンテナクラスとして使用されます。
クラスの種類	構造体クラス
SuperClasses	ユーザー
属性	dellRAC4Privileges

表 7-7 dellProduct クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.5
説明	すべての Dell 製品が派生するメインクラス。
クラスの種類	構造体クラス
SuperClasses	コンピュータ
属性	dellAssociationMembers

表 7-8 Active Directory スキーマに追加された属性のリスト

属性名 / 説明	割り当てられる OID / 構文オブジェクト識別子	単一値
dellPrivilegeMember この属性に属する dellPrivilege オブジェクトのリスト	1.2.840.113556.1.8000.1280.1.1.2.1 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers この役割に属する dellRacDevice および DellDRACDevice オブジェクトのリスト。この属性は dellAssociationMembers バックワードリンクへのフォワードリンクです。 リンク ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser ユーザーにデバイスへのログイン権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin ユーザーにデバイスのカード設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin ユーザーにデバイスのユーザー設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser ユーザーにデバイスのコンソールリダイレクト権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

dellVirtualMediaUser ユーザーにデバイスの仮想メディア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellTestAlertUser ユーザーにデバイスのテスト警告ユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion スキーマのアップデートに現在のスキーマバージョンが使用されます。	1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType この属性は dellIDRACDevice オブジェクトの現在の RACタイプで dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers オブジェクトのリスト。この属性は dellProductMembers リンク属性へのバックワードリンクです。 リンク ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール

Active Directory でスキーマを拡張する場合は、iDRAC デバイス、ユーザーとユーザーグループ、iDRAC 関連付け、iDRAC 権限などを管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『Dell Systems Management Tools and Documentation DVD』を使ってシステム管理ソフトウェアをインストールする場合、インストール手順中に **Active Directory ユーザーとコンピュータ スナップイン**のオプションを選択するとスナップインを拡張できます。システム管理ソフトウェアのインストールの手順については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。64 ビット Windows オペレーティングシステムでは、スナップインのインストールは <DVD ドライブ >:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64 にあります。

Active Directory ユーザーとコンピュータスナップインの詳細に関しては、Microsoft のマニュアルを参照してください。

Administrator Pack のインストール

Active Directory iDRAC オブジェクトを管理している各システムに Administrator Pack をインストールする必要があります。Administrator Pack をインストールしないと、コンテナ内の Dell iDRAC オブジェクトを表示できません。

詳細については、「[Active Directory ユーザーとコンピュータスナップインの開始](#)」を参照してください。

Active Directory ユーザーとコンピュータスナップインの開始

Active Directory ユーザーとコンピュータスナップインを開くには:

- ドメインコントローラにログインしている場合は、**スタート**→**管理ツール**→**Active Directory ユーザーとコンピュータ**の順にクリックします。

ドメインコントローラにログインしていない場合は、適切な Microsoft Administrator Pack がローカルシステムにインストールされている必要があります。この Administrator Pack をインストールするには、**スタート**→**ファイル名を指定して実行**の順にクリックし、MMC と入力して **Enter** を押します。

MMC が表示されます。

- コンソール 1** ウィンドウで、**ファイル** (または Windows 2000 を実行しているシステムでは**コンソール**) をクリックします。
- スナップインの追加と削除** をクリックします。
- Active Directory ユーザーとコンピュータ スナップイン**を選択し、**追加** をクリックします。
- 閉じる** をクリックして OK をクリックします。

Active Directory への iDRAC ユーザーと権限の追加


Dell の拡張 Active Directory ユーザーとコンピュータスナップインを使用して、iDRAC、関連付け、および権限オブジェクトを作成すると、iDRAC のユーザーと権限を追加できます。各オブジェクトタイプを追加するには、次の手順に従います。

- 1 iDRAC デバイスオブジェクトの作成
- 1 権限オブジェクトの作成
- 1 関連オブジェクトの作成
- 1 関連オブジェクトの設定

iDRAC デバイスオブジェクトの作成


1. MMC **コンソールルート** ウィンドウでコンテナを右クリックします。
2. **新規**→ Dell **リモート管理オブジェクトの詳細設定** の順で選択します。
新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。この名前は、「[iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定](#)」のステップ A で入力する iDRAC 名と同一でなければなりません。
4. **iDRAC デバイスオブジェクト** を選択します。
5. **OK** をクリックします。

権限オブジェクトの作成

 **メモ:** 権限オブジェクトは、関係する関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。
2. **新規**→ Dell **リモート管理オブジェクトの詳細設定** の順で選択します。
新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **権限オブジェクト** を選択します。
5. **OK** をクリックします。
6. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。
7. **リモート管理特権** タブをクリックし、ユーザーに与える権限を選択します。

関連オブジェクトの作成

 **メモ:** iDRAC 関連オブジェクトは、グループ から派生し、その範囲は、ドメインローカル に設定されます。

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。
2. **新規**→ Dell **リモート管理オブジェクトの詳細設定** の順で選択します。
新規オブジェクト ウィンドウが開きます。
3. 新しいオブジェクトの名前を入力します。
4. **関連オブジェクト** を選択します。
5. **関連オブジェクト** のスコープを選択します。
6. **OK** をクリックします。

関連オブジェクトの設定

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーまたはユーザーグループ、権限オブジェクト、iDRAC デバイス間の関連付けができます。

ユーザーのグループを追加できます。Dell 関連グループと Dell に関連しないグループを作成する手順は同じです。

ユーザーまたはユーザーグループの追加

1. **関連オブジェクト** を右クリックし、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限オブジェクト タブをクリックして、iDRAC デバイスに認証するときにユーザーまたはユーザーグループの権限を定義する関連付けに、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは 1 つだけです。

権限の追加

1. **権限オブジェクト** タブを選択し、**追加** をクリックします。
2. 権限オブジェクト名を入力し、**OK** をクリックします。

定義されたユーザーまたはユーザーグループが利用できるネットワークに接続された iDRAC デバイスを 1 つ追加するには、**製品** タブをクリックします。関連オブジェクトには複数の iDRAC デバイスを追加できます。


iDRAC デバイスの追加

iDRAC デバイスを追加するには：

1. **製品** タブを選択して **追加** をクリックします。
2. iDRAC デバイス名を入力して、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。


iDRAC6 ウェブベースのインターフェイスを使用した Active Directory と拡張スキーマの設定

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 のウェブインターフェイスにログインします。
3. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
4. **設定** タブをクリックして、**Active Directory** を選択します。
5. **Active Directory 設定と管理** ページの下にスクロールし、**Active Directory の設定** をクリックします。
Active Directory の設定と管理 ページのステップ 1/4 が画面に表示されます。
6. Active Directory の SSL 証明書を検証する場合は、**証明書設定** の下の **Enable Certificate Validation (証明書検証を有効にする)** を選択します。検証しない場合は、ステップ 9 へ進みます。
7. **Active Directory CA 証明書のアップロード** の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照します。

 **メモ:** フルパスおよび正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

8. **アップロード** をクリックします。
アップロードした Active Directory CA 証明書の情報が表示されます。
9. **次へ** をクリックして、**Active Directory 設定と管理 ステップ 2/4** へ進みます。

10. **Active Directory を有効にする** をクリックします。
 11. **追加** をクリックして、ユーザードメイン名を入力します。
 12. 表示されるプロンプトにユーザードメイン名を入力し、**OK** をクリックします。このステップは任意であることをご注意ください。ユーザードメインのリストを設定した場合、ウェブインタフェースのログイン画面で表示されます。リストから選択する場合、ユーザー名のみを入力する必要があります。
 13. iDRAC6 が Active Directory の応答を待つ **タイムアウト** 時間を秒数で指定します。デフォルト値は 120 秒です。
 14. ドメインコントローラサーバーのアドレスを入力します。ログイン処理に最大 3 つの Active Directory サーバーを指定できますが、少なくとも 1 台のサーバーは、IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力して設定する必要があります。iDRAC6 は、設定された各サーバーに、接続が確立されるまで接続を試みます。

 **メモ:** 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject (件名) または Subject Alternative Name (代替名) フィールドの値と一致する必要があります。
 15. **次へ** をクリックして、Active Directory **設定と管理 ステップ 3/4** へ進みます。
 16. **スキーマの選択** の下の **拡張スキーマ** をクリックします。
 17. **次へ** をクリックして、Active Directory **設定と管理 ステップ 4/4** へ進みます。
 18. **拡張スキーマの設定** で、iDRAC デバイスオブジェクトを設定するために、iDRAC 名およびドメイン名を入力します。iDRAC ドメイン名は、iDRAC オブジェクトが作成されるドメインです。
 19. Active Directory 拡張スキーマの設定を保存するには、**完了** をクリックします。

iDRAC6 ウェブサーバーは、自動的に **Active Directory 設定と管理** ページに戻ります。
 20. Active Directory 拡張スキーマの設定を確認するには、**設定のテスト** をクリックします。
 21. Active Directory ユーザー名およびパスワードを入力します。

テスト結果およびテストログが表示されます。詳細については、「[設定のテスト](#)」を参照してください。
-  **メモ:** Active Directory ログインをサポートするには、iDRAC 上で DNS サーバーが正しく設定されている必要があります。 **リモートアクセス** → **設定** → **ネットワーク** ページに移動し、手動で DNS サーバーを入力するか、DHCP を使用して DNS サーバーを取得します。

これで、拡張スキーマの Active Directory の設定を完了しました。

RACADM を使用した拡張スキーマの Active Directory の設定

ウェブインタフェースの代わりに RACADM CLI ツールを使用して、拡張スキーマで iDRAC Active Directory 機能を設定するには、次のコマンドを使用します。

1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1


racadm config -g cfgActiveDirectory -o
cfgADRacName <RAC コモンネーム>


racadm config -g cfgActiveDirectory -o cfgADRacDomain <完全修飾ドメイン名>

racadm config -g cfgActiveDirectory -o cfgDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

racadm config -g cfgActiveDirectory -o cfgDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

racadm config -g cfgActiveDirectory -o cfgDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

 **メモ:** 3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。拡張スキーマのオプションが選択されている場合、iDRAC デバイスが所在するドメインコントローラの FQDN または IP アドレスとなります。拡張スキーマモードでは、グローバルカタログサーバーは全く使用されません。

 **メモ:** 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject (件名) または Subject Alternative Name (代替名) フィールドの値と一致する必要があります。

SSL ハンドシェイク中の証明書の検証を無効にしたい場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

この場合、CA 証明書をアップロードする必要はありません。

SSL ハンドシェイク中の証明書の検証を強制したい場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

```
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

次の RACADM コマンドは任意で実行できます。詳細については、「[iDRAC6 ファームウェア SSL 証明書のインポート](#)」を参照してください。

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. iDRAC で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <二次 DNS IP アドレス>
```

4. iDRAC6 ウェブインタフェースにログインする際、ユーザー名のみを入力するために、ユーザードメインのリストを設定したい場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName -i <索引>
```

1 から 40 の索引番号で、最大 40 のユーザードメインを設定できます。

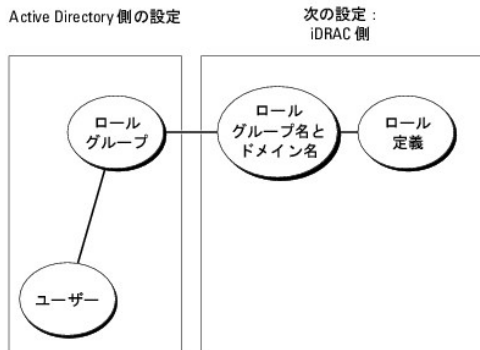
ユーザードメインの詳細については、「[Active Directory を使用した iDRAC6 へのログイン](#)」を参照してください。

5. 拡張スキーマの Active Directory 設定を完了するには、Enter キーを押します。

標準スキーマの Active Directory の概要

[図 7-3](#) に示すように、Active Directory を統合するために標準スキーマを使用する場合は、Active Directory と iDRAC6 の両方で設定が必要になります。

図 7-3 Microsoft Active Directory と標準スキーマで iDRAC の設定



Active Directory 側では、標準グループオブジェクトがロール(役割)グループとして使用されます。iDRAC6 へのアクセス権を持つユーザーは役割グループのメンバーとなります。指定した iDRAC6 へのアクセスをこのユーザーに与えるには、役割グループ名とそのドメイン名を特定の iDRAC6 で設定する必要があります。拡張スキーマソリューションとは異なり、役割と権限レベルは Active Directory でなく、各 iDRAC6 で定義されます。各 iDRAC6 について、5 つまでのロール(役割)グループを設定および定義できます。[表 7-9](#) は、デフォルトのロールグループの権限を示しています。

表 7-9 デフォルトの役割グループの特権

ロール(役割)グループ	デフォルトの権限レベル	許可する権限	ビットマスク
ロールグループ 1	システム管理者	iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバーコントロールコマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。	0x000001ff
ロールグループ 2	オペレータ	iDRAC へのログイン、iDRAC の設定、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。	0x000000f9

ロールグループ 3	読み取り専用。	iDRAC へのログイン	0x00000001
ロールグループ 4	なし	権限の割り当てなし	0x00000000
ロールグループ 5	なし	権限の割り当てなし	0x00000000

 **メモ:** ビットマスク値を使用するのは、RACADM で標準スキーマを設定する場合に限ります。

シングルドメインとマルチドメインのシナリオ

すべてのログインユーザー、ロールグループ、そしてネストされたグループが同じドメインに属する場合、ドメインコントローラのアドレスのみを iDRAC6 上で設定する必要があります。このようなシングルドメインのシナリオでは、すべてのグループタイプがサポートされています。

すべてのログインユーザー、ロールグループまたはネストされたグループがそれぞれ異なるドメインに属する場合、iDRAC6 上でグローバルカタログサーバーのアドレスを設定する必要があります。このようなマルチドメインのシナリオでは、すべてのロールグループおよびネストされたグループは、ユニバーサルグループタイプである必要があります。


iDRAC にアクセスするために標準スキーマ Active Directory を設定する方法

Active Directory ユーザーが iDRAC6 にアクセスできるように、まず次の手順に従って Active Directory を設定する必要があります。

- Active Directory サーバー(ドメインコントローラ)で、Active Directory ユーザーとコンピュータスナップインを開きます。
- グループを作成するか、既存のグループを選択します。グループとドメインの名前は、ウェブインタフェースまたは RACADM を使用して iDRAC6 上で設定する必要があります(「[iDRAC6 ウェブインタフェースを使用した Active Directory と標準スキーマの設定](#)」または「[RACADM を使用した標準スキーマの Active Directory の設定](#)」を参照)。
- iDRAC にアクセスする Active Directory グループのメンバーとして Active Directory ユーザーを追加します。

iDRAC6 ウェブインタフェースを使用した Active Directory と標準スキーマの設定

- サポートされているウェブブラウザのウィンドウを開きます。
- iDRAC6 のウェブベースのインタフェースにログインします。
- システム ツリーを拡張し、リモートアクセス をクリックします。
- 設定 タブをクリックして、Active Directory を選択します。
- Active Directory 設定と管理 ページの下にスクロールし、Active Directory の設定 をクリックします。
Active Directory の設定と管理 ページのステップ 1/4 が表示されます。
- Active Directory の SSL 証明書を検証する場合は、証明書設定 の下の Enable Certificate Validation (証明書検証を有効にする) を選択します。検証しない場合は、ステップ 9 へ進みます。
- Active Directory CA 証明書のアップロード の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照します。

 **メモ:** フルパスおよび正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

- アップロード をクリックします。
アップロードした Active Directory CA 証明書の情報が表示されます。
- 次へ をクリックして、Active Directory 設定と管理 ステップ 2/4 へ進みます。
- Active Directory を有効にする をクリックします。
- 追加 をクリックして、ユーザードメイン名を入力します。

12. 表示されるプロンプトにユーザードメイン名を入力し、OK をクリックします。
13. iDRAC6 が Active Directory の応答を待つ **タイムアウト**時間を秒数で指定します。デフォルト値は 120 秒です。
14. ドメインコントローラサーバーのアドレスを入力します。ログイン処理に最大 3 つの Active Directory サーバーを指定できますが、少なくとも 1 台のサーバーは、IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力して設定する必要があります。iDRAC6 は、設定された各サーバーに、接続が確立されるまで接続を試みます。
 **メモ:** 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject (件名) または Subject Alternative Name (代替名) フィールドの値と一致する必要があります。
15. **次へ** をクリックして、Active Directory **設定と管理 ステップ 3/4** へ進みます。
16. **スキーマの選択** の下の **拡張スキーマ** をクリックします。
17. **次へ** をクリックして、Active Directory **設定と管理 ページのステップ 4a/4** へ進みます。
18. **標準スキーマの設定** で、Active Directory におけるグローバルカタログサーバー場所を指定するためのアドレスを入力します。少なくとも 1 つのグローバルカタログサーバーの場所を設定する必要があります。
 **メモ:** 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject (件名) または Subject Alternative Name (代替名) フィールドの値と一致する必要があります。
 **メモ:** ユーザーアカウントとロールグループが異なるドメインにある場合、グローバルカタログサーバーは標準スキーマのみに必要です。また、このようなマルチドメインのシナリオでは、ユニバーサルグループのみを使用できます。
19. **役割グループ** の下の **役割グループ** をクリックします。
ステップ 4b/4 ページが表示されます。
20. **役割グループ名** を指定します。
役割グループ名 は、Active Directory における iDRAC に関連付けられた役割グループを識別します。
21. 役割グループのドメインとなる **役割グループドメイン** を指定します。
22. **役割グループの権限レベル** を選択して、**役割グループの権限** を指定します。たとえば、**システム管理者** を選択すると、同権限レベルのすべての特権がされます。
23. **適用** をクリックして、役割グループの設定を保存します。
iDRAC6 ウェブサーバーは、設定が表示される Active Directory **設定と管理 ステップ 4a/4** ページに自動的に戻ります。
24. 追加の役割グループを設定する場合は、ステップ 18 から 22 を繰り返します。または、**完了** をクリックして、すべての標準スキーマ設定が**表示される Active Directory 設定と管理ページ**に戻ります。
25. Active Directory 標準スキーマの設定を確認するには、**設定のテスト** をクリックします。
26. iDRAC6 ユーザー名とパスワードを入力します。
テスト結果およびテストログが表示されます。詳細については、「[設定のテスト](#)」を参照してください。
 **メモ:** Active Directory ログインをサポートするには、iDRAC 上で DNS サーバーが正しく設定されている必要があります。**リモートアクセス**→ **設定**→ **ネットワーク** ページに移動し、手動で DNS サーバーを入力するか、DHCP を使用して DNS サーバーを取得します。

これで、標準スキーマの Active Directory の設定を完了しました。


RACADM を使用した標準スキーマの Active Directory の設定

ウェブインタフェースの代わりに RACADM CLI を使用して、標準スキーマの iDRAC Active Directory 機能を設定するには、次のコマンドを使用します。

1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1  
  
racadm config -g cfgActiveDirectory -o cfgADType 2  
  
racadm config -g cfgStandardSchema -i <索引> -o  
cfgSSADRoleGroupName <役割グループのコモンネーム>  
  
racadm config -g cfgStandardSchema -i <索引> -o  
cfgSSADRoleGroupDomain <完全修飾ドメイン名>
```


```
racadm config -g cfgStandardSchema -i <索引> -o
cfgSSADRoleGroupPrivilege <特定のユーザー権限の
ビットマスク番号>
```


 **メモ:** ビットマスク番号については、「[表 B-2](#)」を参照してください。


```
racadm config -g cfgActiveDirectory -o cfgDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

```
racadm config -g cfgActiveDirectory -o cfgDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

```
racadm config -g cfgActiveDirectory -o cfgDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

 **メモ:** 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject (件名) または Subject Alternative Name (代替名) フィールドの値と一致する必要があります。


 **メモ:** ドメインの FQDN のみではなく、ドメインコントローラの FQDN を入力します。たとえば、`de11.com` ではなく、`servername.de11.com` と入力します。


 **メモ:** 3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。標準スキーマでは、ユーザーアカウントと役割グループが存在するドメインコントローラのアドレスとなります。

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

 **メモ:** ユーザーアカウントとロールグループが異なるドメインにある場合、グローバルカタログサーバーは標準スキーマのみに必要です。また、このようなマルチドメインのシナリオでは、ユニバーサルグループのみを使用できます。

 **メモ:** 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject (件名) または Subject Alternative Name (代替名) フィールドの値と一致する必要があります。

SSL ハンドシェイク中の証明書の検証を無効にしたい場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

この場合、認証局 (CA) の証明書をアップロードする必要はありません。

SSL ハンドシェイク中の証明書の検証を強制したい場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

```
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

次の RACADM コマンドは任意で実行できます。詳細については、「[iDRAC6 ファームウェア SSL 証明書のインポート](#)」を参照してください。

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

2. iDRAC6 で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. iDRAC6 で DHCP が無効になっている場合、または手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <二次 DNS IP アドレス>
```

4. iDRAC6 ウェブインタフェースにログインする際、ユーザー名のみを入力するようにするため、ユーザードメインのリストを設定したい場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName -i <索引>
```

1 から 40 の索引番号で、最大 40 のユーザードメインを設定できます。

ユーザードメインの詳細については、「[Active Directory を使用した iDRAC6 へのログイン](#)」を参照してください。

設定のテスト

設定が正常に動作するか、Active Directory ログインの失敗を診断する必要がある場合は、iDRAC6 ウェブインタフェースから設定をテストすることができます。

iDRAC6 ウェブインタフェースで設定を終えたら、画面下部の **設定のテスト** をクリックします。テストを実行するには、ユーザー名 (例: ユーザー名@ドメイン.com) とパスワードを入力する必要があります。設定によっては、テストのすべてのステップを実行し、各ステップの結果を表示するまでに、多少の時間がかかる場合もあります。結果ページの下部に詳細なテストログが表示されます。

いずれかのステップにエラーが発生した場合は、テストログで詳細を確認し、問題と解決策を特定します。一般的なエラーについては、[「よくあるお問い合わせ \(FAQ\)」](#)を参照してください。

設定に変更を加えたい場合は、Active Directory タブをクリックし、順を追って設定を変更します。


ドメインコントローラの SSL を有効にする


iDRAC は Active Directory ドメインコントローラに対してユーザーを認証するとき、ドメインコントローラと SSL セッションを開始します。このとき、ドメインコントローラは認証局 (CA) によって署名された証明書を発行し、そのルート証明書も iDRAC にアップロードされます。つまり、iDRAC が (ルートまたは子ドメインコントローラにかかわらず) どのドメインコントローラに対しても認証できるようにするためには、ドメインコントローラはそのドメインの CA によって署名された SSL が有効な証明書を保有している必要があります。

Microsoft エンタープライズのルート CA を利用して自動的にすべてのドメインコントローラ SSL 証明書を割り当てる場合は、次の手順を実行して各ドメインコントローラの SSL を有効にする必要があります。

1. 各コントローラの SSL 証明書をインストールして、各ドメインコントローラで SSL を有効にします。
 - a. **スタート**→ **管理ツール**→ **ドメインセキュリティポリシー** をクリックします。
 - b. **公開キーのポリシー** フォルダを展開し、**自動証明書要求の設定** を右クリックして **自動証明書要求** をクリックします。
 - c. **自動証明書要求の設定ウィザード** で **次へ** をクリックし、**ドメインコントローラ** を選択します。
 - d. **次へ** をクリックして、**完了** をクリックします。

iDRAC へのドメインコントローラのルート CA 証明書のエクスポート

 **メモ:** システムで Windows 2000 が実行されている場合は、次の手順は異なっている可能性があります。


 **メモ:** スタンドアロンの CA を利用している場合は、下記の手順が異なる場合もあります。

1. Microsoft Enterprise CA サービスを実行しているドメインコントローラを見つけてます。
2. **スタート**→ **ファイル名を指定して実行** の順にクリックします。
3. **ファイル名を指定して実行** のフィールドに「mmc」と入力し、OK をクリックします。
4. **コンソール 1 (MMC)** ウィンドウで、**ファイル** (Windows 2000 システムでは **コンソール**) をクリックし、**スナップインの追加 / 削除** を選択します。
5. **スナップインの追加と削除** ウィンドウで **追加** をクリックします。
6. **スタンドアロンスナップイン** ウィンドウで **証明書** を選択して **追加** をクリックします。
7. **コンピュータアカウント** を選択して **次へ** をクリックします。
8. **ローカルコンピュータ** を選択して **完了** をクリックします。
9. **OK** をクリックします。
10. **コンソール 1** ウィンドウで、**証明書** フォルダを展開し、**パーソナル** フォルダを展開して、**証明書** フォルダをクリックします。
11. ルート CA 証明書を探して右クリックし、**すべてのタスク** を選択してから **エクスポート...** を選択します。
12. **証明書のエクスポート** ウィザードで **次へ** を選択し、**いいえ、秘密キーをエクスポートしない** を選択します。
13. **次へ** をクリックし、フォーマットとして **Base-64 エンコード X.509 (.cer)** を選択します。
14. **次へ** をクリックし、システムのディレクトリに証明書を保存します。
15. **手順 14** に保存した証明書を iDRAC にアップロードします。


RACADM を使って証明書をアップロードする場合は、[「iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定」](#)または[「RACADM を使用した標準スキーマの Active Directory の設定」](#)を参照してください。


ウェブインタフェースを使って証明書をアップロードする場合は、[「iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定」](#)または[「iDRAC6 ウェブインタフェースを使用した Active Directory と標準スキーマの設定」](#)を参照してください。

iDRAC6 ファームウェア SSL 証明書のインポート

 **メモ:** Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証する設定になっている場合、iDRAC サーバー証明書を Active Directory ドメインコントローラにもアップロードする必要があります。Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証する設定になっていない場合は、この手順は必要ありません。

次の手順に従って、すべてのドメインコントローラの信頼された証明書のリストに iDRAC6 ファームウェア SSL 証明書をインポートします。

 **メモ:** システムで Windows 2000 が実行されている場合は、次の手順は異なっている可能性があります。

 **メモ:** iDRAC6 ファームウェア SSL 証明書がよく知られている CA によって署名され、その CA の証明書が既にドメインコントローラの信頼できるルート認証局のリストに含まれている場合は、本項の手順に従う必要はありません。

iDRAC の SSL 証明書は、iDRAC のウェブサーバーで使用される証明書と同じです。iDRAC のコントローラにはすべて、デフォルトの自己署名付き証明書が付随しています。

iDRAC SSL 証明書をダウンロードするには、次の RACADM コマンドを実行します。

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

1. ドメインコントローラで、MMC **コンソール** ウィンドウを開き、**証明書**→**信頼できるルート認証局**の順に選択します。
2. **証明書** を右クリックし、**すべてのタスク** を選択して **インポート** をクリックします。
3. **次へ** をクリックして SSL 証明書ファイルまで参照します。
4. 各ドメインコントローラの**信頼できるルート認証局**に iDRAC SSL 証明書をインストールします。

独自の証明書をインストールした場合は、その証明書に署名する CA が **信頼できるルート認証局** リストにあるかどうか確認してください。この認証局がリストにない場合、それを使用するすべてのドメインコントローラにインストールする必要があります。

5. **次へ** をクリックし、証明書の種類に基づいて証明書の保存場所を Windows に自動的に選択させるか、希望の場所まで参照します。
6. **完了** をクリックして OK をクリックします。

Active Directory を使用した iDRAC6 へのログイン

Active Directory と次のいずれかの方法を利用して、iDRAC6 にログインできます。

1. ウェブインタフェース
1. リモート RACADM
1. シリアルまたは Telnet コンソール

ログイン構文は、3 つの方法にすべて共通です。


<ユーザー名@ドメイン>

または

<ドメイン>\<ユーザー名> または <ドメイン>/<ユーザー名>


ユーザー名 は 1~256 バイトの ASCII 文字列です。

ユーザー名、ドメイン名ともに空白スペースや特殊文字 (\, /, @ など) は使用できません。

 **メモ:** "Americas" などの NetBIOS ドメイン名は名前解決できないため、指定できません。

ウェブインタフェースからログインし、ユーザードメインが設定されている場合、ウェブインタフェースのログイン画面のプルダウンメニューにすべてのユーザードメインが表示されます。プルダウンメニューからユーザードメインを選択する場合、ユーザー名のみを入力してください。This iDRAC(この iDRAC) を選択する場合、上記「[Active Directory を使用した iDRAC6 へのログイン](#)」に記載されるログイン構文を利用することで、Active Directory ユーザーとしてログインすることもできます。

スマートカードを使用して iDRAC6 にログインすることもできます。詳細については、「[スマートカードを使用した iDRAC6 へのログイン](#)」を参照してください。

 **メモ:** Windows 2008 Active Directory サーバーは、最長 256 文字の <ユーザー名>@<ドメイン名> 文字列のみをサポートしています。

よくあるお問い合わせ(FAQ)

Active Directory ログインに失敗しました。どうやって問題をトラブルシュートできますか。

iDRAC6 は、ウェブインタフェースで診断ツールを提供しています。ウェブインタフェースからシステム管理者権限を持つローカルユーザーでログインしてください、リモートアクセス→設定→Active Directory へ移動します。Active Directory 設定と管理 ページの下にスクロールし、**設定の設定** をクリックします。テストユーザー名とパスワードを入力し、Start Test(テストの開始) をクリックします。iDRAC6 は、順を追ってテストを実行し、各ステップの結果を表示します。いかなる問題の解決を支援するために、詳細なテスト結果が記録されます。Active Directory 設定と管理 ページに戻るには、Active Directory タブをクリックします。設定を変更し、テストユーザーが認証ステップに合格するまでテストを再実行するには、ページの下までスクロールし、Active Directory の**設定** をクリックします。

証明書の検証を有効にしましたが、Active Directory ログインに失敗しました。GUI から診断を実行しましたが、テスト結果に次のエラーメッセージが表示されています。

ERROR(エラー): Can't contact LDAP server(LDAP サーバーと通信できません), error(エラー): 14090086:SSL routines(SSL ルーチン): SSL3_GET_SERVER_CERTIFICATE: certificate verify failed(証明書の検証に失敗しました): Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC(iDRAC に正しい認証局(CA)証明書がアップロードされていることを確認してください。) iDRAC の日付が証明書の有効期限内であること、そして iDRAC で設定されたドメインコントローラのアドレスがディレクトリサーバーの証明書の件名と一致するか確認してください。

問題は何ですか。また、どのように修復できますか。

証明書の検証が有効になっている場合、iDRAC6 がディレクトリサーバーとの SSL 接続を確立したときに、iDRAC6 はアップロードされた CA 証明書を使用してディレクトリサーバーの証明書を検証します。認証の検証を失敗する最も一般的な理由として、次が挙げられます。

1. iDRAC6 の日付がサーバー証明書または CA 証明書の有効期限内ではない。証明書の iDRAC6 の日付と有効期限を確認してください。
2. iDRAC6 で設定されたドメインコントローラのアドレスがディレクトリサーバー証明書の件名または代替名と一致しない。IP アドレスを使用している場合、次の質問と回答をお読みください。FQDN を使用している場合、ドメインではなく、ドメインコントローラの FQDN を使用していることを確認してください。たとえば、example.com ではなく、servername.example.com 。

ドメインコントローラのアドレスに IP アドレスを使用していますが、証明書の検証に失敗します。問題は何ですか。

ドメインコントローラ証明書の 件名または代替名 フィールドを確認してください。通常、Active Directory はドメインコントローラ証明書の 件名または代替名 フィールドにドメインコントローラの IP アドレスではなく、ホスト名を利用します。この問題は複数の方法で修復できます。

1. サーバー証明書の件名または代替名と一致するように、iDRAC6 で指定するドメインコントロールアドレスにドメインコントローラのホスト名(FQDN)を設定します。
2. iDRAC6 で設定された IP アドレスと一致するように、件名または代替名に IP アドレスを使用するようサーバー証明書を再発行します。
3. SSL ハンドシェイク時に証明書の検証がなくても、このドメインコントローラを信頼する場合は、証明書の検証を無効にします。

マルチドメイン環境において、拡張スキーマを使用していますが、ドメインコントローラのアドレスはどのように設定すればよいですか。

iDRAC6 オブジェクトが属するドメインのドメインコントローラのホスト名(FQDN)または IP アドレスを使用します。

いつグローバルカタログアドレスを設定する必要がありますか。

拡張スキーマを使用している場合、グローバルカタログアドレスは使用されません。

標準スキーマを使用し、ユーザーとロールグループが異なるドメインに属する場合は、グローバルカタログアドレスを設定する必要があります。この場合、ユニバーサルグループのみを利用できます。

標準スキーマを使用し、すべてのユーザーとロールグループが同じドメインに属する場合は、グローバルカタログアドレスを設定する必要はありません。

標準スキーマクエリはどのように動作しますか。

iDRAC6 はまず設定されたドメインコントローラアドレスに接続し、ユーザーと役割グループが同じドメインに属する場合、権限が保存されます。

グローバルカタログアドレスが設定されている場合、iDRAC6 は継続してグローバルカタログクエリします。グローバルカタログから追加の権限が取得された場合、これらの権限は上乗せされません。

iDRAC6 は、常に LDAP オーバー SSL を使用しますか。

はい。すべての伝送は、636 および/または 3269 のセキュアポートを介して行われます。

設定のテストにおいて、iDRAC6 は問題を特定するためにのみ、LDAP CONNECT を行いますが、安全ではない接続において、LDAP BIND を行いません。

iDRAC6 で、証明書の検証がデフォルトで有効になっているのはなぜですか。

iDRAC6 は、接続先となるドメインコントローラの身元を確認するために、強力なセキュリティ対策を実施しています。証明書を検証しない場合、ハッカーはドメインコントローラになりすまし、SSL 接続を乗っ取ることも可能です。証明書の検証を行わなくても、自身のセキュリティ境界に属するすべてのドメインコントローラを信頼する場合は、GUI または CLI を介して無効にしても構いません。

iDRAC6 は NetBIOS 名をサポートしていますか。

本リリースでは、サポートされていません。

Active Directory を使用して iDRAC6 にログインできない場合は、何を確認すればいいですか。

iDRAC6 ウェブインタフェースの Active Directory 設定と管理 ページの下の 設定のテスト をクリックすることで、問題を診断できます。次に、テスト結果で特定される問題を修正します。詳細については、「[設定のテスト](#)」を参照してください。

本項では、最もよくある問題が説明されます。一般的に、以下の事項を確認してください。

1. ログインに NetBIOS 名でなく、正しいユーザードメイン名が使用されていることを確認します。
2. ローカル iDRAC6 ユーザーアカウントがある場合は、ローカルの資格情報を使用して iDRAC6 にログインします。

ログインした後、以下を行います。

- a. iDRAC6 Active Directory 設定と管理 ページにある Active Directory を有効にする ボックスが選択されているのを確認します。
- b. iDRAC6 ネットワーク設定 ページの DNS 設定が正しいことを確認します。
- c. 証明書の検証が有効にした場合、iDRAC6 に正しい Active Directory ルート CA 証明書がアップロードされていることを確認します。iDRAC6 の時刻が CA 証明書の有効期限内であることを確認します。
- d. 拡張スキーマを使用している場合は、iDRAC6 名 と iDRAC6 ドメイン名 がご利用の Active Directory 環境設定と一致していることを確認します。

標準スキーマを使用している場合は、**グループ名** と **グループドメイン名** がご利用の Active Directory 環境設定と一致していることを確認します。

3. iDRAC6 の時刻がドメインコントローラ SSL 証明書の有効期限内であることを確認します。

[目次ページに戻る](#)

[目次ページに戻る](#)

スマートカード認証の設定

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

- [iDRAC6 へのスマートカードログインの設定](#)
- [ローカル iDRAC6 ユーザーをスマートカードログイン用に設定する](#)
- [Active Directory ユーザーがスマートカードログインできるように設定する](#)
- [スマートカードの設定](#)
- [スマートカードを使用した iDRAC6 へのログイン](#)
- [Active Directory スマートカード認証を使用した iDRAC6 へのログイン](#)
- [iDRAC6 へのスマートカードログインのトラブルシューティング](#)

iDRAC6 では、**スマートカードログオン Smart Card Logon** を有効化することにより、2 要素認証がサポートされています。

従来方式の認証スキームでは、ユーザーの認証にユーザー名とパスワードが使用されています。これは最小レベルのセキュリティを提供します。

一方 TFA は、ユーザーに 2 つの認証要素 (持っているもの - スマートカード、と知っているもの - パスワードと PIN などのシークレットコード) を入力してもらうことにより高いレベルのセキュリティを実現します。

2 要素認証では、ユーザーが両方の要素を提供することで身元を証明することが要求されます。

iDRAC6 へのスマートカードログインの設定


ウェブインタフェースから iDRAC6 SNMP スマートカードログオン機能を有効にするには、**リモートアクセス** → **設定** → **スマートカード** に進み、**有効化** を選択します。

以下の事項に留意してください。


- 1 スマートカードを**有効にする** または **リモート racadm で有効にする**と、ウェブインタフェースを使った以降のログイン時にスマートカードを使うように求められます。

有効にする を選択すると、telnet、SSH、シリアル、リモート RACADM、IPMI オーバー LAN などのコマンドラインインタフェース (CLI) の帯域外インタフェースのサービスは単一要素認証しかサポートしないため、無効になります。

リモート RACADM で有効にする を選択すると、CLI 帯域外インタフェース (リモート racadm 以外) はすべて無効になります。

 **メモ:** デルでは、iDRAC6 管理者はリモート RACADM コマンドを使ってスクリプトを実行する iDRAC6 ユーザーインタフェースにアクセスするときのみ **リモート RACADM で有効にする** 設定を使うことを推奨しています。リモート RACADM を使用する必要がないときは、スマートカードログインを**有効にする**設定を選択してください。また、iDRAC6 のローカルユーザー設定や Active Directory の設定が完了してから、**スマートカードログオン** を有効にしてください。

- 1 **スマートカード**設定を無効化します (デフォルト)。これを選択すると、TFA スマートカードログイン機能が無効化され、次に iDRAC6 GUI にログインすると、ウェブインタフェースからデフォルトでログインメッセージとして表示される指示に従って Microsoft® Active Directory® またはローカルログインユーザー名およびパスワードを入力します。
- 1 **スマートカードログオンCRL チェックを有効にする**。証明書失効リスト (CRL) 配信サーバーからダウンロードしたユーザーの iDRAC 証明書に照合してチェックします。

 **メモ:** CRL 配信サーバーは、ユーザーのスマートカード証明書に含まれています。


ローカル iDRAC6 ユーザーをスマートカードログイン用に設定する

ローカル iDRAC6 ユーザーがスマートカードを使って iDRAC6 にログインするように設定できます。**リモートアクセス** → **設定** → **ユーザー**の順に選択します。

ただし、ユーザーがスマートカードを使用して iDRAC6 にログインするには、まずユーザーのスマートカード証明書と信頼されている認証局 (CA) の証明書を iDRAC6 にアップロードする必要があります。

スマートカード証明書のエクスポート

カード管理ソフトウェア (CMS) を使ってスマートカード証明書をスマートカードから Base64 符号化形式ファイルにエクスポートすることでユーザーの証明書を取得できます。CMS は通常、スマートカードのベンダーから入手できます。この符号化ファイルをユーザーの証明書として iDRAC6 にアップロードしてください。スマートカードのユーザー証明書を発行する信頼される認証局も、CA 証明書を Base64 エンコード形式でファイルにエクスポートする必要があります。ユーザー用の信頼される CA 証明書としてこのファイルをアップロードします。スマートカード証明書内でユーザーのユーザープリンシパル名 (UPN) を形成するユーザー名でユーザーを設定します。

 **メモ:** iDRAC6 にログインするには、iDRAC6 で設定するユーザー名が、大文字と小文字の区別を含めてスマートカード証明書の User Principal Name (UPN) と同じでなければなりません。

たとえば、スマートカード証明書が "sampleuser@domain.com" というユーザーに対して発行されたとする、ユーザー名は "sampleuser" となります。


Active Directory ユーザーがスマートカードログインできるように設定する

Active Directory ユーザーがスマートカードを使って iDRAC6 にログインできるように設定するには、iDRAC6 管理者は DNS サーバーを設定して、Active Directory CA 証明書を iDRAC6 にアップロードし、Active Directory ログオンを有効にします。Active Directory ユーザーの設定方法については、[「Microsoft Active Directory での iDRAC6 の使用」](#)を参照してください。

 **メモ:** スマートカードユーザーが Active Directory にいる場合、SC PIN とともに Active Directory パスワードが必須です。今後のリリースでは、Active Directory パスワードが必要なくなる可能性があります。

リモートアクセス→ 設定 → Active Directory の順に選択して、Active Directoryを設定することができます。

スマートカードの設定

 **メモ:** これらの設定を変更するには、iDRAC の設定 権限が必要です。

1. システム ツリーを拡張し、リモートアクセス をクリックします。
2. 設定 タブをクリックし、スマートカード をクリックします。
3. スマートカードのログオン設定を指定します。
[表 B-1](#) に、スマートカード ページの設定を示します。


4. 変更の適用 をクリックします。

表 8-1 スマートカードの設定

設定	説明
スマートカードログオンの設定	<ul style="list-style-type: none">1 無効 - スマートカードログオンを無効にします。その後のグラフィカルユーザーインターフェース (GUI) からのログインでは、通常のログインページが表示されます。セキュアシェル (SSH)、Telnet、シリアル、リモート RACADM を含むすべての帯域外インタフェースはデフォルト状態に戻ります。1 有効 - スマートカードログオンを有効にします。変更を適用した後、ログアウトして、スマートカードを挿入し、ログイン をクリックしてスマートカード PIN を入力します。スマートカードログインを有効にすると、SSH、Telnet、シリアル、リモート RACADM、IPMI オーバー LAN を含むすべての CLI 帯域外インタフェースにできなくなります。1 リモート racadm と共に有効にする - スマートカードログオンとリモート RACADM を有効にします。その他の CLI 帯域外インタフェースがすべて無効になります。 <p>メモ: スマートカードログインにはローカル iDRAC6 ユーザーを適切な証明書で設定する必要があります。スマートカードログオンを Microsoft Active Directory ユーザーのログインに使用する場合は、そのユーザーの Active Directory ユーザー証明書を設定する必要があります。ユーザー証明書は、ユーザー → ユーザーメインメニュー ページで設定できます。</p>
スマートカードログオン用 CRL チェックを有効にする	<p>このチェックは、Active Directory ログインユーザーに対してのみ使用可能です。このオプションは、ユーザーのスマートカード証明書を失効させるために iDRAC6 で証明書失効リスト (CRL) をチェックする場合に選択します。</p> <p>以下の場合には、ユーザーはログインできません。</p> <ul style="list-style-type: none">1 ユーザー証明書が CRL ファイルに失効として含まれている1 iDRAC6 が CRL 配信サーバーと通信できない。1 iDRAC6 が CRL をダウンロードできない。 <p>メモ: このチェックを正しく行うためには、設定 → ネットワーク ページで DNS サーバーの IP アドレスを正しく設定する必要があります。</p>

スマートカードを使用した iDRAC6 へのログイン

iDRAC6 ウェブインターフェースに、スマートカードを使用するように設定されているすべてのユーザー用のスマートカードログオンページが表示されます。

 **メモ:** ユーザー用のスマートカードログオンを有効にする前に、iDRAC6 のローカルユーザーと Active Directory の設定が完了していることを確認してください。

 **メモ:** ブラウザの設定によっては、この機能を初めて使うときに Smart Card reader ActiveX プラグインをダウンロードしてインストールするように要求される場合があります。

1. https を使用して iDRAC6 のウェブページにアクセスします。

https://<IP アドレス>

デフォルトの HTTPS ポート番号 (ポート 443) が変更されている場合は、次のように入力します。

https://<IP アドレス>:<ポート番号>

<IP address> は iDRAC6 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

iDRAC6 ログイン ページが表示され、スマートカードの挿入を要求されます。

2. スマートカードをリーダーに挿入して **ログイン** をクリックします。

スマートカードの PIN を入力するように指示されます。

- ローカルスマートカードのスマートカード PIN を入力すると、ユーザーがローカルで作成されていない場合、ユーザーの Active Directory アカウントのパスワードを入力するよう指示が表示されます。

メモ: Active Directory ユーザーで **スマートカードログオンの CTL チェックを有効にする** が選択されていれば、iDRAC6 はダウンロードを試みます。証明書がCRL に失効として含まれているか何らかの理由で CRL をダウンロードできない場合は、Active Directory を通してのログインは失敗します。

これで、iDRAC6 にログインできます。

Active Directory スマートカード認証を使用した iDRAC6 へのログイン

- https を使用して iDRAC6 にログインします。

https://<IP アドレス>

デフォルトの HTTPS ポート番号(ポート 443)が変更されている場合は、次のように入力します。

https://<IP アドレス>:<ポート番号>

<IP address> は iDRAC6 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

iDRAC6 ログイン ページが表示され、スマートカードの挿入を要求されます。

- スマートカードを挿入し、**ログイン** をクリックします。

PIN ポップアップダイアログボックスが表示されます。

- パスワードを入力して、**OK** をクリックします。

- ユーザーの Active Directory パスワードを入力して、スマートカードを認証し、**OK** をクリックします。

Active Directory に設定した資格情報で iDRAC6 にログインします。

メモ: スマートカードユーザーが Active Directory にいる場合、SC PIN とともに Active Directory パスワードが必須です。今後のリリースでは、Active Directory パスワードが不要になる可能性があります。

iDRAC6 へのスマートカードログインのトラブルシューティング

以下は、スマートカードにアクセスできないときのデバッグに役立つヒントです。

ActiveX プラグインがスマートカードリーダーを検出しません

スマートカードが Microsoft Windows[®] オペレーティングシステムでサポートされていることを確認します。Windows がサポートしているスマートカード暗号サービスプロバイダ (CSP) の数は限られています。

ヒント: スマートカード CSP が特定のクライアントに含まれているかを調べるために使用します。Windows のログオン (Ctrl-Alt-Del) 画面で、Windows がスマートカードを検出して PIN ダイアログボックスに表示するかを調べます。

不正なスマートカード PIN

不正な PIN を使ってログインを試みた回数が多すぎるためにスマートカードがロックアウトされたかを確認します。このような場合は、組織でのスマートカードの発行することによって新しいスマートカードを手に入れます。

ローカル iDRAC6 へのログインを無効にする

ローカル iDRAC6 ユーザーがログインできない場合、iDRAC6 にアップロードしたユーザー名とユーザー証明書をチェックします。iDRAC6 追跡ログによって、エラーに関する重要なログメッセージが得られることがあります。ただし、セキュリティ上の理由でエラーメッセージは内部的で、曖昧なものになっている場合があります。

Active Directory ユーザーとして iDRAC6 にログインできません

Active Directory ユーザーとして iDRAC6 にログインできない場合は、スマートカードログオンを有効にしないで iDRAC6 にログインしてみてください。CRL チェックを有効にしている場合は、CRL チェックを有効にしない状態で Active Directory にログインしてみてください。iDRAC6 追跡ログには、CRL が失敗したときの重要なメッセージが入っています。

次のコマンドを使用してローカル racadm からスマートカードログオンを無効にすることもできます。

```
racadm config -g cfgActiveDirectory -o cfgADSmartCardLogonEnable 0
```

[目次ページに戻る](#)

[目次ページに戻る](#)

GUI コンソールリダイレクトの使用

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

- [概要](#)
- [コンソールリダイレクトの使用](#)
- [ビデオビューアの使用](#)
- [よくあるお問い合わせ\(FAQ\)](#)


本項では、iDRAC6 コンソールリダイレクト機能の使用法について説明します。


概要


iDRAC6 コンソールリダイレクト機能を使用すると、ローカルのコンソールにリモートからグラフィックモードまたはテキストモードでアクセスできます。この機能を使用すると、1 つの場所から単一または複数の iDRAC6 システムを制御できます。

日常的なメンテナンスを各サーバーの前に座って行う必要はありません。デスクトップまたはラップトップコンピュータを使ってリモートからサーバーを管理できます。また、リモートから即座に他のユーザーと情報を共有することもできます。

コンソールリダイレクトの使用

 **メモ:** コンソールリダイレクトセッションを開いたとき、管理下サーバーはそのコンソールがリダイレクトされていることを示しません。

 **メモ:** 管理ステーションから iDRAC6 へのコンソールリダイレクトのセッションがすでに開かれている場合、同じ管理ステーションからその iDRAC6 への新しいセッションを開こうとすると、既存のセッションがアクティブになります。新しいセッションは生成されません。

 **メモ:** 一つの管理ステーションから複数の iDRAC6 カードへ、複数のコンソールリダイレクトのセッションを同時に開くことが可能です。

コンソールリダイレクト ページでは、ローカルの管理ステーションのキーボード、ビデオ、およびマウスを使ってリモートシステムを管理し、リモート管理下サーバーでそのデバイスを制御できます。この機能を仮想メディア機能と併用すると、リモートでソフトウェアのインストールを実行できます。

コンソールリダイレクトセッションには次の規則が適用されます。

- 1 同時にサポートされているコンソールリダイレクトセッション数は、最大 2 つです。両セッションで、同じ管理下サーバーコンソールを同時に表示します。
- 1 同じクライアントコンソール（管理ステーション）からリモートサーバー（iDRAC6）に対して開くことができるセッション数は、1 つに限りです。ただし、同じクライアントから複数のリモートサーバーに対しては、複数のセッションを開くことができます。
- 1 管理下システムのウェブブラウザからコンソールリダイレクトセッションを開始しないでください。
- 1 1 MB/秒以上のネットワーク帯域幅が必要です。

iDRAC への最初のコンソールリダイレクトセッションは、フルアクセスのセッションとなります。2 番目のユーザーがコンソールリダイレクトセッションを要求すると、最初のユーザーは通知を受け取り、拒否、**読み取り専用で許可**、または**許可**のオプションから選択できます。2 番目のユーザーには、別のユーザーがコントロールしていることが通知されます。1 番目のユーザーが 30 秒以内に応答しないと、2 番目のユーザーには自動的にフルアクセスが拒否されます。


最後のフルアクセスのセッションが終了すると、すべての**読み取り専用で許可**のセッションは自動的に終了します。

管理ステーションの設定

管理ステーションでコンソールリダイレクトを使用するには、次の手順を実行してください。

1. 対応ウェブブラウザをインストールして設定します。詳細については、以下の項を参照してください。

- 1 「[対応ウェブブラウザ](#)」
- 1 「[対応ウェブブラウザの設定](#)」

 **メモ:** コンソールリダイレクト機能が正常に動作するには、管理ステーション上に Java Run Time Environment (JRE) がインストールされている必要があります。

2. Internet Explorer を使用している場合、次の手順に従って、ブラウザが暗号化されたコンテンツをダウンロードできるようにします。

- 1 Internet Explorer で **ツール** → **インターネットオプション** → **詳細設定** の順で選択します。
- 1 **セキュリティ** のセクションまでスクロールし、次のオプションを選択解除します。

暗号化されたページをディスクに保存しない

3. 画面解像度は 1280x1024 ピクセル以上に設定することをお勧めします。

- メモ:** アクティブなコンソールリダイレクトセッションがあり、iDRAC KVM に解像度が低いモニターが接続されている場合、ローカルコンソールでサーバーを選択すると、サーバーのコンソール解像度がリセットされることがあります。サーバーで Linux オペレーティングシステムを実行している場合は、ローカルモニターで X11 コンソールが表示されない可能性があります。iDRAC KVM で <Ctrl><Alt><F1> キーを押すと、Linux がテキストコンソールに切り替わります。
- メモ:** 時折、「Expected: 」の JavaScript コンパイルエラーが発生する場合があります。この問題を解決するには、JavaWebStart で「ダイレクト接続」を使用するようにネットワーク設定を調整します。編集->プリファレンス->全般->ネットワーク設定 の順で選択し、「ブラウザ設定を使用する」の代わりに「ダイレクト接続」を選択します。

iDRAC6 ウェブインタフェースでのコンソールリダイレクトの設定

iDRAC6 ウェブインタフェースでコンソールリダイレクトを設定するには、次の手順を実行してください。

1. iDRAC コンソールリダイレクトを設定するには、**システム**→**コンソール/メディア**→**設定** の順でクリックします。
2. コンソールリダイレクトのプロパティを設定します。[表 9-1](#) は、コンソールリダイレクトの設定について説明しています。
3. 設定が完了したら、**適用** をクリックします。
4. 適切な **ボタン** をクリックして続行します。[表 9-2](#) を参照してください。

表 9-1 コンソールリダイレクトの設定プロパティ

プロパティ	説明
有効	クリックして、コンソールリダイレクトを有効または無効にします。 チェックボックスがオン の場合は、コンソールリダイレクトが有効です。 チェックボックスがオフ の場合は、コンソールリダイレクトが無効です。 デフォルトは 有効 です。
最大セッション数	コンソールリダイレクトの最大セッション数(1 から 4)が表示されます。コンソールリダイレクトで許可する最大セッション数を変更するには、ドロップダウンメニューを使用します。デフォルトは 2 です。
アクティブセッション数	アクティブなコンソールセッション数を表示します。このフィールドは読み取り専用です。
リモートプレゼンスポート	コンソールリダイレクトのキーボード/マウスオプションへの接続に使用するネットワークポート番号。トラフィックは常に暗号化されます。別のプログラムでデフォルトのポートが使用されている場合は、この番号を変更しなければならない可能性があります。デフォルトは 5900 です。
ビデオ暗号化有効	チェックボックスがオン の場合は、ビデオ暗号化が有効です。ビデオポートを経由するすべてのトラフィックは、暗号化されます。 チェックボックスがオフ の場合は、ビデオ暗号化が無効です。ビデオポートを経由するトラフィックは暗号化されません。 デフォルトは、 暗号化 されます。 暗号化を無効にすると、低速なネットワークのパフォーマンスを改善できる場合があります。
ローカルサーバービデオ有効	チェックボックスがオンの場合は、コンソールリダイレクト中 iDRAC KVM モニターへの出力は無効になります。これにより、 コンソールリダイレクト を使って実行したタスクは、管理下サーバーのローカルモニターに表示されなくなります。

- メモ:** コンソールリダイレクトで仮想メディアを使用する方法については、「[仮想メディアの設定と使用法](#)」を参照してください。

[表 9-2](#) のボタンは **コンソール/メディア設定** ページにあります。

表 9-2 設定ページのボタン

ボタン	定義
印刷	ページを印刷します。
更新	設定 ページを再ロードします。
変更の適用	新しいまたは変更された設定を保存します。

コンソールリダイレクトセッションの開始

コンソールリダイレクトセッションを開くと、Dell™ 仮想 KVM ビューアアプリケーションが開始し、リモートシステムのデスクトップがビューアに表示されます。この仮想 KVM ビューアアプリケーションを使用すると、ローカル管理ステーションからリモートシステムのマウスとキーボードの機能を制御できます。

ウェブインタフェースでコンソールリダイレクトセッションを開くには、次の手順を実行してください。

1. **システム**→**コンソール/メディア**→**設定** の順でクリックします。
2. 「[表 9-3](#)」の情報を使用して、コンソールリダイレクトセッションが利用可能であることを確認します。

表示されているプロパティ値の設定を変更する場合は、「[iDRAC6 ウェブインタフェースでのコンソールリダイレクトの設定](#)」を参照してください。

表 9-3 コンソールリダイレクト

プロパティ	説明
コンソールリダイレクト有効	はい/いいえ(チェックあり/チェックなし)
ビデオ暗号化有効	はい/いいえ(チェックあり/チェックなし)
最大セッション数	サポートされているコンソールリダイレクトの最大セッション数を表示します。
アクティブセッション数	現在アクティブなコンソールリダイレクトセッション数を表示します。
ローカルサーバービデオ有効	ローカルコンソールが無効になっていない場合は、チェックボックスがオフです。チェックが入っている場合、ローカル iDRAC KVM 接続が現在リモートから使用されていると、コンソールにアクセスすることはできません。
リモートプレゼンスポート	コンソールリダイレクトのキーボード/マウスオプションへの接続に使用するネットワークポート番号。トラフィックは常に暗号化されます。別のプログラムでデフォルトのポートが使用されている場合は、この番号を変更しなければならない可能性があります。デフォルトは 5900 です。



 **メモ:** コンソールリダイレクトで仮想メディアを使用する方法については、「[仮想メディアの設定と使用法](#)」を参照してください。


表 9-4 のボタンは、[コンソールリダイレクトおよび仮想メディア](#) ページで利用可能です。

表 9-4 コンソールリダイレクトおよび仮想メディアページのボタン

ボタン	定義
更新	コンソールリダイレクトの設定 ページを再ロードします。
ビューアの起動	目的のリモートシステムのコンソールリダイレクトセッションを開きます。
印刷	コンソールリダイレクトの設定 ページを印刷します。

3. コンソールリダイレクトセッションが使用可能な場合は、**ビューアの起動** をクリックします。

 **メモ:** アプリケーションが起動した後、メッセージボックスがいくつか表示される場合があります。アプリケーションへの不正アクセスを防ぐために、これらのメッセージボックスは 3 分間内に参照する必要があります。そうしないと、アプリケーションの再起動を要求されます。


 **メモ:** 以下の手順の途中で **セキュリティ警告** ウィンドウが表示された場合は、その内容を読んでから、**はい** をクリックして続行します。

管理ステーションが iDRAC6 に接続し、iDRAC KVM ビューアアプリケーションにリモートシステムのデスクトップが表示されます。

4. 2 つのマウスポインタ(1 つはリモートシステム用、もう 1 つはローカルシステム用)がビューアウィンドウに表示されます。iDRAC KVM メニューの **ツール** で **Single Cursor(シングルカーソル)** オプションを選択することで、単一のカーソルに変更できます。

ビデオビューアの使用

ビデオビューアは管理ステーションと管理下サーバー間のユーザーインターフェースを提供するので、管理ステーション側から管理下サーバーのデスクトップを表示して、マウスやキーボードの機能を制御できます。リモートシステムに接続すると、ビデオビューアが別のウィンドウで開始します。

 **メモ:** リモートサーバーの電源がオフの場合、**No Signal(シグナルなし)** のメッセージが表示されます。

ビデオビューアは、マウスの同期、スナップショット、キーボードマクロ、仮想メディアへのアクセスなど、さまざまなコントロール調整機能を提供します。これら機能の詳細については、**システム** → **コンソール/メディア** をクリックし、**コンソールリダイレクトおよび仮想メディア ページ** 上で **ヘルプ** をクリックします。

コンソールリダイレクトセッションを開始し、ビデオビューアが表示されたら、マウスポインタを同期させる必要がある場合があります。

ローカルサーバービデオを有効または無効にする


iDRAC6 ウェブインターフェースを使用して iDRAC KVM 接続を無効にするように iDRAC6 を設定できます。

管理下サーバーのコンソールへの排他的アクセスを確保する場合は、ローカルコンソールを無効にし、また **コンソールリダイレクトの設定 ページ** で **最大セッション数** を 1 に再設定する必要があります。

 **メモ:** サーバー上のローカルビデオを無効にする(オフにする)と、iDRAC KVM に接続しているモニター、キーボード、マウスが無効になります。

ローカルコンソールを無効または有効にするには、次の手順を実行してください。

1. 管理ステーション上で、対応ウェブブラウザを開いて iDRAC6 にログインします。詳細については、「[ウェブインターフェースへのアクセス](#)」を参照してください。
2. **システム** → **コンソール/メディア** → **設定** の順でクリックします。
3. サーバー上でローカルビデオを無効にする(オフにする)には、**設定** ページで **ローカルサーバービデオ有効** チェックボックスを選択解除してから **適用** をクリックします。デフォルト値は オフです。

 **メモ:** ローカルサーバービデオをオンにした場合、オフにするまで 15 秒かかります。

- サーバー上でローカルビデオを有効にする(オンにする)には、**設定** ページで **ローカルサーバービデオ有効** チェックボックスを選択してから **適用** をクリックします。

よくあるお問い合わせ(FAQ)

表 9-5 は、よくあるお問い合わせとその回答です。


表 9-5 コンソールリダイレクトの使用 :よくあるお問い合わせ(FAQ)


質問	回答
サーバー上のローカルビデオがオフになっている場合に、新しいリモートコンソールビデオセッションを開始できますか。	はい。
ローカルビデオをオフにするように要求してからサーバー上のローカルビデオがオフになるまで 15 秒もかかるのはなぜですか。	ビデオがオフに切り替わる前に、ローカルユーザーが必要に応じて別の操作を実行できるように配慮されています。
ローカルビデオをオンにする場合に、遅延時間は発生しますか。	いいえ。ローカルビデオを オン にする要求を iDRAC6 が受信すると、ビデオは瞬時にオンになります。
ローカルユーザーはビデオをオフにすることもできますか。	ローカルコンソールを無効にすると、ローカルユーザーはビデオをオンにすることはできません。
ローカルユーザーはビデオをオンにすることもできますか。	ローカルコンソールを無効にすると、ローカルユーザーはビデオをオンにすることはできません。
ローカルビデオをオフに切り替えると、ローカルキーボードとマウスもオフに切り替わりませんか。	いいえ
ローカルコンソールをオフにすると、リモートコンソールセッションのビデオはオフになりますか。	いいえ。ローカルビデオのオン / オフを切り替えても、リモートコンソールセッションには影響しません。
iDRAC6 ユーザーがローカルサーバービデオをオン / オフにするために必要な権限は何ですか。	iDRAC6 の設定権限を持つユーザーであれば、ローカルコンソールをオン / オフにできます。
ローカルサーバービデオの現在のステータスを取得するにはどのようにしますか。	ステータスは iDRAC6 ウェブインタフェースの コンソールリダイレクトの設定 ページに表示されます。 RACADM CLI コマンドの <code>racadm getconfig -g cfgRacTuning</code> は、 <code>cfgRacTuneLocalServerVideo</code> のオブジェクトにステータスを表示します。
コンソールリダイレクトウィンドウからシステム画面の下部が見えませんか。	管理ステーションのモニターの解像度が 1280x1024 に設定されていることを確認してください。また、iDRAC KVM 上のスクロールバーを使用することも可能です。
コンソールウィンドウが文字化けします。	Linux のコンソールビューアには UTF-8 文字コードが必要です。ローケルを確認し、必要に応じて文字コードをリセットしてください。
Linux テキストコンソールでマウスが同期しないのはなぜでしょうか。	仮想 KVM は USB マウスドライバを必要としますが、USB マウスドライバは X-Window オペレーティングシステムでしか使用できません。。
マウスの同期の問題がまだ解決しません。	コンソールリダイレクトセッションの開始前に、オペレーティングシステム用に正しいマウスが選択されていることを確認します。 iDRAC KVM クライアント上の iDRAC6 KVM メニューの ツール で Single Cursor(シングルカーソル) オプションが選択されていることを確認します。
iDRAC6 コンソールリダイレクトを使ってリモートで Microsoft® オペレーティングシステムをインストール中に、キーボードやマウスを使用できないのはなぜですか。	BIOS でコンソールリダイレクトが有効になっているシステムで、Microsoft の対応オペレーティングシステムをリモートからインストールすると、EMS 接続メッセージが表示され、続行する前に OK を選択するように要求されます。リモートでマウスを使って OK を選択することはできません。ローカルシステムで OK を選択するか、リモートで管理下サーバーを再起動し、再インストールしてから、BIOS でコンソールリダイレクトをオフにする必要があります。 このメッセージは、コンソールリダイレクトが有効になったことをユーザーに知らせるために Microsoft によって生成されます。このメッセージが表示されないようにするには、オペレーティングシステムをリモートインストールする前に、必ずコンソールリダイレクトを BIOS でオフにしてください。
管理ステーションの Num Lock インジケータにリモートサーバーの Num Lock のステータスが反映されないのはなぜですか。	iDRAC6 からアクセスした場合、管理ステーションの Num Lock インジケータは必ずしもリモートサーバーの Num Lock 状態と一致するとは限りません。Num Lock の状態は、管理ステーションの Num Lock の状態にかかわらず、リモートセッションが接続されたときのリモートサーバーの設定に依存します。
ローカルホストからコンソールリダイレクトセッションを確立すると、複数のセッションビューアウィンドウが表示されるのはなぜですか。	コンソールリダイレクトセッションをローカルシステムから設定しているからです。この操作はサポートされていません。
コンソールリダイレクトセッションを実行中に、ローカルユーザーが管理下サーバーにアクセスした場合、警告メッセージが表示されますか。	いいえ。ローカルユーザーがシステムにアクセスした場合は、双方がシステムを制御できます。
コンソールリダイレクトセッションを実行するために必要な帯域幅はどれくらいですか。	良好なパフォーマンスを得るためには、5 MB/秒の接続を推奨します。最低限必要なパフォーマンスを得るためには 1 MB/秒の接続が必要です。
管理ステーションでコンソールリダイレクトを実行するために最低限必要なシステム要件を教えてください。	管理ステーションには、256 MB 以上の RAM を搭載した Intel® Pentium® III 500 MHz プロセッサが必要です。
iDRAC KVM ビデオビューア内に No Signal(シグナルなし) のメッセージが表示されるのはなぜですか。	iDRAC Virtual KVM プラグインがリモートサーバーのデスクトップビデオを受信していない場合に、このメッセージが表示されます。一般的に、これはリモートサーバーの電源がオフになると、この現象が発生します。時折、リモートサーバーのビデオ受信の誤動作により、このメッセージが表示される場合もあります。
iDRAC KVM ビデオビューア内に Out of Range(範囲外) のメッセージが表示されるのはなぜですか。	ビデオをキャプチャするために必要なパラメータが、iDRAC がビデオをキャプチャできる範囲を超えている場合に、このメッセージが表示されます。ディスプレイの解像度やリフレッシュレートなどのパラメータが高すぎると、範囲外の現象が発生させます。通常、パラメータの最大範囲は、ビデオのメモリサイズや帯域幅などの物理的な制限に基づいて設定されます。

[目次ページに戻る](#)

[目次ページに戻る](#)

Integrated Dell™ リモートアクセスコントローラ 6 (iDRAC6) バージョン 1.0ユーザーズガイド

 **メモ:** メモは、コンピュータを使いやすくするための重要な情報を説明しています。

 **注意:** 注意は、手順に従わない場合は、ハードウェアの損傷やデータの損失の可能性があることを示しています。

本書の内容は予告なく変更されることがあります。
© 2009 すべての著作権は Dell Inc. にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

この文書中使用されている商標(Dell, DELL ログ、Dell OpenManage、および PowerEdge は Dell Inc. の商標です。また、Microsoft、Windows、Windows Server、Windows Vista および Active Directory は Microsoft 社の米国および他の国における商標または登録商標です。Red Hat および Linux は、Red Hat, Inc. の米国および他の国における登録商標です。SUSE は、Novell, Inc. の登録商標です。Intel and Pentium は、米国および他の国における Intel Corporation の登録商標です。UNIX は、米国および他の国における The Open Group Inc. の登録商標です。VMware は、米国および他の国における VMware, Inc. の登録商標または商標です。

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、OpenLDAP の公開ライセンスによって許可されている限度内でのみ許可されます。このライセンスのコピーは、配布の最上位ディレクトリにある「ライセンス」ファイルまたは www.OpenLDAP.org/license.html から入手できます。OpenLDAP は OpenLDAP Foundation の登録商標です。個々のファイルや提供パッケージは、他社が著作権を所有している場合があります。この製品には、公共ソースから派生した材料も含まれています。この製品には、公共ソースから派生した材料も含まれています。OpenLDAP に関する情報は www.openldap.org/ から入手できます。Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、OpenLDAP の公開ライセンスによって許可されている限度内でのみ許可されます。Portions Copyright 1999-2003 Howard Y. H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Halvard B. Furuseth. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、この通知が保持された形式でのみ許可されます。事前の書面による許可なくこの著作権所有者をこのソフトウェアから派生した製品を推薦または促進するために使用することはできません。このソフトウェアは「そのまま」の形で、明示または黙示を問わず一切の保証なく提供されます。Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. ソースおよびバイナリ形式の再配布は変更の有無を問わず、この通知を保持し、アン・アーバー所在のミシガン大学へのしるべき功績を認めた上でのみ許可されます。事前の書面による許可なくこの大学名をこのソフトウェアから派生した製品を推薦または促進するために使用することはできません。このソフトウェアは「そのまま」の形で、明示または黙示を問わず一切の保証なく提供されます。商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。Dell Inc. はデル以外の商標や社名に対する所有権を一切否認します。

2009 年 3 月 リビジョン A00

[目次ページに戻る](#)