

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

[iDRAC6 Enterprise 概要](#)

[iDRAC6 Enterprise の設定](#)

[管理ステーションの設定](#)

[管理下サーバーの設定](#)

[ウェブインタフェースを使用した iDRAC6 Enterprise の設定](#)

[iDRAC6 テレメトリサービスの使用](#)

[スマートカード認証の設定](#)

[Kerberos 認証を有効にする方法](#)

[管理下サーバーの設定と正常性の表示](#)

[シリアルオーバー LAN の設定と使用](#)

[GUI コンソールリダイレクトの使用](#)

[iDRAC6 と使用するための VFlash メディアカードの設定](#)

[仮想メディアの設定と使用法](#)

[RACADM コマンドラインインタフェースの使用](#)

[電源モニタおよび電源管理](#)

[iDRAC6 Enterprise の使用 SM-CLP コマンドラインのインタフェース](#)

[WS-MAN インタフェースの使用](#)

[iVMCLI を使用したオペレーティングシステムの導入](#)


[iDRAC6 設定ユーティリティの使用](#)


[管理下システムの修復とトラブルシューティング](#)

[RACADM サブコマンドの概要](#)

[iDRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義](#)

メモおよび注意

 **メモ:** コンピュータを使いやすくな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。

本書で使用される商標権: Dell, DELL ログ, OpenManage, および PowerEdge は、Dell Inc. の商標です。Microsoft, Windows, Windows Server, Internet Explorer, MS-DOS, Windows Vista, ActiveX, および Active Directory は、米国およびその他の国における Microsoft Corporation の商標または登録商標です。Red Hat および Red Hat Enterprise Linux は、米国 およびその他の国における Red Hat, Inc. の登録商標です。Novell および SUSE は、米国およびその他の国における Novell, Inc. の登録商標です。Intel は、米国およびその他の国における Intel Corporation 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 の登録商標です。Thawte は、米国およびその他の国における Thawte, その関連会社および子会社の登録商標です。VeriSign は、米国およびその他の国における VeriSign, Inc. の登録商標です。Sun および Java は、米国およびその他の国における Sun Microsystems, Inc. またはその子会社の登録商標です。

Copyright 1998-2009 The OpenLDAP Foundation. All rights reserved. ソースおよびバイナリ形式での再配布と使用は、変更の有無を問わず、OpenLDAP の公開ライセンスで承認されている範囲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。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. 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での再配布と使用は、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範囲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 Hailvard B. Furuseth. All rights reserved. ソースおよびバイナリ形式での再配布と使用は、変更の有無を問わず、この著作権表示を含めた形式でのみ許可されます。著作権所有者の名前を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示または黙示の保証なしに「現状のまま」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での再配布と使用は、この著作権表示を含め、米国アン・アバーのミシガン大学への謝辞を記載した場合にのみ許可されます。この大学名を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示または黙示の保証なしに「現状のまま」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。それらの商標や会社名は、一切 Dell Inc. に帰属するものではありません。

2009 年 12 月

[目次ページに戻る](#)

RACADM サブコマンドの概要

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [help](#)
- [config](#)
- [getconfig](#)
- [getssninfo](#)
- [getsysinfo](#)
- [getractime](#)
- [setniccfg](#)
- [getniccfg](#)
- [getsvctag](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [getraclog](#)
- [clrraclog](#)
- [getsel](#)
- [clrsel](#)
- [gettracelog](#)
- [sslcsrgen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [testemail](#)
- [testtrap](#)
- [vmdisconnect](#)
- [clearasrscreen](#)
- [localconredirdisable](#)
- [fwupdate](#)
- [krbkeytabupload](#)
- [vmkey](#)
- [version](#)
- [arp](#)
- [coredump](#)
- [coredumpdelete](#)
- [ifconfig](#)
- [netstat](#)
- [ping](#)
- [ping6](#)
- [racdump](#)
- [traceroute](#)
- [traceroute6](#)
- [remoteimage](#)
- [sshpkauth](#)

この項では、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。

 **注意:** 最新の iDRAC6 ファームウェアは RACADM の最新バージョンのみをサポートしています。最新のファームウェアを使用している iDRAC6 に、旧バージョンの RACADM からクエリを発行すると、エラーが発生する可能性があります。Dell™ OpenManage™ 6.2 DVD メディアに同梱される RACADM バージョンをインストールします。

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をすべて列挙し、各サブコマンドに一行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、指定したサブ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
- 1 telnet/ssh RACADM

config

表 A-2 に、config サブコマンドについて説明します。

表 A-2 config/getconfig

サブコマンド	定義
config	IDRAC6 を設定します。

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 RACADM

説明

config サブコマンドを使用すると、iDRAC6 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 iDRAC6 オブジェクトが新しい値で書き込まれます。

 **メモ:** このコマンドで使用するグループとオブジェクトについては、「[iDRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義](#)」を参照してください。

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、iDRAC6 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 <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。この場合、インデックスは「名前付き」の値ではなく、インデックス値で指定されます。
-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場合は、その行番号とエラーの短い説明が表示されます。書き込みは iDRAC6 に発生しません。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、インデックス、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 ファイル内にあったオブジェクトの総数と、そこから書き込まれた設定オブジェクトの数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
```

iDRAC6 を設定するか再設定します。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 サブコマンドを使用すると、iDRAC6 設定パラメータを個別に取得するか、iDRAC6 設定グループをすべて取得して 1 つのファイルに保存することもできます。

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、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 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。また、現在のリリースでは cfgIpmiPet と cfgIpmiPef は、リモートおよび telnet/ssh RACADM でのみ保存可能で、ローカル RACADM で保存することはできません。
-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。グループがインデックス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をすべて表示します。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> 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。-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、インデックスは「名前付き」の値ではなく、インデックス値で指定されます。
-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、インデックス、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。

 **メモ:** このコマンドで使用するグループとオブジェクトについては、「[iDRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義](#)」を参照してください。

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 のすべてのグループ設定オブジェクトを 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 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 <インデックス>]
```

```
racadm getconfig -u <ユーザー名>
```

```
racadm getconfig -h
```

```
racadm getconfig -g <グループ名> -o <オブジェクト名>
```

```
[-i インデックス]
```

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 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、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（例：SSH または Telnet）

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 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。

```
C:\>racadm -r 10.35.155.185 -u root -p calvin getssninfo
```

Security Alert: Certificate is invalid - Certificate is not signed by Trusted Third Party (セキュリティ警告: 証明書が無効です - 証明書が信頼される第三者機関によって署名されていません)

Continuing execution. Use -S option for racadm to stop execution on certificate-related errors. (実行を継続します。証明書関連のエラーが発生した場合に、racadm に実行を停止させるには、-S オプションを使用します。)

表 A-7 getssninfo サブコマンド出力例

ユーザー	IP アドレス	タイプ
root	192.168.1.1	RACADM

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	iDRAC6 に関連する情報を表示します。

概要

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-4] [-6]
```

説明

getsysinfo サブコマンドは、iDRAC6、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。

対応インターフェース

- 1 ローカル RACADM

- 1 リモート RACADM
- 1 telnet/ssh 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	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。
-4	iDRAC6 IPv4 の情報を表示します。
-6	iDRAC6 IPv6 の情報を表示します。

出力

`getsysinfo` サブコマンドは、iDRAC6、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。

 **メモ:** Linux でのローカル `racadm getsysinfo` サブコマンドは、IPv6 アドレス 2 から IPv6 アドレス 15 のプレフィックス長とリンクローカルアドレスを個別のラインに表示します。

出力例

RAC Information:

RAC Date/Time = Tue Apr 15 03:52:56 2036

Firmware Version = 02.20

Firmware Build = 25

Last Firmware Update = Mon Oct 26 18:01:39 2009

Hardware Version = 0.0

MAC Address = 00:21:9b:fe:6b:21

Common settings:

Register DNS RAC Name = 0

DNS RAC Name = iDRAC-tt

Current DNS Domain =

Domain Name from DHCP = 1

IPv4 settings:

Enabled = 1

Current IP Address = 192.168.1.166

Current IP Gateway = 0.0.0.0

Current IP Netmask = 255.255.255.0

DHCP Enabled = 1

Current DNS Server 1 = 0.0.0.0

Current DNS Server 2 = 0.0.0.0

DNS Servers from DHCP = 1

IPv6 settings:

Enabled = 0

Current IP Address 1 = ::

Current IP Gateway = ::

Prefix Length = 64

Autoconfig = 0

Link Local IP Address = ::

Current IP Address 2 = ::

Current IP Address 3 = ::

Current IP Address 4 = ::

Current IP Address 5 = ::

Current IP Address 6 = ::

Current IP Address 7 = ::

Current IP Address 8 = ::

Current IP Address 9 = ::

Current IP Address 10 = ::

Current IP Address 11 = ::

Current IP Address 12 = ::

Current IP Address 13 = ::

Current IP Address 14 = ::

Current IP Address 15 = ::

DNS Servers from DHCPv6 = 0

Current DNS Server 1 = ::

Current DNS Server 2 = ::

System Information:

System Model = PowerEdge M710

System BIOS Version = 1.1.4

Service Tag = 2JWK22S

Host Name = WIN-IHF5D2BF5SN

OS Name = Microsoft Windows Server 2008 R2, Standard x64 Edition

Power Status = ON

Watchdog Information:

Recovery Action = None

Present countdown value = 0 seconds

Initial countdown value = 0 seconds

Embedded NIC MAC Addresses:

NIC1 Ethernet = 00:23:AE:EC:2E:38

iSCSI = 00:23:AE:EC:2E:39

NIC2 Ethernet = 00:23:AE:EC:2E:3A

iSCSI = 00:23:AE:EC:2E:3B

NIC3 Ethernet = 00:23:AE:EC:2E:3C

iSCSI = 00:23:AE:EC:2E:3D

NIC4 Ethernet = 00:23:AE:EC:2E:3E

iSCSI = 00:23:AE:EC:2E:3F

例

```
racadm getsysinfo -A -s  
"System Information:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"
```

```
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 =  
PowerStatus = ON
```

```
Watchdog Information:  
Recovery Action = None  
Present countdown value = 0 seconds  
Initialcountdownvalue = 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 Server Administrator 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。管理下サーバーにインストールされていない場合は、これらのフィールドは空白または不正確な情報になる可能性があります。その例外が VMware® オペレーティングシステム名で、これは管理下システムに Server Administrator がインストールされていない場合でも表示されます。

getractive

[表 A-10](#) に、**getractive** サブコマンドについて説明します。

表 A-10 getractive

サブコマンド	定義
getractive	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 getractive [-d]
```

説明

オプションを指定しないと、**getractive** サブコマンドは時刻を一般的な可読形式で表示します。

-d オプションを指定すると、**getractive** 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

getractive サブコマンドは出力を 1 行で表示します。

出力例

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

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 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 サブコマンドによって、iDRAC6 の IP アドレスが設定されます。

- 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 の有効）。
- 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> 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 -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、メッセージが表示されます。

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 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
getniccfg	iDRAC6 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。

IPv4 settings:

```
NIC Enabled          = 1
DHCP Enabled         = 1
IP Address           = 10.35.0.64
Subnet Mask          = 255.255.255.0
Gateway              = 10.35.0.1
```

IPv6 settings:

```
IPv6 Enabled = 0
DHCP6 Enabled = 0
IP Address 1 = ::
Prefix Length = 64
Gateway = ::
Link Local Address = ::
IP Address 2 = ::
IP Address 3 = ::
IP Address 4 = ::
IP Address 5 = ::
IP Address 6 = ::
IP Address 7 = ::
IP Address 8 = ::
IP Address 9 = ::
IP Address 10 = ::
IP Address 11 = ::
IP Address 12 = ::
IP Address 13 = ::
IP Address 14 = ::
IP Address 15 = ::
```

 **メモ:** IPv6 情報は、iDRAC6 が IPv6 をサポートしている場合にのみ表示されます。

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 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
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。

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 RACADM

racreset

[表 A-14](#) に、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	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 2 分かかる場合があります。

概要

```
racadm racreset [hard | soft]
```

説明

racreset サブコマンドは iDRAC6 をリセットします。リセットイベントは iDRAC6 のログに書き込まれます。ハードリセットは iDRAC6 にディープリセットを実行します。ハードリセットは、iDRAC6 を回復するときの最後の手段としてのみ実行してください。ソフトリセットは iDRAC6 に正常な再起動を実行します。

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。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh RACADM

racresetcfg

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

表 A-15 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。 メモ: racresetcfg サブコマンドは cfgDNSRacName オブジェクトをリセットしません。

概要


```
racadm racresetcfg
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh 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、iDRAC6 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。

 **メモ:** このコマンドは iDRAC6 の現在の設定を削除し、DHCP を無効にして、iDRAC6 の設定をデフォルト設定にリセットします。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 <処置>
```

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
<処置>	処置を指定します。<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してシステムの電源を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に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の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 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	iDRAC6 のログエントリの数を表示します。
getraclog	iDRAC6 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 iDRAC6 のログに記録されているエントリの数を表示します。

 **メモ:** オプションを指定しなければ、すべてのログが表示されます。


以下のオプションを使用すると、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。
-i	iDRAC6 のログエントリの数を表示します。
-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。

 **メモ:** 「racadm getraclog」のローカル racadm コマンドを使用して表示される SystemBoot の Rac ログエントリは、正しい書式になっていない場合があります。たとえば、「説明」フィールドに余分な文字が表示されたり、「ソース」フィールドが空白になっている場合があります。

出力例

```
レコード:      1
日時:         Dec 8 08:10:11
ソース:       login[433]
説明:         192.168.1.1 からのルートログイン
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh RACADM

clrraclog

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。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用します。


 **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。
-i	SEL 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)。

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
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh 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

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh RACADM

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

<code>gettracelog -i</code>	IDRAC6 トレースログ のエントリ数を表示します。
<code>gettracelog</code>	IDRAC6 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` エントリを使用し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
<code>-i</code>	IDRAC6 トレースログ のエントリ数を表示します。
<code>-m</code>	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 <code>more</code> コマンドに類似)。
<code>-o</code>	出力を 1 行で表示します。
<code>-c</code>	表示するレコード数を指定します。
<code>-s</code>	表示を開始するレコードを指定します。
<code>-A</code>	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分されます。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。

例:

```
Record: 1
```

```
Date/Time: Dec 8 08:21:30
```

```
Source: ssnmgrd[175]
```

```
Description: root from 192.168.1.1: 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 RACADM

sslcsrgen

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

表 A-24 `sslcsrgen`

サブコマンド	説明
<code>sslcsrgen</code>	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ければ、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。

オプションを指定しなければ、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
```

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh RACADM（生成できるだけで、ダウンロードはできません。-f オプションは該当しません）

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
<code>sslcertupload</code>	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 IDRAC6 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 <code>sslcert</code> 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、成功しなければゼロ以外の値を返します。

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
- 1 リモート 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
<code>sslcertdownload</code>	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 <code>sslcert</code> 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、成功しなければゼロ以外の値を返します。

例

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

対応インターフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
-

sslcertview

[表 A-30](#) に、`sslcertview` サブコマンドについて説明します。

表 A-30 sslcertview

サブコマンド	説明
<code>sslcertview</code>	iDRAC6 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、`sslcertview` サブコマンドオプションについて説明します。

表 A-31 sslcertview サブコマンドオプション

オプション	説明
<code>-t</code>	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
<code>-A</code>	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
- 1 リモート RACADM
- 1 telnet/ssh 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	iDRAC6 の電子メール警告機能をテストします。

概要

```
racadm testemail -i <インデックス>
```

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。

testemail コマンドを実行する前に、SMTP サーバーが構成され、RACADM [cfgEmailAlert](#) グループの指定したインデックスが有効になり、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 <インデックス> <インデックス> 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インデックスを指定します。-i のインデックスは、1 から 4 にします。

出力

成功: テストメールに成功しました

失敗: テストメールを送信できません

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh 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	IDRAC6 の SNMP トラップ警告機能をテストします。

概要

```
racadm testtrap -i <インデックス>
```

説明

testtrap サブコマンドは、ネットワーク上の指定した宛先トラップリスナに IDRAC6 からテストトラップを送信して、IDRAC6 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 グループの指定したインデックス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 グループと関連するコマンドのリストを示します。

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 <インデックス> <インデックス> 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	テストに使用するトラップ設定のインデックスを指定します。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 RACADM
-

vmdisconnect

概要

racadm vmdisconnect

説明

vmdisconnect サブコマンドを使用すると、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。一度切断すると、ウェブインタフェースに正しい接続状態が反映されます。

vmdisconnect サブコマンドを使用すると、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 のウェブインタフェースまたは 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
 - 1 telnet/ssh RACADM
-

clearasrscreen

概要

racadm clearasrscreen

説明

前回クラッシュ画面 (ASR) を消去します。 [「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」](#) および [「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。

対応インタフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
 - 1 telnet/ssh RACADM
-

localConRedirDisable

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。

説明

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。

有効値


0 = 有効

1 = 無効

対応インタフェース

- 1 ローカル 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。

[表 A-38](#) に、fwupdate サブコマンドについて説明します。

表 A-38 fwupdate

サブコマンド	定義
fwupdate	iDRAC6 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 サブコマンドを使用すると、ユーザーが iDRAC6 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 のファームウェアをアップデートする
- 1 スタンバイファームウェアへのロールバック

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh RACADM

入力

[表 A-39](#) に fwupdate サブコマンドのオプションについて説明します。


 **メモ:** -p オプションはリモートコンソールまたは Telnet/SSH コンソールではサポートされていません。-p オプションは Linux オペレーティングシステムでもサポートされていません。

表 A-39 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 はソフトウェアを実行します。
-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、常に単独で使用します。
-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 -a と -d オプションも指定する必要があります。-a オプションを指定しないと、デフォルトでは、プロパティ <code>cfgRhostsFwUpdateIpAddr</code> と <code>cfgRhostsFwUpdatePath</code> を使用して、グループ <code>cfgRemoteHosts</code> に含まれているプロパティを読み込みます。
-a	IP アドレス オプションは TFTP サーバーの 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 サーバーまたは iDRAC6 のホストサーバーのディレクトリを指定します。
-r	ロールバック オプションを使用すると、スタンバイファームウェアにロールバックできます。

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 192.168.1.1 -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します。完了すると、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。

krbkeytabupload

 **メモ:** このコマンドを使用するには、iDRAC の **設定** 権限が必要です。

[表 A-40](#) に、`krbkeytabupload` サブコマンドについて説明します。

表 A-40 krbkeytabupload

サブコマンド	説明
<code>krbkeytabupload</code>	Kerberos keytab ファイルをアップロードします。

概要

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

<ファイル名> はパスを含めたファイルの名前です。

オプション

[表 A-41](#) に、`krbkeytabupload` サブコマンドのオプションについて説明します。

表 A-41 krbkeytabupload サブコマンドのオプション

オプション	説明
-f	アップロードする keytab 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 keytab ファイルが選択されます。

`krbkeytabupload` コマンドは、成功すると 0 を返し、失敗するとゼロ以外の数字を返します。

例

```
racadm krbkeytabupload -f c:\keytab\krbkeytab.tab
```

対応インタフェース

- 1 リモート RACADM
 - 1 ローカル RACADM
-

vmkey

概要

```
racadm vmkey reset
```

説明

vmkey サブコマンドは、仮想フラッシュのパーティションをデフォルトサイズの 256MB にリセットし、同パーティション上のすべてのデータを削除します。

有効値

reset は、仮想フラッシュのパーティションをデフォルトサイズの 256 MB にリセットし、同パーティション上のすべてのデータを削除します。

対応インタフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
 - 1 telnet/ssh RACADM
-

version

概要

```
racadm version
```

説明

RACADM のバージョンを表示します。

対応インタフェース

- 1 リモート RACADM
 - 1 ローカル RACADM
 - 1 ssh/telnet RACADM
-

arp


 **メモ:** このコマンドを使用するには、**システム管理者** 権限が必要です。

表 A-42 に arp コマンドを示します。

表 A-42 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
```

説明

アドレス解決プロトコル (ARP) テーブルを表示します。

例

IP アドレス HW タイプ フラグ HW アドレス マスク デバイス

```
192.168.1.1 0x1 0x2 00:00:0C:07:AC:0F * eth0
```

対応インターフェース

- 1 リモート RACADM
- 1 telnet/ssh 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** 権限が必要です。

表 A-43 に、coredump サブコマンドについて説明します。

表 A-43 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、iDRAC6 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、以下の状態が発生するまで保持されます。


- 1 coredumpdelete サブコマンドで coredump 情報がクリアされた。
- 1 別の重要な状況が iDRAC6 で発生した。この場合、coredump 情報は最後に発生した重大エラーに関するものです。

coredump のクリアに関する詳細は、coredumpdelete 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 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** 権限が必要です。

[表 A-44](#) に、coredumpdelete サブコマンドについて説明します。

表 A-44 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 サブコマンドを使用すると、現在 iDRAC6 に保存されている coredump データをクリアできます。


 **メモ:** coredumpdelete コマンドを発行したときに coredump が iDRAC6 に保存されていなかった場合は、成功のメッセージが表示されます。これは 正常な動作です。

coredump の表示の詳細については、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 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 **iDRAC6 の設定** 権限が必要です。

[表 A-45](#) に、ifconfig サブコマンドについて説明します。

表 A-45 ifconfig

サブコマンド	定義
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。

概要

```
racadm ifconfig
```

例

```
$ racadm ifconfig
```

```
eth0 Link encap: Ethernet HWaddr 00:1D:09:FF:DA:23
```

inet addr: 10.35.155.136 Bcast: 10.35.155.255 Mask: 255.255.255.0

UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1

RX packets: 2550665 errors: 0 dropped: 0 overruns: 0 frame: 0

TX packets: 0 errors: 0 dropped: 0 overruns: 0 carrier: 0

collisions: 0 txqueuelen: 1000

RX bytes: 272532097 (259.9 MiB) TX bytes: 0 (0.0 B)

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh RACADM

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** 権限が必要です。

表 A-46 に、netstat サブコマンドについて説明します。

表 A-46 netstat

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 RACADM

ping


 **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 **iDRAC6 の設定** 権限が必要です。

表 A-47 に、ping サブコマンドについて説明します。

表 A-47 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 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、目的の 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 RACADM

ping6

 **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 **iDRAC6 の設定** 権限が必要です。

[表 A-48](#) に、ping6 サブコマンドについて説明します。

表 A-48 ping6

サブコマンド	定義
ping6	現在のルーティングテーブルの内容を使用して iDRAC6 から送信先の IPv6 アドレスに到達可能かどうかを確認します。送信先の IPv6 アドレスが必要です。ICMP 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、目的の IPv6 アドレスに送信されます。


概要

```
racadm ping6 <ipv6 のアドレス>
```

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh RACADM

racdump

 **メモ:** このコマンドを使用するには、**デバッグ** 権限が必要です。

[表 A-49](#) に racdump サブコマンドについて説明します。

表 A-49 racdump

サブコマンド	定義
racdump	ステータスおよび iDRAC6 の一般的な情報を表示します。

概要

```
racadm racdump
```

説明

racdump サブコマンドは、ダンプ、ステータス、iDRAC6 の一般的な基板情報を取得する単独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

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh RACADM

traceroute

 **メモ:** このコマンドを使用するには、**システム管理者** 権限が必要です。

[表 A-50](#) に、**traceroute** サブコマンドについて説明します。

表 A-50 traceroute

サブコマンド	定義
traceroute	パケットがシステムから目的の IPv4 アドレスに転送されるときに通るルーターのネットワーク経路をトレースします。

概要

```
racadm traceroute <IPv4 のアドレス>
racadm traceroute 192.168.0.1
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max,
40 byte packets
1 192.168.0.1 (192.168.0.1) 0.801 ms 0.246 ms 0.253 ms
```


説明

IPv4 を使用してネットワーク上の目的地点までの経路をトレースします。

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh RACADM

traceroute6

 **メモ:** このコマンドを使用するには、**システム管理者** 権限が必要です。

[表 A-51](#) に、**traceroute6** サブコマンドについて説明します。

表 A-51 traceroute6

サブコマンド	定義
traceroute6	パケットがシステムから目的の IPv6 アドレスに転送されるときに通るルーターのネットワーク経路をトレースします。

概要

```
racadm traceroute6 <IPv6 のアドレス>
racadm traceroute6 fd01::1
traceroute to fd01::1 (fd01::1) from fd01::3, 30 hops
max, 16 byte packets
```

1 fd01::1 (fd01::1) 14.324 ms 0.26 ms 0.244 ms

説明

IPv6 を使用してネットワーク上の目的地点までの経路をトレースします。

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh RACADM

remoteimage


 **メモ:** このコマンドを使用するには、**システム管理者** 権限が必要です。

表 A-52 に、remoteimage サブコマンドについて説明します。

表 A-52 remoteimage

サブコマンド	定義
remoteimage	リモートサーバーのメディアファイルの接続、切断、配布を実行します。

概要

racadm remoteimage <オプション>

以下のオプションがあります。

- c: イメージを接続
- d: イメージを切断
- u <ユーザー名>: ネットワーク共有にアクセスするユーザー名
- p <パスワード>: ネットワーク共有にアクセスするパスワード
- l <イメージの場所>: ネットワーク共有上のイメージの場所; 場所を二重引用符で囲む
- s: 現在の状態を表示; 指定しない場合は -a と想定される

説明

リモートサーバーのメディアファイルの接続、切断、配布を実行します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh RACADM

sshpkauth

概要

racadm sshpkauth

アップロード

アップロードモードでは、キーファイルのアップロードまたはコマンドライン上にキーテキストをコピーできます。キーのアップロードとコピーを同時に行うことはできません。

表示

表示モードでは、ユーザーが指定するキーまたはすべてのキーを表示できます。

削除

削除モードでは、ユーザーが指定するキーまたはすべてのキーを削除できます。

説明

ユーザーごとに、最大 4 つの異なる SSH 公開キーのアップロードおよび管理ができます。キーファイルまたはキーテキストのアップロード、キーの表示または削除を行えます。このコマンドには、アップロード、表示、削除の 3 つの相互に排他的なモードがあります。これらのモードは、コマンドと共に提供されるオプション（[表 A-53](#)を参照）によって決定されます。

オプション

表 A-53 sshpkauth サブコマンドオプション

オプション	説明
-i <ユーザーインデックス>	ユーザーのインデックスです。<ユーザーインデックス> は、iDRAC6 上の 2 から 16 の間にする必要があります。
-k [<キーインデックス> all]	アップロードされる PK キーを指定するためのインデックス。「all」は、-v または -d オプションと併用する場合のみ利用できます。<キーインデックス> は、iDRAC6 の 1 から 4 の間、または「all」にする必要があります。
-t <PK キーテキスト>	SSH 公開キーのキーテキスト。
-f <ファイル名>	アップロードするキーテキストが含まれるファイル。-f のオプションは、telnet/ssh RACADM ではサポートされていません。
-v	指定されるインデックスのキーテキストを表示する。
-d	指定されるインデックスのキーを削除する。

例

文字列を使用して iDRAC6 ユーザー 2 の最初のキースペースに無効なキーをアップロードする場合：

```
$ racadm sshpkauth -i 2 -k 1 -t "This is invalid key Text"
```

```
ERROR: Invalid SSH key
```

ファイルを使用して iDRAC6 ユーザー 2 の最初のキースペースに有効なキーをアップロードする場合：

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

```
PK SSH Authentication Key file successfully uploaded to the RAC.
```

iDRAC6 のユーザー 2 のすべてのキーを取得する場合：

```
$ racadm sshpkauth -v -i 2 -k all
```

```
***** User ID 2 *****
```

```
Key ID 1:
```

```
ssh-rsa AAAAB3NzaClyc2EAAAABIwAAAIEAzzy+k2mpnKqVEXGXIzo0sbr6JgA5YNbWs3ekoxXV  
fe3yJvpVc/5zrrr7XrwkBJAJTqSw8Dg3iR4n3vUaP+lPHmUv5Mn55Ea6LHUs1AXFqXmOd1Thd w1lU2VLw/iRH1ZymUFnut8gggPQgqV2L8bsUaMqb5PooIIvV6hy4isCNJU= 1024-bit  
RSA, converted from OpenSSH by xx_xx@xx.xx
```

```
Key ID 2:
```

```
SSH Key not available
```

```
Key ID 3:
```

```
SSH Key not available
```

```
Key ID 4:
```

```
SSH Key not available
```

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 RACADM

[目次ページに戻る](#)

[目次ページに戻る](#)

idRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [表示可能な文字](#)
- [idRacInfo](#)
- [cfgOobSnmp](#)
- [cfgLanNetworking](#)
- [cfgIPv6URL](#)
- [cfgIPv6LanNetworking](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgRemoteHosts](#)
- [cfgUserDomain](#)
- [cfgServerPower](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgIpmiLan](#)
- [cfgIpmiPetIpv6](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)
- [cfgSmartCard](#)
- [cfgActiveDirectory](#)
- [cfgLDAP](#)
- [cfgIpmiRoleGroup](#)
- [cfgStandardSchema](#)
- [cfgIpmiSol](#)

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分類されています。この項では、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 のリストを掲載します。

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。

△ 注意: 本章で説明する一部のグループとオブジェクトは、Dell™ OpenManage™ バージョン 6.2 のリリースで使用できません。Dell OpenManage バージョン 6.3 のリリースでサポートが追加される予定です。

表示可能な文字

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、クエリ先 iDRAC6 の詳細を提供するための表示パラメータが含まれています。

グループの 1 つのインスタンスが許可されています。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。

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

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をすべて提供しています。

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

なし

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)

有効値

プロダクト ID

デフォルト

8

説明

Remote Access Controller の種類を iDRAC6 として識別します。

cfgOobSnmpp

このグループには、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が含まれています。

グループの 1 つのインスタンスが許可されています。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。

cfgOobSnmppAgentCommunity (読み取り / 書き込み)

有効値

文字列 最大 31 文字

デフォルト

public

説明

SNMP トラップに使用する SNMP コミュニティ名を指定します。

cfgOobSnmppAgentEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC で SNMP エージェントを有効または無効にします。

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含まれています。

グループの 1 つのインスタンスが許可されています。このグループのすべてのオブジェクトは iDRAC6 NIC のリセットを必要とするため、接続が一時的に途絶える可能性があります。iDRAC6 NIC IP アドレス設定を変更するオブジェクトが、アクティブなユーザーセッションをすべて終了するので、ユーザーはアップデート後の IP アドレス設定を使用して再接続する必要があります。

 **メモ:** iDRAC6 に加えたネットワークプロパティの変更が RACADM で正しく実行されるには、最初に iDRAC6 の NIC を有効にする必要があります。

 **メモ:** 「racadm getconfig -g cfgLanNetworking」のローカル RACADM コマンドを使用して表示される、または「racadm getconfig -f <ファイル名>」のローカル RACADM コマンドを使用して生成される設定ファイルに表示される VLAN オブジェクト (cfgNicVlanEnable、cfgNicVlanId、および cfgNicVlanPriority) には、これらのオブジェクトが読み取り専用であることを示す先頭に表示される「#」が抜けています。

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 の IPv4 スタックを有効または無効にします。

cfgDNSDomainNameFromDHCP (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0


説明

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。使用できる文字は、英数字、ハイフン、ピリオドに限られています。

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

デフォルト

(空白)


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

idrac-サービスタグ

説明

デフォルトの RAC 名が表示されます。デフォルトは、rac-サービスタグ です。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 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

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、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

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 を無効にすると、iDRAC6 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 iDRAC6 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

iDRAC6 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

iDRAC6 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、iDRAC6 の IP アドレス、サブネットマスク、および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

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。

cfgNicVlanEnable (読み取り専用)

 **メモ:** VLAN 設定は、CMC ウェブインタフェースを介して設定することができます。iDRAC6 では VLAN の現在の設定が表示されるだけで、iDRAC6 から設定を変更することはできません。

有効値

- 1 (TRUE)
- 0 (FALSE)

デフォルト

0

説明

iDRAC6 の VLAN 機能を CMC から有効または無効にします。

cfgNicVlanID (読み取り専用)

有効値

1~4094

デフォルト

1

説明

CMC のネットワーク VLAN 設定で 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 (読み取り専用)

有効値

0~7

デフォルト

0

説明

CMC のネットワーク VLAN 設定で 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。

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 URL。

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 の 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 の 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

0

説明

iDRAC6 IPv6 アドレス 1 のプレフィックスの長さ。

cfgIPv6AutoConfig (読み取り/書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

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 の 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 と cfgIPv6DNSServer2 が静的アドレスか DHCP IPv6 アドレスかを指定します。

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 サーバーのアドレス

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 サーバーのアドレス

cfgIPv6Address3 (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

<空白>

cfgIPv6Address4（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

<空白>

cfgIPv6Address5（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

<空白>

cfgIPv6Address6（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

<空白>

cfgIPv6Address7（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

<空白>

cfgIPv6Address8（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

<空白>

cfgIPv6Address9（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

<空白>

cfgIPv6Address10（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

<空白>

cfgIPv6Address11（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

<空白>

cfgIPv6Address12（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

<空白>

cfgIPv6Address13（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

<空白>

cfgIPv6Address14（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

<空白>

cfgIPv6Address15（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

<空白>

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。各インスタンスは個々のユーザーの設定を表します。

cfgUserAdminIndex（読み取り専用）

有効値

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。

デフォルト

1 ~ 16

説明

ユーザーの固有のインデックス

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、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 ユーザー権限に応じたビットマスク

ユーザー権限	権限ビットマスク
iDRAC6 へのログイン	0x00000001
iDRAC6 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-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 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 iDRAC6 にアクセスできません。	0x00000000
ユーザーは iDRAC6 にログインして iDRAC6 とサーバーの設定情報を表示するだけが許可されます。	0x00000001
ユーザーは iDRAC6 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

（空白）

説明

このインデックスのユーザーの名前。インデックス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インデックスが作成されます。二重引用符（""）の文字列を書き込むと、そのインデックス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

（空白）

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

0

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

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インデックス。

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 (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。

デフォルト

(空白)

説明

警告元の電子メールアドレス。

cfgEmailAlertCustomMsg (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

(空白)

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、iDRAC6 に接続できるセッション数を設定するパラメータが含まれています。

グループの 1 つのインスタンスが許可されています。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。

cfgSsnMgtConsRedirMaxSessions (読み取り / 書き込み)

有効値

1~2

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の最大セッション数を指定します。

cfgSsnMgtWebserverTimeout (読み取り / 書き込み)

有効値

60 ~ 10800

デフォルト

1800

説明

ウェブサーバーのタイムアウト時間を指定します。このプロパティでは、アイドル状態が何秒続くと、接続がタイムアウトになるかを指定します。このプロパティで設定した制限時間が過ぎると、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、ログアウトしてからログインし直す必要があります）。

ウェブサーバーセッションが時間切れになると、現在のセッションからログアウトされます。

cfgSsnMgtSshIdleTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60 ~ 10800

デフォルト

1800

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、アイドル状態が何秒続くと、接続がタイムアウトになるかを指定します。このプロパティで設定した制限時間が過ぎると、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。

Warning: Session no longer valid, may have timed out（警告：セッションは有効でなくなりました。タイムアウトになった可能性があります。）

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。

cfgSsnMgtTelnetTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60 ~ 10800

デフォルト

1800

説明

Telnet の無動作タイムアウト時間を指定します。このプロパティでは、アイドル状態が何秒続くと、接続がタイムアウトになるかを指定します。このプロパティで設定した制限時間が過ぎると、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）。

Telnet が時間切れになった後 <Enter> キーを押すと、次のエラーメッセージが表示されます。

Warning: Session no longer valid, may have timed out（警告：セッションは有効でなくなりました。タイムアウトになった可能性があります。）

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、iDRAC6 サービスの設定パラメータが含まれます。

グループの 1 つのインスタンスが許可されています。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。

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。

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。

cfgRhostsSmtplibAddr (読み取り / 書き込み)

有効値

有効な SMTP サーバー IP アドレスを表す文字列。例: 192.168.0.56

デフォルト

0.0.0.0

説明

ネットワーク SMTP サーバーの IP 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、RAC から電子メール警告を送信します。

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 IP アドレスを表す文字列。

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処理に使用されるネットワーク TFTP サーバー IP 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 の ASCII 文字の文字列。

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。

サーバーのドライブを指定しなければならない場合があります (例: C:)。

cfgRhostsSyslogEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

リモートシスログを有効または無効にします。

cfgRhostsSyslogPort (読み取り / 書き込み)

有効値

0 ~ 65535

デフォルト

514

説明

リモートシスログのポート番号。

cfgRhostsSyslogServer1 (読み取り / 書き込み)

有効値

0 ~ 511 文字の文字列。

デフォルト

<空白>

説明

リモートシスログサーバーの名前。

cfgRhostsSyslogServer2 (読み取り / 書き込み)

有効値

0 ~ 511 文字の文字列。

デフォルト

<空白>

説明

リモートシスログサーバーの名前。

cfgRhostsSyslogServer3（読み取り / 書き込み）

有効値

0 ～ 511 文字の文字列。

デフォルト

<空白>

説明

リモートシスログサーバーの名前。

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。最大 40 のドメイン名を設定できます。

cfgUserDomainIndex（読み取り専用）

有効値

1 ～ 40

デフォルト

<インスタンス>

説明

特定のドメインを表します。

cfgUserDomainName（読み取り / 書き込み）

有効値

最大 255 文字の文字列。

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

このグループは複数の電源管理機能を提供します。

cfgServerPowerStatus（読み取り専用）

有効値

1 = TRUE

0 = FALSE

デフォルト

0

説明

サーバーの電源状況を **オン** または **オフ** で表します。

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

現時点でサーバーが消費している電力を表します。

cfgServerPeakPowerConsumption（読み取り専用）

有効値

最大 32 文字の文字列。

デフォルト

（空白）

説明

現在までにサーバーが消費した最大電力量を表します。

cfgServerPeakPowerConsumptionTimestamp（読み取り専用）

有効値

最大 32 文字の文字列。

デフォルト

（空白）

説明

最大電力消費量が記録された時刻。

cfgServerPowerConsumptionClear（書き込み専用）

有効値

0、1

デフォルト

0

説明

cfgServerPeakPowerConsumption プロパティを 0 に、cfgServerPeakPowerConsumptionTimestamp プロパティを現在の iDRAC6 の時刻にリセットします。

cfgServerPowerCapWatts（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

サーバーの電力しきい値をワットで表します。

cfgServerPowerCapBtuhr（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

サーバーの電力しきい値を BTU/ 時で表します。

cfgServerPowerCapPercent (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

サーバーの電力しきい値をワットで表します。

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。

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

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

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 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

cfgRacTuneIpBIKEnable

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

時間枠 (cfgRacTuneIpBlkFailWindow) 内で何回ログインに失敗すると、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

iDRAC6 の SSH インタフェースに使用され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または無効にします。

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され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

iDRAC6 のコンソールリダイレクトの処理中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

iDRAC6 のコンソールリダイレクトの処理中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 iDRAC6 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

1

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。

 **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。

cfgRacTuneWebserverEnable (読み取り / 書き込み)

有効値

0 (FALSE)

1 (TRUE)

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。

cfgRacTuneLocalServerVideo (読み取り / 書き込み)

有効値

1 (Enables)

0 (Disables)

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。

cfgRacTuneDaylightOffset (読み取り / 書き込み)

有効値

0 ~ 60

デフォルト

0

説明

RAC 時間に使用する夏時間のオフセットを分単位で指定します。

cfgRacTuneTimezoneOffset (読み取り / 書き込み)

有効値

-720 ~ 780

デフォルト

0

説明

RAC 時間に使用するタイムゾーンのオフセットを GMT/UTC から分単位で指定します。

RAC 時間 米国内の時間帯に使用する一般的なタイムゾーンのオフセットは以下のとおりです。

状態は以下のとおりです。

-480 (PST - 太平洋標準時)

-420 (MST - 山岳部標準時)

-360 (CST - 中央標準時)

-300 (EST - 東部標準時)

cfgRacTuneLocalConfigDisable (読み取り / 書き込み)

有効値

0 (Enables)

1 (Disables)

デフォルト

0

説明

iDRAC6 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 iDRAC6 ウェブインタフェースを使用して無効にできますが、一度無効にしたアクセスを再び有効にするには、iDRAC6 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について説明するプロパティが含まれています。

グループの 1 つのインスタンスが許可されています。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。

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 の 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。

cfgSecCsrCommonName (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。

cfgSecCsrOrganizationName (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。

cfgSecCsrOrganizationUnit (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。

cfgSecCsrLocalityName (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。

cfgSecCsrStateName (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。

cfgSecCsrCountryCode (読み取り / 書き込み)

有効値

2 文字の文字列

デフォルト

(空白)

説明

CSR 国名 (CC) を指定します。

cfgSecCsrEmailAddr (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。

cfgSecCsrKeySize (読み取り / 書き込み)

有効値

512

1024

2048

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 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。グループの 1 つのインスタンスが許可されています。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。

cfgRacVirMediaAttached (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、システムに接続している有効な USB 大容量記憶装置を認識します。これは、ローカル USB CDROM/ 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。デバイスを連結すると、iDRAC6 の ウェブインタフェースまたは CLI を使用して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。

cfgVirMediaBootOnce (読み取り / 書き込み)

有効値

- 1 (Enabled)
- 0 (Disabled)

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。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。

cfgVirMediaKeyEnable (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 VFlash メディアキーを有効または無効にします。

cfgVirtualFloppyEmulation (読み取り / 書き込み)

有効値

- 1 (TRUE)
- 0 (FALSE)

デフォルト

0

説明

0 に設定すると、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で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 に設定すると、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で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。

cfgSDWriteProtect (読み取り専用)

有効値

- 1 (TRUE)
- 0 (FALSE)

デフォルト

0

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。

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

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 / 無効のプロパティをオーバーライドします。

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 進数の偶数の文字列。

デフォルト

00

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

<インデックス値>

説明

トラップに対応するインデックスの固有の識別子。

cfgIpmiPetIPv6AlertDestIpAddr

有効値

有効な IPv6 アドレスを表す文字列。

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連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

インデックスフィルタの名前。

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 ~ 9

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インデックス値。

説明

特定のプラットフォームイベントフィルタのインデックスを指定します。

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インデックス値。

説明

トラップに対応するインデックスの固有の識別子。

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

個々のトラップを有効または無効にします。

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)

デフォルト

0

説明

スマートカードを使用して iDRAC6 にアクセスする機能のサポートを有効または無効にします。

cfgActiveDirectory

このグループには、iDRAC6 の Active Directory 機能を設定するためのパラメータが含まれています。

cfgADSSOEnable (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 のシングルサインオン認証を有効または無効にします。

cfgADRadDomain (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

DRAC 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 の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。

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)。最大文字数は 254 です。

デフォルト

デフォルト値なし

説明

iDRAC6 はここで指定した値を使って LDAP サーバーでユーザー名を探します。

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)。最大文字数は 254 です。

デフォルト

デフォルト値なし。

説明

iDRAC6 はここで指定した値を使って LDAP サーバーでユーザー名を探します。

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)。最大文字数は 254 です。

デフォルト

デフォルト値なし。

説明

iDRAC6 はここで指定した値を使って LDAP サーバーでユーザー名を探します。

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)。最大文字数は 254 です。

デフォルト

デフォルト値なし。

説明

iDRAC6 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)。最大文字数は 254 です。

デフォルト

デフォルト値なし。

説明

iDRAC6 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)。最大文字数は 254 です。

デフォルト

デフォルト値なし。

説明

iDRAC6 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

説明

Active Directory と併用するスキーマタイプを指定します。

cfgADCertValidationEnable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

<空白>

説明

Active Directory 証明書の検証を有効または無効にします。

cfgADDcSRVLookupEnable (読み取り / 書き込み)

有効値

1 (TRUE) - DNS を使用してドメインコントローラをルックアップする

0 (FALSE) - あらかじめ設定されたドメインコントローラを使用する

デフォルト

0

定義

あらかじめ設定されたドメインコントローラを使用、またドメインコントローラを検索するために DNS を使用するように、iDRAC6 を設定します。あらかじめ設定されたドメインコントローラを使用する場合、使用するドメインコントローラは、cfgAdDomainController1、cfgAdDomainController2、および cfgAdDomainController3 で指定されています。DNS ルックアップが失敗した場合、あるいは DNS ルックアップで返されるサーバーが機能しない場合でも、iDRAC6 は指定したドメインコントローラにフェールオーバーしません。

cfgADDcSRVLookupbyUserdomain (読み取り / 書き込み)

有効値

1 (TRUE) -ドメインコントローラをルックアップする検索ドメインにユーザードメインを使用する。ユーザードメインは、ユーザードメインリストから選択するか、ログインユーザーによって入力されま

す。

0 (FALSE) -ドメインコントローラの ルックアップに設定された検索ドメイン、cfgADDcSrvLookupDomainName を使用する。

デフォルト

1

例

「MyDomain」の Active Directory ドメインを持つ「userid」というユーザーが存在する場合：

このオプションを有効にすると、ユーザーは ログイン時に、ユーザーフィールドに「MyDomain/userid」と入力します。このオプションを無効にすると、「MyDomain」の値が含まれるように、cfgADDcSRVLookupDomainName を設定する必要があります。ユーザーはログイン時に、ユーザーフィールドに「userid」と入力します。

定義

Active Directory でユーザードメインがどのようにルックアップされるか決定します。

cfgADDcSRVLookupDomainName (読み取り / 書き込み)

有効値

文字列 最大 254 文字

デフォルト

Null

定義

cfgAddcSrvLookupbyUserDomain が 0 に設定されている場合、この Active Directory ドメインが使用されます。

cfgADGcSRVLookupEnable (読み取り / 書き込み)

有効値

0 (FALSE) -あらかじめ設定されたグローバルカタログサーバー (GCS) を使用する

1 (TRUE) - DNS を使用して GCS をルックアップする

デフォルト

0

定義

グローバルカタログサーバーがどのようにルックアップされるか決定します。あらかじめ設定されたグローバル カタログサーバーを使用する場合、iDRAC6 は cfgAdGlobalCatalog1、cfgAdGlobalCatalog2、および cfgAdGlobalCatalog3 の値を使用します。

cfgADGcRootDomain (読み取り / 書き込み)

有効値

文字列 最大 254 文字

デフォルト

Null

例

ドメインが「ROOTDOMAIN.sub1」である場合、この値は「ROOTDOMAIN」として設定されます。

説明

グローバルカタログサーバーを見つけるために、DNS ルックアップで使用される Active Directory ルートドメインの名前です。

cfgLDAP

このグループのユーザーは、LDAP 関連の設定を設定できます。

cfgLdapEnable (読み取り / 書き込み)

有効値

1 (TRUE) - LDAP サービスを有効にする

0 (FALSE) - LDAP サービスを無効にする

デフォルト

0

説明

LDAP サービスをオンまたはオフにします。

cfgLdapServer (読み取り / 書き込み)

有効値

文字列 最大 1024 文字

デフォルト

Null

説明

LDAP サーバーのアドレスを設定します。

cfgLdapPort (読み取り / 書き込み)

有効値

1 ~ 65535

デフォルト

636

説明

LDAP オーバー SSL で使用するポート。非 SSL ポートはサポートされていません。

cfgLdapBasedn (読み取り / 書き込み)

有効値

文字列 最大 254 文字

デフォルト

Null

説明

すべての検索が開始されるディレクトリのブランチにおけるドメイン名。

cfgLdapUserAttribute (読み取り / 書き込み)

有効値

文字列 最大 254 文字

デフォルト

Null

設定されていない場合は uid。

説明

検索するユーザー属性を指定します。設定されていない場合は、デフォルトで uid が使用されます。選択したベース DN 内で一意であることが推奨されます。そうでない場合は、ログインユーザーの一意性を確保できるように検索フィルタを設定する必要があります。ユーザー DN を一意に識別できない場合は、エラーが発生し、ログインに失敗します。

cfgLdapGroupAttribute (読み取り / 書き込み)

有効値

文字列 最大 254 文字

デフォルト

Null

説明

グループメンバーシップを確認するために使用する LDAP 属性を指定します。これは、グループクラスの属性である必要があります。指定しない場合、iDRAC6 は member および unique member の属性を使用します。

cfgLdapGroupAttributeIsDN（読み取り / 書き込み）

有効値

1 (TRUE) -LDAP サーバーの userDN を使用する

0 (FALSE) -ログインユーザーによって提供される userDN を使用する

デフォルト

1

説明

1 に設定した場合、iDRAC6 はディレクトリから取得した userDN とグループのメンバーを比較します。0 に設定した場合、ログインユーザーによって提供されるユーザー名でグループのメンバーと比較します。これは、バインドの検索アルゴリズムに影響を及ぼしません。iDRAC6 は、常に userDN を検索し、バインドに userDN を使用します。

cfgLdapBinddn（読み取り / 書き込み）

有効値

文字列 最大 254 文字

デフォルト

Null

説明

ログインユーザーの DN を検索する際に、サーバーへのバインドに使用するユーザーの識別名です。提供されない場合、匿名バインドが使用されます。これはオプションではありますが、匿名バインドがサポートされていない場合には、必須となります。

cfgLdapBindpassword（書き込み専用）

有効値

文字列 最大 254 文字

デフォルト

Null

説明

バインド DN と共に使用されるバインドパスワード。バインドパスワードは機密性の高いデータであるため、適切に保護する必要があります。これはオプションではありますが、匿名バインドがサポートされていない場合には、必須となります。

cfgLdapSearchFilter（読み取り / 書き込み）

有効値

文字列 最大 254 文字

デフォルト

(objectclass=*)

ツリー内のすべてのオブジェクトを検索します。

説明

有効な LDAP 検索フィルタ。ユーザー属性を使用して、選択した baseDN 内でログインユーザーを一意に識別できない場合に使用されます。「検索フィルタ」は、userDN 検索のみに適用され、グループメンバーシップの検索には適用されません。

cfgLDAPCertValidationEnable（読み取り / 書き込み）

有効値

1 (TRUE) -iDRAC6 は、SSL ハンドシェイク時に、LDAP サーバー証明書を検証するために CA 証明書を使用する

0 (FALSE) -iDRAC6 は、SSL ハンドシェイク時に、証明書の検証ステップをスキップする

デフォルト

1-有効

説明

SSL ハンドシェイク時の証明書の検証を制御します。

cfgLdapRoleGroup

このグループのユーザーは、LDAP 用に役割グループを設定できます。このグループには、1 から 5 のインデックスが付けられます。

cfgLdapRoleGroupIndex（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

役割グループオブジェクトのインデックス値です。

cfgLdapRoleGroupDN（読み取り / 書き込み）

有効値

文字列 最大 1024 文字

デフォルト

Null

説明

このインデックスのグループのドメイン名です。

cfgLdapRoleGroupPrivilege（読み取り / 書き込み）

有効値

0x00000000 ~ 0x000001ff

デフォルト

0x000

説明

この特定グループに関連付けられた権限を定義するビットマスク。

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

説明

Active Directory で記録した役割グループのインデックス。

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

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用して、役割グループの役割ベースの権限を設定します。

表 B-3 役割グループの権限のビットマスク

役割グループの権限	ビットマスク
iDRAC6 へのログイン	0x00000001
iDRAC6 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

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。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 Enterprise 概要

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [IPv6 対応証明ロゴ](#)
- [iDRAC6 のセキュリティ機能](#)
- [iDRAC6 Enterprise および VFlash メディア](#)
- [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) はシステム管理のハードウェアと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修復機能、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、管理下 Dell PowerEdge サーバーとシステム基板上で共存します。サーバーのオペレーティングシステムがアプリケーションプログラムを実行します。iDRAC6 はオペレーティングシステム外でサーバーの環境と状態を監視および管理します。

警告やエラーの場合に、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。

管理下サーバーは、モジュール電源装置、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、一次 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 iDRAC6 へのアクセスを提供します。シャーシ内の各ブレードに iDRAC6 があります。M1000e には合計 16 のブレードを搭載できます。

iDRAC6 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、内部の専用ネットワークを使用してトラフィックをブレードの iDRAC6 デバイスに転送します。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、つまり帯域外にあります。管理下サーバーの帯域内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。

 **メモ:** iDRAC6 と CMC によって使用されるシャーシ管理ネットワークと運用ネットワークを分離することを推奨しています。管理ネットワークと運用またはアプリケーションネットワークのトラフィックを混合すると、輻輳やネットワーク飽和が発生して、CMC と iDRAC6 の通信が遅延する可能性があります。また、遅延によってシャーシの動作が予測不可能になることがあります。たとえば、iDRAC6 が正常に稼働しているのに CMC にはオフラインと表示されたりします。これにより、他の予期しない動作を起こす恐れがあります。

iDRAC6 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、iDRAC6 にアクセスできません。ネットワークで iDRAC6 を有効にして設定すると、iDRAC6 ウェブインタフェース、Telnet、SSH や、Intelligent Platform Management Interface (IPMI) などのサポートされてい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。

IPv6 対応証明ロゴ

IPv6 対応証明ロゴ委員会の任務は、IPv6 準拠と相互運用性テストのテスト仕様を定義して、セルフテストツールへのアクセスを提供したり、IPv6 に対応していることを証明するロゴを配布したりすることです。

iDRAC6 は **フェーズ-2 IPv6 対応証明ロゴ** に認定されており、ロゴ ID は **02-C-000380** です。IPv6 対応証明ロゴプログラムの詳細については、<http://www.ipv6ready.org/> を参照してください。

iDRAC6 のセキュリティ機能

- 1 Microsoft Active Directory、汎用 LDAP ディレクトリサービス、またはローカルで管理されるユーザー ID およびパスワードを使用したユーザー認証。
- 1 スマートカードログオン機能で提供される 2 要素認証。2 要素認証は、ユーザーが所有するもの (スマートカード) とユーザーが知っている情報 (暗証番号) に基づきます。
- 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ベースの許可
- 1 ユーザー ID およびパスワードの設定
- 1 SM-CLP およびウェブインタフェースが SSL 3.0 規格を使用して、128 ビットと 40 ビット (128 ビットが認められていない国の場合) の暗号化をサポート
- 1 セッションタイムアウトの設定 (秒数指定)
- 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回数の制限により、制限を超えた IP アドレスからのログインを阻止
- 1 iDRAC6 に接続するクライアントの IP アドレス範囲を設定可能

iDRAC6 Enterprise および VFlash メディア

iDRAC6 Enterprise は VFlash メディアに SD スロットを 1 つ提供しています。iDRAC6 Enterprise と VFlash メディアの詳細については、support.dell.com/manuals で『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。

[表 1-1](#) は、iDRAC6 Enterprise と VFlash メディアに搭載されている機能のリストです。

表 1-1 iDRAC6 の機能リスト

機能	iDRAC6 Enterprise	VFlash を使用した iDRAC6 Enterprise
インタフェースと標準サポート		
IPMI 2.0	✓	✓
ウェブ GUI	✓	✓
SNMP	✓	✓
WS-MAN	✓	✓
SM-CLP	✓	✓
RACADM コマンドライン	✓	✓
接続性		
共有 / フェールオーバーネットワークモード	✓	✓
IPv4	✓	✓
VLAN タグ	✓	✓
IPv6	✓	✓
ダイナミック DNS	✓	✓
専用 NIC	✓	✓
セキュリティと認証		
役割ベースの許可	✓	✓
ローカルユーザー	✓	✓
Active Directory	✓	✓
2 要素認証	✓	✓
シングルサインオン	✓	✓
SSL 暗号化	✓	✓
リモート管理と改善		
リモートファームウェアアップデート	✓	✓
サーバーの電源制御	✓	✓
serial-over-LAN(プロキシあり)	✓	✓
serial-over-LAN(プロキシなし)	✓	✓
電力制限	✓	✓
前回クラッシュ画面のキャプチャ	✓	✓
起動キャプチャ	✓	✓
仮想メディア	✓	✓
リモートファイル共有	✓	✓
仮想コンソール	✓	✓
仮想コンソールの共有	✓	✓
仮想フラッシュ	✗	✓
監視		
センサー監視と警告	✓	✓
リアルタイムの電源監視	✓	✓
リアルタイムの電源グラフ	✓	✓
電源カウンタ履歴	✓	✓
ロギング		
システムイベントログ (SEL)	✓	✓

RAC ログ	✓	✓
トレースログ	✓	✓
リモートシスログ	✓	✓
 = 対応  = 未対応		

対応プラットフォーム


最新の対応プラットフォームについては、iDRAC6 Readme ファイルと support.dell.com/manuals にある『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。

対応 OS

最新の情報については、iDRAC6 Readme ファイルと support.dell.com/manuals にある『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。

対応ウェブブラウザ

最新の情報については、iDRAC6 Readme ファイルと support.dell.com/manuals にある『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:** SSL 2.0 にはセキュリティ上の不具合があるため、サポートされなくなりました。お使いのブラウザで SSL 3.0 が有効に設定されていることを確認してください。

対応リモートアクセス接続

[表 1-2](#) は接続機能のリストです。

表 1-2 対応リモートアクセス接続

接続	機能
iDRAC6 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 iDRAC6 設定、システム起動、リセット、電源投入、シャットダウンなどの操作を行うための SM-CLP シェルおよび RACADM コマンドは、SSH と Telnet を介してサポートされています。 IPMITool や ipmish などの IPMI ユーティリティのサポート

iDRAC6 のポート

[表 1-3](#) は、iDRAC6 が接続を待ち受けるポートのリストです。[表 1-4](#) 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。

 **注意:** iDRAC6 は、設定可能なポート間の競合を確認しません。ポートを設定する際は、ポートの割り当てがお互いに競合しないことを確認してください。

表 1-3 iDRAC6 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
3670、3671	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

5988*	WSMAN に使用
*設定可能なポート	

表 1-4 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。

- 1 iDRAC6 オンラインヘルプは、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 システムソフトウェアサポートマトリックス』は、各種デルシステム、これらのシステムでサポートされているオペレーティングシステム、これらのシステムにインストールできる Dell OpenManage™ コンポーネントについての情報が記載されています。
- 1 『Dell OpenManage Server Administrator インストールガイド』では、Dell OpenManage Server Administrator のインストール手順が説明されています。
- 1 『Dell OpenManage Management Station Software インストールガイド』では、Dell OpenManage Management Station Software(ベースボード管理ユーティリティ、DRAC ツール、Active Directory スナップインを含む)のインストール手順が説明されています。
- 1 『Dell Chassis Management Controller ユーザーガイド』および『Dell Chassis Management Controller システム管理者リファレンス ガイド』は、Dell PowerEdge サーバーが格納されているシャーシ内のすべてのモジュールを管理するコントローラの使用法について説明しています。
- 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 Management Console ユーザーズガイド』は、デル管理コンソール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の一環としての Dell Update Packages の入手と使用法について説明しています。
- 1 『Dell Lifecycle Controller ユーザーズガイド』は、Unified Server Configurator(USC)、Unified Server Configurator - Lifecycle Controller Enabled(USC - LCE)、および Remote Services について説明しています。
- 1 www.delltechcenter.com の Dell Enterprise Technology Center から入手可能な『iDRAC6 CIM Element Mapping』および『iDRAC6 SM-CLP Property Database』には、iDRAC6 SM-CLP プロパティデータベース、WS-MAN クラスと SM-CLP ターゲット間のマッピング、およびデル実装に関する情報が記載されています。

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含まれています。

- 1 システムに付属のマニュアルの「安全にお使いいただくために」には、安全および認可機関に関する重要な情報が記載されています。規制の詳細については、www.dell.com/regulatory_complianceにある Regulatory Compliance(法規制の遵守)ホームページを参照してください。保証情報は、このマニュアルに含まれている場合と、別の文書として付属する場合があります。
- 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。

本書で使用されている用語の詳細については、デルサポートサイト support.dell.com/manuals の用語集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 Enterprise の設定

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [作業を開始する前に](#)
- [iDRAC6 を設定するためのインタフェース](#)
- [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\(フレックスアドレス\)メザンカードのファブリック接続の表示](#)
- [リモートシスログ](#)
- [リモートファイル共有](#)
- [iDRAC6 ファームウェアのアップデート](#)
- [USC 修復パッケージのアップデート](#)
- [IT Assistant で使用するために iDRAC6 を設定する](#)
- [iDRAC6 設定ユーティリティを使用して検出と監視を有効にする方法](#)
- [iDRAC6 ウェブインタフェースを使用して検出と監視を有効にする方法](#)
- [IT Assistant を使用して iDRAC6 ステータスおよびイベントを表示する](#)

本項では、iDRAC6 へのアクセスの確立方法と、iDRAC6 を使用する管理環境を設定する方法を説明します。

作業を開始する前に

iDRAC6 を設定する前に、下記をご用意ください。

- 1 Dell Chassis Management Controller ファームウェアユーザーガイド
- 1 DellSystems Management Tools and Documentation DVD

『Dell Systems Management Tools and Documentation DVD』には、次のコンポーネントが含まれています。

- 1 DVD ルート - サーバースettings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。
- 1 SYSMGMT - 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。

詳細については、デルサポートウェブサイト support.dell.com/manuals にある『Dell OpenManage Server Administrator インストールガイド』および『Dell OpenManage Management Station Software インストールガイド』を参照してください。

iDRAC6 を設定するためのインタフェース

iDRAC6 の設定は、iDRAC6 設定ユーティリティ、iDRAC6 ウェブインタフェース、Chassis Management Controller(CMC)ウェブインタフェース、シャーシの LCD パネル、ローカルおよびリモート RACADM CLI、iVMCLI、または SM-CLP CLI を使用して実行できます。管理下サーバーにオペレーティングシステムと Dell OpenManage 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、iDRAC6 設定ユーティリティまたはローカル RACADM CLI から iDRAC6 設定へのアクセスを 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)を使って無効にすることもできます。


 **メモ:** 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
iDRAC6 設定ユーティリティ	起動時にアクセスできる iDRAC6 設定ユーティリティは、新しい Dell PowerEdge™ サーバ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。
iDRAC6 ウェブインタフェース	iDRAC6 ウェブインタフェースは、iDRAC6 の管理と管理下サーバーの監視をインタラクティブに実行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 iDRAC6 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	シャーシの監視と管理に加えて、CMC ウェブインタフェースは、管理下サーバーの状態の確認、iDRAC6 ファームウェアのアップデート、iDRAC6 ネットワークの指定、iDRAC6 ウェブインタフェースへのログオン、管理下サーバーの開始、終了、リセットなどに使用できます。
シャーシ LCD パネル	iDRAC6 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き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 iDRAC6 ネットワークの DHCP 設定を有効にできます。
ローカルおよびリモート 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 iDRAC6 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。 リモート RACADM は、管理ステーションで実行されるクライアントユーティリティです。帯域外のネットワークインタフェースを使用して、管理下サーバーに RACADM コマンドを実行します。-r オプションはネットワーク経由で RACADM コマンドを実行します。 RACADM コマンドは、iDRAC6 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、iDRAC6 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、iDRAC6 の設定値の変更、ローカルユーザーの管理、機能の有効 / 無効化、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。
iVMCLI	iDRAC6 仮想メディアコマンドラインインタフェース(iVMCLI)は、管理下サーバーが管理ステーションのメディアにアクセスできるようにします。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、iDRAC6 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 または SSH を使用して iDRAC6 にログインし、CLI プロンプトで smc1p と入力してアクセスします。

	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。
IPMI	<p>IPMI は、iDRAC6 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。</p> <p>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)を設定するには、iDRAC6 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。</p> <p>PEF は、特定の状態を検知した際に、iDRAC6 に特定の処置(たとえば、管理下サーバーの再起動)を実施させます。PET は、特定のイベントまたは状態を検知したときに電子メールまたは IPMI 警告を送信するよう iDRAC6 に命令します。</p> <p>また iDRAC6 では、IPMI オーバー LAN を有効にしている場合に IPMI tool や ipmish などの標準的な IPMI ツールも使用できます。</p>

設定タスク

本項では、管理ステーション、iDRAC6、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、iDRAC6 をリモートからアクセスするための設定、使用する iDRAC6 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、Dell PowerEdge™ サーバーもシャーシ内に物理的に取り付ける必要があります。

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。「[管理ステーションの設定](#)」を参照してください。

iDRAC6 ネットワークの設定

iDRAC6 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 のアドレスを設定します。

 **メモ:** iDRAC6 設定ユーティリティまたはローカル RACADM CLI から iDRAC6 設定へのアクセスを 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)を使用して無効にすることもできます。

 **メモ:** iDRAC6 ネットワーク設定を変更すると、iDRAC6 との現在のネットワーク接続がすべて切断されます。


 **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。シャーシを一度導入すると、LCD パネルを使用して iDRAC6 を再設定することはできません。

 **メモ:** LCD パネルは、DHCP を有効にして iDRAC6 ネットワークを設定する目的でのみ使用できます。


- 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 iDRAC6 設定ユーティリティ - 「[iDRAC6 設定ユーティリティの使用](#)」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 リモートおよびローカル RACADM - 「[cqlanNetworking](#)」を参照してください。

iDRAC6 ユーザーの設定

ローカル iDRAC6 のユーザーと権限を設定します。iDRAC6 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、および役割を設定できます。

 **メモ:** <, >, および \ はユーザー名またはパスワードには使用できません。

- 1 iDRAC6 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 iDRAC6 ウェブインタフェース - 「[iDRAC6 ユーザーの追加と設定](#)」を参照してください。
- 1 リモートおよびローカル RACADM - 「[iDRAC6 ユーザーの追加](#)」を参照してください。

 **メモ:** Active Directory / 汎用 LDAP ディレクトリサービスの環境で iDRAC6 を使用する場合、ユーザー名が Active Directory / 汎用 LDAP ディレクトリサービスの命名規則に従っていることを確認してください。

ディレクトリサービスの設定

ローカル iDRAC6 ユーザーに加え、iDRAC6 ユーザーログインの認証には Microsoft® Active Directory® または汎用 LDAP ディレクトリサービスも使用できます。

詳細については、「[iDRAC6 ディレクトリサービスの使用](#)」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せん。

- 1 iDRAC6 ウェブインタフェース - 「[IP フィルタと 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](#)」および「[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、iDRAC6 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 iDRAC6 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 iDRAC6 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](#)」を参照してください。

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 iDRAC6 設定ユーティリティに対して (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。iDRAC6 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。RACADM コマンドについては、「[cfoRacTuning](#)」を参照してください。

iDRAC6 サービスの設定

iDRAC6 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の設定を変更したりします。

- 1 iDRAC6 ウェブインタフェース - 「[iDRAC6 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 iDRAC6 Telnet および SSH サービスの設定](#)」を参照してください。

Secure Socket Layer (SSL) の設定

iDRAC6 ウェブサーバーの SSL 設定

- 1 iDRAC6 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 - 「[cfoRacSecurity](#)」、「[ssicsrqlen](#)」、「[ssicertupload](#)」、「[ssicertdownload](#)」および「[ssicertview](#)」を参照してください。

仮想メディアの設定

Dell 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 iDRAC6 ウェブインタフェース - 「[仮想メディアの設定と使用方法](#)」を参照してください。
- 1 iDRAC6 設定ユーティリティ - 「[仮想メディアの設定](#)」を参照してください。

VFlash メディアカードの設定

iDRAC6 で使用する VFlash メディアカードをインストールおよび設定します。

- 1 iDRAC6 ウェブインタフェース - 「[iDRAC6 と使用するための VFlash メディアカードの設定](#)」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 Dell 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し、Dell 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 iVMCLI - 「[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 iDRAC6 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](#)」および「[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 iDRAC6 ネットワーク設定を行うには、シャーン設定のシステム管理者権限が必要です。

 **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ことで、iDRAC6 ウェブインタフェースに表示されます。この画面から CMC ウェブインタフェースを起動することもできます。

CMC からの iDRAC6 ウェブインタフェースの起動

CMC は、サーバーなどの個別シャーシコンポーネントの限定された管理機能を提供します。個々のコンポーネントを完全に管理するために、CMC はサーバーの iDRAC6 ウェブインタフェースへの起動ポイントを提供しています。

サーバー 画面から iDRAC6 を起動するには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで **サーバー** を選択します。
サーバーステータス 画面が表示されます。
3. 管理するサーバーの iDRAC6 GUI の **起動** アイコンをクリックします。

システムツリーの **サーバー** リストを使用して、1 台のサーバーの iDRAC6 ウェブインタフェースを起動することもできます。


1. CMC ウェブインタフェースにログインします。
2. システムツリーで **サーバー** を展開します。
すべてのサーバー(1~16)が展開された**サーバー** リストに表示されます。
3. 表示するサーバーをクリックします。
選択したサーバーの **サーバーステータス** 画面が表示されます。
4. iDRAC6 GUI の **起動** アイコンをクリックします。

シングルサインオン

シングルサインオン機能を利用すると、2 度ログインしなくても CMC から iDRAC6 ウェブインタフェースを起動できます。以下に、シングルサインオンの詳細について説明します。


1 **ユーザー特権** で Server Administrator の権限が設定されている CMC ユーザーは、シングルサインオンを使用して iDRAC6 ウェブインタフェースに自動的にログインされます。ログイン後、ユーザーには自動的に iDRAC6 Administrator 権限が付与されます。これは、iDRAC6 のアカウントを持たない同じユーザーや、アカウントに Administrator 権限がない場合でも同様です。


1 **ユーザー特権** で Server Administrator の権限が設定されていないが、iDRAC6 上で同じアカウントを保有している場合は、シングルサインオンを利用して自動的に iDRAC6 ウェブインタフェースにログインされます。iDRAC6 ウェブインタフェースに一度ログインすると、このユーザーには iDRAC6 アカウントに作成されている権限が付与されます。

 **メモ:** 上記の「同じアカウント」とは、CMC と iDRAC6 のどちらでも、ログイン名とパスワードが同じであることを意味します。同じログイン名を持つが、異なるパスワードを持つユーザーは、有効なユーザーとして認識されません。

1 **ユーザー特権** で Server Administrator の権限が設定されておらず、iDRAC6 上で同じアカウントを保有していない場合は、シングルサインオンを利用して自動的に iDRAC6 ウェブインタフェースにログインできません。このユーザーは、iDRAC6 GUI の **起動** をクリックした後、iDRAC6 ログイン画面にリダイレクトされます。

 **メモ:** この場合、ユーザーは iDRAC6 にログインすることが求められます。

 **メモ:** iDRAC6 ネットワーク LAN が無効(LAN 有効=オフ)の場合は、シングルサインオンを利用できません。

 **メモ:** サーバーをシャーシから取り外した場合、iDRAC6 の IP アドレスを変更した場合、または iDRAC6 ネットワーク接続に問題がある場合に iDRAC6 GUI の **起動** アイコンをクリックすると、エラー画面が表示される可能性があります。

iDRAC6 ネットワークの設定

1. **システム** → **リモートアクセス** → **iDRAC6** の順にクリックします。
2. **ネットワーク / セキュリティ** タブをクリックします。

シリアルオーバー LAN を有効または無効にするには:


- a. **シリアルオーバー LAN** をクリックします。
シリアルオーバー LAN 画面が表示されます。
- b. **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ます。**ポーレート** および **チャンネル権限レベルの制限** 設定を変更することも可能です。
- c. **適用** をクリックします。

IPMI オーバー LAN を有効または無効にするには:

- a. **ネットワーク** をクリックします。
ネットワーク 画面が表示されます。
- b. **IPMI の設定** をクリックします。
- c. **IPMI オーバー LAN を有効にする** チェックボックスを選択します。**チャンネル権限レベルの制限** および **暗号化キー** の設定を変更することも可能です。
- d. **適用** をクリックします。


DHCP を有効または無効にするには:

- a. **ネットワーク** をクリックします。
ネットワーク 画面が表示されます。
- b. **IPv4 の設定** セクションの **DHCP 有効** チェックボックスと **IPv6 の設定** の **自動構成有効** チェックボックスをオンにして DHCP を有効にします。DNS サーバーアドレスの取得に DHCP を使用するには、**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ンにします。
- c. **適用** をクリックします。

 **メモ:** DHCP を有効にしない場合は、サーバーに対して、静的な IP アドレス、ネットマスクおよびデフォルトゲートウェイを入力する必要があります。

FlexAddress(フレックスアドレス)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 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、シャーシ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。

 **メモ:** 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ことが必要です。

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については、『Dell Chassis Management Controller ユーザーガイド』と『Chassis Management Controller(CMC)セキュアデジタル(SD)カード仕様』の文書を参照してください。

シャーシに対して FlexAddress 機能を有効にして設定した後、**システム** → **プロパティ** タブ → **WWN/MAC** をクリックして、取り付けられているメザニンカード、カードが接続しているファブリック、ファブリックの種類、組み込み Ethernet とオプションのメザニンカードポートのそれぞれのサーバー割り当てまたはシャーシ割り当ての MAC アドレスなどを一覧表示します。

サーバー割り当て 列には、コントローラのハードウェアに組み込まれているサーバー割り当ての WWN/MAC アドレスが表示されます。「**該当なし**」と表示される WWN/MAC アドレスは、指定されたファブリックのインタフェースがインストールされていないことを示します。


シャーシ割り当て 列には、特定のスロットに使用されるシャーシ割り当ての WWN/MAC アドレスが表示されます。「**該当なし**」と表示される WWN/MAC アドレスは、FlexAddress 機能がインストールされていないことを示します。**サーバー割り当て** 列と **シャーシ割り当て** 列の緑色のチェックマークは、アクティブなアドレスを示します。


iDRAC6 用 FlexAddress MAC

FlexAddress 機能は、サーバー割り当ての MAC アドレスをシャーシ割り当ての MAC アドレスで置き換える機能で、ブレード LOM、メザニンカード、および I/O モジュールと共に、iDRAC6 に実装されています。iDRAC6 FlexAddress 機能はシャーシ内の iDRAC6 のスロットに固有の MAC アドレスの保存をサポートしています。シャーシ割り当ての MAC アドレスは、CMC の非揮発性メモリに格納され、iDRAC6 の起動時、または CMC FlexAddress ページの設定が変更された時に、iDRAC6 に送信されます。

CMC がシャーシ割り当ての MAC アドレスを有効にすると、iDRAC6 は以下の画面の **MAC アドレス** フィールドに値を表示します。

- 1 **システム** → **プロパティ** タブ → **システム詳細** → **iDRAC6 情報**
- 1 **システム** → **プロパティ** タブ → **WWN/MAC**
- 1 **システム** → **リモートアクセス** → **iDRAC6** → **プロパティ** タブ → **リモートアクセス情報** → **ネットワークの設定**
- 1 **システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ → **ネットワーク** → **ネットワークインタフェースカードの設定**

 **注意:** FlexAddress が有効な状態で、サーバー割り当ての MAC アドレスからシャーシ割り当ての MAC アドレスに切り替えた場合 (その逆も同様)、iDRAC6 IP アドレスも変更されます。

 **メモ:** FlexAddress 機能は CMC からのみ有効または無効にできません。iDRAC6 の GUI は状態のみを報告します。CMC FlexAddress ページで FlexAddress の設定を変更すると、既存の vKVM または vMedia のセッションがすべて終了します。

RACADM から FlexAddress を有効にする方法

iDRAC6 から FlexAddress を有効にすることはできません。CMC からスロットおよびファブリックレベルで FlexAddress を有効にします。

1. CMC コンソールから次の RACADM コマンドを使用し、管理下サーバーのスロットに対して FlexAddress を有効にします。

```
racadm setflexaddr -i <スロット番号> 1。ここで、<スロット番号> は、FlexAddress を有効にするスロットの番号です。
```

2. 次に、CMC コンソールから次の RACADM コマンドを実行し、ファブリックレベルで FlexAddress を有効にします。

```
racadm setflexaddr -f <ファブリック名> 1。ここで、<ファブリック名> は、A、B、または C です。
```

3. シャーシ内のすべての iDRAC6 に対して FlexAddress を有効にするには、CMC コンソールから次の RACADM コマンドを実行します。

```
racadm setflexaddr -f idrac 1
```

CMC RACADM サブコマンドの詳細については、『Dell Chassis Management Controller システム管理者リファレンスガイド』を参照してください。

リモートシスログ

iDRAC6 のリモートシスログ機能を使用すると、RAC のログとシステムイベントログ (SEL) を外部のシスログサーバーにリモートで書き込むことができます。サーバーファーム全体のすべてのログを中央ログから読むことができます。

リモートシスログプロトコルはユーザー認証を必要としません。ログをリモートシスログサーバーに入力するには、iDRAC6 とリモートシスログサーバー間に正しいネットワーク接続があり、リモートシスログサーバーが iDRAC6 と同じネットワークで実行していることを確認してください。リモートシスログのエントリは、リモートシスログサーバーのシスログポートに送信される UDP パケットです。ネットワーク障害が発生した場合、iDRAC6 は同じログを再送信しません。リモートのログ記録は、ログが iDRAC6 の RAC ログと SEL ログに記録されるときにリアルタイムで発生します。iDRAC6 のリモートシスログ設定は CMC から変更できます。


リモートシスログはリモートのウェブインタフェースから有効にできます。

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。
2. iDRAC6 ウェブインタフェースにログインします。
3. システムツリーで、システム → 設定 タブ → リモートシスログの設定 の順に選択します。リモートシスログの設定 画面が表示されます。

表 2-2 はリモートシスログの設定一覧です。

表 2-2 リモートシスログの設定

属性	説明
リモートシスログ有効	指定したサーバーのシスログの転送とリモートキャプチャを有効にするには、このオプションを選択します。シスログが有効になると、新しいログエントリがシスログサーバーに送信されます。
シスログサーバー 1 ~ 3	SEL ログや RAC ログなどの iDRAC6 のログメッセージをログ記録するリモートシスログサーバーのアドレスを入力します。シスログサーバーのアドレスには英数字、「-」、「.」、「:」、および「_」記号を使用できます。
ポート番号	リモートシスログサーバーのポート番号を入力します。ポート番号は 1 ~ 65535 の範囲で指定します。デフォルトは 514 です。


 **メモ:** リモートシスログプロトコルによって定義される重要度レベルは、標準的な IPMI システムイベントログ (SEL) の重要度と異なります。したがって、iDRAC6 リモートシスログのすべてのエントリが **注意** のレベルで報告されます。

次の例で、リモートシスログの設定を変更するための設定オブジェクトと RACADM コマンドの使い方を示します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogEnable [1/0] ; デフォルトは 0  
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer1 <サーバー名1> ; デフォルトは空白  
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer2 <サーバー名2>; デフォルトは空白  
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer3 <サーバー名3>; デフォルトは空白  
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPort <ポート番号>; デフォルトは 514
```

リモートファイル共有

iDRAC6 からリモートファイル共有 (RFS) 機能を使用すると、ネットワーク共有にある CD/DVD ISO イメージファイルを指定し、NFS または CIFS を使って CD または DVD としてマウントして、管理下サーバーのオペレーティングシステムで仮想ドライブとして使用可能にできます。

 **メモ:** この機能は IPv4 アドレスでのみ機能します。IPv6 アドレスは現在サポートされていません。

CIFS 共有イメージのパスは次の形式で指定します。

//<IP アドレスまたはドメイン名>/<共有名>/<イメージのパス>

NFS 共有イメージのパスは次の形式で指定します。


<IP アドレス>:/<イメージファイルのパス>

ユーザー名にドメイン名が含まれる場合、ユーザー名は <ユーザー名>@<ドメイン> の形式で入力する必要があります。たとえば、user1@dell.com は有効なユーザー名ですが、dell\user1 は有効なユーザー名ではありません。

IMG 拡張子が付くファイル名は、仮想フロッピーとしてリダイレクトされ、ISO 拡張子が付くファイル名は、仮想 CDROM としてリダイレクトされます。リモートファイル共有は、イメージファイル形式 .IMG と .ISO のみをサポートしています。

RFS 機能は、iDRAC6 の基礎となる仮想メディア実装を利用します。RFS のマウントを行うには、仮想メディアの権限が必要です。仮想ドライブが既に仮想メディアによって使用されている場合、同ドライブを RFS としてマウントすることはできません。その逆も同様です。RFS が機能するためには、iDRAC6 の仮想メディアは、連結 または 自動連結 モードになっている必要があります。

RFS の接続状態は、iDRAC6 ログでご覧になれます。接続が完了すると、RFS マウントされた仮想ドライブは、iDRAC6 からログアウトしても、切断されません。iDRAC6 がリセットされた、あるいはネットワーク接続が切断された場合に、RFS 接続が終了します。また、RFS 接続を終了するために、CMC で GUI およびコマンドラインオプションも利用できます。CMC からの RFS 接続は、iDRAC6 の既存の RFS マウントに常に優先します。

 **メモ:** iDRAC6 VFlash 機能と RFS には、関連性がありません

iDRAC ウェブインタフェースを介してリモートファイル共有を有効にするには、次のようにします。

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。
2. iDRAC6 ウェブインタフェースにログインします。
3. **システム** → **リモートファイル共有** タブの順に選択します。


リモートファイル共有 画面が表示されます。

[表 2-3](#) はリモートファイル共有の設定一覧です。

表 2-3 リモートファイルサーバーの設定

属性	説明
ユーザー名	NFS/CIFS ファイルシステムに接続するユーザー名。
パスワード	NFS/CIFS ファイルシステムに接続するパスワード。
イメージファイルのパス	リモートファイル共有を通して共有するファイルのパス。
状態	接続済み: ファイルが共有されています。 未接続: ファイルは共有されていません。 接続中... : 共有に接続中のビジー状態です。

ファイル共有の接続を確立するには、**接続** をクリックします。接続が確立した後、**接続** ボタンは無効になります。

 **メモ:** リモートファイル共有を設定した場合でも、セキュリティ上の理由から、GUI はこの情報を表示しません。


リモートファイル共有の場合、リモート RACADM コマンドは

racadm remotefileshare です。

racadm remotefileshare <オプション>

以下のオプションがあります。

- c: イメージを接続
- d: イメージを切断
- u <ユーザー名>: ネットワーク共有にアクセスするユーザー名
- p <パスワード>: ネットワーク共有にアクセスするパスワード
- l <イメージの場所>: ネットワーク共有上のイメージの場所 (場所を二重引用符で囲む)
- s: 現在の状態を表示

 **注意:** ユーザー名、パスワード、イメージの場所には、英数字と特殊文字を含むすべての文字を使用できますが、例外は '(一重引用符)'、'"(二重引用符)'、'(コンマ)'、<(小なり記号)'、>(大なり記号)の文字です。リモートファイル共有を使用するとき、上記の文字はユーザー名、パスワード、およびイメージの場所には使用できません。

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と、フラッシュメモリに新しいファームウェア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 iDRAC6 ウェブインタフェース
- 1 RACADM CLI
- 1 Dell アップデートパッケージ(Linux または Microsoft Windows 用)
- 1 DOS iDRAC6 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

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。


iDRAC6 ウェブインタフェースを使用して iDRAC6 ファームウェアをアップデートするか、CMC ウェブインタフェースを使用して iDRAC6 を復元するには、自動解凍アーカイブとしてパッケージ化されたバイナリイメージをダウンロードしてください。

管理下サーバーから iDRAC6 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 iDRAC6 のサーバーで稼動す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 iDRAC6 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 iDRAC6 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:** iDRAC6 ファームウェアのアップデートが開始すると、既存の iDRAC6 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を開始できません。


 **メモ:** シャーシのファンは iDRAC6 ファームウェアのアップデート中 100% で稼動します。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。

iDRAC6 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開いている管理ステーションにアクセス可能なディスク上に、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。「[iDRAC6 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:** iDRAC6 ウェブインタフェースを使用すると、iDRAC6 の設定を出荷時の設定にリセットすることもできます。

CMC ウェブインタフェースまたは CMC RACADM を使用して、iDRAC6 ファームウェアをアップデートできます。この機能は、iDRAC6 ファームウェアが通常モード、または破損している場合でも、利用できます。「[CMC を使用した iDRAC6 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:** ファームウェアアップデート中に設定を保存していない場合は、SSL 証明書の SHA1 キーと MD5 キーが新規生成されます。このキーは、開い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、iDRAC6 に接続しているブラウザウィンドウをすべて閉じる必要があります。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:** iDRAC6 ファームウェアを以前のバージョンに戻す場合は、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、Window ベースの管理ステーションにインストールされている既存の Internet Explorer ActiveX® ブラウザ プラグインを削除する必要があります。


Linux DUP の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. lists.us.dell.com に移動し、**Dell GPG 公開鍵** リンクをクリックして、Dell Linux の GnuPG 公開鍵を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、公開鍵を GPG 信頼データベースにインポートします。

```
gpg --import <公開鍵のファイル名>
```

 **メモ:** プロセスを完了するには秘密鍵が必要です。

3. 信頼できない鍵という警告を回避するには、Dell GPG 公開鍵の信用レベルを変更します。

- a. 次のコマンドを入力します。

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

- b. 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 (プライマリ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。

- c. 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.) (パスポートや異なるソースのフィンガープリントの確認などによって) 他のユーザーのキーを検証するうえで、このユーザーをどこまで信用するかを決定します。)

```
1 = I don't know or won't say (不明または判断できない)
2 = I do NOT trust (信用しない)
3 = I trust marginally (少しだけ信用する)
4 = I trust fully (全面的に信用する)
5 = I trust ultimately (絶対的に信用する)
m = back to the main menu (メインメニューに戻る)
```

Your decision? (どこまで信用しますか?)

- d. 「5」と入力し、<Enter> キーを押します。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))

- e. 「y」と入力し、<Enter> キーを押します。

- f. GPG キーエディタを終了するには、「quit」と入力し、<Enter> キーを押します。

公開鍵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デル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 と同じファイル名に .sign の拡張子が付いたものです。たとえば、iDRAC6 ファームウェアのイメージには、.sign ファイル (IDRAC_FRMW_LX_2.2.BIN.sign) が関連付けられ、ファームウェアイメージ (IDRAC_FRMW_LX_2.2.BIN) と共に自動解凍アーカイブに含まれています。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て、**名前を付けて保存** オプションを使用します。

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>
```

次の例では、Dell PowerEdge M610 iDRAC6 アップデートパッケージを検証する手順を示します。

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

```
1 IDRAC_FRMW_LX_2.2.BIN.sign
1 IDRAC_FRMW_LX_2.2.BIN
```

2. 次のコマンドラインを実行して公開鍵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: キー 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed (変更なし)
gpg: Total number processed (合計処理数): 1
gpg: unchanged (変更なし): 1
```

3. まだ設定していない場合は、Dell 公開鍵に対して、GPG 信頼レベルを設定します。

- 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. メニューから **絶対的に信頼する** を選択するには、「5」と入力し、<Enter> I trust ultimately (キーを押します。)

- d. 「y」と入力し、<Enter> キーを押します。

- e. GPG キーエディタを終了するには、「quit」と入力し、<Enter> キーを押します。

これで、Dell 公開鍵の検証が完了します。

4. 次のコマンドを実行して、Dell PowerEdge M610 iDRAC6 パッケージのデジタル署名を検証します。

```
gpg --verify iDRAC_FRMW_LX_2.2.BIN.sign iDRAC_FRMW_LX_2.2.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: Fri Jul 11 15:03:47 2008 CDT に DSA キー ID 23B66A9D  
で施された署名 )  
gpg: Good signature from "Dell, Inc. (Product Group) <linux-security@dell.com>" (gpg: "Dell, Inc. (Product Group) <linux-  
security@dell.com>" からの正しい署名)
```

手順 3 で示した方法でキーを検証していない場合は、次のような追加メッセージが表示されます。

```
gpg: WARNING: This key is not certified with a trusted signature! (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: There is no indication that the signature belongs to the owner. (gpg: この署名が所有者のものかどうか識別できません。)  
Primary key fingerprint (プライマリキーのフィンガープリント): 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
```


iDRAC6 ウェブインタフェースの使用


 **メモ:** 完了前に iDRAC6 ファームウェアアップデートの進行を中断すると、iDRAC6 ファームウェアの破損を招く恐れがあります。そのような場合は、CMC 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。アップデート中に、iDRAC6 設定を工場出荷時のデフォルト設定にリセットするオプションが提供されます。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。iDRAC6 設定ユーティリティを使用して、ネットワークを有効にして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始します。
2. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** の順に選択します。
3. **アップデート** タブをクリックします。

ファームウェアアップデート 画面が表示されます。

 **メモ:** ファームウェアをアップデートするには、iDRAC6 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 iDRAC6 は自動的にリセットされます。


4. **アップロード(ステップ 1/4)** セクションで、 **参照** をクリックし、ダウンロードしたファームウェアイメージを指定します。テキストフィールドにパスを入力することも可能です。例:

```
C:\Updates\V2.2\<イメージ名>
```

デフォルトのファームウェアイメージ名は `firming.lmc` です。


5. **アップロード** をクリックします。

ファイルが iDRAC6 にアップロードされます。これには、数分かかる場合があります。

 **メモ:** アップロード中にファームウェアのアップグレードプロセスを中断するには、**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、iDRAC6 が通常の動作モードにリセットされます。

アップロードが完了すると、**ファームウェアアップデート - 検証 (2/4 ページ)** 画面が表示されます。

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検証されたことを示すメッセージが表示されます。
1. イメージのアップロードに失敗、または検証チェックに合格しなかった場合、**ファームウェアアップデート** 画面に戻ります。再び iDRAC6 のアップグレードを試みるか、**キャンセル** をクリックして、通常の動作モードにリセットします。

 **メモ:** **設定の保存** チェックボックスをオフにすると、iDRAC6 が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 が無効になっているため、iDRAC6 ウェブインタフェースにログインできません。LAN 設定は、BIOS POST 中または CMC から iDRAC6 **設定ユーティリティ** を使用して再設定する必要があります。

6. デフォルトでは、アップグレード後も iDRAC6 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。
7. **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。
8. **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。
9. 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 ページ)** ウィンドウが表示され、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。

RACADM を使用した iDRAC6 ファームウェアのアップデート

リモート RACADM を使用して iDRAC6 ファームウェアをアップデートできます。

1. デルのサポートウェブサイト 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.imc
```

2. 次の RACADM コマンドを実行します。

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.imc` が保存されている TFTP サーバー上の場所です。

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 iDRAC6 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 iDRAC6 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。

- 1 `-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。
- 1 `-i=<ファイル名>` - ファームウェアイメージの名前を指定します。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。
- 1 `-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記録します。このオプションはデバッグに使用します。



メモ: `idrac16d` コマンドに誤ったパラメータを入力、または、`-h` オプションを追加した場合、追加オプションの `-nopresconfig` が利用可能になります。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、およびパスワードなどの既存の iDRAC6 設定情報がすべて削除されてしまうため、このオプションを**使用しない**ことをお勧めします。

ブラウザのキャッシュをクリアします。

iDRAC6 の最新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、システムに保管されている可能性のある古いウェブページを除去 / 削除してください。

USC 修復パッケージのアップデート

iDRAC6 ウェブインタフェースから USC 修復パッケージをアップデートする方法については、『Dell Lifecycle Controller ユーザーガイド』を参照してください。

IT Assistant で使用するために iDRAC6 を設定する

Dell OpenManage IT Assistant は、Simple Network Management Protocol (SNMP) バージョン 1 とバージョン 2c および Intelligent Platform Management Interface (IPMI) バージョン 2.0 に準拠した管理下デバイスを検出できます。


iDRAC6 は、IPMI v2.0 に準拠しています。本項では、iDRAC6 を IT Assistant で検出、監視するように設定する手順を説明します。これには、iDRAC6 設定ユーティリティを使用する方法と iDRAC6 のグラフィカルウェブインタフェースを使用する方法があります。

iDRAC6 設定ユーティリティを使用して検出と監視を有効にする方法

iDRAC6 が IPMI を検出して iDRAC6 設定ユーティリティレベルで警告トラップを送信するように設定するには、管理下サーバー(ブレード)を再起動し、iKVM とリモートモニタとキーボードかコンソールキーボードまたはシリアルオーバー LAN (SOL) 接続を使用して電源を入れる必要があります。リモートアクセスセットアップに `アクセスマスク <Ctrl> <E> for Remote Access Setup` (スするには `<ctrl> <E>` キーを押しますが)、表示されたら、`<Ctrl> <E>` キーを押します。


iDRAC6 **設定ユーティリティ** 画面が表示されたら、方向キーを使用して下へスクロールします。

1. **IPMI** オーバー LAN を有効にする
2. サイトの **RMCP+** **暗号化キー** を入力します (使用されている場合)。

 **メモ:** このオプションはセキュリティ保護を強化しますが、正しく機能するためにはサイト全体に導入するため、上級ネットワーク管理者または CIO とこのオプションの導入について話し合ってください。

3. **LAN パラメータ** で <Enter> キーを押して、サブ画面を開きます。画面内を移動するには、上下の矢印を使用します。
4. スペースバーを使って **LAN 警告有効** を **オン** にします。
5. 管理ステーションの IP アドレスを **警告送信先 1** に入力します。
6. データセンターの命名規則に従った名前の文字列を **iDRAC6 名** に入力します。デフォルトは iDRAC6-{サービスタグ} です。

<Esc>、<Esc> の次に <Enter> キーを押すと、iDRAC6 設定ユーティリティが終了して変更が保存されます。サーバーは通常の動作モードで起動し、IT Assistant の次の検出パス時に検出されます。

 **メモ:** 検出と監視を有効にするには、次世代 1 対多数のシステム管理アプリケーション、デル管理コンソールを使用することもできます。詳細については、デルのサポートウェブサイト support.dell.com/manuals で『Dell 管理コンソールユーザーズガイド』を参照してください。

iDRAC6 ウェブインターフェースを使用して検出と監視を有効にする方法

IPMI 検出は、リモートウェブインターフェースを使って有効にすることもできます。

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。
2. システム管理者権限のあるユーザー名とパスワードで、iDRAC6 ウェブインターフェースにログインします。
3. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** の順に選択します。
4. **ネットワーク / セキュリティ** タブをクリックします。
ネットワーク 画面が表示されます。
5. **IPMI の設定** をクリックします。
6. **IPMI オーバー LAN を有効にする** チェックボックスがオンになっていることを確認します。
7. **チャネル権限レベルの制限** ドロップダウンメニューから **システム管理者** を選択します。
8. サイトの **RMCP+ 暗号化キー** を入力します (使用されている場合)。
9. この画面で変更を加えた場合は、**適用** をクリックします。
10. システムツリーで **システム** を選択します。
11. **警告管理** タブをクリックして、**プラットフォームイベント** をクリックします。
プラットフォームイベント 画面が表示され、電子メール警告を生成するために、iDRAC6 に設定できるイベントの一覧が現れます。
12. **警告の生成** 列でチェックボックスを選択して、1 つまたは複数のイベントの電子メール警告を有効にします。
13. この画面で変更を加えた場合は、**適用** をクリックします。
14. **トラップの設定** をクリックします。
トラップの設定 画面が表示されます。
15. **IPv4 送信先リスト** セクションの最初の **送信先 IP アドレス** フィールドで、**有効** チェックボックスを選択し、管理ステーションの IP アドレスを入力します。
16. この画面で変更を加えた場合は、**適用** をクリックします。

トラップのテスト 行の **送信** リンクをクリックすることで、テストトラップを送信することができます。

デルでは、セキュリティ上、IPMI コマンドごとに固有のユーザーアカウントを作成し、IPMI オーバー LAN 特権およびパスワードを設定することを強くお勧めします。

1. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** の順に選択します。
2. **ネットワーク / セキュリティ** タブをクリックして **ユーザー** をクリックします。

ユーザー 画面が表示され、(定義済みまたは未定義の)すべてのユーザーが一覧になります。

- 未定義のユーザーの **ユーザー ID** をクリックします。

選択したユーザー ID の **ユーザー設定** 画面が表示されます。


- ユーザーを有効にする** チェックボックスを選択し、ユーザー名とパスワードを入力します。
- IPMI LAN 権限** セクションで、**付与する最大 LAN ユーザー特権** が **システム管理者** に設定されていることを確認します。
- 必要に応じて、他のユーザー権限も設定します。
- 新しいユーザー設定を保存するには、**適用** をクリックします。

IT Assistant を使用して iDRAC6 ステータスおよびイベントを表示する

検出が完了したら、iDRAC6 デバイスが **ITA デバイス詳細** 画面の **サーバー** カテゴリに表示されます。iDRAC6 の名前をクリックすると、その情報を表示できます。これは RAC グループに管理カードが表示される DRAC5 システムとは異なります。

iDRAC6 エラーと警告トラップが IT Assistant のプライマリ **警告ログ** に表示されるようになりました。**不明** カテゴリに表示されますが、トラップの説明と重要度は正確です。

データセンターを管理するために IT Assistant を使用する詳細については、『Dell OpenManage IT Assistant ユーザーズガイド』を参照してください。

 **メモ:** iDRAC6 の状態とイベントを表示するには、1 対多数のシステム管理アプリケーション、デル管理コンソールを使用することもできます。詳細については、デルサポートウェブサイト support.dell.com/manuals で『Dell 管理コンソールユーザーズガイド』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](#)

管理ステーションの設定

Integrated Dell™ Remote Access Controller (iDRAC6) Enterprise for Blade Servers バージョン 2.2 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](#)
- [管理ステーションへの iDRAC6 ソフトウェアのインストール](#)
- [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](#)
- [Dell 管理コンソールのインストール](#)

管理ステーションは、Dell PowerEdge™ サーバー、およびシャーシ内の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、iDRAC6 Enterprise 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。iDRAC6 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® ランタイム環境 (JRE) (Firefox を使用している場合に必要) をインストールします。
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)。
7. Dell Management Console (DMC) 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

iDRAC6 にアクセスするには、管理ステーションが「GB1」のラベルが付いた 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 iDRAC6 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するため、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。


iDRAC6 コンソールリダイレクト機能 ([「シリアルオーバー LAN の設定と使用」](#)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がない場合でも、管理下サーバーのコンソールにアクセスできます。また、コンピュータの再起動や iDRAC6 の機能の使用など、複数の管理機能を管理下サーバーに実行できます。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バーにアクセスするには、管理下サーバーに追加の NIC が必要な場合があります。

対応ウェブブラウザの設定

以下の項では、サポートされているウェブブラウザで iDRAC6 ウェブインタフェースを使用できるように設定する手順について説明します。

ウェブブラウザの開き方

iDRAC6 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で、サポートされているウェブブラウザから表示できるように設計されています。インタフェースを表示してすべての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 iDRAC6 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。
3. ツール → インターネットオプション → セキュリティ → ローカルネットワーク の順に選択します。
4. カスタムレベル をクリックします。
5. ドロップダウンメニューから 中低 を選択し、リセット をクリックします。OK をクリックして確定します。カスタムレベル ダイアログに戻るには、もう一度このボタンをクリックする必要があります。

6. Internet Explorer の異なるバージョンでは 中低 状態の設定が異なるため、ActiveX コントロールとプラグイン のセクションまでスクロールダウンし、各設定を確認します。

- 1 ActiveX コントロールに対して自動的にダイアログを表示: 有効にする
- 1 バイナリビヘイビアとスクリプトビヘイビア: 有効にする
- 1 署名された ActiveX コントロールのダウンロード: ダイアログを表示する
- 1 スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行: ダイアログを表示する
- 1 ActiveX コントロールとプラグインの実行: 有効にする
- 1 スクリプトを実行しても安全だとマークされている ActiveX のスクリプトの実行: 有効にする

ダウンロードのセクション:

- 1 ファイルのダウンロード時に自動的にダイアログを表示: 有効にする
- 1 ファイルのダウンロード: 有効にする
- 1 フォントのダウンロード: 有効にする

その他 のセクション:

- 1 ページの自動読み込み: 有効にする
- 1 Internet Explorer のウェブブラウザのコントロールのスクリプトの実行: 有効にする
- 1 サイズや位置の制限なしにスクリプトでウィンドウを開くことを許可する: 有効にする
- 1 既存のクライアント証明書が 1 つ、または存在しない場合の証明書の選択: 有効にする
- 1 IFRAME のプログラムとファイルの起動: 有効にする
- 1 拡張子ではなく、内容によってファイルを開く: 有効にする
- 1 ソフトウェアチャンネルのアクセス許可: 安全性 - 低
- 1 暗号化されていないフォームデータの送信: 有効にする
- 1 ポップアップブロックの使用: 無効にする

スクリプト セクション:

- 1 アクティブスクリプト: 有効にする
- 1 スクリプトによる貼り付け処理の許可: 有効にする
- 1 Java[®] アプレットのスクリプト: 有効にする

7. ツール → インターネットオプション → 詳細 の順に選択します。

8. 以下の項目にチェックが付いているか、いないかを確認します。

ブラウザ のセクション:

- 1 常に UTF-8 として URL を送信する: チェック付き
- 1 スクリプトのデバッグを使用しない(Internet Explorer): チェック付き
- 1 スクリプトのデバッグを使用しない(その他): チェック付き
- 1 スクリプトエラーごとに通知を表示する: チェックなし
- 1 オンデマンドでのインストールを有効にする(その他): チェック付き
- 1 ページの切り替えを行う: チェック付き
- 1 サードパーティ製のブラウザ拡張を有効にする: チェック付き
- 1 ショートカットの起動時にウィンドウを再使用する: チェックなし

HTTP 1.1 設定 セクション:

- 1 HTTP 1.1 を使用する: チェック付き

- 1 プロキシ接続で HTTP 1.1 を使用する:チェック付き

Java(Sun) セクション:

- 1 JRE 1.6.x_yz を使用する: チェック付き(任意選択、バージョンが異なることがある)

マルチメディア セクション:

- 1 自動的にイメージのサイズを変更する:チェック付き
- 1 ウェブページのアニメーションを再生する:チェック付き
- 1 ウェブページのサウンドを再生する:チェック付き
- 1 画像を表示する:チェック付き

セキュリティ セクション:

- 1 発行元証明書の取り消しを確認する:チェックなし
- 1 ダウンロードしたプログラムの署名を確認する:チェックなし
- 1 ダウンロードしたプログラムの署名を確認する:チェック付き
- 1 SSL 2.0 を使用する:チェックなし
- 1 SSL 3.0 を使用する:チェック付き
- 1 TLS 1.0 を使用する:チェック付き
- 1 無効なサイト証明書について警告する:チェック付き
- 1 保護付き/保護なしのサイト間を移動する場合に警告する:チェック付き
- 1 フォームの送信がリダイレクトされた場合に警告する:チェック付き



メモ: 上記のいずれかの設定を変更する場合は、その結果について事前に学び、理解しておくことをお勧めします。たとえば、ポップアップをブロックすると、iDRAC6 ウェブユーザーインターフェースの一部が正しく機能しなくなります。

9. **適用** をクリックし、**OK** をクリックします。
10. **接続** タブをクリックします。
11. **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。
12. **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。
13. **OK** を 2 度クリックします。
14. ブラウザを閉じてから再起動し、すべての変更が適用されることを確認します。

信用できるドメインリストへの iDRAC6 の追加

ウェブブラウザから iDRAC6 ウェブインターフェースにアクセスし、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可能性があります。完了したら、**更新** をクリックするか、ウェブブラウザを再起動して、iDRAC6 ウェブインターフェースへの接続を確立します。

一部のオペレーティングシステムでは、iDRAC6 IP アドレスが Internet Explorer (IE) 8 の信頼済みドメインのリストに含まれていなくても、同アドレスをリストに追加するように求められない場合があります。

IE8 の信頼済みドメインのリストに iDRAC6 IP アドレスを追加するには、次の手順を行います。

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** → **サイト** の順で選択します。
2. **この Web サイトをゾーンに追加する** に、iDRAC6 IP アドレスを入力します。
3. **追加** をクリックします。
4. **OK** をクリックします。
5. **閉じる** をクリックします。
6. **OK** をクリックし、ブラウザを更新します。

Active-X プラグインを使用した IE8 から初めて vKVM を起動する際、「証明書エラー: ナビゲーションはブロックされました」のメッセージが表示される場合があります。

1. **このサイトの閲覧を続行する** をクリックします。

2. **セキュリティ警告** ウィンドウで Active-X コントロールをインストールするには、**インストール** をクリックします。

VKM セッションが起動します。


他言語のウェブインタフェースの表示

iDRAC6 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の言語タイプを表します。その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、意図したように機能しない可能性があります。一部の対応言語ですべての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。

iDRAC6 ウェブインタフェースは、上記の言語専用ローカライズされたキーボードと連携するように設計されています。コンソールリダイレクトなど、iDRAC6 ウェブインタフェースの一部の機能を使用するには、特定の機能キーや文字にアクセスするための追加手順が必要になる場合があります。このような状況で、ローカライズされたキーボードを使用する方法の詳細については、[「ビデオビューアの使用」](#)を参照してください。その他のキーボードの使用はサポートされておらず、予想外の問題を引き起こす可能性があります。

 **メモ:** さまざまな言語の設定方法と、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方法については、ブラウザのマニュアルを参照してください。

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。

Linux クライアント上で簡体中国語 GUI 文字のセットを設定するには:

1. コマンド端末を開きます。
2. 次に locale を入力して <Enter> キーを押します。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 iDRAC6 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> キーを押します。
3. **プリファレンス名** 列で、`xpinstall.whitelist.required` を見つけてダブルクリックします。
プリファレンス名、**ステータス**、**タイプ**、**値** の値は太字になります。**ステータス** の値は `user set` に変わり、**値** の値は `false` に変わります。
4. **プリファレンス名** 列で、`xpinstall.enabled` を見つけます。
値 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 **値** を `true` に設定します。

管理ステーションへの iDRAC6 ソフトウェアのインストール

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。

1. DVD ルート - サーバーのセットアップとシステムのインストール情報を提供する Dell Systems Build and Update Utility が入っています。
1. SYSMGMT - Dell OpenManage Server Administrator など、システム管理ソフトウェアの製品が含まれます。

管理ステーションへの RACADM のインストールおよびアンインストール

リモート RACADM 機能を使用するには、管理ステーションに RACADM をインストールします。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への DRAC ツールのインストール方法については、support.dell.com/manuals にある『Dell OpenManage Management Station Software インストールガイド』を参照してください。

Linux への RACADM のインストールおよびアンインストール

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 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、iDRAC6 ソフトウェアのインストールに使用した RPM パッケージを指します。

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
```

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


 **メモ:** Internet Explorer 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、iDRAC6 ウェブインタフェースでコンソールビューアを起動前に設定すると、Firefox でも Java コンソールビューアを使用できます。詳細については、『[iDRAC6 ウェブインタフェースでのコンソールリダイレクトと仮想メディアの設定](#)』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 ビューア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 Java アプリケーションで、iDRAC6 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した後 Java Web Start を使用して起動します。


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` 拡張子タイプを Java Web Start アプリケーションに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** → **デスクトップの表示とテーマ** → **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:** ファイルには既に `PATH` 修正行が含まれている可能性があります。入力したパス情報によって競合が発生し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

デフォルトでは、iDRAC6 の Telnet サービスは無効、SSH サービスは有効になっています。Telnet プロトコルはセキュアではないため、SSH クライアントをインストールできない場合、ネットワーク接続のセキュリティが別の方法で保護されている場合にのみ使用してください。


 **メモ:** iDRAC6 は最大 4 つの Telnet セッションと 4 つの SSH セッションを同時にサポートします。

iDRAC6 のあるTelnet

Telnet は、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に、便利な機能が追加された市販またはフリーウェアの 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 SP1 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い、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もあります。

この問題を解決するには、Microsoft のサポートウェブサイト support.microsoft.com から修正プログラム `hotfix 824810` をダウンロードします。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。

 **メモ:** このホットフィックスが必要なのは Windows XP SP1 と Windows 2003 だけです。Windows XP SP2 が問題を解決しました。

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。ただし、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、以下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、以下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
```

iDRAC6 のある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セッションネゴシエーションと暗号化の機能を備えています。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。SSH は iDRAC6 上のデフォルトで有効になっています。

管理下サーバーの iDRAC6 に接続するには、管理ステーションで PuTTY や OpenSSH などのフリーウェアを使用できます。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、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、グラフィックスが表示されません)。

iDRAC6 は最大 4 つの Telnet セッションと 4 つの SSH セッションを同時にサポートします。ただし、それら 8 つのセッション中 1 つだけが SM-CLP を使用できます。つまり、iDRAC6 がサポートしているのは一度に 1 つの SM-CLP セッションのみです。セッションタイムアウトは、「[iDRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義](#)」で説明したように、`cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。

iDRAC6 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 暗号化スキーマ

スキーマの種類	スキーマ
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	<ul style="list-style-type: none">1 AES256-CBC1 RIJNDAEL256-CBC1 AES192-CBC1 RIJNDAEL192-CBC1 AES128-CBC1 RIJNDAEL128-CBC1 BLOWFISH-128-CBC1 3DES-192-CBC1 ARCFour-128
メッセージの整合性	<ul style="list-style-type: none">1 HMAC-SHA1-1601 HMAC-SHA1-961 HMAC-MD5-1281 HMAC-MD5-96
認証	<ul style="list-style-type: none">1 パスワード

TFTP サーバーのインストール

メモ: SSL 証明書の転送と新しい iDRAC6 ファームウェアのアップロードに iDRAC6 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。iDRAC6 とのファイル転送には、SM-CLP および RACADM コマンドラインインタフェースが併用されます。

iDRAC6 とのファイル複写が必要になるのは、iDRAC6 ファームウェアをアップデートしたとき、あるいは iDRAC6 の証明書をインストールするときだけです。これらのタスクを実行するときに RACADM を使用する場合は、iDRAC6 が IP アドレスまたは 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状態にあ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で `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、市販またはフリーウェアの 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 Tools and Documentation DVD
- 1 デルサポートウェブサイトと Readme ファイル: デル製品に関する最新情報については、Readme ファイルまたはデルサポートウェブサイト support.dell.com/manuals を参照してください。

IT Assistant のインストールについては、support.dell.com/manuals にある『Dell OpenManage IT Assistant ユーザーズガイド』を参照してください。

Dell 管理コンソールのインストール

Dell 管理コンソール (DMC) は 1 対多数のシステム管理に使用する次世代アプリケーションで、Dell OpenManage IT Assistant とよく似た機能を提供しますが、検出、資産管理、監視、レポート生成などの機能が強化されています。DMC はウェブベースの GUI で、ネットワーク環境で管理ステーションにインストールします。

DMC は『Dell Management Console DVD』からインストールするか、デルウェブサイト www.dell.com/openmanage からダウンロードできます。

このソフトウェアのインストール手順については、support.dell.com/manuals で『Dell 管理コンソールユーザズガイド』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](#)

管理下サーバーの設定

Integrated Dell™ Remote Access Controller (iDRAC6) Enterprise for Blade Servers バージョン 2.2 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の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

デル管理ソフトウェアには、次の機能が含まれています。

- 1 RACADM CLI - iDRAC6 の設定と管理ができます。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 Server Administrator - iDRAC6 の前回クラッシュ画面機能を使用する場合に必要なになります。
- 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。

『Dell Systems Management Tools and Documentation DVD』を使用して Dell OpenManage Server Administrator をインストールします。このソフトウェアのインストール方法については、support.dell.com/manuals にある『Dell OpenManage Server Administrator 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

iDRAC6 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。詳細については、『Dell OpenManage Server Administrator インストールガイド』および『Dell OpenManage 管理ステーションソフトウェアインストールガイド』を参照してください。これらの文書は、デルサポートウェブサイト support.dell.com/manuals から入手できます。
2. Windows を実行している場合は、Windows 起動と回復 画面の **自動的に再起動する** のチェックがオフになっ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. iDRAC6 ウェブインタフェースの **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。

iDRAC6 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 P リモートアクセス P iDRAC6P ネットワーク / セキュリティ タブ P サービス** の順でクリックし、**自動システムリカバリエージェント** 設定の見出しの下にある **有効** チェックボックスをオンにします。

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、管理下サーバー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** に設定します。

自動リカバリ タイマーの設定の詳細については、『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。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。デフォルト値は 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

iDRAC6 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、Windows Server または Windows Vista® を実行している管理下サーバーで **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. **自動再起動** チェックボックスを選択解除します。

5. **OK** を 2 回クリックします。

[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 iDRAC6 Enterprise の設定

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [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](#)
- [IPMI オーバー LAN を設定します。](#)
- [iDRAC6 ユーザーの追加と設定](#)
- [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](#)
- [Microsoft 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](#)
- [iDRAC6 サービスの設定](#)
- [iDRAC6 ファームウェアのアップデート](#)

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が可能なウェブインタフェースを提供します。通常は、ウェブインタフェースを使用して日常のシステム管理タスクを実行します。この章では、iDRAC6 のウェブインタフェースから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。

ウェブインタフェースを使用する設定タスクの大半は、ローカルおよびリモートの 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。リモート RACADM は、管理ステーションで実行するクライアントユーティリティで、帯域外のインタフェースを利用して管理下サーバーと通信します。このユーティリティを `-r` オプションと一緒に使用してネットワーク経由でコマンドを実行します。RACADM の詳細については、「[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 接続でリモートからアクセスできるシェルで実行されます。SM-CLP の詳細については、「[iDRAC6 Enterprise の使用 SM-CLP コマンドラインのインタフェース](#)」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。
2. **アドレス** フィールドに、`https://<iDRAC6 の 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://<iDRAC6 の IP アドレス>:<ポート番号>`

iDRAC6 IP アドレスは 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** ウィンドウが表示されます。

ログイン


iDRAC6 ユーザー、Microsoft® Active Directory® ユーザー、または LDAP 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。

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 iDRAC6 ユーザー名。

 **メモ:** 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`、`IT_user`、`john_doe` などです。

- 1 Active Directory (AD) ユーザー名。AD ドメイン名は、ドロップダウンメニューから選択することもできます。

Active Directory の名前には、<ドメイン>\<ユーザー名>、<ドメイン>/<ユーザー名> または <ユーザー>@<ドメイン> の形式を利用できます。大文字と小文字は区別されません。たとえば、`dell.com\john_doe` または `JOHN_DOE@DELL.COM` などです。あるいは、**ドメイン** フィールドにドメイン名を入力することも可能です。

- 1 LDAP ユーザー名(ドメイン名の入力なし)。


- 1 **パスワード** フィールドに、iDRAC6 ユーザーパスワード、Active Directory ユーザーパスワード、または LDAP パスワードのいずれかを入力します。パスワードは、大文字と小文字が区別されます。


- 1 **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隅にある **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:** ログインするまでは **ログアウト** ボタンが表示されません。

 **メモ:** 正常なログアウトをしないでブラウザを閉じると、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可能性があります。**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。

 **メモ:** Internet Explorer® 内で、ウィンドウ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。

 **注意:** <Ctrl+T> または <Ctrl+N> を使用して複数のウェブ GUI を開いて同じ管理ステーションから同じ iDRAC6 にアクセスした後で、いずれかのセッションからログアウトした場合、すべてのウェブ GUI セッションが終了します。

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。Microsoft Internet Explorer 6 はタブをサポートしないため、開いたブラウザウィンドウのそれぞれが新しい iDRAC6 ウェブインタフェースセッションになります。Internet Explorer (IE) 7 および IE 8 では、ウィンドウだけでなくタブを開くオプションもあります。各タブは、最後に開いたタブの特性を継承します。新しいタブを開くには <Ctrl+T> を押し、アクティブなセッションから新しいブラウザウィンドウを開くには <Ctrl+N> を押します。すでに認証済みの資格情報でログインします。いずれか 1 つのタブを閉じると、すべての iDRAC6 ウェブインタフェースタブが終了します。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、システム管理者権限で別のタブにログインすると、開いている両方のタブがシステム管理者権限を持ちます。

Firefox 2 と Firefox 3 のタブの動作は、IE 7 と IE 8 と同様で、新しいタブは新しいセッションです。ただし、Firefox でのウィンドウの動作は異なります。Firefox のウィンドウは、最後に開かれたウィンドウと同じ権限で動作します。たとえば、1 つの Firefox ウィンドウがパワーユーザー権限で開かれ、別のウィンドウがシステム管理者権限で開かれた場合、両ユーザーは管理者権限を持つこととなります。


表 5-1 対応ブラウザでのユーザー権限動作


ブラウザ	タブの動作	ウィンドウの動作
Microsoft Internet Explorer 6	なし	新しいセッション
Microsoft IE7 と IE8	最後に開かれたセッションから	新しいセッション
Firefox 2 と Firefox 3	最後に開かれたセッションから	最後に開かれたセッションから

iDRAC6 NIC の設定

ここでは、iDRAC6 が既に設定され、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。iDRAC6 ネットワークの初期設定については、「[iDRAC6 ネットワークの設定](#)」を参照してください。

ネットワーク、IPMI、VLAN 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。

 **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(たとえば iDRAC6)が DHCP ネゴシエーション中に提供する必要があります。iDRAC6 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。

1. システム → リモートアクセス → iDRAC6 の順にクリックします。
2. ネットワーク / セキュリティ タブをクリックします。
ネットワーク 画面が表示されます。
3. 必要に応じて、ネットワーク、IPMI、および VLAN を設定します。ネットワーク、IPMI、および VLAN の設定 オプションの説明は、「[表 5-2](#)」、「[表 5-3](#)」、および「[表 5-4](#)」を参照してください。
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 5-2 ネットワークの設定

設定	説明
ネットワークインタフェースカードの設定	
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 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と、ネットワーク経由の iDRAC6 とのすべての通信がブロックされます。

	デフォルトは チェックボックスがオフ です。
共通設定	
IDRAC6 を DNS に登録する	DNS サーバーに IDRAC6 の名前を登録します。 デフォルトは チェックボックスがオフ です。
DNS IDRAC6 名前	IDRAC6 の名前を表示します。デフォルト名は idrac-service_tag で、service_tag はデルサーバーのサービスタグ番号です。例: IDRAC-HM8912S
DNS ドメイン名に DHCP を使用	チェックボックスがオン : DHCP からの DNS 取得を有効にします。 チェックボックスがオフ : DHCP からの DNS 取得を無効にします。
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オンの場合、この オプションはグレー表示になっており、フィールドの内容を変更できません。
IPv4 の設定	
有効	IPv4 プロトコルのサポートを有効(チェックボックスがオン)または無効(チェックボックスがオフ)にします。この設定をアクティブにするには、NIC を 有効にする オプションをオンにする必要があります。
DHCP 有効	チェックボックスがオン の場合、Server Administrator は IDRAC6 NIC の IP アドレスを DHCP サーバーから取得します。また、 IP アドレス、サブネットマスク、および ゲートウェイ のフィールドも無効にします。
IP アドレス	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 有効 オプションを選択解除します。
サブネットマスク	IDRAC6 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、 DHCP 有効 オプションを選択解除します。
ゲートウェイ	IDRAC6 NIC の静的 IPv4 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 有効 オプションを選択解除します。
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オンにして DNS サーバーのアドレスを取得するには、 DHCP 有効 オプションを選択します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、 優先 DNS サーバー フィールドと 代替 DNS サーバー フィールドに IP アドレスを入力します。
優先 DNS サーバー	優先 DNS サーバーの静的 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、最初に DHCP を使用して DNS サーバーアドレスを取得する オプションを選択解除します。
代替 DNS サーバー	二次 DNS サーバー IP アドレスは、 DHCP を使用して 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。
IPv6 の設定	
有効	チェックボックスがオン の場合は、IPv6 が有効になります。 チェックボックスがオフ の場合は、IPv6 が無効になります。デフォルトは チェックボックスがオフ です。
自動構成有効	このチェックボックスをオンにすると、iDRAC6 は動的ホスト設定プロトコル(DHCPv6)サーバーから iDRAC6 NIC の IPv6 アドレスを取得できます。 自動構成有効 を有効にすると、 IPv6 アドレス、プレフィックス長、および ゲートウェイ の静的な値も無効にして消去します。
IPv6 アドレス	iDRAC6 NIC の IPv6 アドレスを設定します。この設定を変更するには、まず関連付けられたチェックボックスをオフにして 自動構成有効 を無効にする必要があります。 メモ : ネットワーク設定で IPv6 DHCP が構成されている場合、表示されるのは 2 つの IPv6 アドレス(リンクローカルアドレスとグローバルアドレス)だけで、ネットワークルータがルータアダプタサイズメントメッセージを送信するように設定されている場合は 16 の IPv6 アドレスすべてが表示されます。 メモ : 8 を超えるグループから成る IPv6 アドレスを入力した場合は、設定を保存できません。
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、まず関連付けられたチェックボックスをオフにして 自動構成有効 を無効にする必要があります。
ゲートウェイ	iDRAC6 NIC の静的な IPv6 ゲートウェイを設定します。この設定を変更するには、まず関連付けられたチェックボックスをオフにして 自動構成有効 を無効にする必要があります。
DHCPv6 を使用して DNS サーバーアドレスを取得する	DHCPv6 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ンにし、DHCP を有効にして IPv6 DNS サーバーの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、 優先 DNS サーバー フィールドと 代替 DNS サーバー フィールドに IP アドレスを入力します。デフォルト値は チェックボックスがオフ です。 メモ : DHCPv6 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オンの場合は、 優先 DNS サーバー フィールドと 代替 DNS サーバー フィールドに IP アドレスを入力できません。
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、 DHCPv6 を使用して DNS サーバーアドレスを取得する を選択解除します。
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、 DHCPv6 を使用して DNS サーバーアドレスを取得する を選択解除します。

表 5-3 IPMI 設定

設定	説明
IPMI オーバー LAN を有効にする	選択されていると、IPMI LAN チャンネルが有効であることを示します。デフォルトは チェックボックスがオフ です。
チャンネル権限レベルの制限	LAN チャン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、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 です。
暗号化キー	暗号化キーを設定します。暗号化キーは、40 文字までの偶数の 16 進数で指定します。デフォルトの IPMI 暗号化キーはすべてゼロです。

表 5-4 VLAN の設定


--	--

ボタン	説明
VLAN ID を有効にする	はい:有効になります。いいえ:無効になります。有効の場合は、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。 メモ: VLAN 設定は CMC ウェブインタフェースからのみ設定できます。iDRAC6 は現在の有効状態を表示するだけで、この画面で設定を変更することはできません。
VLAN ID	802.1g フィールドの VLAN ID フィールド。4001 ~ 4020 を除く 1 ~ 4094 の値を表示します。
優先度	802.1g フィールドの 優先度 フィールド。これは VLAN ID の優先順位の識別に使用され、VLAN 優先順位として 0 ~ 7 の値を表示します。

表 5-5 ネットワーク設定のボタン

ボタン	説明
詳細設定	ネットワークセキュリティ画面を表示します。ここで IP 範囲と IP ブロックの属性を入力できます。
印刷	画面に表示される ネットワーク 設定の値を印刷します。
更新	ネットワーク画面を再ロードします。
適用	ネットワーク設定画面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 アドレス設定を使用して iDRAC6 ウェブインタフェースに再接続する必要があります。その他の変更でも、NIC をリセットする必要があるため、このため接続が一時的に途絶える場合があります。

IP フィルタと IP ブロックの設定

 **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 → リモートアクセス → iDRAC6 の順にクリックします。
2. ネットワーク / セキュリティ タブをクリックします。
ネットワーク画面が表示されます。
3. 詳細設定 をクリックします。
ネットワークセキュリティ画面が表示されます。
4. 必要に応じて、IP フィルタおよびブロック設定を行います。IP フィルタおよびブロック 設定の説明については、「表 5-6」を参照してください。
5. 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 5-7を参照してください。

表 5-6 IP フィルタとブロックの設定

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。これにより、iDRAC6 にアクセスできる IP アドレスの範囲を定義できます。デフォルトは 無効 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 無効 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帯	ここで指定した時間帯(秒)内に IP ブロックエラーカウントが制限値を超えると、IP ブロックペナルティ時間がトリガされます。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 5-7 ネットワークセキュリティのボタン

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 画面を再ロードします。
適用	ネットワークセキュリティ 画面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る	ネットワーク 画面に戻ります。

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 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 5-8 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 5-8 フィルタ可能なプラットフォームイベント

インデックス	プラットフォームイベント
1	バッテリーブロープ警告
2	バッテリーブロープエラー
3	離散的電圧ブロープエラー
4	温度ブロープ警告
5	温度ブロープエラー
6	プロセッサエラー
7	プロセッサがありません
8	ハードウェアログエラー
9	自動システム回復
10	SD カードの不具合
11	冗長性喪失


プラットフォームイベント(たとえば、バッテリーブロープ警告)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、有効になっ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は、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処置(システムの再起動など)を実行するように設定すると、その処置が実行されます。


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を設定する前に、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. iDRAC6 ウェブインタフェースにログインします。
2. **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 画面が表示されます。
3. 警告を生成するイベントごとに、その横にある **警告の生成** オプションを選択します。

 **メモ:** **警告の生成** 列見出しの横にあるチェックボックスをクリックすると、すべてのイベントの 警告生成を有効または無効にできます。

4. 各イベントに対し、有効にする動作の下にあるラジオボタンをクリックします。各イベントに対して、一つの動作しか選択できません。
5. **適用** をクリックします。

 **メモ:** イベントの警告が送信されるには、そのイベントの **警告の生成** チェックボックスをオン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 警告を追加または有効 / 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. iDRAC6 ウェブインタフェースにログインします。

- 必ず「[プラットフォームイベントフィルタ\(PEF\)の設定](#)」の手順に従ってください。
- 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 画面が表示されます。
- トラップの設定** をクリックします。
トラップの設定 画面が表示されます。
- 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オンにします。
 - 該当する IPv4 または IPv6 の **送信先 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 iDRAC6 コミュニティ文字列と同じである必要があります。

- 適用** をクリックします。

 **メモ:** トラップを正しく送信するには、**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、iDRAC6 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され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 iDRAC6 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。

- 設定した警告をテストするには、**送信** をクリックします。
- 宛先 IP アドレスを追加するには、「[手順_a](#)」から「[手順_d](#)」の手順を繰り返します。最大 4 個の IPv4 アドレスと最大 4 個の IPv6 送信先アドレスを指定できます。

電子メール警告の設定


- iDRAC6 ウェブインタフェースにログインします。
- 必ず「[プラットフォームイベントフィルタ\(PEF\)の設定](#)」の手順に従ってください。
- 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 画面が表示されます。
- 電子メール警告の設定** をクリックします。
電子メール警告の設定 画面が表示されます。
- 電子メール警告の宛先を指定します。
 - 最初の未定義の電子メール警告に対して、**有効** チェックボックスを選択します。
 - 送信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、**電子メール警告設定** 画面で **SMTP(電子メール)サーバーアドレス設定** セクションの SMTP(電子メール)サーバーを設定する必要があります。提供されるフィールドに、ドット区切り形式(例:192.168.1.1)または DNS 名で SMTP サーバーを指定します。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 iDRAC6 と通信して電子メール警告を送信します。

- 電子メールの差出人名を変更する** フィールドに、電子メール警告の差出人を入力します。デフォルトの差出人を使用する場合は、空白のままにします。デフォルトは、blade_slot@iDRAC6 IP アドレスです。
 - 電子メールの差出人名を変更する** フィールドが空白で、iDRAC6 ホスト名が設定されており、かつ DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<iDRAC6 ホスト名>@<DNS ドメイン名> となります。
 - フィールドと iDRAC6 ホスト名が共に空白で、DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<iDRAC6 Slotx>@<DNS ドメイン名> となります。
 - フィールド、iDRAC6 ホスト名、および DNS ドメイン名が空白の場合、差出人の電子メールアドレスは、<iDRAC6 Slotx>@<iDRAC6 IP アドレス> となります。
 - フィールドに @ マークがない文字列が入力され、DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<@ が含まれない文字列>@<DNS ドメイン名> となります。
 - フィールドに @ マークがない文字列が入力され、DNS ドメイン名が空白の場合、差出人の電子メールアドレスは、<@ が含まれない文字列>@<iDRAC6 IP アドレス> となります。
 - フィールドに @ マークがない文字列が入力され、DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<@ が含まれない文字列>@<DNS ドメイン名> となります。
 - フィールドに @ マークを含んだ文字列が入力され、DNS ドメイン名が空白の場合、差出人の電子メールアドレスは、<@ を含んだ文字列>@<iDRAC6 IP アドレス> となります。
- 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。
- 電子メール警告の送信先を追加するには、「[手順_a](#)」から「[手順_e](#)」の手順を繰り返します。電子メール警告の送信先は、最大 4 つまで指定できます。

IPMI オーバー LAN を設定します。

- iDRAC6 ウェブインタフェースにログインします。
- IPMI オーバー LAN を設定します。
 - システム** > **リモートアクセス** > **iDRAC6** 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。
ネットワーク 画面が表示されます。
 - IPMI の設定** をクリックします。
 - IPMI オーバー LAN を有効にする** チェックボックスを選択します。
 - 必要に応じて、**チャネル権限レベルの制限** 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 規格を参照してください。

IPMI の設定 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、**システム管理者**、**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。


- 必要に応じて、IPMI LAN チャネルの暗号化キーを設定します。

 **メモ:** iDRAC6 IPMI は RMCP+ プロトコルに対応しています。

IPMI の設定 の **暗号化キー** フィールドに暗号化キーを入力します。

- 適用** をクリックします。

- IPMI シリアルオーバー LAN (SOL)を設定します。
 - システム** > **リモートアクセス** > **iDRAC6** 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。
ネットワーク 画面が表示されます。
 - シリアルオーバー LAN** タブをクリックします。
 - シリアルオーバー LAN を有効にする** を選択します。
 - 必要に応じて、**ボーレート** ドロップダウンメニューからデータ速度を選択して、IPMI SOL の **ボーレート** を更新します。


 **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 **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。


- 適用** をクリックします。
- 必要に応じて、**詳細設定** ページで IP フィルタとブロックの設定を指定します。

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

- システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **ユーザー** をクリックします。
ユーザー 画面には、各ユーザーの **ユーザー ID**、**状態**、**ユーザー名**、**IPMI LAN 権限**、iDRAC6 権限、および **シリアルオーバー LAN 機能** 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、設定できません。
- 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(「[表 5-9](#)」、「[表 5-10](#)」、および「[表 5-11](#)」を参照)では、ユーザーの設定、SSH 公開キーファイルのアップロード、指定した SSH キーまたはすべての SSH キーを表示あるいは削除することができます。

SSH 経由の公開キー認証

iDRAC6 では、SSH 経由の公開キー認証(PKA)もサポートされています。この認証方法を使用すると、ユーザー ID / パスワードの組み込みや入力を行う必要がないため、SSH スクリプトの自動化

が向上します。

作業を開始する前に

SSH インタフェースを介して使用できる公開キーをユーザーごとに最大 4 つ設定できます。公開キーを追加または削除する前に、表示コマンドを使って設定済みのキーを確認してください。これは、キーを誤って上書きしたり削除したりするのを防ぐためです。SSH 経由の PKA を設定し、正しく使用すると、iDRAC6 へのログイン時にパスワードを入力する必要がなくなります。これは、自動化されたスクリプトを設定してさまざまな機能を実行する場合に便利です。

この機能の設定準備をする際は、以下の点に気をつけてください。

- 1 この機能は、RACADM、そして GUI から管理できます。
- 1 新しい公開キーを追加する場合は、追加時に既存のキーがインデックスにないことを確認します。iDRAC6 では、新しいキーを追加する前に、前のキーが削除されているかどうかの確認作業は行われません。新しいキーを追加すると、SSH インタフェースが有効な間、自動的に有効になります。

Windows 用の公開キーの生成

アカウントを追加する前に、SSH 経由で iDRAC6 にアクセスするシステムで公開キーが必要になります。公開 / 秘密キーのペアを生成する方法は 2 通りあります。1 つは、Windows が稼動するクライアントに対して PuTTY キージェネレータ アプリケーションを使用する方法で、もう 1 つは、Linux が稼動するクライアントに対して ssh-keygen CLI を使用する方法です。ssh-keygen CLI ユーティリティは、すべての標準インストールにデフォルトで付いています。

この項では、両方のアプリケーションで使用する公開 / 秘密キーペアを生成する簡単な手順について説明します。これらのツールの使用法の詳細については、アプリケーションヘルプを参照してください。

Windows クライアント用の PuTTY キージェネレータを使用して基本キーを作成する場合:


1. アプリケーションを起動し、生成するキータイプとして SSH-2 RSA または SSH-2 DSA のいずれかを選択します。SSH-1 はサポートされていません。
2. キーのビット数を入力します。サポートされるキー生成アルゴリズムは、RSA と DSA のみです。RSA の場合は、768 ~ 4096 の間のビット数、DSA の場合は 1024 ビットにする必要があります。
3. **生成** をクリックし、指示に従ってマウスをウィンドウ内に移動します。キーを作成したら、キーコメントフィールドを変更できます。パスフレーズを入力すると、キーをセキュリティ保護することもできます。プライベートキーを必ず保存します。
4. 公開キーファイルを後でアップロードできるように、**公開キーを保存する** オプションを使用して公開キーをファイルに保存できます。アップロードされるすべてのキーは、RFC4716 または openSSH 形式である必要があります。これら形式になっていない場合は、変換する必要があります。

Linux 用の公開キーの生成

Linux クライアント用の ssh-keygen アプリケーションは、グラフィカルユーザーインタフェースのないコマンドラインツールです。

ターミナルウィンドウを開き、シェルプロンプトで次を入力します。

```
ssh-keygen -t rsa -b 1024 -C testing
```

 **メモ:** オプションは、大文字と小文字を区別します。


ここで、


-t は dsa または rsa です。

-b オプションは 768~4096 の間で、ビット暗号化サイズを指定します。

-C オプションを使用すると、公開キーコメントを変更できます。これはオプションです。

コマンドが実行されたら、公開キーファイルをアップロードします。

 **メモ:** ssh-keygen を使用して Linux 管理ステーションから生成されたキーは、RFC4716 ではなく、openSSH 形式になっています。openSSH 公開キーは、iDRAC6 にアップロードすることができます。iDRAC6 公開キーアルゴリズムは、openSSH と RFC4716 キーのどちらも検証し、RFC4716 キーを openSSH 形式に変換して、キーを内部に保管します。

 **メモ:** iDRAC6 は、ssh-agent によるキーの転送をサポートしていません。

公開キー認証を使用したログイン

公開キーがアップロードされたら、パスワードを入力せずに、SSH 経由で iDRAC6 にログインすることができます。また、1 つの RACADM コマンドをコマンドライン引数として SSH アプリケーションに送信することも可能です。コマンドラインオプションは、セッションがコマンドの完了時に終了するという点で、リモート RACADM と同じように動作します。

例:

ログイン

```
ssh username@<ドメイン>
```

または

ssh username@<IP アドレス>

<IP アドレス> には、iDRAC6 の IP アドレスを指定します。

RACADM コマンドの送信:

ssh username@<ドメイン> racadm getversion

ssh username@<ドメイン> racadm getsel

RACADM を使用した SSH キーのアップロード、表示、および削除方法については、「[RACADM を使用した SSH キーのアップロード、表示、および削除](#)」を参照してください。

表 5-9 SSH キー設定

オプション	説明
SSH キーのアップロード	ローカルユーザーが SSH 公開キーファイルをアップロードできます。キーがアップロードされると、 ユーザー設定 ページの編集不可のテキストボックスに、キーファイルの内容が表示されます。
SSH キーの表示 / 削除	ローカルユーザーが指定した SSH キー、またはすべての SSH キーを表示または削除できます。

SSH キーのアップロード ページでは、SSH 公開キーファイルをアップロードできます。キーがアップロードされると、SSH キーの表示 / 削除 ページの編集不可のテキストボックスに、キーファイルの内容が表示されます。

表 5-10 SSH キーのアップロード

オプション	説明
ファイル / テキスト	ファイル オプションを選択し、キーの保存場所へのパスを入力します。 テキスト オプションを選択して、ボックスにキーファイルの内容を貼り付けることもできます。新しいキーをアップロード、または既存のキーを上書きできます。キーファイルをアップロードするには、 参照 をクリックしてファイルを選択し、 適用 ボタンをクリックします。 メモ: キーテキストを貼り付けるオプションは、openSSH 形式の公開キーでサポートされています。RFC4716 形式のキーでは、テキストを貼り付けるオプションはサポートされていません。
参照	キーの完全パスとファイル名を指定するには、このボタンをクリックします。

SSH キーの表示 / 削除 ページでは、ユーザーの SSH 公開キーを表示または削除できます。

表 5-11 SSH キーの表示 / 削除

オプション	説明
削除	アップロードされたキーはボックスに表示されています。既存のキーを削除するには、 削除 オプションを選択して、 適用 をクリックします。

1. **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。

2. **ユーザーの設定** 画面で、ユーザーのプロパティと権限を設定します。

[表 5-12](#)は、iDRAC6 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 5-13](#) 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 5-14](#) では、IPMI LAN 権限 と iDRAC6 **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 5-15](#)では、iDRAC6 **グループ**権限について説明しています。iDRAC6 **ユーザー権限** を **システム管理者**、**パワーユーザー**、または **ゲストユーザー** に追加すると、iDRAC6 **グループ**が **カスタム** グループに変わります。

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 5-16](#)」参照してください。

表 5-12 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	チェックボックスをオン にすると、iDRAC6 へのユーザーのアクセスが有効になります。 チェックボックスをオフ にすると、ユーザーアクセスが無効になります。
ユーザー名	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。

	<p>メモ: iDRAC6 のユーザー名には、@、#、\$、%、/、. (ピリオド)の文字を含めることはできません。また、大文字と小文字は区別されます。</p> <p>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。</p>
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。選択解除すると、ユーザーのパスワードを変更できません。
新しいパスワード	iDRAC6 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。
	<p>メモ: <、>、\ などの特殊文字は使用不可で、ユーザーパスワードの作成時にブロックされます。</p>
新しいパスワードの確認	確認のために、iDRAC6 ユーザーのパスワードを再入力します。

表 5-13 IPMI LAN 権限

プロパティ	説明
LAN ユーザーに許可する最大権限	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、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。チェックボックスをオンにすると、権限が有効になります。

表 5-14 その他の権限

プロパティ	説明
iDRAC6 グループ	ユーザーの最大 iDRAC6 ユーザー権限を システム管理者、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。 iDRAC6 グループ 権限については、「 表 5-15 」を参照してください。
iDRAC6 へのログイン	iDRAC6 にログインできます。
iDRAC6 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。 注意: SSH キーのアップロード、表示、および削除の各機能は、「ユーザーの設定」ユーザー権限に基づきます。この権限を持つユーザーは、他のユーザーの SSH キーを設定することができます。SSH キーは非常に重要であるため、この権限の付与は慎重に行ってください。
ログのクリア	ユーザーが 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	現在設定されている警告受信者にユーザーがテスト警告(電子メールと PET)を送信できます。
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 5-15 iDRAC6 グループ権限

ユーザーグループ	許可する権限
管理者	iDRAC6 へのログイン、iDRAC6 の設定、ユーザーの設定、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。
パワーユーザー	iDRAC6 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。
ゲストユーザー	iDRAC6 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。iDRAC6 へのログイン、iDRAC6 の設定、ユーザーの設定、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。
なし	権限の割り当てなし

表 5-16 ユーザー設定のボタン

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 画面を再ロードします。
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	ユーザー画面 に戻ります。

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)

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。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、デフォルトでデルの署名付き SSL デジタル証明書(サーバー ID)があります。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、大手認証局(CA)によって署名された証明書に置き換えてください。認証局(CA)は、IT 業界で認知されたビジネス組織で、信頼性の高い審査、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 の例としては、Thawte® と VeriSign® が挙げられます。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 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。セキュアサーバー証明書を使用すると、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されたセッションを交渉できます。

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存されている CSR 情報が、証明書に含まれている情報と一致する必要があります。つまり、証明書は iDRAC6 で作成された CSR に則して生成されている必要があります。

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 → iDRAC6 → 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 画面を開きます。

[表 5-17](#) 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 5-18](#) に、SSL メインメニュー 画面上のボタンについて説明します。

表 5-17 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 画面を開きます。 メモ: 新しい CSR はそれぞれ、ファームウェアの以前の 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 画面を開き、CA から送信された 証明書をアップロードします。 メモ: 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。

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 画面を開き、既存のサーバー証明書を表示します。
------------	--

表 5-18 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 の値を印刷します。
更新	SSL 画面を再ロードします。
次へ	SSL 画面の情報を処理し、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、iDRAC6 は証明書を受け入れません。

- SSL 画面で、**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** 画面で、各 CSR 属性の値を入力します。
[表 5-19](#) に、**証明書署名要求 (CSR) の生成** 画面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。
- ダウンロード** をクリックして CSR ファイルをリモート管理ステーションに保存します。
- 適切なボタンをクリックして続行します。「[表 5-20](#)」を参照してください。

表 5-19 証明書署名要求 (CSR) の生成のオプション


フィールド	説明
共通名	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、スペース、ハイフン、アンダースコア、ピリオドのみが有効です。
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、アンダースコア、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、アンダースコア、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市または地域 (たとえば Kobe)。英数字とスペースのみが有効です。アンダースコア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 Texas)。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。会社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。このフィールドは省略可能です。
キーサイズ	生成する証明書署名要求 (CSR) キーのサイズ。サイズの選択肢は 1024 KB または 2048 KB です。

表 5-20 証明書署名要求 (CSR) の生成のボタン

ボタン	説明
印刷	画面に表示されている 証明書署名要求の生成 の値を印刷します。
更新	証明書署名要求 (CSR) の生成 画面を再ロードします。
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 画面に戻ります。

サーバー証明書のアップロード

- SSL 画面で **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 画面が表示されます。
- ファイルパス** 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、管理ステーションの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 5-21」を参照してください。

表 5-21 証明書のアップロードのボタン

ボタン	説明
印刷	証明書のアップロード 画面に表示されている値を印刷します。
更新	証明書のアップロード 画面を再ロードします。
適用	証明書を iDRAC6 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 画面に戻ります。

サーバー証明書の表示

1. SSL 画面で **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 5-22 に、サーバー証明書の表示 ウィンドウに表示されるフィールドとその説明を示します。
2. 適切なボタンをクリックして続行します。「表 5-23」を参照してください。



表 5-22 サーバー証明書情報の表示

フィールド	説明
シリアル番号	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 5-23 サーバー証明書の表示のボタン

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 画面を再ロードします。
SSL メインメニューに戻る	SSL メインメニュー 画面に戻ります。

Microsoft 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、「[iDRAC6 ディレクトリサービスの使用](#)」を参照してください。

Microsoft Active Directory 概要画面にアクセスするには、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** → **Microsoft Active Directory** の順でクリックします。

表 5-24 に、Active Directory 概要のオプションを一覧にします。適切なボタンをクリックして続行します。

表 5-24 Active Directory のオプション

フィールド	説明
共通設定	共通して設定される Active Directory の設定を表示します。
Active Directory CA 証明書	すべてのドメインコントローラの SSL サーバー証明書に署名をする CA の証明書を表示します。
標準スキーマの設定 / 拡張スキーマの設定	Active Directory の設定によって、拡張スキーマの設定または標準スキーマの設定が表示されます。
Active Directory の設定	Active Directory の設定で手順 1/4 を設定するには、このオプションをクリックします。Active Directory 手順 1/4 ページでは、Active Directory の CA 証明書を iDRAC6 にアップロードしたり、iDRAC6 にアップロードされた現在の Active Directory CA 証明書を表示したり、証明書の検証を有効にしたりできます。

設定のテスト	指定した設定を使用して Active Directory の設定をテストするには、このオプションをクリックします。
Kerberos Keytab のアップロード	iDRAC6 に Kerberos Keytab をアップロードするには、このオプションをクリックします。keytab ファイルの作成方法については、「 Kerberos 認証を有効にする方法 」を参照してください。

表 5-25 Active Directory のボタン

ボタン	定義
印刷	画面に表示されている Active Directory の値を印刷します。
更新	Active Directory 画面を再ロードします。

Active Directory の設定 (標準スキーマと拡張スキーマ)

- Active Directory 概要画面で、Active Directory の設定 をクリックします。
- Active Directory 手順 1/4 画面で、証明書の検証を有効にしたり、iDRAC6 で Active Directory CA 証明書をアップロードしたり、現在の Active Directory CA 証明書を表示したりできます。

[表 5-26](#) に、Active Directory の設定と管理 プロセスのステップごとの設定と選択項目について説明します。適切なボタンをクリックして続行します。

表 5-26 Active Directory 設定の設定

設定	説明
Active Directory の設定と管理 手順 1/4	
証明書検証が有効	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。 チェックボックスをオン にすると、証明書の検証が有効になります。iDRAC6 は Active Directory への接続中、SSL (Secure Socket Layer) で LDAP を使用します。デフォルトでは、iDRAC6 は、iDRAC6 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の SSL サーバー証明書を SSL ハンドシェイク中に検証する強力なセキュリティを提供します。証明書の検証はテスト目的で無効にできません。
Active Directory CA 証明書のアップロード	Active Directory CA 証明書をアップロードするには、 参照 をクリックし、ファイルを選択して アップロード をクリックします。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、iDRAC6 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。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。証明書を参照しない場合は、完全パスと正式ファイル名とファイル拡張子を含めてファイルのパスを入力してください。
現在の Active Directory CA 証明書	iDRAC6 にアップロードされた Active Directory CA 証明書を表示します。
Active Directory の設定と管理 手順 2/4	
Active Directory が有効	Active Directory を有効にする場合は、このオプションを選択します。
スマートカードログインを有効にする	スマートカードログインを有効にするには、このオプションを選択します。以降 GUI を使用してログイン試行すると、スマートカードログインのプロンプトが表示されます。 メモ: スマートカードベースの 2 要素認証 (TFA) とシングルサインオンは、Internet Explorer を搭載した Microsoft Windows オペレーティングシステムでのみサポートされています。また、Windows XP® 下のターミナルサービス (リモートデスクトップ) はスマートカードの操作をサポートしていません。ただし、Windows Vista® はこのような使用方法をサポートしています。
シングルサインオンを有効にする	ユーザー名やパスワードなどのドメインユーザー認証情報を入力せずに iDRAC6 にログインする場合は、このオプションを選択します。シングルサインオン (SSO) を有効にしてからログアウトした場合は、SSO を使用して再ログインできます。既に SSO を使用してログインしてからログアウトした場合や、SSO に失敗した場合は、通常のログインウェブページが表示されます。 メモ: スマートカードログインまたはシングルサインオンを有効にしても、SSH、Telnet、リモート RACADM、および IPMI オーバー LAN などのコマンドラインの帯域外インタフェースは無効になりません。 メモ: Active Directory に拡張スキーマが設定されている場合、スマートカードベースの 2 要素認証 (TFA) 機能とシングルサインオン (SSO) 機能はサポートされません。
ユーザードメイン名	ユーザードメイン名のエントリを入力します。設定されている場合は、ログインページにユーザードメイン名のリストがドロップダウンメニューとして表示されます。設定されていない場合でも、Active Directory ユーザーはユーザー名を user_name@domain_name または domain_name\user_name の形式で入力するとログインできます。 追加: 新しいユーザードメイン名のエントリをリストに加えます。 編集: 既存のユーザードメイン名エントリを編集します。 削除: ユーザードメイン名のエントリをリストから削除します。
タイムアウト	Active Directory のクエリが完了するまで待つ最大時間を秒で指定します。
DNS を使用したドメインコントローラのルックアップ	DNS ルックアップで Active Directory ドメインコントローラを取得するには、DNS でドメインコントローラをルックアップする オプションを選択します。このオプションを選択すると、ドメインコントローラサーバーのアドレス 1-3 は無視されます。ログインユーザーのドメイン名で DNS ルックアップを行うには、 ログインのユーザードメイン を選択します。そうでない場合は、 ドメインを指定する を選択し、DNS ルックアップに使用するドメイン名を入力します。iDRAC6 は、接続が確立されるまで、各アドレス (DNS ルックアップによって返される最初の 4 つのアドレス) 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、ドメインコントローラは、iDRAC6 デバイスオブジェクトと関連オブジェクトが存在する場所になります。 標準スキーマ を選択した場合、ドメインコントローラは、ユーザーアカウントと役割グループが存在する場所になります。
ドメインコントローラのアドレスの指定	iDRAC6 に指定した Active Directory ドメインコントローラのサーバーアドレスを使用させるには、 ドメインコントローラアドレスを指定する オプションを選択します。このオプションを選択すると、DNS ルックアップは実行されません。ドメインコントローラの IP アドレスまたは完全修飾ドメイン名 (FQDN) を指定します。 ドメインコントローラアドレスを指定する オプションが選択されている場合、3 つのアドレスのうち、少なくとも 1 つのアドレスが設定されている必要があります。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 を選択した場合、これら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です。 拡張スキーマ を選択した場合、これらは

	IDRAC6 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のアドレスです。
Active Directory の設定と管理 手順 3/4	
拡張スキーマの選択	<p>Active Directory で拡張スキーマを使用する場合は、このオプションを選択します。</p> <p>次へ をクリックして、Active Directory 設定と管理 手順 4/4 ページを表示します。</p> <p>IDRAC6 名: Active Directory で IDRAC6 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は NULL になっています。</p> <p>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は NULL になっています。</p> <p>これらの設定は、拡張 Active Directory スキーマで IDRAC6 を使用するように設定されている場合にのみ表示されます。</p>
標準スキーマの選択	<p>Active Directory で標準スキーマを使用する場合は、このオプションを選択します。</p> <p>次へ をクリックして、Active Directory 手順 4a/4 ページを表示します。</p> <p>Active Directory グローバルカタログサーバーを取得するには、DNS でグローバルカタログサーバーをルックアップする オプションを選択し、DNS ルックアップで使用する ルートドメイン名 を入力します。このオプションを選択すると、グローバルカタログサーバーのアドレス 1-3 は無視されます。IDRAC6 は、接続が確立されるまで、各アドレス(DNS ルックアップによって返される最初の 4 つのアドレス)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に限り、標準スキーマにグローバルカタログサーバーが必要です。</p> <p>グローバルカタログサーバーアドレスを指定する オプションを選択し、グローバルカタログサーバーの IP アドレスまたは FQDN を入力します。このオプションを選択すると、DNS ルックアップは実行されません。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。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に限り、標準スキーマにグローバルカタログサーバーが必要です。</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: 役割グループが存在するグループドメインを指定します。</p> <p>役割グループの特権: グループの特権レベルを指定します。(「表 5-27」を参照)</p> <p>これらの設定は、標準 Active Directory スキーマで IDRAC6 を使用するように設定されている場合にのみ表示されます。</p>

表 5-27 役割グループの権限

設定	説明
役割グループの権限レベル	<p>ユーザーの最大 IDRAC6 ユーザー権限を システム管理者、パワーユーザー、ゲストユーザー、なし、カスタム から指定します。</p> <p>役割グループ 権限については、「表 5-28」を参照してください。</p>
IDRAC6 へのログイン	グループに IDRAC6 へのログインアクセスを許可します。
IDRAC6 の設定	IDRAC6 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 5-28 役割グループの権限

プロパティ	説明
管理者	IDRAC6 へのログイン、IDRAC6 の設定、ユーザーの設定、、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。
パワーユーザー	IDRAC6 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。
ゲストユーザー	IDRAC6 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。IDRAC6 へのログイン、IDRAC6 の設定、ユーザーの設定、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。
なし	権限の割り当てなし


Active Directory CA 証明書の表示

Active Directory 概要ページで、Active Directory の設定 をクリックし、次へ をクリックします。現在の Active Directory CA 証明書 セクションが表示されます。「表 5-29」を参照してください。

表 5-29 Active Directory CA 証明書の情報

フィールド	説明
シリアル番号	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。

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 → iDRAC6 → ネットワーク / セキュリティ → サービス をクリックします。
2. ローカル設定 で、iDRAC6 ローカルユーザー設定のアップデートを無効にする をクリックして チェックボックスをオフ にし、アクセスを有効にします。
3. 適用 をクリックします。


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 → iDRAC6 → ネットワーク / セキュリティ → サービス をクリックします。
2. ローカル設定 で、iDRAC6 ローカルユーザー設定のアップデートを無効にする をクリックして選択し、アクセスを無効にします。
3. 適用 をクリックします。

iDRAC6 サービスの設定

 **メモ:** これらの設定を変更するには、iDRAC6 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、変更は即時に反映されます。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:** 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 P リモートアクセス P iDRAC6 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 画面を開きます。
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 5-30](#)」を参照
 1. SSH - SSH 設定については「[表 5-31](#)」を参照
 1. Telnet - Telnet の設定については「[表 5-32](#)」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 5-33](#)」を参照
4. 適用 をクリックします。

表 5-30 ウェブサーバーの設定

設定	説明
有効	iDRAC6 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オン の場合は、ウェブサーバーが有効であることを示します。デフォルト値は チェックボックスがオン です。
最大セッション数	このシステムで同時に許可される最大ウェブサーバーセッション数。このフィールドは編集できません。最大 4 つのウェブサーバーセッションが同時に存在できます。
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 (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はられる秒数。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。タイムアウトの範囲は 60～10800 秒です。デフォルトは 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	セキュアなブラウザ接続で iDRAC6 が通信するポート。デフォルトは 443 です。

表 5-31 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オン の場合は、SSH が有効であることを示します。
最大セッション数	システムで同時に許可される最大 SSH セッション数。最大 4 つの SSH セッションが同時にサポートされます。このフィールドは編集できません。
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。このフィールドは編集できません。
タイムアウト	セキュアなアイドルタイムアウト(秒)。タイムアウトの範囲は 60～10800 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 1800 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 5-32 Telnet の設定


設定	説明
有効	Telnet 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、Telnet が有効になります。デフォルト値は チェックボックスがオフ です。
最大セッション数	システムで同時に許可される最大 Telnet セッション数。最大 4 つの Telnet セッションが同時にサポートされます。このフィールドは編集できません。
アクティブセッション数	システムの現在の Telnet セッション数。このフィールドは編集できません。
タイムアウト	Telnet のアイドルタイムアウト(秒)。タイムアウトの範囲は 60～10800 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 1800 です。
ポート番号	iDRAC6 が Telnet 接続を待ち受けるポート。デフォルトは 23 です。

表 5-33 自動システム回復エージェント


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。

iDRAC6 ファームウェアのアップデート

 **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は、CMC を使用して iDRAC6 を修復できます。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 iDRAC6 設定を保持します。アップデート中に、iDRAC6 設定を工場出荷時のデフォルト設定にリセットするオプションが提供されます。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。iDRAC6 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. iDRAC6 ウェブインタフェースを開始します。
2. **システム** → **リモートアクセス** → **iDRAC6** 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、iDRAC6 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 iDRAC6 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 - アップロード(1/4 ページ)** ウィンドウで、**参照** をクリックし、ファームウェアイメージを選択します。

例:

C:\Updates\V2.2\

デフォルトのファームウェアイメージ名は `firmimg.imc` 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。これには、数分かかる場合があります。
5. **アップロード(手順 2/4)** ページで、アップロードしたイメージファイルに実行し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、検証チェックのすべてに合格した場合、ファームウェアイメージの有効性が確認されたことを示すメッセージが表示されます。
 1. イメージが正しくアップロードされなかった場合や、検証チェックに合格しなかった場合は、iDRAC6 をリセットし、現在のセッションを終了してから再度アップロードしてください。


 **メモ:** **設定の保存** チェックボックスをオフにすると、iDRAC6 が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ません。BIOS POST 中に iDRAC6 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 の設定を再設定する必要があります。

6. デフォルトでは、アップグレード後も iDRAC6 の現在の設定を維持するための **設定の保存 チェックボックスがオン**になっています。設定を維持しない場合は、**設定の保存** チェックボックスをオフにします。
7. **アップデート中(手順 3/4)** ウィンドウに、アップグレードの状態が表示されます。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。
8. 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 ページ)** ウィンドウが表示され、iDRAC6 は自動的にリセットされます。引き続きウェブインタフェースから iDRAC6 にアクセスするには、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用して iDRAC6 に再接続します。

CMC を使用した iDRAC6 ファームウェアのアップデート

通常、iDRAC6 ファームウェアは、iDRAC6 ウェブインタフェースなどの iDRAC6 ユーティリティ、または support.dell.com からダウンロードできるオペレーティングシステムの特定のアップデートパッケージを使用してアップデートします。

CMC ウェブインタフェースまたは RACADM を使用して、iDRAC6 ファームウェアをアップデートできます。この機能は、iDRAC6 ファームウェアが通常モード、または破損している場合でも、利用できます。

 **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、『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。

iDRAC6 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 iDRAC6 ファームウェアをダウンロードします。
2. CMC ウェブ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。**ファームウェアアップデート** 画面が表示されます。
5. **ターゲットのアップデート** チェックボックスをオンにして、同じモデルの iDRAC6 を選択します(複数可)。
6. iDRAC6 コンポーネントのリストの下にある **iDRAC6 Enterprise アップデートの適用** ボタンをクリックします。
7. **参照** をクリックして、ダウンロードした iDRAC6 ファームウェアイメージに移動し、**開く** をクリックします。
8. **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を CMC にアップロードすると、iDRAC6 はそのイメージを使用して自動的にアップデートされます。

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できます。任意のファームウェアイメージから起動(またはその時点までロールバック)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** → iDRAC6 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。

2. **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は **ロールバック(手順 2/3)** ページに表示されます。
3. **次へ** をクリックしてファームウェアのロールバックプロセスを開始します。

ロールバック中(手順 3/3) ページに、ロールバック処理の状態が表示されます。ロールバックが正常に完了すると、プロセスが成功したことが示されます。

ファームウェアのロールバックに成功すると、iDRAC6 は自動的にリセットされます。引き続きウェブインタフェースから iDRAC6 にアクセスするには、現在のブラウザを閉じ、新しいブラウザウィンドウを使用して iDRAC6 に再接続します。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。

 **メモ:** iDRAC6 ファームウェアをバージョン 2.2 から 2.1 にロールバックすると、**設定の保存** 機能が機能しなくなります。

[目次ページに戻る](#)

[目次ページに戻る](#)

iDRAC6 ディレクトリサービスの使用

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [Microsoft Active Directory での iDRAC6 の使用](#)
- [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 の認証メカニズム](#)
- [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](#)
- [Active Directory シングルサインオンの使用](#)
- [iDRAC6 と LDAP ディレクトリサービスの使用](#)
- [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、プリンタなどの情報を格納する共通のデータベースを管理します。会社で Microsoft® Active Directory® または LDAP ディレクトリサービスの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、ディレクトリサービス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。

Microsoft Active Directory での iDRAC6 の使用

メモ: Active Directory を使用して iDRAC6 ユーザーを認識する機能は、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サポートされています。

表 6-1 は、iDRAC6 Active Directory ユーザー権限を示しています。

表 6-1 iDRAC6 ユーザー権限

権限	説明
iDRAC6 へのログイン	iDRAC6 にログインできます。
iDRAC6 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 のウェブサイトを参照してください。

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ので、Active Directory のインフラストラクチャにも PKI を統合する必要があります。

PKI の設定については、Microsoft のウェブサイトを参照してください。

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 の認証メカニズム

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 つは、デル定義の 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を使用する方法です。もう一つは、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を使用する方法です。これらのソリューションの詳細については、以降の各項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利点は次のとおりです。

- 1 アクセス制御オブジェクトのすべてを Active Directory で管理できます。
- 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使用する利点は、スキーマ拡張子が必要ないことです。必要なオブジェクトクラスはすべて、Active Directory スキーマの Microsoft のデフォルト設定で提供されています。

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使用する場合は、次の項で説明するように、Active Directory スキーマの拡張が必要になります。

Active Directory スキーマの拡張

重要: この製品のスキーマ拡張は、旧世代のデルリモート管理製品とは異なります。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。古いスキーマはこの製品には対応していません。

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 スキーマの拡張」と「Active Directory ユーザーとコンピュータスナップインへのデル拡張のインストール」を参照してください。iDRAC6 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 で『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: iDRAC6 関連オブジェクトまたは iDRAC6 デバイスオブジェクトを作成する場合は、**デルリモート管理オブジェクトの詳細設定** を選択してください。

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して、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。業界で一意の ID の保持するため、Microsoft では 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場合、それらが他社と重複しないようにしています。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 を受け取りました。

- 1 デルの拡張子: dell
- 1 デルベースの OID: 1.2.840.113556.1.8000.1280
- 1 RAC LinkID の範囲: 12070 ~ 12079

iDRAC6 スキーマ拡張の概要

デルでは、さまざまな顧客環境に柔軟に対応できるように、ユーザーが目標とする成果に応じて設定できるプロパティを用意しています。デルは、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 iDRAC6 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、iDRAC6 権限、およびネットワーク上の iDRAC6 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

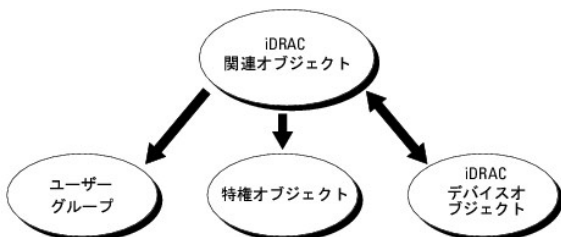
認証と許可のために Active Directory に統合するネットワーク上の物理 iDRAC6 の 1 台につき、少なくとも 1 個ずつ関連オブジェクトと iDRAC6 デバイスオブジェクトを作成しておきます。関連オブジェクトは必要な数だけ作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、iDRAC6 デバイスオブジェクトの数にも制限はありません。ユーザーと iDRAC6 デバイスオブジェクトは、企業内のどのドメインのメンバーでもかまいません。

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、iDRAC6 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、システム管理者は特定の iDRAC6 で各ユーザーの権限を制御できます。

iDRAC6 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 iDRAC6 ファームウェアへのリンクです。iDRAC6 をネットワークに追加した場合、システム管理者は iDRAC6 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、システム管理者はユーザーが認証できるように、iDRAC6 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 6-1 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、iDRAC6 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 iDRAC6 デバイスごとに iDRAC6 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、iDRAC6 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、iDRAC6 デバイスに権限のある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 iDRAC6 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 iDRAC6 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。

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。

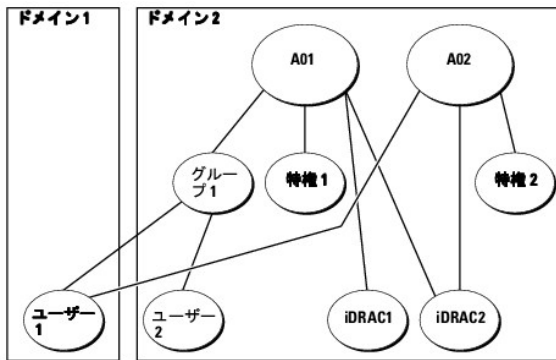
任意のドメインのユーザー、ユーザーグループ、またはネストされたユーザーグループを関連オブジェクトに追加できます。拡張スキーマソリューションは、Microsoft Active Directory によって許可されている複数のドメインにわたってネストされたユーザーグループやユーザーグループの種類をサポートしています。

拡張スキーマを使用した権限の蓄積

拡張スキーマ認証メカニズムは、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た異なる権限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して、同じユーザーに関連付けられた異なる権限オブジェクトに対応して割り当てられた権限すべてのスーパーセットをユーザーに許可します。

図 6-2 に、拡張スキーマを使用した権限の蓄積例を示します。

図 6-2 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、両方の関連オブジェクトを通して、iDRAC2 に関連付けられています。したがって、ユーザー 1 には iDRAC2 でオブジェクト Priv1 と Priv2 に設定された権限を組み合わせて蓄積された権限が与えられます。

たとえば、Priv1 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、Priv2 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、Priv1 と Priv2 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た権限を考慮し、このように権限を蓄積して、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 では Priv1 と Priv2 を持っています。ユーザー 1 は、iDRAC1 では Priv1 だけ持っています。ユーザー 2 は、iDRAC1 と iDRAC2 の両方で Priv1 を持っています。さらに、この図では、ユーザー 1 は異なるドメインに属し、グループのメンバーであることも許可されていることを示しています。

iDRAC6 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 のユーザーとコンピュータのスナップインを拡張します(「[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 iDRAC6 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 のプロパティを設定します(「[iDRAC6 ウェブインタフェースを使用して Active Directory と拡張スキーマを設定する方法](#)」または「[RACADM を使用した拡張スキーマの Active Directory の設定](#)」を参照してください)。

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)役割所有者のスキーマ 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

 **注意:** Dell Schema Extender 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、以下のものがあることを確認します。

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

MMC および Active Directory スキーマスナップインの使用法の詳細については、Microsoft のマニュアルを参照してください。

表 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	割り当てられた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 6-3 dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.1
説明	Dell iDRAC6 デバイスを表します。iDRAC6 は、Active Directory で dellIDRACDevice として設定する必要があります。この設定により、iDRAC6 から Active Directory に Lightweight Directory Access Protocol(LDAP)クエリを送信できるようになります。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 6-4 dellIDRACAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.2
説明	デル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の間の接続を提供します。
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	iDRAC6 の権限(認証権限)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	デルの権限(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	すべてのデル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	割り当てられた 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 DellIDRACDevice 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

dell sLogClearAdmin 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
dell sServerResetUser 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
dell sConsoleRedirectUser 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
dell sVirtualMediaUser 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
dell sTestAlertUser 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
dell sDebugCommandAdmin 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
dell SchemaVersion 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
dell RacType 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パスワードリンクです。	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
dell AssociationMembers 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 リンク属性へのパスワードリンクです。 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、iDRAC6 デバイス、ユーザーとユーザーグループ、iDRAC6 関連付け、iDRAC6 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 ビットの 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ラは、次の場所にあります。

<DVDドライブ>:\SYSMGMT\ManagementStation\support\OActiveDirectory_SnapIn64

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 iDRAC6 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 iDRAC6 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、以下の手順を実行します。

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** の順で選択し、MMC と入力して、**Enter** キーを押します。

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、**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 iDRAC6 ユーザーと権限の追加


デルの拡張 Active Directory ユーザーとコンピュータスナップインを使用して、iDRAC6、関連付け、および権限オブジェクトを作成すると、iDRAC6 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. iDRAC6 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

iDRAC6 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 ウェブインタフェースを使用して Active Directory と拡張スキーマを設定する方法](#)」の手順 A で入力する iDRAC6 名と同一である必要があります。
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。

特権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 P 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. **リモート管理権限** タブをクリックし、ユーザーまたはグループに付与する権限を選択します(「[表 5-14](#)」を参照)。

関連オブジェクトの作成

 **メモ:** iDRAC6 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 に設定されています。

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 P 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、iDRAC6 デバイスまたは iDRAC6 デバイスグループ間の関連付けができます。

ユーザーおよび iDRAC6 デバイスのグループを追加できます。デル関連グループとデル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。

権限の追加

1. **特権オブジェクト** 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。

権限オブジェクト タブをクリックして、iDRAC6 デバイスに認証するとき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。

iDRAC6 デバイスまたは iDRAC6 デバイスグループの追加

iDRAC6 デバイスまたは iDRAC6 デバイスグループを追加するには:

1. **製品** タブを選択して **追加** をクリックします。
2. iDRAC6 デバイスまたは iDRAC6 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。

定義済みの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している iDRAC6 デバイスを 1 台追加するには、**製品** タブをクリックします。1 つの関連オブジェクトに対して複数の iDRAC6 デバイスを追加できます。

iDRAC6 ウェブインタフェースを使用して Active Directory と拡張スキーマを設定する方法

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. iDRAC6 ウェブインタフェースにログインします。
3. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** → **Microsoft Active Directory** の順でクリックします。

Active Directory 概要の画面が表示されます。


4. 画面の下までスクロールし、**Active Directory** の **設定** をクリックします。

Active Directory 手順 1/4 画面が表示されます。

5. **Active Directory** サーバーの SSL 証明書を検証するには、**証明書の設定** で **証明書の検証有効** チェックボックスをオンにします。

Active Directory サーバーの SSL 証明書を検証しない場合は、手順 7 に進んでください。

6. **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て、**アップロード** をクリックします。


 **メモ:** 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。

アップロードした Active Directory CA 証明書の証明書情報は、**現在の Active Directory CA 証明書** セクションに表示されます。

7. **次へ** をクリックします。

Active Directory の設定と管理 手順 2/4 画面が表示されます。


8. **Active Directory ログイン有効** チェックボックスをオンにします。

 **メモ:** このリリースでは、Active Directory に**拡張スキーマ**が設定されている場合、スマートカードベースの 2 要素認証 (TFA) 機能とシングルサインオン (SSO) 機能はサポートされません。

9. **追加** をクリックして、**ユーザードメイン名** を入力します。テキストフィールドにドメイン名を入力して OK をクリックします。このステップは省略できます。ユーザードメインのリストを設定した場合は、ウェブインタフェースのログイン画面に表示されます。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。

10. **タイムアウト** フィールドに、iDRAC6 が Active Directory の応答を待つ時間を秒数で入力します。

11. DNS ルックアップで Active Directory ドメインコントローラを取得するには、**DNS でドメインコントローラをルックアップする** オプションを選択します。既に設定されている場合は、**ドメインコントローラサーバーのアドレス 1-3** は無視されます。ログインユーザーのドメイン名で DNS ルックアップを行うには、**ログインのユーザードメイン** を選択します。そうでない場合は、**ドメインを指定する** を選択し、DNS ルックアップに使用するドメイン名を入力します。iDRAC6 は、接続が確立されるまで、各アドレス (DNS ルックアップによって返される最初の 4 つのアドレス) 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、ドメインコントローラは、iDRAC6 デバイスオブジェクトと関連オブジェクトが存在する場所になります。**標準スキーマ** を選択した場合、ドメインコントローラは、ユーザーアカウントと役割グループが存在する場所になります。

 **メモ:** DNS ルックアップが失敗した、または DNS ルックアップによって返されるサーバーが機能しない場合、iDRAC6 は指定したドメインコントローラにフェールオーバーしません。

12. iDRAC6 に指定した Active Directory ドメインコントローラのサーバーアドレスを使用させるには、**ドメインコントローラアドレスを指定する** オプションを選択します。DNS ルックアップは実行されません。ドメインコントローラの IP アドレスまたは FQDN を指定します。**ドメインコントローラアドレスを指定する** オプションが選択されている場合、3 つのアドレスのうち、少なくとも 1 つのアドレスが設定されている必要があります。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。**拡張スキーマ** を選択した場合、これらは iDRAC6 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のアドレスです。

 **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 **件名** または **代替名** フィールドの値と一致する必要があります。

13. **次へ** をクリックします。

Active Directory の設定と管理 手順 3/4 画面が表示されます。

14. **スキーマの選択** で、**拡張スキーマの選択** チェックボックスを選択します。

15. **次へ** をクリックします。

Active Directory 手順 4/4 画面が表示されます。

16. **拡張スキーマの設定** で、iDRAC6 名と iDRAC6 ドメイン名を入力して iDRAC6 のデバイスオブジェクトと Active Directory での場所を設定します。

17. 変更を保存するには、**終了** をクリックし、次に **完了** をクリックします。


Active Directory の設定と管理 メイン概要ページが表示されます。次に、指定した Active Directory の設定をテストする必要があります。

18. 画面の下までスクロールし、**テストの設定** をクリックします。

Active Directory 設定のテスト 画面が表示されます。

19. iDRAC6 ユーザー名とパスワードを入力し、**テストの開始** をクリックします。

テスト結果と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、iDRAC6 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。**ネットワーク** 画面に移動して (**システム** → **リモートアクセス** → **iDRAC6** をクリックし、**ネットワーク / セキュリティ** → **ネットワーク タブ** の順にクリック)、DNS サーバーを手動で設定するか、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ではなく、RACADM コマンドラインインタフェース(CLI)を使用して拡張スキーマを備えた iDRAC6 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 共通名>

racadm config -g cfgActiveDirectory -o cfgADRacDomain <完全修飾ルートドメイン名>

racadm config -g cfgActiveDirectory -o cfgADDomainController1 <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 cfgADDomainController2 <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 cfgADDomainController3 <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。拡張スキーマでは、iDRAC6 デバイスが位置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まったく使用されません。

SSL ハンドシェイク中に証明書の検証を実行する場合は、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 ハンドシェイク中に証明書の検証を実行する場合は、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ときにユーザー名を入力だけで済むように、ユーザードメインのリストを設定しておく場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName <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> -i <インデックス>
```

1 から 40 のインデックス番号で、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。

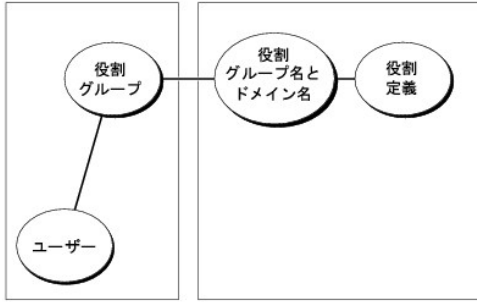
標準スキーマの Active Directory の概要

[図 6-3](#) に示すように、標準スキーマを使用して Active Directory を統合する場合は、Active Directory と iDRAC6 の両方で設定が必要となります。

図 6-3 Microsoft Active Directory と標準スキーマの iDRAC6 の設定

Active Directory 側の設定

次の設定：
iDRAC6 側



Active Directory 側では、標準グループオブジェクトが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。このユーザーに特定の iDRAC6 カードへのアクセスを与えるには、その iDRAC6 カードで役割グループ名とドメイン名を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 ではなく各 iDRAC6 カード上で定義されます。各 iDRAC6 につき最大 5 つの役割グループを設定および定義できます。表 6-9 は、デフォルトの役割グループの権限を示しています。

表 6-9 デフォルトの役割グループの権限

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
役割グループ 1	なし	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
役割グループ 2	なし	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
役割グループ 3	なし	iDRAC へのログイン	0x00000001
役割グループ 4	なし	権限の割り当てなし	0x00000000
役割グループ 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があります。

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、役割グループ、およびネストされたグループが同じドメインに属する場合は、ドメインコントローラのアドレスのみを iDRAC6 で設定する必要があります。このような単一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。

ログインユーザーと役割グループのすべて、またはネストされたグループのいずれかが異なるドメインに属する場合は、iDRAC6 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、すべての役割グループとネストされたグループがユニバーサルグループタイプであることが必要です。

iDRAC6 にアクセスするための標準スキーマ Active Directory の設定

Active Directory ユーザーが iDRAC6 にアクセスするためには、まず以下の手順に従って 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。グループ名とドメイン名は、ウェブインタフェースまたは RACADM を使用して iDRAC6 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て Active Directory を標準スキーマで設定する方法](#)」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)。
- Active Directory ユーザーを、iDRAC6 にアクセスする Active Directory グループのメンバーとして追加します。

iDRAC6 ウェブインタフェースを使用して Active Directory を標準スキーマで設定する方法

- 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 ウェブインタフェースにログインします。
- システムツリーで、システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティタブ → ディレクトリサービス → Microsoft Active Directory の順でクリックします。


Active Directory 概要ページが表示されます。

- 画面の下までスクロールし、**Active Directory の設定** をクリックします。

Active Directory 手順 1/4 画面が表示されます。

- 証明書の設定** で、**証明書の検証有効** を選択します。

- 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て、**アップロード** をクリックします。

 **メモ:** フルパスおよび完全な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。

アップロードした Active Directory CA 証明書の証明書情報は、**現在の Active Directory CA 証明書** セクションに表示されます。

- 次へ** をクリックします。

Active Directory の設定と管理 手順 2/4 画面が表示されます。

- Active Directory 有効 チェックボックスをオンにします。

- スマートカードログインを有効にするには、**スマートカードログインを有効にする** を選択します。以降、GUI を使用してログインするときに、スマートカードログインのプロンプトが表示されます。


- ユーザー名やパスワードなどのドメインユーザー認証情報を入力せずに iDRAC6 にログインする場合は、**シングルサインオンを有効にする** を選択してください。

- 追加** をクリックして、**ユーザードメイン名** を入力します。テキストフィールドにドメイン名を入力して OK をクリックします。このステップは省略できます。ユーザードメインのリストを設定した場合は、ウェブインタフェースのログイン画面に表示されます。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。

- タイムアウト** フィールドに、iDRAC6 が Active Directory の応答を待つ時間を秒数で入力します。

- DNS ルックアップで Active Directory ドメインコントローラを取得するには、**DNS でドメインコントローラをルックアップする** オプションを選択します。既に設定されている場合は、**ドメインコントローラのサーバーアドレス 1-3** は無視されます。ログインユーザーのドメイン名で DNS ルックアップを行うには、**User Domain from Login (ログインのユーザードメイン)** を選択します。そうでない場合は、**ドメインを指定する** を選択し、DNS ルックアップに使用するドメイン名を入力します。iDRAC6 は、接続が確立されるまで、各アドレス (DNS ルックアップによって返される最初の 4 つのアドレス) に対して、一つずつ接続を試みます。**標準スキーマ** を選択した場合、ドメインコントローラは、ユーザーアカウントと役割グループが存在する場所になります。

- iDRAC6 に指定した Active Directory ドメインコントローラのサーバーアドレスを使用させるには、**ドメインコントローラアドレスを指定する** オプションを選択します。DNS ルックアップは実行されません。ドメインコントローラの IP アドレスまたは FQDN を指定します。**ドメインコントローラアドレスを指定する** オプションが選択されている場合、3 つのアドレスのうち、少なくとも 1 つのアドレスが設定されている必要があります。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** を選択した場合、これら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です。

 **メモ:** DNS ルックアップが失敗した、または DNS ルックアップによって返されるサーバーが機能しない場合、iDRAC6 は指定したドメインコントローラにフェールオーバーしません。

- 次へ** をクリックします。


Active Directory の設定と管理 手順 3/4 画面が表示されます。

- スキーマの選択** で、**標準スキーマの選択** チェックボックスを選択します。


- 次へ** をクリックします。

Active Directory 手順 4a/4 画面が表示されます。

- Active Directory グローバルカタログサーバーを取得するには、**標準スキーマ設定** で、**DNS でグローバルカタログサーバーをルックアップする** オプションを選択し、DNS ルックアップで使用する **ルートドメイン名** を入力します。既に設定されている場合は、グローバルカタログサーバーのアドレス 1-3 は無視されます。iDRAC6 は、接続が確立されるまで、各アドレス (DNS ルックアップによって返される最初の 4 つのアドレス) 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に限り、標準スキーマにグローバルカタログサーバーが必要です。

 **メモ:** DNS ルックアップが失敗した、または DNS ルックアップによって返されるサーバーが機能しない場合、iDRAC6 は指定したグローバルカタログサーバーにフェールオーバーしません。

- グローバルカタログサーバーアドレスを指定する** オプションを選択し、グローバルカタログサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。DNS ルックアップは実行されません。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。

 **メモ:** グローバルカタログサーバーは、ユーザーアカウントと役割グループがそれぞれ異なるドメインに属する標準スキーマの場合においてのみ、必要となります。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。iDRAC6 ウェブ GUI を使用して Active Directory を設定する場合は、ユーザーとグループが同じドメインでもグローバルアドレスを入力する必要があります。


- 役割グループを追加するには、**役割グループ** ボタンをクリックします。

役割グループの設定 手順 4b/4 画面が表示されます。

21. **グループ名** を入力します。グループ名は、iDRAC6 に関連付けられた Active Directory における役割グループを識別します。

22. **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。

23. **役割グループの権限** で、グループの権限を設定します。役割グループ権限については、「[表 5-14](#)」を参照してください。

 **メモ:** 権限を変更すると、既存の役割グループの権限（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役割グループの権限に変更されます。

24. **OK** をクリックして、役割グループの設定を保存します。

設定が変更されたことを示す警告ダイアログが表示されます。OK をクリックして、Active Directory の **設定と管理 手順 4a/4** 画面に戻ります。

25. 役割グループを追加するには、[手順 20](#) から [手順 24](#) の手順を繰り返します。

26. **完了** をクリックしてから、**終了** をクリックします。


Active Directory の **設定と管理** メイン概要ページが表示されます。指定した Active Directory の設定をテストする必要があります。

27. 画面の下までスクロールし、**テストの設定** をクリックします。

Active Directory **設定のテスト** 画面が表示されます。

28. iDRAC6 ユーザー名とパスワードを入力し、**テストの開始** をクリックします。

テスト結果と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、iDRAC6 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。**ネットワーク** 画面に移動して（**システム** → **リモートアクセス** → **iDRAC6** をクリックし、**ネットワーク / セキュリティ** → **ネットワーク** タブの順にクリック）、DNS サーバーを手動で設定するか、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ではなく、RACADM CLI を使用して iDRAC6 Active Directory 機能を標準スキーマで設定するには、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 <インデックス> -o  
cfgSSADRoleGroupName <役割グループの共通名>
```

```
racadm config -g cfgStandardSchema -i <インデックス> -o  
cfgSSADRoleGroupDomain <完全修飾ドメイン名>
```


```
racadm config -g cfgStandardSchema -i <インデックス> -o  
cfgSSADRoleGroupPrivilege <特定の役割グループ権限の  
ビットマスク値>
```

 **メモ:** 特定の役割グループ権限のビットマスク値については、「[表 6-9](#)」を参照してください。

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <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 cfgADDomainController2 <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 cfgADDomainController3 <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:** ドメインの FQDN 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、dell.com ではなく、servername.dell.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:** グローバルカタログサーバーは、ユーザーアカウントと役割グループがそれぞれ異なるドメインに属する標準スキーマの場合においてのみ、必要となります。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 **件名** または **代替名** フィールドの値と一致する必要があります。

SSL ハンドシェイク中に証明書の検証を実行する場合は、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 ハンドシェイク中に証明書の検証を実行する場合は、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 上で 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 上で 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. ウェブインタフェースにログインするときにユーザー名だけの入力で済むように、ユーザードメインのリストを設定しておく場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName <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> -i <インデックス>
```

1 から 40 のインデックス番号で、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確認する場合や、Active Directory へのログイン失敗の問題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できます。

iDRAC6 ウェブインタフェースで設定を完了したら、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、テストユーザーの名前(例: `username@domain.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、各ステップの結果が表示されるまでに時間がかかる場合があります。結果画面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。

設定に変更を加える場合は、**Active Directory** タブをクリックし、手順に従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


iDRAC6 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 iDRAC6 にアップロードされます。つまり、iDRAC6 が(ルートか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ためには、その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 対応証明書を持っている必要があります。

Microsoft Enterprise のルート CA を使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、次の手順で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。

iDRAC6 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、以下の手順が異な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、以下の手順が異なる可能性があります。

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** 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。
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 iDRAC6 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、「[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用して証明書をアップロードする場合は、「[iDRAC6 ウェブインタフェースを使用して Active Directory を標準スキーマで設定する方法](#)」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は、iDRAC6 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しない場合、この手順は不要です。

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、以下の手順が異なる可能性があります。

 **メモ:** iDRAC6 ファームウェア SSL 証明書が知名度の高い 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、この項の手順を実行する必要はありません。

iDRAC6 の SSL 証明書は、iDRAC6 のウェブサーバーで使用される証明書と同じです。iDRAC6 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。

iDRAC6 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 iDRAC6 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、保存する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 ローカル RACADM
- 1 SM-CLP CLI 用の SSH 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。

ユーザー名またはドメイン名に空白スペースと特殊文字 (\, /, @ 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、ユーザードメインを設定している場合は、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は、ユーザー名のみを入力します。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。

Active Directory シングルサインオンの使用

iDRAC6 が Kerberos (ネットワーク認証プロトコルの 1 つ) を使用できるようにして、シングルサインオンを有効にできます。iDRAC6 が Active Directory シングルサインオン機能を使用するように設定する方法については、「[Kerberos 認証を有効にする方法](#)」を参照してください。

iDRAC6 にシングルサインオンの使用を設定する方法

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. iDRAC6 ウェブインタフェースにログインします。
3. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ → **ネットワーク** の順に選択します。**ネットワーク** ページで、DNS **iDRAC6 名** が正しく、iDRAC6 の完全修飾ドメイン名に使用されている名前と同じかどうか確認します。
4. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** → **Microsoft Active Directory** の順でクリックします。

Active Directory 概要の画面が表示されます。


5. 画面の下までスクロールし、**Active Directory の設定** をクリックします。

Active Directory **手順 1/4** 画面が表示されます。

6. Active Directory サーバーの SSL 証明書を検証するには、**証明書の設定** で **証明書の検証有効** チェックボックスをオンにします。

Active Directory サーバーの SSL 証明書を検証しない場合は、このステップを実行する必要はありません。「[手順 7](#)」に進んでください。

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て、**アップロード** をクリックします。

 **メモ:** フルパスおよび完全な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。

アップロードした Active Directory CA 証明書の証明書情報は、**現在の Active Directory CA 証明書** セクションに表示されます。

8. **次へ** をクリックします。

Active Directory の **設定と管理 手順 2/4** 画面が表示されます。

9. **Active Directory 有効** チェックボックスをオンにします。

10. **シングルサインオンを有効にする** オプションを使用すると、ユーザ名やパスワードなどのドメインユーザー認証情報を入力せずに、ワークステーションにログインした後、iDRAC6 に直接ログインできます。

この機能を使用して iDRAC6 にログインするには、有効な Active Directory ユーザーアカウントを使用してシステムに既にログインしている必要があります。また、Active Directory の資格情報を使用して iDRAC6 にログインするようにユーザーアカウントを設定しておく必要があります。キャッシュに入っている Active Directory 資格情報によって iDRAC6 にログインできます。

CLI を使用してシングルサインオンを有効にするには、次の RACADM コマンドを実行します。

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

11. **ユーザードメイン名** を追加し、ドメインコントローラサーバーアドレスの IP アドレスを入力します。DNS でドメインコントローラをルックアップする または **ドメインコントローラアドレスを指定する** のいずれかを選択します。**次へ** を選択します。
12. **Active Directory の設定と管理 手順 3/4 ページで 標準スキーマの設定** を選択します。**次へ** を選択します。
13. **Active Directory 手順 4a/4 ページで、グローバルカタログサーバーの IP アドレスを入力するか、DNS でグローバルカタログサーバーをルックアップする** オプションを選択し、Active Directory グローバルカタログサーバーの取得するために DNS ルックアップで使用する **ルートドメイン名** を入力します。役割グループの 1 つを選択して(手順 4B/4)有効な Active Directory ユーザーが所属する役割グループ情報を追加します。役割グループ名、グループドメイン、および役割グループの権限レベルを入力します。**OK**、**終了** の順に選択します。**完了** を選択し、Active Directory 概要ページを表示します。

シングルサインオンを使用した iDRAC6 へのログイン

1. 有効な Active Directory ネットワークアカウントを使用して管理ステーションにログインします。
2. iDRAC6 完全修飾ドメイン名を使用して iDRAC6 ウェブページにログインします。

`http://idracname.domain.com`

有効な Active Directory ネットワークアカウントを使用してログインすると、オペレーティングシステムにキャッシュされている資格情報によって iDRAC6 にログインできます。


iDRAC6 と LDAP ディレクトリサービスの使用


iDRAC6 は、LDAP ベースに認証をサポートする汎用的なソリューションを提供します。この機能は、ディレクトリサービス上でいかなるスキーマ拡張も必要としません。

iDRAC6 LDAP の実装を汎用的なものにするには、ユーザーをグループ化し、ユーザーとグループの関係をマッピングするために、異なるディレクトリサービスの共通点が使用されます。ディレクトリサービスの特定のアクションがスキーマです。たとえば、ユーザーとグループは、グループ、ユーザー、およびリンクにそれぞれ異なる属性名を付けることができます。これらのアクションは、iDRAC6 で設定できます。

ログインの構文(ディレクトリユーザーとローカルユーザー)


Active Directory とは異なり、LDAP ユーザーとローカルユーザーを区別するために、特殊文字(「@」、「\」、および「/」)を使用することはできません。ログインユーザーには、ドメイン名を除いたユーザー名を入力する必要があります。iDRAC6 は、ユーザー名をそのまま受け入れるため、ユーザー名とユーザードメインを分けることはしません。汎用 LDAP が有効な場合、iDRAC6 は最初に、ディレクトリユーザーとしてユーザーのログインを試みます。これに失敗すると、ローカルユーザーのルックアップが有効になります。

 **メモ:** Active Directory のログイン構文には、変化はありません。汎用 LDAP が有効な場合、GUI ログインページは、ドロップダウンメニューにこの iDRAC のみを表示します。


 **メモ:** 本リリースでは、openLDAP および openDS ベースのディレクトリサービスのみがサポートされています。openLDAP および OpenDS では、ユーザー名に「<」と「>」の文字は使用できません。

iDRAC6 ウェブインタフェースを使用した汎用 LDAP ディレクトリサービスの設定


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 ウェブインタフェースにログインします。
3. **システム ツリー**を展開し、**リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ**タブ → **ディレクトリサービス** → **汎用 LDAP ディレクトリサービス** の順でクリックします。
4. 汎用 LDAP の **設定と管理** ページでは、現在の iDRAC6 の汎用 LDAP 設定が表示されます。**汎用 LDAP の設定と管理** ページの下までスクロールし、**汎用 LDAP の設定** をクリックします。

 **メモ:** 本リリースでは、拡張なしの標準スキーマ Active Directory (SSAD) のみがサポートされます。


汎用 LDAP の設定と管理 手順 1/3 ページが表示されます。このページは、汎用 LDAP サーバーと通信する際、SSL 接続の開始時に使用されるデジタル証明書の設定に使用します。これらの通信は、LDAP オーバー SSL (LDAPS) を使用します。証明書の検証を有効にする場合、SSL 接続の開始時に LDAP サーバーによって使用される認証局 (CA) が発行した証明書をアップロードします。CA の証明書は、SSL 接続時に LDAP サーバーが提供する証明書が本物であるか検証するために使用されます。

 **メモ:** 本リリースでは、非 SSL ポートベースの LDAP バインドはサポートされていません。LDAP オーバー SSL のみがサポートされています。

5. 証明書の検証を有効にするには、**証明書の設定** の下の **証明書の検証を有効にする** を選択します。有効にすると、iDRAC6 は SSL ハンドシェイク時に CA 証明書を使用して LDAP サーバー証明書を検証します。無効にすると、iDRAC6 は SSL ハンドシェイク時の証明書の検証ステップをスキップします。システム管理者が SSL 証明書の検証を行わなくとも、セキュリティ境界内のドメインコントローラを信頼する場合、またはテスト中にいつでも証明書の検証を無効にすることができます。

 **注意:** 証明書の生成時に、LDAP サーバー証明書の件名フィールドに、CN = open LDAP の FQDN が設定されていることを確認してください(例: CN= openldap.lab)。証明書の検証を行うには、サーバー証明書の CN フィールドの値が iDRAC6 の LDAP サーバーアドレス フィールドの値と一致する必要があります。

6. **ディレクトリサービス 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:** フルパスと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。


7. **アップロード** をクリックします。

すべてのドメインコントローラの SSL サーバー証明書を署名するルート CA の証明書がアップロードされます。

8. **次へ** をクリックして、**汎用 LDAP の設定と管理手順 2/3** ページへ移動します。このページで、汎用 LDAP サーバーおよびユーザーアカウントの場所情報を設定します。

 **メモ:** 本リリースでは、汎用 LDAP ディレクトリサービスに対して、スマートカードベースの 2 要素認証(TFA)およびシングルサインオン(SS)はサポートされていません。

9. **汎用 LDAP を有効にする** を選択します。

 **メモ:** 本リリースでは、ネストされたグループはサポートされていません。ファームウェアは、グループに所属するメンバーを検索し、ユーザー DN を照合します。また、シングルドメインのみがサポートされています。クロスドメインはサポートされていません。

10. グループメンバーとして識別名(DN)を使用する場合は、**グループメンバーシップの検索に識別名を使用する** オプションを選択します。iDRAC6 は、ディレクトリから取得したユーザー DN とグループのメンバーを比較します。このオプションを選択しない場合、ログインユーザーによって提供されるユーザー名がグループのメンバーと比較されます。

11. **LDAP サーバーアドレス** フィールドに、LDAP サーバーの FQDN または IP アドレスを入力します。同じドメイン用の複数の冗長 LDAP サーバーを指定するには、カンマ区切りですべてのサーバーをリストします。iDRAC6 は、接続が確立されるまで、各サーバーに対して一つずつ接続を試みます。

12. **LDAP サーバーポート** フィールドに、LDAP オーバー SSL で使用するポート番号を入力します。デフォルトは 636 です。

13. ログインユーザーの DN を検索する際に、サーバーへのバインドに使用するユーザーの DN を **バインド DN** フィールドに入力します。指定しない場合は、匿名バインドが使用されます。

14. **バインド DN** と共に使用する **バインドパスワード** を入力します。匿名バインドが許可されていない場合には、これは必須となります。

15. **検索するベース DN** フィールドに、すべての検索が開始されるディレクトリの DN を入力します。

16. **ユーザーログインの属性** フィールドに、検索するユーザー属性を入力します。デフォルトは UID です。選択したベース DN 内で一意であることが推奨されます。そうでない場合は、ログインユーザーの一意性を確保できるように検索フィルタを設定する必要があります。属性と検索フィルタの組み合わせでユーザー DN を一意に識別できない場合は、ログインに失敗します。

17. **グループメンバーシップの属性** フィールドで、グループメンバーシップの確認に使用する LDAP 属性を指定します。これは、グループクラスの属性である必要があります。指定しない場合、iDRAC6 は member および unique member の属性を使用します。

18. **検索フィルタ** フィールドに、有効な LDAP 検索フィルタを入力します。ユーザー属性で選択したベース DN 内のログインユーザーを一意に識別できない場合は、フィルタを使用します。指定しない場合、ツリー内のすべてのオブジェクトを検索する objectClass=* のデフォルト値が使用されます。ユーザーによって設定されるこの追加の検索フィルタは、userDN 検索のみに適用され、グループメンバーシップの検索には適用されません。

19. **次へ** をクリックして、**汎用 LDAP の設定と管理手順 3a/3** ページへ移動します。このページでは、ユーザー認証に使用する権限グループを設定できます。汎用 LDAP が有効な場合、iDRAC6 ユーザーの認証ポリシーを指定するために、役割グループが使用されます。

20. **役割グループ** の下の **役割グループ** をクリックします。

汎用 LDAP の設定と管理手順 3b/3 ページが表示されます。このページでは、ユーザーの認証ポリシーの制御に使用される各役割グループを設定できます。

21. iDRAC6 と関連付けられる汎用 LDAP ディレクトリサービスで、役割グループを識別する **グループ識別名(DN)** を入力します。


22. **役割グループの特権** セクションでは、**役割グループの特権レベル** を選択して、グループに関連付けられる特権を指定します。たとえば、**システム管理者** を選択すると、そのアクセス権レベルのすべての特権が選択されます。

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 Web Server は、役割グループの設定が表示されている **汎用 LDAP の設定と管理手順 3a/3 ページ**に戻します。

24. 必要に応じて、追加の役割グループを設定します。

25. **汎用 LDAP の設定と管理** 概要ページに戻るには、**完了** をクリックします。
26. 汎用 LDAP 設定を確認するには、**テスト設定** をクリックします。
27. LDAP 設定をテストするディレクトリユーザーのユーザー名とパスワードを入力します。フォーマットは、使用される ユーザーログインの属性 に依存し、入力されるユーザー名は選択した属性値と一致する必要があります。

 **メモ:** 「証明書の検証を有効にする」が選択された状態で LDAP 設定をテストする場合、LDAP サーバーは IP アドレスではなく、FQDN で識別されなければなりません。IP アドレスで LDAP サーバーが識別される場合、iDRAC6 が LDAP サーバーと通信できないため、証明書の検証は失敗します。

テスト結果およびテストログが表示されます。これで、**汎用 LDAP ディレクトリサービス**の設定を完了しました。

よくあるお問い合わせ(FAQ)

Active Directory ログインの問題

Active Directory シングルサインオンを使用して iDRAC6 にログインするには約 4 分かかります。

通常の Active Directory シングルサインオンによるログインの所要時間は、10 秒以内ですが、iDRAC6 ネットワーク ページで **優先 DNS サーバー** と **代替 DNS サーバー** を指定し、優先 DNS サーバーでエラーが発生した場合には、4 分近くかかることがあります。DNS サーバーがダウンしていると、タイムアウトになります。iDRAC6 は代替 DNS サーバーを使用してログインを処理します。

Windows Server 2008 Active Directory にあるドメインに Active Directory を設定し、次のように設定しました。ドメインには子ドメイン(サブドメイン)があり、ユーザーとグループは同じ子ドメインにあります。ユーザーはグループのメンバーです。この場合、子ドメインにあるユーザーを使用して iDRAC6 にログインしようとすると、Active Directory シングルサインオンに失敗します。

これはグループタイプの間違いが原因と考えられます。Active Directory サーバーには次の 2 種類のグループがあります。

1. **セキュリティ:** セキュリティグループを使用すると、ユーザーとコンピュータの共有リソースへのアクセスを管理したり、グループポリシーの設定をフィルタしたりできます。
1. **配布:** 配布グループは、電子メール配布リストとして使用するだけが目的です。

グループタイプが常に **セキュリティ** であることを確認してください。配布グループを使用してオブジェクトに権限を割り当てたり、グループポリシー設定をフィルタすることはできません。

Active Directory ログインに失敗しました。どうすればいいですか。

iDRAC6 は、ウェブインタフェースで診断ツールを提供します。

1. ウェブインタフェースから、システム管理者権限のあるローカルユーザーとしてログインします。
2. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** → **Microsoft Active Directory** の順でクリックします。

Active Directory 概要の画面が表示されます。

3. 画面の下までスクロールし、**テストの設定** をクリックします。

Active Directory **設定のテスト** 画面が表示されます。

4. テストユーザー名とパスワードを入力し、**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。また、iDRAC6 は問題解決に役立つ詳細なテスト結果もログに記録します。

問題が解消されない場合は、Active Directory 設定を設定し、ユーザー設定を変更して、テストユーザーが認証手順に成功するまで、テストを繰り返し実行します。

証明書の検証を有効にしましたが、Active Directory の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。問題は何ですか。また、どのように修復できますか。

```
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かどうか、また 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どうか確認してください。
```

証明書の検証が有効になっていると、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。iDRAC6 の日付と証明書の有効期限を確認してください。
1. 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。
 - o IP アドレスを使用している場合は、「[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した。何が問題なのでしょう。](#)」を参照してください。
 - o FQDN を使用している場合は、ドメインの FQDN 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 を使用します。

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。

まず、設定のテスト機能を用いて、問題を診断します。手順については、「[Active Directory ログインに失敗しました。どうすればいいですか。](#)」を参照してください。

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。

最も一般的な問題については、本項で説明します。なお、一般的には、次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。
 - a. Active Directory の **設定と管理 手順 2/4** ページで **Active Directory 有効** チェックボックスがオンであることを確認します。
 - b. 証明書の検証を有効にしている場合は、iDRAC6 に正しい Active Directory ルート CA 証明書をアップロードしたことを確認します。証明書は **現在の Active Directory CA 証明書** 領域に表示されます。iDRAC6 の日時が CA 証明書の有効期限内であることを確認します。
 - c. 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 Active Directory の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** が Active Directory の設定と一致することを確認します。
 - d. **ネットワーク** 画面に移動します。**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **ネットワーク** の順に選択します。
DNS の設定が正しいことを確認します。
 - e. ドメインコントローラの SSL 証明書を調べて、iDRAC6 の日時が証明書の有効期限内であることを確認します。

Active Directory 証明書の検証

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した。何が問題なのでしょう。

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。次のいずれかの処置を実施することで、問題を解決できます。

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。
1. 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。
1. 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。

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と、ハッカーはドメインコントローラになりすまし、SSL 接続を乗っ取る危険があります。証明書の検証なしに、自分のセキュリティ境界内のドメインコントローラをすべて信頼する場合は、GUI または CLI を使用して無効にすることもできます。

拡張および標準スキーマ

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。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いいですか。

iDRAC6 オブジェクトが存在するドメインにサービスを提供している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。

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、拡張スキーマで使用されないグローバルカタログアドレスを設定できません。

標準スキーマを使用し、ユーザーと役割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使用できます。

標準スキーマを使用し、すべてのユーザーと役割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の仕組みを教えてください。

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ます。ユーザーおよび役割グループがそのドメインに属する場合は、権限が保存されます。

グローバルコントローラ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をクエリします。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す。

その他

iDRAC6 は、常に LDAP オーバー SSL を使用しますか。

はい。伝送はすべて、636 または 3269、あるいはその両方のセキュアポートを経由します。

設定のテスト中、iDRAC6 は問題を特定するためにのみ、LDAP 接続を行います。不安定な接続では LDAP バインドを行いません。

iDRAC6 は NetBIOS 名をサポートしていますか。

このリリースでは、サポートされていません。

[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™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [iDRAC6 へのスマートカードログインの設定](#)
- [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イン** を有効にすると、2 要素認証 (TFA) 機能がサポートされます。

従来の認証方式では、ユーザーの認証にユーザー名とパスワードを使用します。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、つまり使用している装置 (スマートカード、物理デバイス) と知っている情報 (パスワードや PIN などのシークレットコード) の入力を義務付けて、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**の要素を提供して身元を証明する必要があります。


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 スマートカードログイン機能を有効にするには、以下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。
2. iDRAC6 ウェブインタフェースにログインします。
3. **Active Directory の設定と管理 手順 1/4** 画面が表示されます。
4. Active Directory サーバーの SSL 証明書を検証するには、**証明書の設定** で **証明書の検証有効** チェックボックスをオンにします。Active Directory の SSL 証明書を検証しない場合は、「[手順 6](#)」に進んでください。
5. **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て、**アップロード** をクリックします。フルパスおよび完全な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。アップロードした Active Directory CA 証明書の証明書情報は、**現在の Active Directory CA 証明書** セクションに表示されます。
6. **次へ** をクリックします。Active Directory の設定と管理 **手順 2/4** 画面が表示されます。
7. **Active Directory 有効** チェックボックスをオンにします。
8. **スマート カードログインを有効にする** を選択してスマートカードログインを有効にします。以降 GUI を使用してログイン試行すると、スマートカードログインのプロンプトが表示されます。
9. **ユーザードメイン名** を追加し、ドメインコントローラサーバーアドレスの IP アドレスを入力します。**次へ** を選択します。
10. **Active Directory の設定と管理 手順 3/4** ページで **標準スキーマの設定** を選択します。**次へ** を選択します。
11. **Active Directory 手順 4a/4** ページで、**グローバルカタログサーバー** の IP アドレスを入力します。役割グループの 1 つを選択して (**役割グループの設定 手順 4B/4** ページ)、有効な Active Directory ユーザーが属する役割グループの情報を追加します。**グループ名**、**グループのドメイン**、**役割グループの権限** を入力します。OK、終了 の順に選択します。完了を選択した後、**Active Directory** 概要ページの一番下にスクロールして、**Kerberos Keytab アップロード** を選択します。
12. 有効な Kerberos Keytab ファイルをアップロードします。Active Directory サーバーと iDRAC6 の時刻が同期していることを確認してください。keytab ファイルをアップロードする前に、時刻とタイムゾーンの両方が正しいことを確認してください。keytab ファイル作成の詳細については、「[Kerberos 認証を有効にする方法](#)」を参照してください。

スマート カードログインを有効にする オプションをクリアして、TFA スマートカードログイン機能を無効にします。次回 iDRAC6 の GUI にログインしたときに、Microsoft® Active Directory® またはローカルログインのユーザー名とパスワードの入力を要求されます。これはウェブインタフェースのデフォルトのログインプロンプトとして表示します。

Active Directory スマートカード認証を使用した iDRAC6 へのログイン

 **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、スマートカードリーダー 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 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 アドレス> 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. スマートカードを挿入します。
3. PIN を入力して、**ログイン** 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:** スマートカードをリーダーに入れたままにしないで、ログイン状態を継続できます。

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。

Active Directory スマートカードログインを使用して iDRAC6 にログインするのに約 4 分かかります。

標準的な Active Directory スマートカードログインは通常 10 秒を要しますが、iDRAC6 の **ネットワーク** ページで **優先 DNS サーバー** と **代替 DNS サーバー** を指定している場合、優先 DNS サーバーでエラーが発生すると、iDRAC6 へのログインに 4 分近くかかることがあります。DNS サーバーがダウンしていると、タイムアウトになります。iDRAC6 は代替 DNS サーバーを使用してログインを処理します。

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どうかを確認する一般的なチェックとして、Windows のログオン(Ctrl-Alt-Del) 画面で、スマートカードをリーダーに挿入し、Windows でスマートカードが検出され、PIN ダイアログボックスが表示されるかどうかを調べます。

不正なスマートカード PIN

間違った PIN で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どうかをチェックします。このような場合は、新しいスマートカードの入手方法について、組織のスマートカード発行者に問い合わせてください。

Active Directory ユーザーとして iDRAC6 にログインできません

- 1 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。スマートカードログオンを無効にするには、RACADM で次のコマンドを使用します。

```
racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0
```

- 1 64 ビット Windows プラットフォームの場合、64 ビットバージョンの「Microsoft Visual C++ 2005 再配布可能パッケージ」が導入されていると、iDRAC6 認証プラグインが正しくインストールされません。プラグインが正常にインストールされて実行されるには、32 ビットバージョンの「Microsoft Visual C++ 2005 再配布可能パッケージ」を導入する必要があります。
- 1 エラーメッセージ「スマートカードプラグインをロードできません。Not able to load the Smart Card Plug-in. Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in (IE の設定を確認するか、スマートカードプラグインを使用する権限がない可能性があります)」が表示された場合は、「Microsoft Visual C++ 2005 再配布可能パッケージ」をインストールしてください。このファイルは Microsoft のウェブサイト www.microsoft.com にあります。C++ 再配布可能パッケージの 2 種類の配布バージョンがテストされ、Dell スマートカードプラグインをロードできます。

表 7-1 C++ 再配布可能パッケージの配布バージョン

再配布パッケージのファイル名	バージョン	リリース日	サイズ	説明
vc redistrib_x86.exe	6.0.2900.2180	2006 年 3 月 21 日	2.56 MB	MS Redistributable 2005
vc redistrib_x86.exe	9.0.21022.8	2007 年 11 月 7 日	1.73 MB	MS Redistributable 2008

- 1 Kerberos 認証が機能するには、iDRAC6 とドメインコントローラサーバーの時差が 5 分以内であることを確認してください。iDRAC6 の時刻は **システム → リモートアクセス → iDRAC6 → プロパティ → リモートアクセス情報** ページ、ドメインコントローラの時刻は画面の右下隅の時刻を右クリックして表示します。タイムゾーンのオフセットはポップアップ画面に表示されます。米国中央標準時(CST)の場合、これは -6 です。iDRAC6 の時刻を同期するには(リモートまたは Telnet/SSH RACADM から)、次の RACADM のタイムゾーンオフセットコマンドを使用します。racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <オフセット値の分> たとえば、システムの時刻が GMT -6(米国中央標準時)で、時刻が 2PM であれば、iDRAC6 の時刻を GMT 時刻の 18:00 に設定します。その場合、上記のコマンドのオフセット値に「360」と入力します。また、cfgRacTuneDaylightoffset を使用すると、夏時間の調整ができます。この操作により、毎年 2 回夏時間の調整をするときに時刻を変更しなくても済みます。あるいは、上の例のオフセットに「300」を使用して誤差を見込みます。

[目次ページに戻る](#)

[目次ページに戻る](#)

Kerberos 認証を有効にする方法

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [シングルサインオンとスマートカードを使用した Active Directory 認証の必要条件](#)
- [iDRAC6 にシングルサインオン認証とスマートカード使用の Active Directory 認証を設定する方法](#)
- [シングルサインオンログインに使用する Active Directory ユーザーの設定](#)
- [Active Directory ユーザーのシングルサインオンを使用した iDRAC6 へのログイン](#)
- [Active Directory ユーザーに対するスマートカードログインの設定](#)
- [TFA と SSO を使用する iDRAC6 ログインのシナリオ](#)

Kerberos は、セキュリティ保護されていないネットワークでシステムが安全に通信できるネットワーク認証プロトコルです。システムが本物であることをシステム自体が証明できるようになっています。高レベルの認証基準を満たすため、iDRAC6 では Kerberos ベースの Active Directory® 認証を使用して、Active Directory のスマートカードログインとシングルサインオンログインをサポートするようになりました。

Microsoft® Windows® 2000、Windows XP、Windows Server® 2003、Windows Vista®、および Windows Server 2008 では、デフォルトの認証方式として Kerberos を使用しています。

iDRAC6 では、Kerberos を使用して Active Directory シングルサインオンと Active Directory スマートカードログインという 2 種類の認証方式をサポートしています。シングルサインオンでログインする場合は、ユーザーが有効な Active Directory アカウントでログインした後、オペレーティングシステムにキャッシュされているユーザー資格情報が使用されます。

Active Directory スマートカードでログインする場合は、Active Directory ログインを有効にするために、スマートカードベースの 2 要素認証 (TFA) が資格情報として使用されます。

iDRAC6 の時刻がドメインコントローラの時刻と異なる場合は、iDRAC6 の Kerberos 認証に失敗します。最大 5 分のオフセットが許可されています。認証に成功するには、サーバーの時刻をドメインコントローラの時刻と同期してから iDRAC6 をリセットしてください。

また、次の RACADM タイムゾーンオフセットコマンドを使用して時刻を同期することもできます。

```
racadm config -g cfgRacTuning -o  
cfgRacTuneTimeZoneOffset <オフセット値>
```

シングルサインオンとスマートカードを使用した Active Directory 認証の必要条件

- 1 iDRAC6 に Active Directory ログインを設定します。
- 1 Active Directory のルートドメインに iDRAC6 をコンピュータとして登録します。
 - a. システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → ネットワーク サブタブの順にクリックします。
 - b. 有効な 優先 / 代替 DNS サーバー の IP アドレスを入力します。この値は、ルートドメインの一部である DNS の IP アドレスで、ユーザーの Active Directory アカウントを認証します。
 - c. DNS に iDRAC6 を登録する を選択します。
 - d. 有効な DNS ドメイン名 を入力します。
 - e. ネットワーク DNS の設定が Active Directory の DNS 情報と一致することを確認します。

詳細については、iDRAC6 オンラインヘルプを参照してください。

新しい 2 種類の認証方式をサポートするため、Windows Kerberos ネットワークで Kerberos サービスとして iDRAC6 が自動的に有効になる設定がサポートされています。iDRAC6 で Kerberos を設定するには、Windows Server の Active Directory で Windows Server 以外の Kerberos サービスをセキュリティプリンシパルとして設定すると同じ手順を実行します。


Microsoft ツール ktpass (Microsoft がサーバーインストール CD/DVD の一部として提供) は、ユーザーアカウントにバインドされているサービスプリンシパル名 (SPN) を作成し、信頼情報を MIT 形式の Kerberos keytab ファイルにエクスポートするときに使用します。これにより、外部ユーザーまたはシステムと、キー配付センター (KDC) の間の信頼関係が確立されます。keytab ファイルには暗号キーが含まれており、これを使用してサーバーと KDC の間の情報を暗号化します。ktpass ツールを使用すると、Kerberos 認証をサポートする UNIX ベースのサービスは Windows Server の Kerberos KDC サービスによって提供される相互運用性を使用できます。

ktpass ユーティリティから取得した keytab はファイルアップロードとして iDRAC6 で使用可能になり、ネットワークで Kerberos 対応サービスとして有効になります。

iDRAC6 は Windows 以外のオペレーティングシステムを搭載するデバイスであるため、iDRAC6 を Active Directory のユーザーアカウントにマッピングするドメインコントローラ (Active Directory サーバー) で、ktpass ユーティリティ (Microsoft Windows の一部) を実行します。

たとえば、次の ktpass コマンドを使用して、Kerberos keytab ファイルを作成します。

```
C:\> ktpass.exe -princ HTTP/idracname.domainname.com@DOMAINNAME.COM -mapuser DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5 -ptype  
KRB5_NT_PRINCIPAL -pass <パスワード> +DesOnly -out c:\krbkeytab
```


 **メモ:** 作成した keytab ファイルの iDRAC6 ユーザーに問題が検出された場合は、新しいユーザーと keytab ファイルを作成してください。最初に作成したファイルを再実行すると、正しく設定されません。


上記のコマンドが正しく実行されたら、次のコマンドを実行します。

```
C:\> setspn -a HTTP/idracname.domainname.com username
```


iDRAC6 が Kerberos 認証に使用する暗号タイプは DES-CBC-MD5 です。プリンシパルタイプは KRB5_NT_PRINCIPAL です。サービスプリンシパル名のマッピング先ユーザーアカウントのプロパティで、次のアカウントプロパティが **有効** になっている必要があります。

- 1 このアカウントに DES 暗号化を使用する

 **メモ:** ktpass コマンドの -mapuser オプションで使用する Active Directory ユーザーアカウントを作成する必要があります。また、生成した keytab ファイルのアップロード先となる iDRAC6 DNS 名と同じ名前である必要があります。

 **メモ:** 最新の ktpass ユーティリティを使用して keytab ファイルを作成することをお勧めします。また、keytab ファイルの生成中、idracname と サービスプリンシパル名 に小文字を使用してください。

この手順によって、iDRAC6 にアップロードする keytab ファイルが生成されます。

 **メモ:** keytab には暗号化キーが含まれているので、安全な場所に保管してください。

ktpass ユーティリティの詳細については、Microsoft のウェブサイト [http://technet.microsoft.com/en-us/library/cc779157\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx) を参照してください。

- 1 iDRAC6 の時刻が Active Directory ドメインコントローラと同期している必要があります。

iDRAC6 にシングルサインオン認証とスマートカード使用の Active Directory 認証を設定する方法

Active Directory のルートドメインから取得した keytab を iDRAC6 にアップロードするには、以下の手順を実行します。

1. システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → ディレクトリサービス → Microsoft Active Directory の順でクリックします。
2. Active Directory 概要ページの一番下の Kerberos Keytab のアップロード をクリックします。
3. Kerberos Keytab のアップロード ページで、アップロードする keytab ファイルを選択し、適用 をクリックします。

CLI RACADM コマンドを使用してファイルを iDRAC6 にアップロードすることもできます。次のコマンドで keytab ファイルを iDRAC6 にアップロードします。

```
racadm krbkeytabupload -f <ファイル名>
```


<ファイル名> は keytab ファイルの名前です。

シングルサインオンログインに使用する Active Directory ユーザーの設定


Active Directory のシングルサインオンログイン機能を使用する前に、iDRAC6 に Active Directory ログインを設定し、システムへのログインに使用するドメインユーザーアカウントで iDRAC6 Active Directory ログインを有効にする必要があります。

Active Directory のログイン設定を有効にしていることも確認してください。また、Active Directory のルートドメインから取得した有効な keytab ファイルを iDRAC6 にアップロードして、iDRAC6 を Kerberos サービスとして有効にする必要があります。

Active Directory ユーザーのシングルサインオンを使用した iDRAC6 へのログイン

 **メモ:** iDRAC6 にログインするには、Microsoft Visual C++ 2005 Libraries の最新の実行時 コンポーネントが必要です。詳細については、Microsoft のウェブサイトを参照してください。

1. Active Directory の有効なアカウントを使ってシステムにログインします。
2. ブラウザのアドレスバーに次の形式で iDRAC6 の名前を入力します。https://idracname.domainname.com(例: https://idrac-test.domain.com)。

 **メモ:** ブラウザの設定によっては、この機能を最初に使用するとき、シングルサインオンプラグインのダウンロードとインストールを要求されることがあります。

 **メモ:** SSO の場合、Internet Explorer を使用しているときは、ツール → インターネットオプション → セキュリティタブ → ローカルイントラネット → に移動し、サイト → をクリックし、詳細 をクリックしてからエントリ *.domain.com をゾーンに追加します。Firefox を使用している場合は、about:config と入力し、domain.com をプロパティ network.negotiate-auth.delegation-uris と network.negotiate-auth.trusted-uris に追加します。


次の場合は、適切な Microsoft Active Directory 特権で iDRAC6 にログインできます。


- 1 Microsoft Active Directory のユーザーである
- 1 iDRAC6 で Active Directory にログインできるように設定されている
- 1 iDRAC6 で Kerberos Active Directory 認証が有効になっている

Active Directory ユーザーに対するスマートカードログオンの設定

Active Directory スマートカードのログオン機能を使用する前に、iDRAC6 に Active Directory ログインを設定し、スマートカードを発行したユーザーアカウントで iDRAC6 Active Directory ログインを有効にする必要があります。

Active Directory のログイン設定を有効にしていることも確認してください。また、Active Directory のルートドメインから取得した有効な keytab ファイルを iDRAC6 にアップロードして、iDRAC6 を Kerberos サービスとして有効にする必要があります。

 **メモ:** Active Directory に拡張スキーマが設定されている場合、スマートカードベースの 2 要素認証(TFA)機能とシングルサインオン(SSO)機能はサポートされません。さらに、Internet Explorer® を装備した Microsoft Windows オペレーティングシステムでは、スマートカードベースの TFA とシングルサインオンの両方がサポートされます。Firefox ブラウザでは、スマートカードベースの TFA は**サポートされませんが**、iDRAC6 へのシングルサインオンはサポートされます。

 **注意:** iDRAC6 にログインするには、Microsoft Visual C++ 2005 Libraries の**最新の実行時コンポーネント(32 ビットの C++ ライブラリ)**がインストールされていることを確認してください。これがインストールされていないと、スマートカードプラグインがロードされず、iDRAC6 にログインできません。詳細については、Microsoft のウェブサイト www.microsoft.com を参照してください。

次の場合は、適切な Microsoft Active Directory 特権で iDRAC6 にログインできます。

- 1 Microsoft Active Directory のユーザーである
- 1 iDRAC6 で Active Directory にログインできるように設定されている
- 1 iDRAC6 で Kerberos Active Directory 認証が有効になっている
- 1 ログインしようとする Active Directory ユーザーに関連付けられているスマートカードの正しい 暗証番号を入力した

TFA と SSO を使用する iDRAC6 ログインのシナリオ

CMC のウェブ GUI から iDRAC6 にログインすると、iDRAC/iDRAC6 と CMC のバージョンの違いや TFA が有効か SSO が有効かによって、以下のようなログイン画面が表示されます。

- 1 TFA が有効の CMC バージョン 2.1 以降と、TFA が有効の iDRAC6 バージョン 2.1 以降:暗証番号を入力する iDRAC6 ログイン。
- 1 TFA が有効の CMC バージョン 2.1 以降と、TFA が無効で SSO が無効の iDRAC6 バージョン 2.1 以降:ユーザー名、ドメイン、パスワードを入力する iDRAC6 ログインプロンプト。
- 1 TFA が有効の CMC バージョン 2.1 以降と、TFA が無効で SSO が有効の iDRAC6 バージョン 2.1 以降: SSO を使用する iDRAC6 の自動ログイン。
- 1 TFA が有効の CMC バージョン 2.1 以降と iDRAC6 バージョン 2.0:ユーザー名、ドメイン、パスワードを入力する iDRAC6 ログインプロンプト。
- 1 TFA が有効の CMC バージョン 2.1 以降と iDRAC バージョン 1.x:ユーザー名、ドメイン、パスワードを使用する iDRAC6 ログインプロンプト。
- 1 CMC バージョン 2.0 以前と、TFA が有効の iDRAC6 バージョン 2.1 以降:暗証番号を入力する iDRAC6 ログインプロンプト。
- 1 TFA が無効の CMC バージョン 2.1 以降と、TFA が有効で SSO が無効の iDRAC6 バージョン 2.1 以降:暗証番号を入力する iDRAC6 プロンプト。
- 1 TFA が無効の CMC バージョン 2.1 以降と、TFA が無効で SSO が有効の iDRAC6 バージョン 2.1 以降: SSO を使用する iDRAC6 ログイン。

[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™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [システム概要](#)
- [システム詳細](#)
- [WWN/MAC](#)
- [サーバー正常性](#)

システム概要

システム概要 ページでは、ご利用のシステムの正常性とその他の基本的な iDRAC6 情報を一目で把握でき、システム正常性および情報のページへアクセスするためのリンクが提供されます。また、このページから一般的なタスクを素早く実行し、システムイベントログ (SEL) に記録された最近のイベントを閲覧できます。

システム概要 ページにアクセスするには、**システム** → **プロパティ** タブ → **システム概要** の順でクリックします。**システム概要** ページの各項の詳細については、iDRAC6 オンラインヘルプを参照してください。

システム詳細

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 Integrated Dell Remote Access Controller 6 (iDRAC6) - Enterprise

メインシステムエンクロージャ

システム情報

iDRAC6 の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以下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 - 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

 **メモ:** OS 名 フィールドは、管理下システムに Dell OpenManage™ Server Administrator がインストールされている場合にのみ自動入力されます。その例外が VMware® オペレーティングシステム名で、これらは管理下システムに Server Administrator がインストールされていない場合でも表示されます。

I/O メザニカード

iDRAC6 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 メザニカードについて、以下の情報を提供します。

- 1 接続 - 管理下サーバーにインストールされている I/O メザニカードのリスト
- 1 カードタイプ - インストールされているメザニカード / 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カードのモデル番号、タイプ、または説明

内蔵ストレージカード

iDRAC6 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内蔵ストレージコントローラカードについて、以下の情報を提供します。

- 1 カードタイプ - 搭載されているストレージカードのモデル名を表示します (例: SAS6/IR)。

自動リカバリ

iDRAC6 ウェブインタフェースのこの部分は、Open Manage Server Administrator で設定された管理下サーバーの自動リカバリ機能の現在の処理モードについて詳しく説明します。

- 1 リカバリ処置 - システム障害やハング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**、または **パワーサイクル** です。

- 1 初期カウントダウン — システムハング検出後、iDRAC6 がリカバリ処置を実行するまでの時間(秒単位)。
- 1 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(秒単位)。


Integrated Dell Remote Access Controller 6(iDRAC6) - Enterprise

iDRAC6 情報

iDRAC6 ウェブインタフェースのこの部分は、iDRAC6 自体について以下の情報を提供します。


- 1 日付 / 時刻 — iDRAC6 の現在の日付と時刻(前回のページ更新時点)を表示します。
- 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 iDRAC6 ファームウェアの現在のバージョンを表示します。
- 1 CPLD バージョン — Complex Programmable Logic Device(CPLD)ボードのバージョンを表示します。
- 1 ファームウェアのアップデート — iDRAC6 ファームウェアが最後に正しくアップデートされた日時を表示します。
- 1 MAC アドレス — iDRAC6 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 アドレスを表示します。

IPv4 の設定

- 1 有効 — IPv4 プロトコルのサポートが有効か無効かを表示します。
 **メモ:** デフォルトでは IPv4 プロトコルオプションは有効になっています。
- 1 DHCP 有効 — iDRAC6 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 IP アドレス — iDRAC6 (管理下サーバーではない)に関連付けられた IP アドレスを表示します。
- 1 サブネットマスク — iDRAC6 に設定されたTCP/IP サブネットマスクを表示します。
- 1 ゲートウェイ — iDRAC6 に設定されたネットワークゲートウェイの IP アドレスを表示します。
- 1 DHCP を使用して DNS サーバーのアドレスを取得する — DNS サーバーのアドレス取得に DHCP を使用するかどうかを表示します。
- 1 優先 DNS サーバー — 現在アクティブなプライマリ DNS サーバーを表示します。
- 1 代替 DNS サーバー — 代替の DNS サーバーを表示します。

IPv6 の設定

- 1 有効 — IPv6 プロトコルのサポートが有効か無効かを表示します。
- 1 自動設定有効 — 自動設定が有効か無効かを表示します。
- 1 リンクのローカルアドレス — iDRAC6 NIC の IPv6 アドレスを表示します。
- 1 IPv6 アドレス 1-16 — iDRAC6 NIC の IPv6 アドレスを最大 16(IPv6 アドレス 1 ~ IPv6 アドレス 16)表示します。
- 1 ゲートウェイ — iDRAC6 に設定されたネットワークゲートウェイの IP アドレスを表示します。
- 1 DHCPv6 を使用して DNS サーバーのアドレスを取得する — DNS サーバーのアドレス取得に DHCP を使用するかどうかを表示します。
- 1 優先 DNS サーバー — 現在アクティブなプライマリ DNS サーバーを表示します。
- 1 代替 DNS サーバー — 代替の DNS サーバーを表示します。

 **メモ:** この情報は iDRAC6 → **プロパティ** → **リモートアクセス情報** の順にクリックしても表示できます。

内蔵 NIC の MAC アドレス


- 1 NIC 1 — 内蔵ネットワークインタフェースコントローラ(NIC)1 の MAC アドレスを表示します。MAC アドレスは、ネットワーク上の各ノードを、メディアアクセスコントロールレイヤで一意に識別します。iSCSI NIC とは、ホストコンピュータ上で iSCSI スタックを使用しているネットワークインタフェースコントローラです。Ethernet NIC は、サーバーのシステムバスに接続される有線の Ethernet 標準をサポートしています。
- 1 NIC 2 — ネットワーク内で内蔵 NIC 2 を一意に識別する MAC アドレスを表示します。
- 1 NIC 3 — ネットワーク内で内蔵 NIC 3 を一意に識別する MAC アドレスを表示します。内蔵 NIC 3 の MAC アドレスは、すべてのシステムで表示されない場合があります。
- 1 NIC 4 — ネットワーク内で内蔵 NIC 4 を一意に識別する MAC アドレスを表示します。内蔵 NIC 4 の MAC アドレスは、すべてのシステムで表示されない場合があります。

WWN/MAC

インストールされている I/O メザニンカードおよび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するには、**システム** → **プロパティ**タブ → **WWN/MAC** の順にクリックします。CMC で FlexAddress(フレックスアドレス) 機能が有効になっている場合は、グローバルに割り当てられた(シャresh割り当ての)持続的 MAC アドレスが各 LOM のハードウェアに組み込まれている値を置き換えます。

サーバー正常性

iDRAC6 および iDRAC6 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するには、**システム** → **プロパティ**タブ → **システム概要** → **サーバー正常性** の順にクリックします。**状態** 行には、各コンポーネントの状態が表示されます。ステータスアイコンのリストとその意味は、「[表 20-3](#)」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。

iDRAC6

リモートアクセス情報 画面には、iDRAC6 に関する重要な詳細情報が表示されます。これには、iDRAC6 の名前、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、iDRAC6 の時間、IPMI バージョン、CPLD バージョン、サーバーの種類、およびネットワークパラメータなどが含まれます。画面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 画面には、Chassis Management Controller の正常性の状態、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起動** ボタンをクリックしても、CMC ウェブインタフェースを起動できます。詳細については、『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。


 **メモ:** iDRAC6 から CMC ウェブ GUI を起動すると、同じ IP アドレス形式で検索が指定されます。たとえば、IPv6 アドレス形式で iDRAC6 ウェブ GUI を開いた場合は、CMC ウェブページも有効な IPv6 アドレスで開きます。

バッテリー

バッテリー 画面には、管理下システムのリアルタイムクロック(RTC)と CMOS 設定データストレージを管理するシステム基板コインセルバッテリーの状態が表示されます。

温度

温度 画面には、オンボードの周囲温度プローブが表示されます。警告 状態と 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の状態と一緒に表示されます。

 **メモ:** サーバーのモデルによっては、警告 状態と 失敗 状態の温度しきい値やプローブの正常性の状態が表示されない場合があります。


電圧

電圧プローブ 画面には、電圧プローブの状態と測定値が表示され、オンボード電圧レールや CPU コアセンサーなどの状態情報が提供されます。

電源モニタ

電源モニタ 画面では、以下のような監視情報と電力統計情報を表示できます。

- 1 電源モニタ - サーバーが使用している電力量(AC ワットで測定した 1 分間の平均電力値)を表示します。この値はシステムボード電流モニタによって報告されます。
- 1 アンペア数 - アクティブな電源装置の現在の消費量(アンペア単位の AC)を表示します。
- 1 電力追跡統計値 - 読み取り値が最後にリセットされてからシステムが使用した電力量について情報を表示します。
- 1 ピーク統計値 - 読み取り値が最後にリセットされてからシステムが使用したピーク電力量について情報を表示します。
- 1 電力消費量 - 過去 1 分間、過去 1 時間、過去 1 日間、過去 1 週間のシステムの電力消費量の平均、最小、最大と、電力時間の最大と最小を表示します。
- 1 グラフの表示 - 1 時間、24 時間、3 日間、1 週間の電力消費量をグラフで表示します。

 **メモ:** 電力とアンペア数は AC で測定されます。

CPU

CPU 画面は、管理下サーバーの各 CPU の正常性について報告します。この正常性の状態は、熱、電力、機能などの多数の個別テストをまとめたものです。


POST

POST コード 画面には、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後のシステム POST コード(16 進数)が表示されます。

他の正常性

他の正常性 画面からは、次のシステムログにアクセスできます。

- 1 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を表示します。
- 1 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後のシステム POST コード(16 進数)を表示します。
- 1 前回クラッシュ画面 - 一番新しいクラッシュ画面と時間を表示します。
- 1 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 → ログ タブ → システムイベントログ でも表示できます。

[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™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [電源の設定と管理](#)
- [電源モニタ](#)
- [電力バジェット](#)
- [電源制御](#)

Dell™ PowerEdge™システムには、電源管理の新機能と拡張機能が組み込まれています。ハードウェアからファームウェア、さらにシステム管理ソフトウェアへと、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。

メモ: iDRAC6 の電力管理ロジックは、ブレード サーバーに搭載されている Complex Programmable Logic Device (CPLD) を使用します。CPLD デバイスのアップデートは、デルサポートウェブサイト support.dell.com の [システムファームウェア](#) セクションまたは [システムボード](#) セクションから入手できます。CPLD ファームウェアの最新バージョンでブレードサーバーをアップデートすることをお勧めします。現在の CPLD ファームウェアバージョンは iDRAC6 のウェブ GUI に表示されています。

Dell PowerEdge システムは、数多くの電源モニタおよび管理機能を提供しています。

- 1 **電源モニタ:** iDRAC6 は、電力測定履歴を収集し、移動平均やピークなどを計算します。iDRAC6 ウェブインタフェースを使用すると、**電源モニタ** 画面でこれらの情報を確認できます。**電源モニタ** 画面下部の **グラフの表示** をクリックすることで、グラフ形式で情報を表示させることも可能です。詳細については、「[電源モニタ](#)」を参照してください。
- 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。詳細については、「[電力バジェット](#)」を参照してください。
- 1 **電源制御:** iDRAC6 を使用することで、管理下システム上でさまざまな電源管理操作をリモートから実行できます。詳細については、「[電源制御](#)」を参照してください。

電源の設定と管理

iDRAC6 ウェブインタフェースと RACADM コマンドラインインタフェース (CLI) を使用して、Dell PowerEdge システムの電源制御の管理と設定ができます。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。「[電源モニタの表示](#)」を参照してください。
- 1 最小および最大電力消費量を含む、サーバーの電力バジェット情報を表示できます。「[電力バジェットの表示](#)」を参照してください。
- 1 サーバーの電力バジェットのしきい値を表示できます。「[電力バジェットのしきい値](#)」を参照してください。
- 1 サーバーに電源制御操作 (例: 電源オン、電源オフ、システムリセット、パワーサイクル、正常なシャットダウンなど) を実行します。「[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。

電源モニタ

iDRAC6 は、継続的に Dell PowerEdge サーバーの消費電力を監視します。iDRAC6 は以下の電力値を計算し、ウェブインタフェースまたは RACADM CLI から情報を提供します。

- 1 累積システム電力
- 1 システムピーク電力とシステムピークアンペア数
- 1 平均、最小、最大の電力消費量
- 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)
- 1 最大と最小の電力時間

電源モニタの表示

ウェブインタフェースの使用

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 画面に以下の情報が表示されます。

電源モニタ

- 1 **状態:** **緑色のチェックマーク** は、電源状態が正常であること、**警告** は警告が発せられたこと、**重大** はエラー警告が発せられたことを示します。
- 1 **プローブ名:** センサーの名前を表示します。


- 1 **読み取り値**:プローブが報告するワット数を示します。
- 1 **警告しきい値**:システム動作に推奨される消費電力の許容量(ワットおよび BTU/時単位)。消費電力量がこの値を超えると、警告イベントが発生します。
- 1 **エラーしきい値**:システム動作に必要なとされる消費電力の最大許容量(ワットおよび BTU/時単位)。消費電力量がこの値を超えると、重要 / エラーイベントが発生します。

アンペア数

- 1 **場所**:システム基板センサーの名前を表示します。
- 1 **読み取り値**:現在の消費電力量(ACアンペア)。

電力追跡統計値とピーク統計値

- 1 **統計**:
 - **累積システム電力** には、サーバーの現在の累積エネルギー消費量が(キロワット / 時)で表示されます。この値は、システムによって消費される総エネルギー量を表します。表の最終行の **リセット** をクリックすることで、この値を 0 にリセットできます。
 - **システムピーク電力** は、システムのピーク値を AC ワットで示します。
 - **システムピークアンペア数** はシステムのピークアンペア数を示します。ピーク値は、**測定開始時刻** から現在までに記録された最高値です。ピーク時刻は、ピーク値が発生した時点です。テーブルの行の終わりで **リセット** をクリックすると、現在の瞬時値に戻ります(サーバーが実行中の場合、0 にはなりません)。リセットをクリックすると、測定開始時刻も現在の時刻に戻ります。
 - **測定開始時刻** 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。**累積システム電力**、**システムピークアンペア数**、および **システムピーク電力** 統計の場合、リセットするとピーク値に直ちに現在の瞬時値が反映されます。
 - **累積システム電力** の **現在の測定時刻** 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。**システムピークアンペア数** と **システムピーク電力** の場合、**ピーク時間** フィールドは、これらのピークが発生した時刻を表示します。
 - **読み取り値**:カウンタが開始してからの該当する統計値:**累積システム電力**、**システムピーク電力**、および**システムピークアンペア数**。


 **メモ**: 電力追跡統計は、システムのリセット全体にわたって保持されるため、指定した測定開始から現時点までのすべてのアクティビティを反映します。電力消費量表に表示された電力値は、それぞれの期間(過去 1 分間、1 時間、1 日間、1 週間)の累積平均です。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 **平均電力消費量**:過去 1 分間、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る最大および最小電力消費量。
- 1 **最大電力時間** および **最小電力時間**: 電力消費量が最大および最小になった時の時間(分、時間、日、週)。

グラフの表示

過去 1 時間、24 時間、3 日、1 週間の iDRAC6 の電力消費量をワット単位でグラフ表示するには、**グラフの表示** をクリックします。対象期間を選択するには、グラフの上のドロップダウンメニューを使用します。

 **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、電力消費量や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。

電力バジェット

電力バジェット 画面には、高負荷環境のシステムがデータセンターに提供する AC 電力消費量の範囲をカバーする電力しきい値制限が表示されます。


サーバーがパワーアップする前に、iDRAC6 は CMC にその電力エンベロープの要件を提供します。実際にサーバーが消費する電力に応じて、パワーアップ後に小さい電力エンベロープを要求する場合があります。時間の経過に伴い電力消費量が増えて、サーバーが最大割り当てに近い電力を消費している場合、iDRAC6 は最大潜在電力消費量の増大を要求し、電力エンベロープを上げることがあります。iDRAC6 が CMC に要求するのは最大潜在電力消費量の増大分だけです。電力消費量が減った場合に、最小潜在電力の減少は要求しません。

CMC は優先順位の低いサーバーの未使用電力を取り戻し、その電力を優先順位の高いインフラストラクチャモジュールやサーバーに割り当てます。

電力バジェットの表示

サーバーは、電源サブシステムの電力バジェット状態の概要を **電力バジェット** 画面に提供します。

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 ウェブインタフェースにログインします。
2. システム ツリーで **システム** をクリックします。
3. **電源管理** タブをクリックして、**電力バジェット** をクリックします。

電力バジェット 画面が表示されます。


電力バジェット情報 の表には、現在のシステム設定における電力しきい値の最小および最大値が表示されます。これらの情報は、高負荷環境におけるしきい値が設定されたシステムの AC 電力消費量の範囲をカバーします。

1. **最小潜在電力消費量** は、電力バジェットの最小しきい値を表します。
1. **最大潜在電力消費量** は、電力バジェットの最大しきい値を表します。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

管理下サーバーで、コマンドラインインタフェースを開き、次のコマンドを入力します。

```
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

電力バジェットしきい値を有効にすると、システム電力が制限されます。指定したしきい値内に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。


低負荷環境では実際の電力消費量の方が少ない場合もあり、パフォーマンスの調整が完了するまでは、一時的にしきい値を下回る可能性があります。

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. システム ツリーで **システム** をクリックします。
3. **電源管理** タブをクリックして、**電力バジェット** をクリックします。

電力バジェット 画面が表示されます。

4. **電力バジェットしきい値** をクリックします。

 **メモ:** 電力バジェットしきい値は、読み取り専用であるため、iDRAC6 で有効にしたり、設定を変更することはできません。

電力バジェットしきい値 表にはシステムの電力制限に関する情報が表示されます。

1. **有効** は、システムが電力バジェットしきい値を守るかどうかを示します。
1. **ワット単位のしきい値** と **BTU/時単位のしきい値** は、制限値をそれぞれ AC ワット単位と BTU/時で表示します。
1. **パーセント単位のしきい値(最大)** には、電力上限範囲のパーセントが表示されます。

RACADM の使用

管理下サーバーで、コマンドラインインタフェースを開き、次のコマンドを入力します。

ローカル RACADM から電力バジェットしきい値データを表示するには、コマンドプロンプトで次のコマンドを入力します。

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts
```

<電力上限値 AC ワット> を返します

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr
```

<電力上限値 BTU/時> を返します

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent
```


<電力上限値 %> を返します

 **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。

電源制御

iDRAC6 では、電源オン、リセット、正常なシャットダウン、マスク不可割り込み (NMI)、パワーサイクルなどをリモートから実行できます。再起動時と電源のオン / オフ時に、オペレーティングシステムを通じた正常なシャットダウンを実行するには、**電源制御** 画面を使用します。

サーバーに対する電源制御操作の実行

 **メモ:** 電源管理操作を実行するには、**システム管理者** 権限が必要です。

iDRAC6 では、電源オン、リセット、正常なシャットダウン、NMI またはパワーサイクルをリモートから実行できます。

ウェブインタフェースの使用


- iDRAC6 ウェブインタフェースにログインします。
- システムツリーで **システム** を選択します。
- 電源管理** タブをクリックします。
電源制御 画面が表示されます。
- 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)。サーバーの電源が既にオンの場合は、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。サーバーの電源が既にオフの場合、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。NMI は、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を可能にするためにシステム動作を一時停止させます。サーバーの電源が既にオフの場合、このオプションは無効になっています。
 - 正常なシャットダウン** は、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。サーバーの電源が既にオフの場合、このオプションは無効になっています。
 - システムのリセット(ウォームブート)** は、電源を切らずにシステムを再起動します。サーバーの電源が既にオフの場合、このオプションは無効になっています。
 - システムのパワーサイクル(コールドブート)** は、電源を切ってからシステムを再起動します。サーバーの電源が既にオフの場合、このオプションは無効になっています。
- 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。
- 選択した電源管理操作を実行するには、**OK** をクリックします。

RACADM の使用

ローカル RACADM から電源処置を実行するには、コマンドプロンプトで次のコマンドを入力します。

```
racadm serveraction <操作>
```

ここで、<操作> は、電源投入、電源切断、パワーサイクル、ハードリセットまたは電源状態を指します。

 **メモ:** 出力の詳細を含む serveraction の詳細については、「[serveraction](#)」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](#)

シリアルオーバー LAN の設定と使用

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [BIOS でシリアルオーバー LAN を有効にする](#)
- [iDRAC6 ウェブ GUI でのシリアルオーバー LAN の設定](#)
- [シリアルオーバー LAN \(SOL\) の使用](#)
- [オペレーティングシステムの設定](#)

シリアルオーバー LAN (SOL) は、従来シリアル I/O ポートに送信される管理下サーバーのテキストベースのコンソールデータを、iDRAC6 の専用帯域外 Ethernet 管理ネットワーク経由でリダイレクトできるようにする IPMI 機能です。SOL 帯域外コンソールを使うと、システム管理者はブレードサーバーのテキストベースのコンソールをネットワークアクセスのある任意の場所からリモート管理できます。SOL のメリットは次のとおりです。

- 1 タイムアウトなしにオペレーティングシステムにリモートアクセスする。
- 1 Windows の Emergency Management Services (EMS) または Special Administrator Console (SAC)、あるいは Linux シェルでホストシステムを診断する。
- 1 POST 中のブレードサーバーの進行状況を表示し、BIOS セットアッププログラムを再構成する (シリアルポートへのリダイレクト中)。

BIOS でシリアルオーバー LAN を有効にする

サーバーにシリアルオーバー LAN を設定するには、以下に説明する設定手順が必要になります。

1. BIOS でシリアルオーバー LAN を設定する (デフォルトは無効)
2. シリアルオーバー LAN 用に iDRAC6 を設定する
3. シリアルオーバー LAN の初期化方法を選択する (SSH、telnet、SOL プロキシ、IPMI ツール)
4. SOL 用のオペレーティングシステムを設定する

BIOS ではシリアル通信はデフォルトで **オフ** になっています。ホストテキストコンソールデータをシリアルオーバー LAN にリダイレクトするには、COM1 を介したコンソールのリダイレクトを有効にする必要があります。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. POST 中に <F2> キーを押して BIOS セットアップユーティリティを起動します。
3. シリアル通信にスクロールダウンして <Enter> キーを押します。

ポップアップウィンドウにシリアル通信リストと以下のオプションが表示されます。

- 1 オフ
- 1 コンソールリダイレクトなしでオン
- 1 コンソールリダイレクト使用でオン

矢印キーを使用して、オプション間を移動します。


4. **コンソールリダイレクト使用でオン** が有効になっていることを確認します。**シリアルポートアドレス** が COM1 であることを確認します。
5. **フェイルセーフボーレート** が、iDRAC6 で設定されている SOL ボーレートと同一であることを確認します。フェイルセーフボーレートと iDRAC6 の SOL ボーレートのデフォルト値は 115.2 kbps です。
6. **起動後のリダイレクト** が有効になっていることを確認します。このオプションは、以降の再起動でも BIOS SOL リダイレクトを有効にします。BIOS には **リモートターミナルタイプ** の値 VT100/VT220 と ANSI があります。
7. 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。

iDRAC6 ウェブ GUI でのシリアルオーバー 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** → **シリアルオーバー LAN 設定** の順に選択し、**シリアルオーバー LAN 設定** 画面を開きます。
2. **シリアルオーバー LAN を有効にする** オプションが選択されている (有効になっている) ことを確認します。デフォルトで有効になっています。

3. ボーレートドロップダウンメニューからデータ速度を選択して、IPMI SOL ボーレートを更新します。オプションは 9600 bps、19.2 kbps、57.6 kbps、115.2 kbps です。デフォルト値は 115.2 kbps です。
4. シリアルオーバー LAN の特権レベルの制限を選択します。

 **メモ:** SOL ボーレートが、BIOS で設定されているフェイルセーフボーレートと同一であることを確認します。

5. 変更した場合は **適用** をクリックします。

表 10-1 シリアルオーバー LAN 設定画面の設定

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は、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 9600 bps、19.2 kbps、57.6 kbps、 115.2 kbps の中から選択します。
チャネル権限レベルの制限	シリアルオーバー LAN の特権レベルの制限を選択します。

表 10-2 シリアルオーバー LAN 設定画面のボタン

ボタン	説明
印刷	画面に表示されるシリアルオーバー LAN の値を印刷します。
更新	シリアルオーバー LAN 画面を再ロードします。
詳細設定	シリアルオーバー LAN の詳細設定 画面を開きます。
適用	シリアルオーバー LAN 画面の表示中に行った新しい設定を適用します。

6. 必要に応じて、シリアルオーバー LAN 詳細設定 画面で設定を変更します。デフォルト値を使用することをお勧めします。詳細設定 では、文字累積間隔と文字送信しきい値を変更することで SOL のパフォーマンスを調整できます。最適なパフォーマンスを得るためには、デフォルト設定の 10 ミリ秒と 255 文字を使用してください。

表 10-3 シリアルオーバー LAN の詳細設定

設定	説明
文字累積間隔	SOL データパケットの一部を送信するまでの iDRAC6 の標準的な待ち時間。このパラメータはミリ秒で指定します。
文字送信しきい値	SOL データパケットあたりの文字数を指定します。iDRAC6 が受け入れた文字数が文字送信しきい値以上になると、iDRAC6 は文字送信しきい値以下の文字数を含む SOL データパケットの送信を開始します。含まれている文字数がこの値より少ないパケットは、部分 SOL データパケットとして定義されます。



 **メモ:** これらの値を下げると、SOL のコンソールリダイレクト機能のパフォーマンスが低下する可能性があります。また、SOL セッションは次のパケットを送信する前に各パケットの確認メッセージを受信するまで待つ必要があります。このため、パフォーマンス が著しく低下します。

表 10-4 シリアルオーバー LAN 設定の詳細 設定画面のボタン


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 の設定 詳細設定 画面を再ロードします。
適用	シリアルオーバー LAN 設定 画面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 画面に戻ります。

7. SOL 用の SSH と Telnet を **システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ → **サービス** で設定します。

 **メモ:** 各ブレードサーバーはアクティブな SOL セッションを 1 つだけサポートします。

 **メモ:** SSH プロトコルはデフォルトで有効になっています。Telnet プロトコルは デフォルトで無効になっています。

8. **サービス** をクリックして **サービス** 画面を開きます。

 **メモ:** SSH および Telnet プログラムは共にリモートマシンでのアクセスを提供します。

9. 必要に応じて、SSH または Telnet で **有効** をクリックします。

10. **適用** をクリックします。

- ☑ **メモ:** セキュリティと暗号化のメカニズムが優れている SSH を推奨します。
- ☑ **メモ:** タイムアウト値を 0 に設定すると、SSH/Telnet セッション期間が無限になります。デフォルトのタイムアウト値は 1800 秒です。

11. システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → ネットワーク の順に選択して、iDRAC6 帯域外インタフェース (IPMI オーバー LAN) を有効にします。
12. IPMI 設定 の IPMI オーバー LAN を有効にする オプションを選択します。
13. 適用 をクリックします。

シリアルオーバー LAN (SOL) の使用

本項では、Telnet プログラム、SSH クライアント、IPMI tool、SOL プロキシなど、シリアルオーバー LAN セッションの開始方法について説明します。シリアルオーバー LAN 機能の目的は、管理下サーバーのシリアルポートを iDRAC6 を通じて管理ステーションのコンソールにリダイレクトすることです。

Telnet または SSH を通じて SOL をリダイレクトするモデル

Telnet (ポート 23)/SSH (ポート 22) クライアント ↔ WAN 接続 ↔ iDRAC6 サーバー

SSH/Telnet 経由の IPMI ベース SOL を実装すると、シリアルとネットワーク間の変換が iDRAC6 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 SSH または Telnet 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/VT220 ターミナルをエミレートするシェルに接続しています。シリアルコンソールは自動的に SSH または Telnet コンソールにリダイレクトされます。

SOL セッションを開始するには、SSH/Telnet で iDRAC6 に接続して、iDRAC6 コマンドラインコンソールを開きます。次に、ドル記号のプロンプトで「connect」と入力します。

iDRAC6 で Telnet および SSH クライアントを使用する方法の詳細については、「[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。

SOL プロキシのモデル

Telnet クライアント (ポート 623) ↔ WAN 接続 ↔ SOL プロキシ ↔ iDRAC6 サーバー

SOL プロキシは、管理ステーションの Telnet クライアントと通信するとき TCP/IP プロトコルを使用します。一方、SOL プロキシは管理下サーバーの iDRAC6 とは、UDP ベースの RMCP/IPMI/SOL プロトコルを使用して通信します。このため、管理下システムの iDRAC6 に SOL プロキシから WAN 接続経由で通信する場合は、ネットワークパフォーマンスに問題がある可能性があります。推奨される使用モデルは、SOL プロキシと iDRAC6 サーバーを同じ LAN に接続したものです。これによって、Telnet クライアントと管理ステーションを WAN 接続で SOL プロキシに接続できるようになります。この使用モデルでは、SOL プロキシは期待通りに機能します。

IPMI tool を通じて SOL をリダイレクトするモデル

IPMI tool ↔ WAN 接続 ↔ iDRAC6 サーバー

IPMI ベースの SOL ユティリティである IPMI tool は、UDP データグラムを使ってポート 623 に配信された RMCP+ プロトコルを使用します。iDRAC6 では、この RMCP+ 接続が暗号化されている必要があります。暗号化キー (KG キー) には、iDRAC6 ウェブ GUI または iDRAC6 設定ユーティリティで設定できるゼロまたは NULL 文字が含まれている必要があります。また、Backspace キーを押して、暗号化キーを消し、iDRAC6 にデフォルト暗号化キーの NULL 文字を提供させることもできます。RMCP+ を使用する利点としては、認証の強化、データ整合性チェック、暗号化、および複数タイプのペイロードのサポートがあります。詳細については、「[IPMI tool 経由で SOL を使用](#)」または IPMI tool のウェブサイト <http://ipmitool.sourceforge.net/manpage.html> を参照してください。

iDRAC6 コマンドラインコンソールでの SOL セッションの切断

SOL セッションを切断するには、ユーティリティのコマンドを使用します。SOL セッションを完全に終えなければ、ユーティリティを終了できません。SOL セッションを切断するには、iDRAC6 コマンドラインコンソールから SOL セッションを終了します。

SOL リダイレクトを終了する準備ができたなら、<Enter>、<Esc>、<t> の順に続けてキーを押します。それに応答して、SOL セッションが終了します。このエスケープシーケンスは、SOL セッションが接続した直後に、画面にも出力されます。管理下サーバーが **オフ** の場合は、SOL の確立に若干時間がかかります。

- ☑ **メモ:** ユティリティで SOL セッションを正常に閉じないと、それ以上の SOL セッションは使用できなくなる可能性があります。この状況を解決するには、ウェブ GUI の **システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → セッション** でコマンドラインコンソールを終了します。


PuTTY 経由で SOL を使用

Windows 管理ステーションで PuTTY から SOL を起動するには、次の手順を実行してください。

- ☑ **メモ:** 必要に応じて、**システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → サービス** でデフォルトの SSH/Telnet を変更できます。


1. コマンドプロンプトで次のコマンドを使用して iDRAC6 に接続します。

```
putty.exe [-ssh | -telnet] <ログイン名>@<iDRAC IP アドレス> <ポート番号>
```

 **メモ:** ポート番号はオプションです。ポート番号の再割り当てを行った場合のみ必要です。


2. SOL を開始するには、コマンドプロンプトで次のコマンドを入力します。

```
connect
```

 **メモ:** 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 セッションが正常に確立すると、iDRAC6 コマンドラインコンソールは使用できなくなります。エスケープシーケンスの手順に従って、iDRAC6 コマンドラインコンソールにアクセスします。「[iDRAC6 コマンドラインコンソールでの SOL セッションの切断](#)」で説明したコマンドシーケンスを使用して、SOL セッションを終了し、新しいセッションを開始します。


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。

 **メモ:** 必要に応じて、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **サービス** でデフォルトの Telnet タイムアウトを変更できます。

1. シェルを起動します。
2. 次のコマンドで iDRAC6 に接続します。

```
telnet <iDRAC6 の IP アドレス>
```

 **メモ:** Telnet サービスのポート番号をデフォルトポート 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. SOL を開始するには、コマンドプロンプトで次のコマンドを入力します。

```
connect
```

4. Linux 上で Telnet から SOL セッションを終了するには、<Ctrl>+] を押します(<Ctrl> キーを押しながら右角カッコキーを押し、その後手を離します)。Telnet のプロンプトが表示されません。quit と入力して Telnet を終了します。

Linux で OpenSSH 経由で SOL を使用

OpenSSH は、SSH プロトコルを使用するためのオープンソースユーティリティです。Linux 管理ステーションで OpenSSH から SOL を起動するには、次の手順を実行してください。


 **メモ:** 必要に応じて、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **サービス** で SSH のデフォルトのセッションタイムアウトを変更できます。

1. シェルを起動します。
2. 次のコマンドで iDRAC6 に接続します。

```
ssh <iDRAC IP アドレス> -l <ログイン名>
```


3. SOL を開始するには、コマンドプロンプトで次のコマンドを入力します。

```
connect
```

 **メモ:** 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 セッションが正常に確立すると、iDRAC6 コマンドラインコンソールは使用できなくなります。エスケープシーケンスの手順に従って、iDRAC6 コマンドラインコンソールにアクセスします。SOL セッションを終了します(アクティブな SOL セッションを終了するには、「[iDRAC6 コマンドラインコンソールでの SOL セッションの切断](#)」を参照してください)。

IPMI tool 経由で SOL を使用

IPMI tool は『Dell Systems Management Tools and Documentation DVD』からさまざまなオペレーティングシステムにインストールできます。インストールの詳細については、『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。管理ステーションで IPMI tool から SOL を起動するには、次の手順を実行してください。

 **メモ:** 必要に応じて、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **サービス** でデフォルトの SOL タイムアウトを変更できます。

1. 正しいディレクトリから IPMI tool.exe を見つけます。

Windows 32 ビットオペレーティングシステムのデフォルトのパスは C:\Program Files\Dell\SysMgt\bmc で、Windows 64 ビットオペレーティングシステムのデフォルトのパスは C:\Program Files (x86)\Dell\SysMgt\bmc です。


2. システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → ネットワーク → IPMI 設定 で 暗号化キー がすべて 0 であることを確認します。

3. Windows コマンドプロンプトまたは Linux シェルプロンプトで次のコマンドを入力して、iDRAC 経由で SOL を起動します。

```
ipmitool -H <iDRAC IP アドレス> -I lanplus -U <ログイン名> -P <ログインパスワード> sol activate
```

これで、管理下サーバーのシリアルポートに接続します。


4. IPMITool から SOL セッションを終了するには、<-> と <.> を押します(ティルデとピリオドを続けて押す)。iDRAC6 がキーの受け入れでビジー状態になっている可能性があるので、何度か実行してください。SOL セッションが閉じます。


 **メモ:** SOL セッションが正しく終了しなかった場合は、次のコマンドを入力して iDRAC を再起動します。iDRAC6 が起動を完了するまでに最大 2 分かかります。詳細については、「[RACADM サブコマンドの概要](#)」を参照してください。


```
racadm racreset
```


SOL プロキシで SOL を開く

シリアルオーバー LAN プロキシ(SOL プロキシ)は、シリアルオーバー LAN(SOL)と IPMI プロトコルを使用してリモートシステムを LAN ベースで管理できる Telnet のデーモンです。デーモンの機能にアクセスするには、Microsoft Windows の HyperTerminal や Linux の Telnet など、標準的な Telnet クライアントアプリケーションを使用できます。SOL はメニューモードでもコマンドモードでも使用可能です。SOL プロトコルとリモートシステムの BIOS コンソールリダイレクトを組み合わせることで、システム管理者は管理下システムの BIOS 設定を LAN を介して表示したり変更したりできます。Linux シリアルコンソールと Microsoft の EMS/SAC インタフェースも SOL を使用して LAN でアクセスできます。

 **メモ:** Windows オペレーティングシステムのすべてのバージョンに HyperTerminal ターミナルエミュレーションソフトウェアが含まれています。ただし、同梱のバージョンではコンソールリダイレクトに必要な機能が十分に提供されません。代わりに、VT100 / VT220 または ANSI エミュレーションモードをサポートしているターミナルエミュレーションソフトウェアを使用できます。システムでコンソールリダイレクトをサポートしている完全な VT100/VT220 または ANSI ターミナルエミュレータの一例が、Hilgraeve の HyperTerminal Private Edition 6.1 以降です。また、コマンドラインウィンドウを使用して Telnet シリアルコンソールリダイレクトを実行すると、文字化けする場合があります。

 **メモ:** ハードウェアとソフトウェアの要件や、ホストおよびクライアントシステムでコンソールリダイレクトを使用する手順など、コンソールリダイレクトの詳細については、システムのユーザーズガイドを参照してください。

 **メモ:** ハイパーターミナルと Telnet の設定は、管理下システムの設定と同じである必要があります。たとえば、ボーレートとターミナルモードが一致する必要があります。

 **メモ:** MS-DOS® プロンプトから実行する Windows telnet コマンドは ANSI ターミナルエミュレーションをサポートしており、すべての画面を正しく表示するには、BIOS に ANSI ターミナルエミュレーションを設定する必要があります。

SOL プロキシを使用する前に

SOL プロキシを使用する前に、『ベースボード管理コントローラユーティリティユーザーズガイド』で管理ステーションの設定方法を確認してください。BMC 管理ユーティリティは、デフォルトでは Windows オペレーティングシステムの次のディレクトリにインストールされます。

```
C:\Program Files\Dell\SysMgt\bmc - (32 ビットオペレーティングシステム)
```

```
C:\Program Files (x86)\Dell\SysMgt\bmc - (64 ビットオペレーティングシステム)
```

Linux Enterprise オペレーティングシステムではインストールプログラムはファイルを次の場所にコピーします。

```
/etc/init.d/SOLPROXY.cfg
```

```
/etc/SOLPROXY.cfg
```

```
/usr/sbin/dsm_bmu_solproxy32d
```

```
/usr/sbin/solconfig
```

```
/usr/sbin/ipmish
```

SOL プロキシセッションの開始

Windows 2003 の場合

Windows システムで、インストール後に SOL プロキシサービスを開始するには、システムを再起動してください(再起動すると SOL プロキシが自動的に開始します)。または、次の手順で SOL プロキシサービスを手動で開始することもできます。

1. **マイコンピュータ** を右クリックして、**管理** をクリックします。

コンピュータの管理 ウィンドウが表示されます。

2. **サービスとアプリケーション** をクリックしてから **サービス** をクリックします。

右側に使用可能なサービスが表示されます。

3. サービス一覧から **DSM_BMU_SOLProxy** を右クリックして、このサービスを開始します。

使用しているコンソールによっては、SOL プロキシへのアクセス手順が異なる場合があります。本項では、SOL プロキシを実行している管理ステーションを「SOL プロキシサーバー」と呼びます。

Linux の場合

SOL プロキシはシステム起動中に自動的に開始します。または、`etc/init.d` ディレクトリに移動し、次のコマンドを使用して SOL プロキシサービスを管理することもできます。

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

SOL プロキシ経由で Telnet を使用

ここでは、管理ステーションで SOL プロキシサービスが既に実行されていることを前提とします。

Windows 2003 の場合


1. 管理ステーションで、コマンドプロンプトウィンドウを開きます。
2. コマンドラインに `telnet` コマンドを入力し、SOL プロキシサーバーが同じマシンで実行している場合は IP アドレスとして `localhost` を入力し、SOL プロキシインストール時に指定したポート番号（デフォルトは 623）を入力します。例：

```
telnet localhost 623
```

Linux の場合

1. 管理ステーションで Linux シェルを開きます。
2. `telnet` コマンドを入力して、IP アドレスとして `localhost` を入力し、SOL プロキシインストール時に指定したポート番号（デフォルトは 623）を入力します。例：

```
telnet localhost 623
```

 **メモ:** ホストオペレーティングシステムが Windows であるか Linux であるかにかかわらず、SOL プロキシサーバーが管理ステーション以外のマシンで実行されている場合は、`localhost` ではなく SOL プロキシサーバー IP アドレスを入力します。

```
telnet <SOL プロキシサーバー IP アドレス> 623
```


SOL プロキシ経由で HyperTerminal を使用


1. リモートステーションから `HyperTerminal.exe` を開きます。
2. **TCPIP(Winsock)** を選択します。
3. ホストアドレス `localhost` とポート番号 623 を入力します。

リモート管理下システムの BMC への接続


SOL プロキシセッションが確立された後、次の選択肢が表示されます。

1. Connect to the Remote Server's BMC (リモートサーバーの BMC への接続)
2. Configure the Serial-Over-LAN for the Remote Server (リモートサーバーへのシリアルオーバー LAN の設定)
3. Activate Console Redirection (コンソールリダイレクトのアクティブ化)
4. Reboot and Activate Console Redirection (再起動とコンソールリダイレクトのアクティブ化)
5. Help (ヘルプ)
6. Exit (終了)

 **メモ:** 複数の SOL セッションを同時にアクティブにすることはできますが、管理下システムのある時点でアクティブにできるコンソールリダイレクトセッションは 1 つだけです。


 **メモ:** アクティブな SOL セッションを終了するには、<-><-><-> 文字シーケンスを使用します。このシーケンスによって SOL が終了し、トップレベルメニューに戻ります。


1. メインメニューでオプション 1 を選択します。
2. リモート管理下システムの iDRAC6 IP アドレスを入力します。
3. 管理下システムの iDRAC6 に使用する iDRAC6 ユーザー名とパスワードを入力します。iDRAC6 のユーザー名とパスワードを割り当て、これらを iDRAC6 の不揮発性ストレージに保存する必要があります。

 **メモ:** iDRAC6 では一度に 1 つの SOL コンソールリダイレクトのみ許可されます。

 **メモ:** 必要に応じて、iDRAC6 ウェブ GUI で **システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → サービス** で Telnet **タイムアウト** の値をゼロに変更すると、SOL セッション時間を無期限に延長できます。

4. IPMI 暗号化キーを iDRAC6 で設定した場合は、それを入力します。

 **メモ:** iDRAC6 GUI の **システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → ネットワーク → IPMI 設定 → 暗号化キー** で IPMI 暗号化キーを見つげることができます。

 **メモ:** デフォルトの IPMI 暗号化キーはすべてゼロです。暗号化オプションで <Enter> キーを押すと、iDRAC6 はこのデフォルト暗号化キーを使用します。

5. メインメニューの **リモートサーバー用シリアルオーバー LAN の設定** (オプション 2)を選択します。

SOL 設定メニューが表示されます。現在の SOL 状態によって SOL 設定メニューの内容は次のように変わります。

1. SOL が既に有効になっている場合、現在の設定が表示され 3 つの選択肢が提示されます。
 1. Disable Serial-Over-LAN (シリアルオーバー LAN を無効にする)
 2. Change Serial-Over-LAN settings (シリアルオーバー LAN の設定を変更する)
 3. Cancel (キャンセル)
1. SOL が有効になっている場合は、SOL ボーレートが iDRAC6 のボーレートと同じで、ユーザーにシステム管理者権限が付与されていることを確認してください。
1. 現在 SOL が無効になっている場合は、Y と入力して SOL を有効にするか、N を入力して SOL を無効のままにします。

1. メインメニューで **コンソールリダイレクトの起動** (オプション 3)を選択します。

リモート管理下システムのテキストコンソールが管理ステーションにリダイレクトされます。

7. メインメニューで **コンソールリダイレクトの再起動とアクティブ化** (オプション 4)を選択します(省略可能)。


リモート管理下システムの電源状態が確認されます。電源がオンの場合は、正常なシャットダウンか強制シャットダウンかを選択します。

次に、電源状態が **オン** になるまで、状態が監視されます。コンソールリダイレクトが開始し、リモート管理下システムのテキストコンソールが管理ステーションにリダイレクトされます。

管理下システムの再起動中に BIOS システム設定プログラムに切り替えて BIOS の設定や表示ができます。

8. メインメニューで **ヘルプ** (オプション 5)を選択すると、各オプションの詳しい説明が表示されます。

9. メインメニューで **終了** (オプション 6)を選択すると、Telnet セッションが終了して SOL プロキシから切断されます。

 **メモ:** ユーザーが SOL セッションを正しく終了しなかった場合は、次のコマンドを入力して iDRAC を再起動します。iDRAC6 の起動が完了するのに 1~2 分かかります。詳細については、「[RACADM サブコマンドの概要](#)」を参照してください。

```
racadm racreset
```

オペレーティングシステムの設定

汎用 UNIX 系 オペレーティングシステムを設定するには、次の手順を実行します。この設定は、Red Hat Enterprise Linux 5.0、SUSE Linux Enterprise Server 10 SP1、Windows 2003 Enterprise のデフォルトインストールに基づくものです。

Linux Enterprise オペレーティングシステムの場合

1. /etc/inittab ファイルを編集して、ハードウェアフロー制御を有効にし、ユーザーが SOL コンソールからログインできるようにします。次の行を #Run gettys in standard runlevels セクションの末尾に追加します。


```
7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
```

オリジナルの /etc/inittab の例

```
#
# inittab      This file describes how the INIT process should set up (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 )
#              the system in a certain run-level. (セットアップする方法を記述します。)
#
SKIP this part of file

# Run gettys in standard runlevels (gettys を標準ランレベルで実行します。)
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty1
3:2345:respawn:/sbin/mingetty tty1
4:2345:respawn:/sbin/mingetty tty1
5:2345:respawn:/sbin/mingetty tty1
6:2345:respawn:/sbin/mingetty tty1

# Run xdm in runlevel 5 (xdm をランレベル 5 で実行します。)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

変更後の /etc/inittab の例

```
#
# inittab      This file describes how the INIT process should set up (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 )
#              the system in a certain run-level. (セットアップする方法を記述します。)
#
SKIP this part of file

# Run gettys in standard runlevels (gettys を標準ランレベルで実行します。)
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty1
3:2345:respawn:/sbin/mingetty tty1
4:2345:respawn:/sbin/mingetty tty1
5:2345:respawn:/sbin/mingetty tty1
6:2345:respawn:/sbin/mingetty tty1
7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220

# Run xdm in runlevel 5 (xdm をランレベル 5 で実行します。)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

2. /etc/securetty ファイルを編集して、ユーザーが SOL コンソールからルートユーザーとしてログインできるようにします。console の後に次の行を追加します。

```
ttyS0
```

オリジナルの /etc/securetty の例

```
console

vc/1

vc/2

vc/3

vc/4

SKIP the rest of file
```

編集後の /etc/securetty の例

```
console

ttyS0

vc/1

vc/2

vc/3

vc/4

SKIP the rest of file
```

3. /boot/grub/grub.conf または /boot/grub/menu.list ファイルを編集して、SOL の起動オプションを追加します。

a. 各種の UNIX 系オペレーティングシステムで、グラフィカル表示行をコメントアウトします。

- o splashimage=(hd0,0)/grub/splash.xpm.gz (RHEL 5 の場合)
- o gfxmenu (hda0,5)/boot/message (SLES 10 の場合)

b. 最初の title= ... 行の前に次の行を追加します。

Redirect OS boot via SOL (SOL 経由での OS 起動のリダイレクト)

c. 最初の title= ... 行の後に次のエントリを追加します。

SOL リダイレクト

d. 最初の title= ...: の kernel/_ 行の後に次のテキストを追加します。

```
console=tty1 console=ttyS0,115200
```

 **メモ:** Red Hat Enterprise Linux 5 の /boot/grub/grub.conf は /boot/grub/menu.list へのシンボリックリンクです。どちらの設定も変更できます。

RHEL 5 のオリジナル /boot/grub/grub.conf の例:

```
# grub.conf generated by anaconda (grub.conf (作成者: anaconda) )

# Note that you do not have to return grub after making changes to this (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。)

# file (ファイル)

# NOTICE: You have a /boot partition. This means that (通知: /boot パーティションがあります。これは)

# all kernel and initrd paths are relative to /boot/, eg. (すべてのカーネルと initrd パスは /boot/ 相対的であることを意味します。たとえば、)

#       root (hd0,0)

# kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol100

#       initrd /boot/initrd-version.img

#boot=/dev/sda
```

```
default=0

timeout=5

splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu

Red Hat Enterprise Linux 5

    root (hd0,0)

    kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol100 rhgb quiet

    initrd /initrd-2.6.18-8.el5.img
```

変更後の /boot/grub/grub.conf の例:

```
# grub.conf generated by anaconda (grub.conf (作成者: anaconda))

# Note that you do not have to return grub after making changes to this (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。)

# file (ファイル)

# NOTICE: You have a /boot partition. This means that (通知: /boot パーティションがあります。これは)

# all kernel and initrd paths are relative to /boot/, eg. (すべてのカーネルと initrd パスは /boot/ 相対的であることを意味します。たとえば、)

#         root (hd0,0)

# kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol100

#         initrd /boot/initrd-version.img

#boot=/dev/sda

default=0

timeout=5

#splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu

# Redirect the OS boot via SOL (SOL 経由での OS 起動のリダイレクト)

title Red Hat Enterprise Linux 5 SOL redirection

    root (hd0,0)

    kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol100 rhgb quiet console=tty1 console=ttyS0,115200

    initrd /initrd-2.6.18-8.el5.img
```

SLES 10 のオリジナルの /boot/grub/menu.list の例:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09 UTC 2008 (変更者: YaST2 最終変更日時: Sat Oct 11 21:52:09 UTC 2008)

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message

###Don't change this comment - YaST2 identifier: Original name: linux###

SUSE Linux Enterprise Server 10 SP1

    root (hd0,5)

    kernel /boot/vmlinuz-2.6.16-46-0.12-bigsmP root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts

    initrd /boot/initrd-2.6.16.46-0.12-bigsmP
```

SLES 10 の変更後の /boot/grub/menu.list の例:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09 UTC 2008 (変更者: YaST2 最終変更日時: Sat Oct 11 21:52:09 UTC 2008)

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message

###Don't change this comment - YaST2 identifier: Original name: linux###

title SUSE Linux Enterprise Server 10 SP1 SOL redirection

    root (hd0,5)


    kernel /boot/vmlinuz-2.6.16-46-0.12-bigsmpt root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts
    console=tty1 console=ttyS0,115200

    initrd /boot/initrd-2.6.16.46-0.12-bigsmpt
```

Windows 2003 Enterprise

1. Windows コマンドプロンプトで `bootcfg` と入力して、起動エントリ ID を確認します。OS フレンドリ名である **Windows Server 2003 Enterprise** でセクション用の起動エントリ ID を探します。<Enter> キーを押して、管理ステーションの起動オプションを表示します。
2. 次を入力して Windows コマンドプロンプトで EMS を有効にします。

```
bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <起動 ID>
```

 **メモ:** <起動 ID> はステップ 1 からの起動エントリ ID です。

3. <Enter> キーを押して、EMS コンソール設定が有効になることを確認します。

オリジナルの `bootcfg` 設定の例:

```
Boot Loader Settings
-----

timeout:30

default:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Boot Entries
-----

Boot entry ID: 1

Os Friendly Name : Windows Server 2003, Enterprise

Path:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

オリジナルの `bootcfg` 設定の例:

```
Boot Loader Settings
-----

timeout:      30
```

default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

redirect: COM1

redirectbaudrate:115200

Boot Entries

Boot entry ID: 1

Os Friendly Name : Windows Server 2003, Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect

[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™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 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](#)
- [vKVM および仮想メディアのリモートからの起動](#)
- [よくあるお問い合わせ \(FAQ\)](#)

この項では、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、グラフィックまたはテキストモードでローカルコンソールにリモートからアクセスでき、1 台または複数の iDRAC6 対応システムを 1 か所から制御できます。

コンソールリダイレクトの使用

コンソールリダイレクト 画面では、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 各ブレードでサポートできるコンソールリダイレクトは最大 2 セッションです。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、別のユーザーに制御権があることが通知されます。最初のユーザーが 30 秒以内に応答しないと、2 番目のユーザーにアクセスが許可されません。2 つのセッションが同時にアクティブな間には、2 番目のユーザーがアクティブセッションを持つことを示すメッセージが、最初のユーザーの画面の右上隅に表示されます。
- 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。

ブラウザのキャッシュをクリアします。

vKVM の操作時に問題 (範囲外のエラー、同期問題など) が発生した場合は、ブラウザのキャッシュをクリアして、システムに保存されている可能性のあるビューアの古いバージョンを削除してから、再試行してください。

IE6 の Active-X ビューアの古いバージョンをクリアするには、次のとおりになります。

1. コマンドプロンプトを開き、Windows\Downloaded program files のディレクトリへ移動します。
2. `regsvr32 /u VideoViewer.ocx` を実行します。
3. 次のファイルを削除します: AvctKeyboard.dll、AvctVirtualMediaDE.dll、AvctVirtualMediaES.dll、AvctVirtualMediaFR.dll、AvctVirtualMediaJA.dll、AvctVirtualMediaZH.dll、VideoViewerDE.dll、VideoViewerES.dll、VideoViewerFR.dll、VideoViewerJA.dll、VideoViewerZH.dll、および VirtualMediaDLL.dll。
4. Internet Explorer で使用されていた Session Viewer および Video Viewer のアドオンを削除します。

IE7 の Active-X ビューアの古いバージョンをクリアするには、次のとおりになります。

1. Video Viewer および Internet Explorer ブラウザを閉じます。
2. Internet Explorer ブラウザを再び開き、Internet Explorer → ツール → アドオンの管理 の順で選択し、アドオンを有効または無効にする をクリックします。アドオンの管理 ウィンドウが表示されます。
3. 表示 ドロップダウンメニューから Internet Explorer で使用されたアドオン を選択します。
4. Video Viewer アドオンを削除します。

IE8 の Active-X ビューアの古いバージョンをクリアするには、次のとおりになります。

1. Video Viewer および Internet Explorer ブラウザを閉じます。

- Internet Explorer ブラウザを再び開き、Internet Explorer → ツール → **アドオンの管理** の順で選択し、**アドオンを有効または無効にする** をクリックします。**アドオンの管理** ウィンドウが表示されます。
- 表示** ドロップダウンメニューから **すべてのアドオン** を選択します。
- Video Viewer アドオンを選択し、**詳細情報** リンクをクリックします。
- 詳細情報** ウィンドウで **削除** を選択します。
- 詳細情報** および **アドオンの管理** の両ウィンドウを閉じます。

Windows または Linux で古いバージョンの Java® ビューアをクリアするには、次のとおりになります。

- コマンドプロンプトで `javaws -viewer` を実行します。
- Java Cache Viewer が表示されます。
- iDRAC6 コンソールリダイレクトクライアントと JViewer を削除します。

コマンドプロンプトと `javaws -uninstall` を実行して、キャッシュからすべてのアプリケーションを削除することもできます。

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 11-1](#) は、管理下サーバー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 11-1 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、次の手順を実行します。

- 対応ウェブブラウザをインストールして設定します。「[対応ウェブブラウザ](#)」および「[対応ウェブブラウザの設定](#)」を参照してください。
- 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、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。


iDRAC6 ウェブインタフェースでのコンソールリダイレクトと仮想メディアの設定

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、以下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 / メディア** タブをクリックします。
- 設定** をクリックして **設定** 画面を開きます。
- コンソールリダイレクトのプロパティを設定します。[表 11-2](#) 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 11-3](#)」を参照してください。

表 11-2 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	<p>選択して、コンソールリダイレクトを有効または無効にします。</p> <p>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。</p> <p>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。</p> <p>デフォルトは 有効 です。</p>
最大セッション数	<p>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。</p>
アクティブセッション数	<p>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。</p>
キーボードとマウスポート番号	<p>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。</p>
ビデオポート番号	<p>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。</p>
ビデオ暗号化有効	<p>チェックボックスがオン の場合は、ビデオの暗号化が有効です。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。</p> <p>チェックボックスがオフ の場合は、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。</p> <p>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パフォーマンスを改善できる場合があります。</p>
マウスモード	<p>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している場合は、Windows を選択します。</p> <p>管理下サーバーが Linux 環境で実行している場合は、Linux を選択します。</p> <p>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していない場合は、USC/Diags を選択します。</p> <p>メモ: HyperV、Dell Diagnostics、または USC(システムサービス)で USC/Diags を選択する必要があります。</p> <p>デフォルトは Windows です。</p>
IE 用コンソールブラウザタイプ	<p>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。</p> <p>ActiveX - ActiveX コンソールリダイレクト ビューア</p> <p>Java - Java コンソールリダイレクト ビューア</p> <p>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方法」を参照)。</p> <p>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。</p>
ローカルサーバービデオ有効	<p>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 モニタへの出力が有効です。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 を使用して実行するタスクが管理下サーバーのローカルモニターに表示されません。</p>

 **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方法](#)」を参照してください。


コンソールリダイレクトの設定 画面には、[表 11-5](#) に示すボタンがあります。

表 11-3 コンソールリダイレクトの設定画面のボタン

ボタン	定義
印刷	設定 画面を印刷します。
更新	設定 画面を再ロードします。
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。

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 (vKVM)ビューアアプリケーション(iDRACView)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。iDRACView を使用すると、ローカルの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。

 **メモ:** Windows Vista® の管理ステーションから vKVM を起動すると、vKVM 再起動メッセージが表示される場合があります。これを回避するには、以下の場所で適切なタイムアウト値を設定します。**コントロールパネル → 電力オプション → 節電機能 → 詳細設定 → ハードディスク → <タイムアウト値> 後にハードディスクをオフにする**と**コントロールパネル → 電力オプション 高パフォーマンス → 詳細設定 → ハードディスク → <タイムアウト値> 後にハードディスクをオフにする**。

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 タブ → コンソールリダイレクトおよび仮想メディア の順でクリックします。

2. コンソールリダイレクトおよび仮想メディア 画面で、表 11-4 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、「IDRAC6 ウェブインタフェースでのコンソールリダイレクトと仮想メディアの設定」を参照してください。

表 11-4 コンソールリダイレクト情報

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。
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。
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。 ActiveX - 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 IDRAC6 にアクセスする場合は、プラグインの種類として Active-X または Java を選択できます。 メモ: プラグインの種類として Java を選択した場合、Internet Explorer 8 で初回 vKVM が起動しない場合があります。
ローカルサーバービデオ有効	はいの場合は、コンソールリダイレクト中、iKVM モニタへの出力が有効になります。いいえ の場合は、コンソールリダイレクト を使用して実行したタスクが管理下サーバーのローカルモニタに表示されません


 **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の設定 画面には、表 11-5 に示すボタンがあります。

表 11-5 コンソールリダイレクトボタン

ボタン	定義
更新	コンソールリダイレクトの設定 画面を再ロードします。
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 画面を印刷します。

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すると、複数のメッセージボックスが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、リモートシステムのデスクトップが iDRACView に表示されます。

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、電力処置、仮想メディアへのアクセスなど、さまざまな制御調整を提供しています。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 11-6 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 11-6 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	リモートシステムの現在の画面をキャプチャし、.bmp ファイルとして保存します。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	Video Viewer を全画面表示にするには、ビューアの右上隅をクリックします。
	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 Video Viewer 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	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"> Alt+Ctrl+Del Alt+Tab Alt+Esc Ctrl+Esc Alt+Space Alt+Enter Alt+Hyphen Alt+F4 PrtScrn Alt+PrtScrn F1 一時停止 Alt+M Alt+D Alt+PrtScrn+M Alt+PrtScrn+P
	キーボードのバスのルー	キーボードのバスのルーモードでは、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	クライアント上のマウスがサーバー上のマウスへリダイレクトされるよう同期します。
	ローカルカーソルを非表示にする	KVM からのカーソルのみが表示されます。vKVM で USC を実行する場合は、この設定を使用することをお勧めします。
オプション	カラーモード	ネットワークパフォーマンスを向上させるための色深度を選択できます。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、最も低い色深度を選択すると、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て、より多くの帯域幅をメディアからのデータ転送用に残しておくことができます。 色モードは 15 ビットカラーと 7 ビットカラーに設定できます。
電源	システムの電源オン	システムの電源を入れます。
	システムの電源オフ	システムの電源を切ります。
	正常なシャットダウン	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)	電源を切らずにシステムを再起動します。
	システムの電源を入れなおす(コールドブート)	システムの電源を切ってから再起動します。
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"> フロッピードライブ CD DVD ISO フォーマットのイメージ USB フラッシュドライブ <p>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。</p> <p>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。</p>
ヘルプ	iDRACView バージョン情報	iDRACView バージョンを表示します。

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 Dell 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ション速度が管理ステーションのマウスポインタと同期せず、Video Viewer 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 P 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 Enterprise 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、「[iDRAC6 ユーザーガイドでのコンソールリダイレクトと仮想メディアの設定](#)」を参照してください。iDRAC 6 **コンソールリダイレクト** 画面のマウス矢印の制御には、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

iDRAC6 ウェブインタフェースを使用して、iKVM の接続を許可しないように iDRAC6 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 iDRAC6 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、**コンソールリダイレクト画面** 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が無効にする (オフにする) と、iKVM に接続しているモニタ、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、「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. **システム** をクリックし、**コンソール / メディア** タブをクリックして、**設定** をクリックします。
3. サーバーでローカルビデオを無効にする (オフにする) には、**設定** 画面で **ローカルサーバービデオ有効** 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**有効 (オン)** です。
4. サーバーでローカルビデオを有効にする (オンにする) には、**設定** 画面で **ローカルサーバービデオ有効** を選択してから **適用** をクリックします。

コンソールリダイレクト 画面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。


vKVM および仮想メディアのリモートからの起動

iDRAC6 ウェブ GUI から起動する代わりに、対応ブラウザで 1 つの URL を入力することで、vKVM/ 仮想メディアを起動することもできます。ご利用のシステム構成によっては、手動の認証プロセス (ログインページ) を経るか、自動的に vKVM/ 仮想メディアビューア (iDRACView) に転送されます。

 **メモ:** Internet Explorer は、ローカル、Active Directory (AD)、スマートカード (SC)、およびシングルサインオン (SSO) によるログインをサポートしています。Firefox は、SSO、ローカル、および AD ログインをサポートしています。

URL 形式

ブラウザに https://<idrac6_ip>/console のリンクを入力する場合、ログイン設定によっては、通常の手動のログイン手順に従わなければならない場合があります。SSO が無効で、ローカル、AD、または SC ログインが有効な場合、該当するログインページが表示されます。ログインに成功すると、vKVM/vMedia ビューアは起動しません。その代わりに、iDRAC6 GUI ホームページに転送されます。

 **メモ:** iDRACView を起動するために使用する URL は、大文字と小文字が区別され、小文字のみで入力する必要があります。

一般的なエラーのシナリオ

[表 11-7](#) は、一般的なエラーのシナリオ、それらエラーの原因、そして iDRAC6 の動作を記載しています。

表 11-7 エラーのシナリオ

エラーのシナリオ	原因	動作
ログインの失敗	無効なユーザー名または間違ったパスワードを入力しています。	<a href="https://<ip>">https://<ip> を入力し、ログインに失敗した場合と同じ動作が見られます。
権限の不足	コンソールリダイレクトおよび仮想メディアの権限を保有していません。	iDRACView が起動せず、コンソール / メディアの設定 GUI ページにリダイレクトされません。
コンソールリダイレクトが無効	ご利用のシステムでコンソールリダイレクトが無効になっています。	iDRACView が起動せず、コンソール / メディアの設定 GUI ページにリダイレクトされません。
不明な URL パラメータの検出	入力された URL には、未定義のパラメータが含まれています。	ページが見つかりません (404) のメッセージが表示されます。

よくあるお問い合わせ (FAQ)

[表 11-8](#) は、よくあるお問い合わせとその回答です。

表 11-8 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
帯域外のウェブ GUI をログアウトすると、vKVM がログアウトに	ウェブセッションのログアウト後も vKVM と vMedia のセッションがアクティブなままになります。vMedia と vKVM ビューアのア

失敗します。	ブリークセッションを終了して、それぞれのセッションからログアウトしてください。
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。
ローカルユーザーが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。
ローカルユーザーが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なりますか。	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。
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と仮想メディア 画面に表示されます。 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。この <code>racadm</code> コマンドは、Telnet/SSH または iDRAC6 のリモートセッションから実行できます。 リモートの RACADM コマンド: <code>racadm -r <iDRAC の IP アドレス> -u <ユーザー> -p <パスワード> getconfig -g cfgRacTuning</code> ステータスは、iKVM OSCAR モニタにも表示されます。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 iDRAC6 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。詳細については、「 Linux のローケル設定 」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。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。iDRAC6 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。iDRAC6 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、 設定 画面の USC/Diags でマウスモードを設定します。
Linux テキストコンソール (Dell Unified Server Configurator (USC)、Dell Lifecycle Controller (LC) または Dell Unified Server Configurator Lifecycle Controller 有効 (USC-LCE) のいずれかで、マウスが同期しないのはなぜですか。	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、<Alt><M> キーを押すか、 マウス → マウスの同期 の順に選択します。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。
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 Microsoft によって生成され、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通知します。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。	良いパフォーマンスを得るには、5 MB/ 秒 の接続をお勧めします。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](#)

[目次ページに戻る](#)

iDRAC6 と使用するための VFlash メディアカードの設定


Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

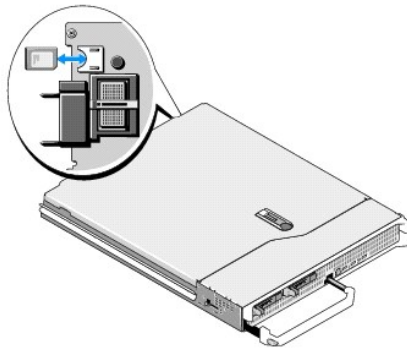
- [VFlash メディアカードの取り付け](#)
- [iDRAC6 ウェブインタフェースからの VFlash メディアカードの設定](#)
- [RACADM を使用して VFlash メディアカードを設定する](#)

VFlash メディアカードは、SD カードの一種で、システム背面の角にあるオプションの iDRAC6 Enterprise カードスロットに挿入します。ストレージ容量を提供し、通常の USB フラッシュキーのように動作します。


VFlash メディアカードの取り付け

1. シャーシからブレードを取り外します。
2. システム背面の角にある VFlash メディアスロットの位置を確認します。

 **メモ:** カードの取り付けや取り出し時に、ブレードカバーを外す必要はありません。



3. ラベル側を上に向けて、SD カードの接続ピン側をモジュールのカードスロットに挿入します。

 **メモ:** スロットは正しい方向にしかカードを挿入できないように設計されています。


4. カードを押し込んでスロットにロックします。
5. ブレードをシャーシに戻します。

VFlash メディアカードの取り外し

VFlash メディアを取り出すには、カードを押し込んでロックを解除し、カードスロットから引き出します。

iDRAC6 ウェブインタフェースからの VFlash メディアカードの設定

SD カードプロパティ

 **メモ:** 読み取り / 書き込み可能な SD カードがサーバーの SD カードスロットに挿入された場合のみ、本項は表示されます。これ以外の場合は、次のメッセージが表示されます。

SD card not detected. Please insert an SD card of size 256MB or greater. (SD カードが検出されませんでした。256 MB 以上の SD カードを挿入してください。)

1. VFlash カードが挿入されていることを確認します。

- サポートされているウェブブラウザを開き、iDRAC6 ウェブインタフェースにログインします。
- システムツリーで **システム** を選択します。
- VFlash タブをクリックします。

VFlash 画面が表示されます。

表 12-1 には、SD カードプロパティのオプションがリストされます。

表 12-1 SD カードプロパティ

属性	説明
仮想キーサイズ	SD カード上で VFlash キーが占有するサイズを選択できます。仮想キーサイズを選択し、 適用 をクリックします。仮想キーは指定したサイズで再初期化し、すべての既存データを削除して、SD カード上の一部分をフォーマットします。 メモ: 1GB のライセンス許可された SD カードを挿入した場合、パーティションサイズとして、256MB または 512MB から選択できます。サイズを問わず、ライセンス許可されていない SD カードを挿入した場合、パーティションサイズとして 256MB しか選択できません。 WS-MAN を使用してイメージをアップロードした場合、最大パーティションサイズはイメージのサイズに依存します。たとえば、500MB のイメージをアップロードした場合、1GB のライセンス許可されたカードに、既に 500MB のイメージが存在するため、1GB の仮想キーサイズを作成することはできません。この場合、 初期化 ボタンをクリックして、カードを再初期化してから、仮想キーサイズに 1GB を選択します。
VFlash メディアタイプ	サーバーの SD カードスロットにデル製またはデル製以外 SD カードのいずれかが挿入されているかを表示します。 SD カードがライセンス許可されている場合は、Dell VFlash と SD カードのサイズを表示します。カードがライセンス許可されていない場合は、デル製以外の SD カードとして表示します。
イメージ	SD カード上に作成されたイメージファイルの名前を表示します。これは、VFlash として使用されます。
ID ファイル	SD カード上に作成されたイメージファイルの名前を表示します。VFlash イメージに関する情報を提供します。
VFlash 連結	VFlash を連結するには、このオプションを選択します。これにより、SD カード上に作成された ManagedStore.IMG のイメージファイルが、選択したサイズの USB キーとして認識されます。 メモ: SD カードに有効な ManagedStore.IMG イメージが存在する場合のみ、VFlash を連結できます。
初期化	初期化 をクリックして、ManagedStore.IMG の VFlash イメージファイルを SD カード上に作成します。 メモ: 初期化 オプションは、VFlash メディアカードが挿入されている場合にのみアクティブになります。また、VFlash 連結 オプションの選択が解除されている場合のみ、SD カードをフォーマットできます。 メモ: VFlash GUI ページに表示される ManagedStore.IMG ファイルと ManagedStore.ID ファイルは、ホストサーバーのオペレーティングシステムには表示されず、SD カードに表示されます。
適用	現在の設定を保存します。ドロップダウンメニューから仮想キーサイズを変更する場合、 適用 をクリックして、指定したサイズで新しい仮想キーを作成します。すべての既存データは削除されます。この操作は、選択した仮想キーのサイズによっては、数分かかる場合があります。

VFlash ドライブ



 **メモ:** イメージファイルのアップロード機能は、SD カード上に有効な ManagedStore.IMG イメージが存在し、かつ VFlash **連結** オプションが選択解除されている場合のみ利用できます。

表 12-2 は、VFlash ドライブ の設定をリストします。

表 12-2 VFlash ドライブ

属性	説明
イメージファイル	リモートサーバーで、VFlash USB キーとして認識させるローカルファイルをクライアントマシンから選択します。VFlash メディア上に直接、緊急用の起動イメージと診断ツールを保存することができます。イメージファイルを DOS ブータブルフロッピーイメージにすることもできます。たとえば、Windows® の場合は *.img ファイル、Linux の Red Hat® Enterprise Linux® の場合は、diskboot.img ファイルとなります。diskboot.img を使用してレスキューディスクを作成したり、ネットワークインストールを行うためのディスクを作成できます。VFlash を使用して、今後の一般的な用途や緊急時の使用に備えて永続的なイメージを格納できます。
アップロード	選択したイメージファイルを SD カードにアップロードするには、このオプションをクリックします。アップロードが完了すると、イメージファイルは SD カード上に ManagedStore.IMG として格納されます。 メモ: 本リリースでは、ISO イメージのアップロードはサポートされておらず、アップロードを試みた場合、エラーが発生する恐れがあります。

 **注意:** 管理下サーバーの Windows オペレーティングシステムから、ドライブを右クリックして、「取り出す」オプションを選択しても、仮想フラッシュドライブを取り外すことはできません。ドライブを安全に取り外すには、ご利用システムの右下隅のシステムトレイで提供されるオプションをご利用ください。

WSMAN プロバイダ、iDRAC6 設定ユーティリティ、または RACADM などのアプリケーションが VFlash を使用している最中に、VFlash ページ上のボタンをクリックした場合、iDRAC6 は空のページに、VFlash is currently in use by another process. Try again after some time. (VFlash は、他のプロセスによって現在使用されています。しばらくしてからお試しください。) のメッセージを表示します。

仮想フラッシュキーサイズの表示

仮想キーサイズ ドロップダウンメニューに、現在のサイズ設定が表示されます。

RACADM を使用して VFlash メディアカードを設定する

VFlash メディアカードを有効または無効にする

サーバーへのローカルコンソールを開いてログイン後、次のように入力します

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 or 0 ]
```


0 は無効、1 は有効を示します。


 **メモ:** 出力の詳細を含む cfgRacVirtual の詳細については、「[cfgRacVirtual](#)」を参照してください。

VFlash メディアカードのリセット

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、次のように入力します。

```
racadm vmkey reset
```

 **注意:** RACADM コマンドを使用して VFlash メディアカードをリセットすると、キーサイズが 256 MB にリセットされ、既存のデータがすべて削除されます。

 **メモ:** vmkey の詳細については、「[vmkey](#)」を参照してください。RACADM コマンドは、VFlash メディアカードが搭載されている場合にのみ機能します。カードが搭載されていない場合は、「エラー: 要求した操作を実行できません」というメッセージが表示されます。SD カードが挿入されていることを確認してください。

[目次ページに戻る](#)

[目次ページに戻る](#)

仮想メディアの設定と使用法

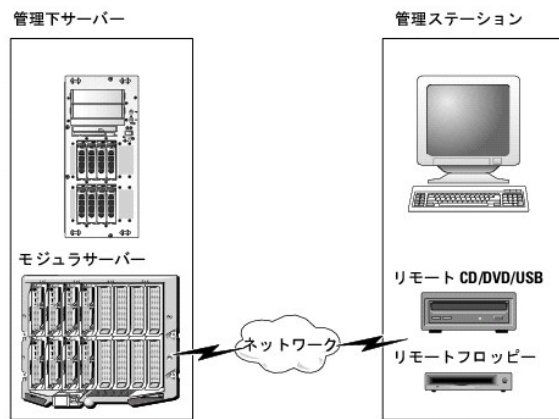
Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [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 13-1 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 13-1 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 およびディスクレット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経由で提供します。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。仮想メディアの接続は、メディアを管理下システムの物理デバイスに挿入する操作と同じように見えます。仮想メディアが連結状態にある場合、管理下システム上の仮想デバイスはドライブ内にメディアがインストールされていない 2 つのドライブとして表示されます。

表 13-1 は、仮想フロッピーと仮想オプティカルドライブでサポートされているドライブ接続です。

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 13-1 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(最小サイズ 128 MB)	

Windows ベースの管理ステーション

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 の対応バージョンと ActiveX Control プラグインをインストールします。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 を起動します。
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. Web コンテンツのゾーンを選択してセキュリティのレベルを設定する 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 を再起動します。

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完了するには、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。

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。

仮想メディアの設定

1. iDRAC6 ウェブインタフェースにログインします。
2. システム コンソール / メディア 設定 の順にクリックします。
3. 仮想メディア セクションで、設定値を選択します。仮想メディアの設定値の詳細については、「表 13-2」を参照してください。
4. 適用 をクリックして設定を保存します。

次のメッセージと一緒に警告ダイアログが表示されます。You are about to change device configuration. All existing redirection sessions will be closed. Do you want to continue? (デバイスの設定を変更しようとしています。既存のリダイレクトセッションすべてが終了します。続行してもよろしいですか?)

5. OK をクリックして続行します。

次のメッセージと一緒に警告ダイアログが表示されます。仮想メディアの設定は正常に設定されました。


表 13-2 仮想メディアの設定値

属性	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	<p>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。この値は常に 1 です。</p> <p>メモ: 仮想メディアユーザーセッションは、1 回のみ認められています。ただし、複数のデバイスを 1 回のセッションで取り付けることが可能です。「仮想メディアの実行」を参照してください。</p>
アクティブセッション数	<p>現在アクティブな仮想メディアセッション数を表示します。</p>

仮想メディア暗号化の有効	仮想メディア接続の暗号化を有効(チェックを入れる)または無効(チェックを外す)にします。
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 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上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。 メモ: 特定の Windows Vista® および Red Hat® Enterprise Linux® 環境において、 フロッピーのエミュレーション を有効にした場合、USB を仮想化できない場合があります。
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(チェックを入れる)または無効(チェックを外す)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。仮想メディアから起動するには、この属性を使用します。次の起動で、システムは起動順序の次のデバイスから起動します。このオプションは、自動展開の際に便利です。

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には `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状態である必要があります。


1. 管理ステーションで対応ウェブブラウザを開きます。
2. iDRAC6 ウェブインタフェースにログインします。
3. **コンソール / メディア** タブをクリックします。

コンソールリダイレクトおよび仮想メディア 画面が表示されます。


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。

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 `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。


5. **メディア P 仮想メディアウィザード** の順に選択します。

メディアリダイレクト ウィンドウが開きます。


6. **メディアリダイレクト** ウィンドウの下部で **状態** セクションを確認します。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。メディアを切断するには、**ステータス** ウィンドウのメディアの横にある **接続解除** をクリックします。

7. 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。

8. **フロッピーイメージ** ボタンと、**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。

 **メモ:** 管理ステーションの CD/DVD メディアが iDRAC6 ブレードによって既に使用中の場合は、同じメディアをリダイレクトすると、別の iDRAC6 ブレードでも使用できます。つまり、iDRAC6 は同じメディア (読み取り専用) を 2 台の iDRAC6 ブレードにリダイレクトする機能をサポートしています。ただし、USB メディアは 2 台の iDRAC6 ブレードに連結できません。iDRAC6 にこれを指摘する警告メッセージが表示されます。


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** ボタンでイメージへ移動します。

 **メモ:** Java ベースの仮想メディアプラグインを使用している場合は、リモートの ISO イメージをマウントできない可能性があります。たとえば、Linux のクライアントでは Java ベースのプラグインが使用されているため、イメージをマウントできません。これを回避するには、ISO イメージをローカルシステムにコピーして、ローカルでイメージファイルを使用できるようにしてください。Java ベースの仮想メディアプラグインでは、`\\computer\share` の形式で共有名を指定することができます。

9. **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。

メディアが接続され、**ステータス** ウィンドウが更新します。

10. **閉じる** をクリックします。

 **メモ:** 仮想メディアセッションが開始、または VFlash が接続されるたびに、「LCDRIVE」の名前のドライブが、ホストオペレーティングシステムおよび BIOS で表示されます。VFlash または仮想メディアセッションが切断されると、このドライブの表示が消えます。

仮想メディアの切断


1. **メディア** → **仮想メディアウィザード** の順に選択します。

メディアリダイレクト ウィザードが開きます。

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。

メディアが切断され、**ステータス** ウィンドウが更新されます。

3. **閉じる** をクリックします。

 **メモ:** iDRACview を起動してから、ウェブ GUI からログオフすると、iDRACview は終了せず、アクティブなままになります。

仮想メディアからの起動

システム BIOS を使用すると、仮想光学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> キーを押して 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、仮想光学ドライブ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

この項では、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 DVD/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 DVD/CD が挿入されている。
1. ローカルの DVD/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 DVD/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. 画面の説明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が連結し、ドライブ文字で設定されていると、それらは自動的にマウントされます。

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 13-3 は、よくあるお問い合わせとその回答です。

表 13-3 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、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て接続を中断します。 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、設定変更を適用すると、接続しているメディアがすべて切断されます。 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すると、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て接続を中断します。また、他の人が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、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。	Windows オペレーティングシステムをインストールしている場合、ネットワーク接続が低速であれば、ネットワーク遅延により、インストール手順で iDRAC6 にアクセスするの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開いてください。
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 VFlash 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。	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 CDRROM/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(最小サイズ 128 MB) 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。 また、Windows 98 起動ディスクを使用して起動し、起動ディスクから USB キーにシステムファイルをコピーすることも可能です。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。
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。
iDRAC6 ウェブインタフェースを使用してリモートでファームウェアのアップデートを実行すると、サーバーの仮想ドライブが削除されてしまいました。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 iDRAC6 がリセットされ、リモート接続が切れて、仮想ドライブのマウントが解除されます。iDRAC6 のリセットが完了すると、ドライブは再表示されます。
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。仮想メディアが接続しているのに、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。

- 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。
- 仮想フロッピードライブに連結し接続していることを確認します。
- Linux のプロンプトで次のコマンドを入力します。

```
mount /dev/sdx /mnt/floppy
```

このコマンドで、

/dev/sdx は手順 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。

[目次ページに戻る](#)

[目次ページに戻る](#)

RACADM コマンドラインインタフェースの使用

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [RACADM サブコマンド](#)
- [サポートされている RACADM インタフェース](#)
- [ローカル RACADM コマンドの使用](#)
- [RACADM ユーティリティを使用した iDRAC6 の設定](#)
- [リモートおよび SSH/Telnet RACADM](#)
- [iDRAC6 設定ファイルの使用](#)
- [複数の iDRAC6 の設定](#)

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 iDRAC6 管理機能へのアクセスを提供します。RACADM を使用して、iDRAC6 ウェブインタフェースにあるほとんどの機能にアクセスできます。インタラクティブな管理に役立つウェブインタフェースの代わりに、RACADM をスクリプトで使用すると、複数のサーバーを簡単に設定できます。

RACADM には次のインタフェースが用意されています。

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 Telnet/SSH RACADM

ローカル RACADM コマンドは、管理下サーバーから iDRAC6 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 iDRAC6 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。リモート RACADM はクライアント側のユーティリティで、管理ステーションから帯域外ネットワークインタフェースを使用して実行できます。SSH/Telnet RACADM は SSH または Telnet プロンプトから RACADM コマンドの使用法を参照するために使用されます。

本項では、以下について説明します。

- 1 RACADM コマンドとサポートされている RACADM インタフェース
- 1 コマンドプロンプトからのローカル RACADM の使用
- 1 リモート RACADM
- 1 SSH/Telnet RACADM
- 1 `racadm` コマンドを使用した iDRAC6 の設定
- 1 RACADM 設定ファイルを使用した複数の iDRAC6 の設定

 **注意:** 最新の iDRAC6 ファームウェアは RACADM の最新バージョンのみをサポートしています。最新のファームウェアを使用している iDRAC6 に、旧バージョンの RACADM からクエリを実行すると、エラーが発生する可能性があります。最新の『Dell™ OpenManage™ DVD』メディアで配布されている RACADM バージョンをインストールしてください。

RACADM サブコマンド

表 14-1 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リストは、『[RACADM サブコマンドの概要](#)』を参照してください。

表 14-1 RACADM サブコマンド

コマンド	説明
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。
clearasrscreen	前回のクラッシュ (ASR) 画面をクリアします
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。
clrraclog	iDRAC6 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。
clrsele	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。
config	iDRAC6 を設定します。
fwupdate	iDRAC6 ファームウェアをアップデートします。
getconfig	現在の iDRAC6 設定のプロパティを表示します。
getniccfg	コントローラの現在の IP 設定を表示します。
getraclog	iDRAC6 のログを表示します。
getractime	iDRAC6 の時刻を表示します。
getsel	SEL エントリを表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsvctag	サービスタグを表示します。
getsysinfo	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 iDRAC6 および管理下サーバーに関する情報を表示します。

gettracelog	IDRAC6 トレースログを表示します。-i と一緒に使用した場合は、iDRAC6 のトレースログのエントリ数を表示します。
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。
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。
krbkeytabupload	Kerberos keytab ファイルをアップロードします。
localconredirdisable	ローカルシステムから、ローカル KVM の無効化を実行します。
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。宛先 IP アドレスが必要です。ICMP 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、目的の IP アドレスに送信されます。
ping6	現在のルーティングテーブルの内容を使用して iDRAC6 から送信先の IPv6 アドレスに到達可能かどうかを確認します。送信先の IPv6 アドレスが必要です。ICMP 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、目的の IPv6 アドレスに送信されます。
racdump	ステータスおよび iDRAC6 の一般的な情報を表示します。
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。
remoteimage	リモートファイル共有
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。
sshpkauth	最大 4 つの SSH 公開キーのアップロード、既存のキーの削除、そして iDRAC6 に既にあるキーの表示を可能にします。
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 iDRAC6 にアップロードします。
sslcertview	iDRAC6 に CA 証明書またはサーバー証明書を表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
testemail	iDRAC6 NIC 経由で iDRAC6 に電子メールを送信させます。
testtrap	iDRAC6 NIC 経由で iDRAC6 に SNMP 警告を送信させます。
traceroute	パケットがシステムから目的の IPv4 アドレスに転送されるときに通るルーターのネットワーク経路をトレースします。
traceroute6	パケットがシステムから目的の IPv6 アドレスに転送されるときに通るルーターのネットワーク経路をトレースします。
version	iDRAC6 のバージョン情報を表示します。
vmdisconnect	リモートクライアントからの iDRAC 仮想メディア接続をすべて閉じます。
vmkey	VFlash パーティションをデフォルトサイズの 256MB にリセットし、同パーティション上のすべてのデータを削除します。

サポートされている RACADM インタフェース

表 14-2 に、RACADM のサブコマンドと、それに対応するインタフェースのサポートについて概要を示します。

表 14-2 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	ローカル RACADM	リモート RACADM
arp	✓	✗	✓
clearasrscreen	✓	✓	✓
clrraclog	✓	✓	✓
clrsel	✓	✓	✓
config	✓	✓	✓
coredump	✓	✓	✓
coredumpdelete	✓	✓	✓
fwupdate	✓	✓	✓
getconfig	✓	✓	✓
getniccfg	✓	✓	✓
getraclog	✓	✓	✓
getractime	✓	✓	✓
getsel	✓	✓	✓
getssninfo	✓	✓	✓

getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
krbkeytabupload	✗	✓	✓
localconredirdisable	✗	✓	✗
netstat	✓	✗	✓
ping	✓	✗	✓
ping6	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
remoteimage	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sshpkauth	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✓ (生成できるだけで、ダウンロードはできません)	✓	✓
sslkeyupload	✗	✗	✗
testemail	✓	✓	✓
testtrap	✓	✓	✓
traceroute	✓	✗	✓
traceroute6	✓	✗	✓
usercertupload	✗	✗	✗
usercertview	✗	✗	✗
version	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓
✓ = サポートされている ✗ = サポートされていない			

ローカル 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 コマンドを次の形式で入力します。

```
1 racadm <サブコマンド> [パラメータ]
1 racadm <getconfig|config> [-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
```

または


```
racadm getconfig -h
```

サブコマンドのリストには、iDRAC6 でサポートされる RACADM 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 ユーティリティを使用した iDRAC6 の設定

この項では、RACADM を使用して、さまざまな iDRAC6 設定タスクを実行する方法を説明します。

現在の iDRAC6 設定の表示

RACADM `getconfig` サブコマンドは、iDRAC6 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、「[iDRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義](#)」を参照してください。

すべての iDRAC6 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 iDRAC6 ユーザーの管理

-  **メモ:** `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 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。
-  **メモ:** ユーザーは長期に渡って有効にしたり、無効にしたりできます。その結果、ユーザーが各 iDRAC6 に異なるインデックス番号を持つ場合があります。
-  **メモ:** Active Directory 環境用に作成されたユーザーとグループは、Active Directory 命名規則に準拠する必要があります。

iDRAC6 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 iDRAC6 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を確認してください。


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 の各インデックスに 1 回ずつ次のコマンドを入力します。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```


-  **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 iDRAC6 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 が現在値と一緒に表示されます。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インデックス番号は使用可能です。「=」の後に名前が表示された場合は、インデックスがそのユーザー名に割り当てられています。

-  **メモ:** Active Directory 環境用に作成されたユーザーとグループは、Active Directory 命名規則に準拠する必要があります。

iDRAC6 ユーザーの追加

新しいユーザーを iDRAC6 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 iDRAC6 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 iDRAC6 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 cfgUserAdminPrivilege -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 iDRAC6 ユーザーを有効にする

ユーザーに特定の管理者権限(役割ベース)を与えるには、`cfgUserAdminPrivilege` プロパティを、[表 14-3](#) 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 14-3 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
iDRAC6 へのログイン	0x00000001
iDRAC6 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** の各権限を与えるには、`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
```

RACADM を使用した SSH キーのアップロード、表示、および削除

アップロード

アップロードモードでは、キーファイルのアップロードまたはコマンドライン上にキーテキストをコピーできます。キーのアップロードとコピーを同時に行うことはできません。

ローカル RACADM を使用する場合:

```
racadm sshpkauth -i <2 ~ 16> -k <1 ~ 4> -f <ファイル名>
```

telnet/ssh RACADM を使用する場合:

```
racadm sshpkauth -i <2 ~ 16> -k <1 ~ 4> -t
```


<キーテキスト>

例:

ファイルを使用して iDRAC6 ユーザー 2 の最初のキースペースに有効なキーをアップロードする場合:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

PK SSH 認証キーファイルは、RAC に正常にアップロードされました。

 **注意:** telnet/ssh/serial RACADM では、「file」オプションはサポートされていません。

表示

表示モードでは、ユーザーが指定するキーまたはすべてのキーを表示できます。

```
racadm sshpkauth -i <2 ~ 16> -v -k <1 ~ 4>
```


```
racadm sshpkauth -i <2 ~ 16> -v -k all
```

削除

削除モードでは、ユーザーが指定するキーまたはすべてのキーを削除できます。

```
racadm sshpkauth -i <2 ~ 16> -d -k <1 ~ 4>
```

```
racadm sshpkauth -i <2 ~ 16> -d -k all
```

 **注意:** SSH キーのアップロード、表示、および削除の各機能は、「ユーザーの設定」ユーザー権限に基づきます。この権限を持つユーザーは、他のユーザーの SSH キーを設定することができます。SSH キーは非常に重要であるため、この権限の付与は慎重に行ってください。

サブコマンドオプションの詳細については、「[sshpkauth](#)」を参照してください。

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、指定したインデックス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。

電子メール警告のテスト

iDRAC6 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、iDRAC6 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
```

(-i 2 は電子メール警告テーブルのインデックスエントリの 2 番です)

 **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。


iDRAC6 SNMP トラップ警告機能のテスト

iDRAC6 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
```

(-i 2 は電子メール警告テーブルのインデックスエントリの 2 番です)

 **メモ:** iDRAC6 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。詳細については、「[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。

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、<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、

[[iDRAC6 LAN](#)]を参照してください。

次に、LAN ネットワークプロパティを設定するコマンドの使用例を示します。


```
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。

IPMI オーバー LAN 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 cfgIpmlan -o cfgIpmlanEnable 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 規格を参照してください。

- a. 次のコマンドを入力して、IPMI チャネル権限をアップデートします。

```
racadm config -g cfgIpmlan -o cfgIpmlanPrivilegeLimit <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(システム管理者)

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 cfgIpmlan -o cfgIpmlanPrivilegeLimit 2
```

- b. 必要に応じて、次のようなコマンドを使用して IPMI LAN チャネルの暗号化キーを設定します。


 **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 規格を参照してください。

```
racadm config -g cfgIpmlan -o cfgIpmlanEncryptionKey <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。

2. 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 cfgIpmlanSol -o cfgIpmlanSolEnable 1
```

 **メモ:** IPMI SOL 最小権限レベルは、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 規格を参照してください。

- a. 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 cfgIpmlanSol -o cfgIpmlanSolMinPrivilege <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(システム管理者)

たとえば、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 経由でリ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。

例:

```
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せん。

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable 1 -i <ID>
```

<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 iDRAC6 が講じる処置を設定できます。[表 14-4](#) 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 14-4 プラットフォームイベントの処置

動作	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 <インデックス> <処置値>
```

<インデックス> は PEF インデックス(「[表 5-8](#)」の「[表 14-4](#)」)で、<処置値> は「」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

- 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
```

- 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 <インデックス> <0|1>
```

<インデックス> は PET の送信先のインデックスで、0 は PET を無効に、1 は PET を有効にします。

たとえば、PET をインデックス 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
```

- 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 <インデックス> <IP アドレス>
```

<インデックス> は PET の送信先のインデックスで、<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 <インデックス> <0|1>
```

<インデックス> は電子メール送信先のインデックスで、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インデックスは 1 ~ 4 の値が可能です。

たとえば、PET をインデックス 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を受け取る送信先電子メールアドレスです。

4. SMTP 電子メールサーバーを設定するには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr <SMTP 電子メールサーバーの IP アドレス>
```

5. 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 <インデックス> <カスタムメッセージ>
```

<インデックス> は電子メール送信先のインデックスで、<カスタムメッセージ> はカスタムメッセージです。

6. 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 <インデックス>
```

<インデックス> は、テストする電子メール送信先のインデックスです。

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 iDRAC6 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 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。

`cfgRacTune` プロパティの全リストは、「[cfgRacTuning](#)」に掲載されています。

表 14-5 IP アドレスフィルタ(IPRange)のプロパティ

プロパティ	説明

cfgRacTuneIpRangeEnable	IP アドレスのチェック機能を有効にします。
cfgRacTuneIpRangeAddr	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 cfgRacTuneIpRangeMask 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。
cfgRacTuneIpRangeMask	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。

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、「[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. 連続する 4 つの IP アドレスにログインを限定するには(たとえば、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自動的に判断し、そのアドレスが iDRAC6 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、「[iDRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義](#)」に掲載されています。

[ログイン再試行制限\(IP ブロック\)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 14-6 ログイン再試行制限(IP ブロック)のプロパティ

プロパティ	定義
cfgRacTuneIpBlkEnable	IP ブロック機能を有効にします。 一定時間内に(cfgRacTuneIpBlkFailWindow)1 つの IP アドレスからの失敗が連続すると(cfgRacTuneIpBlkFailCount)、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(cfgRacTuneIpBlkPenaltyTime)拒否されます。
cfgRacTuneIpBlkFailCount	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。
cfgRacTuneIpBlkFailWindow	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。
cfgRacTuneIpBlkPenaltyTime	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 分間このクライアント 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 3600
```

ローカル RACADM を使用した iDRAC6 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、iDRAC6 の設定 権限が必要です。

 **メモ:** iDRAC6 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、警告なしに終了します。

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
```

iDRAC6 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、「[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。

リモートおよび SSH/Telnet RACADM

リモート RACADM はクライアント側のユーティリティで、管理ステーションから帯域外ネットワークインタフェースを使用して実行できます。管理下システムに接続して、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のオプション(-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 の IP アドレスが必要です。SSH/Telnet RACADM は SSH または Telnet プロンプトから RACADM コマンドの使用法を参照するために使用されます。

同時に実行できるリモート RACADM の最大セッション数は 4 です。これらのセッションは独立しており、Telnet および SSH セッションとは別です。iDRAC6 は 4 つの RACADM セッションに加えて、4 つの SSH セッションと 4 つの Telnet セッションを同時にサポートできます。

 **メモ:** RACADM のリモート機能を使用する前に、iDRAC6 の IP アドレスを設定します。

 **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。

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (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と一致しません)
```

```
Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors. (実行を続けます。証明書関連のエラーが発生したときに racadm に実行を停止するには、-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。

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (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と一致しません)
```


Racadm not continuing execution of the command. (Racadm はコマンドの実行を続行しません。)

ERROR: Unable to connect to iDRAC6 at specified IPaddress (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 リモート機能を使用する場合は、次に示すようなファイル操作に関連して RACADM サブコマンドを使用す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 sslcertdownload -t <種類> [-f <ファイル名>]
```

リモート RACADM の使用方法

```
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>
```

リモート RACADM のオプション

表 14-7 に、リモート RACADM コマンドのオプションを一覧にします。

表 14-7 RACADM コマンドのオプション

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)でない場合は、<ポート番号> を使用してください。
-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、-p 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。

iDRAC6 設定ファイルの使用

iDRAC6 設定ファイルは、iDRAC6 データベースの代表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 iDRAC6 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 iDRAC6 にロードし直すか、設定を他の iDRAC6 にコピーできます。

iDRAC6 設定ファイルの作成

設定ファイルは、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とおりです。

- 1 テキストエディタで作成可能
- 1 RACADM `getconfig` サブコマンドで iDRAC6 から取得
- 1 RACADM `getconfig` サブコマンドで iDRAC6 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、次のコマンドを入力します。

```
racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> 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

メモ: 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 iDRAC6 のデータベースが壊れ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:

```
#  
  
# This is a comment (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、[と] 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。設定データは「[iDRAC6 Enterprise プロパティデータベースグループおよびオブジェクト定義](#)」で定義されているようにグループに分類されます。

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=192.168.1.1(オブジェクト名)
```

- 1 パラメータは、object、=、および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、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、使用するインデックスを指定できません。インデックスが既に存在する場合は、それが使用されます。インデックスがない場合は、そのグループで最初に使用可能なインデックスに新しいエントリが作成されます。

racadm getconfig -f <ファイル名> 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、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、インデックス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 <インデックス> <固有アンカー名>

- 1 インデックス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、手動でインデックス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> ""
```

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。

インデックス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 インデックス付きグループの場合、オブジェクトアンカーは [] の組の後に最初のオブジェクトでなければなりません。次は、現在のインデックス付きグループの例です。

```
[cfgUserAdmin]  
  
cfgUserAdminUserName=<ユーザー名>
```

- 1 パーサーがインデックス付けされたグループを見つけた場合、これはさまざまなインデックス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 iDRAC6 にそのインデックスが作成されます。

- 1 設定ファイルでインデックスを指定することはできません。

インデックス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と未使用のインデックスで断片化してくる可能性があります。インデックスが存在する場合は、変更されます。インデックスが存在しない場合は、最初に使用できるインデックスが使用されます。この方法では、インデックス付きエントリを追加するときに、管理下のすべての RAC 間でインデックスを正確に一致させる必要がないという柔軟性が得られます。新しいユーザーは、最初に使用可能なインデックスに追加されます。すべてのインデックスが一杯で新しいユーザーを追加する必要がある場合は、1 つの iDRAC6 で正しく解析および実行される設定ファイルが別の iDRAC6 でも正しく実行されるとは限りません。

設定ファイルの iDRAC6 IP アドレスの変更

設定ファイル内の iDRAC6 IP のアドレスを変更するには、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、"["と "]" が付いた実際の変数グループのラベルのみが残ります。

例:


```
#  
  
# Object Group "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。


```
#  
  
# Object Group "cfgLanNetworking"  
  
#  
  
[cfgLanNetworking]  
  
cfgNicIpAddress=10.35.9.143  
  
#comment, the rest of this line is ignored (コメント、以下の行は無視されます)  
  
cfgNicGateway=10.35.9.1
```

iDRAC6 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なければ、このファイルの内容で iDRAC6 データベースがアップデートされます。

 **メモ:** 構文のみを検証し、iDRAC6 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ます。設定ファイルで iDRAC6 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。

 **メモ:** `racresetcfg` サブコマンドを使用すると、データベースと iDRAC6 NIC の設定は元のデフォルト設定にリセットされ、ユーザーとユーザー設定がすべて削除されます。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、`racresetcfg` サブコマンドを実行して iDRAC6 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、インデックス、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 iDRAC6 をアップデートするには、次のコマンドを実行します。

```
racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> config -f myconfig.cfg
```

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 iDRAC6 の設定

設定ファイルを使用して、同じプロパティを備えた他の iDRAC6 を設定できます。複数の iDRAC6 を設定するには、次の手順に従ってください。

1. 他の iDRAC6 に複製する iDRAC6 の設定から設定ファイルを作成します。次のコマンドを入力します。

```
racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> getconfig -f <ファイル名>
```

<ファイル名> は `myconfig.cfg` など、iDRAC6 のプロパティを保存するファイルの名前です。

以下の例は、リモート RACADM コマンドを使用して複数の iDRAC6 を設定する方法を紹介しています。管理ステーションでバッチファイルを作成し、バッチファイルからリモート `racadm` コマンドを呼び出します。

例:

```
racadm -r <サーバー IP 1> -u <ユーザー> -p <パスワード> config -f myconfig.cfg
```

```
racadm -r <サーバー IP 2> -u <ユーザー> -p <パスワード> config -f myconfig.cfg
```

...

詳細については、「[iDRAC6 設定ファイルの作成](#)」を参照してください。



メモ: 設定ファイルによっては、他の iDRAC6 にファイルをエクスポートする前に変更する必要がある固有の iDRAC6 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、コピーしない設定を削除またはコメントアウトします。
3. 設定する iDRAC6 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 iDRAC6 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. iDRAC6 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 iDRAC6 にロードします。

```
racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> 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 iDRAC6 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](#)

WS-MAN インタフェースの使用

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [WS 管理の機能](#)
- [対応 CIM プロファイル](#)

Web Services for Management (WS-MAN) は、Simple Object Access Protocol (SOAP) ベースのプロトコルで、システム管理に使用されます。WS-MAN は、ネットワークでデータの共有とやり取りを行うデバイスの相互運用可能なプロトコルを提供します。iDRAC6 は WS-MAN を使用して、Distributed Management Task Force (DMTF) の Common Information Model (CIM) ベースの管理情報を伝送します。CIM 情報は、管理下システムで操作可能なセマンティクスや情報の種類を定義します。Dell™ が組み込まれたサーバープラットフォーム管理インタフェースはプロファイルに分類され、各プロファイルが特定の管理ドメインや機能領域に固有のインタフェースを定義しています。さらに、デルではモデルやプロファイルの拡張を多数定義して、その他の機能のインタフェースも提供しています。

WS-MAN を介して入手できるデータは、DMTF プロファイルと Dell 拡張プロファイルにマッピングされた iDRAC6 計装インタフェースによって提供されます。

WS 管理の機能

WS-Management の仕様は、管理アプリケーションと管理下リソースの相互運用性を促進します。ウェブサービスの規格と使用要件のコアセットを識別して、あらゆるシステム管理の要となる共通操作を明らかにすることで、WS-Management は以下のことができます。

- 1 管理リソースの存在を検出し、リソース間を移動する
- 1 設定や動的な値など、個々の管理リソースを取得、設定、作成、削除する
- 1 大容量テーブルやログなど、コンテナやコレクションの内容を列挙する
- 1 強かに型付けされた入出力パラメータを使用して特定の管理手段を実行する

対応 CIM プロファイル

表 17-1 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. ベースメトリック 管理下要素の取り込まれたメトリックをモデル化して制御する機能を提供する CIM クラスを定義します。
3. サービスプロセッサ サービスプロセッサをモデル化する CIM クラスを定義します。
4. USB リダイレクト USB リダイレクトに関する情報を記述する CIM クラスを定義します。キーボード、ビデオ、およびマウス装置については、装置を USB デバイスとして管理する場合は、このプロファイルを使用する必要があります。
5. 物理的資産 管理要素の物理的資産を表す 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。
6. 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独自の CLP を実行します
7. 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。
8. 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独自の CLP を実行します。
9. IP インタフェース 管理下システムの IP インタフェースを表す CIM クラスを定義します。
10. DHCP クライアント DHCP クライアントとそれに関連付けられた機能や設定を表す CIM クラスを定義します。
11. DNS クライアント 管理下システムの DNS クライアントを表す CIM クラスを定義します。
12. ログ記録

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. 役割ベースの認証 役割を表す 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。
14. 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独自の CLP を実行します。
15. プロファイル登録 プロファイルの実装をアダプタイズする 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、独自で実装したプロファイルをアダプタイズします。
16. 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。
17. Ethernet ポート 管理下システムの Ethernet ポート、それに関連付けられたコントローラ、および Ethernet インタフェースを表す CIM クラスを定義します。ポートの物理面との関連付けとプロファイル実装バージョンの情報はこのプロファイルでモデル化されます。
18. センサー 管理下システムのセンサーを説明する CIM クラスの定義に使用されます。また、センサーと監視されるデバイス間の関係を説明する関連クラスを定義します。
Dell 拡張
1. Active Directory クライアント 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. 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. OS 導入 OS 導入機能の設定を表す CIM クラスと Dell 拡張クラスを定義します。サービスプロセッサが提供する OS 導入機能に手を入れて OS 導入アクティビティをサポートする機能を追加する方法で、参照しているプロファイルの管理機能を拡張します。
4. ソフトウェアインベントリ 現在インストールされている BIOS、コンポーネントのファームウェア、診断、Unified Server Configurator、およびドライババックのバージョンを表す CIM と Dell 拡張を定義します。また、ロールバックおよび再インストール目的で、Lifecycle Controller で利用できる BIOS およびファームウェアアップデートイメージのバージョンを表します。
5. ソフトウェアのアップデート BIOS、診断、ドライババック、コンポーネント、Lifecycle Controller のファームウェアの更新目的で、サービスクラスおよびメソッドを表す CIM と Dell 拡張を定義します。アップデートメソッドは、CIFS、NFS、FTP、HTTP ネットワーク共有場所、そして Lifecycle Controller のアップデートイメージからのアップデートをサポートしています。アップデートリクエストは、ジョブとして計画され、アップデートに適用する再起動の処理方法の選択肢と共に、すぐにあるいは後で実行するようにスケジュールできます。
6. ジョブ制御 アップデートリクエストによって生成されるジョブを管理するための CIM と Dell 拡張を定義します。ジョブを作成、削除、変更、そして 1 回の再起動で複数のアップデートを実行するために、ジョブキューに統合させることもできます。
7. LC 管理 自動検出と部品交換 Lifecycle Controller 機能を管理する目的で、属性の取得および設定を行うための CIM と Dell 拡張を定義します。

iDRAC6 WS-MAN の実装は、ポート 443 上で SSL を使用して送信のセキュリティを確保し、またベーシックおよびダイジェスト認証をサポートしています。ウェブサービスのインタフェースは、Windows[®] WinRM や Powershell CLI などのクライアントインフラストラクチャ、WSMANCLI などのオープンソースのユーティリティ、次のようなアプリケーションプログラミング環境を利用して使うこともできます (Microsoft[®] .NET[®] など)。

そのほか、実装ガイド、ホワイトペーパー、プロファイル、コード例などが www.delltechcenter.com のデルエンタープライズテクノロジーセンターで入手可能です。詳細については、以下も参照してください。

- 1 DTMF ウェブサイト: www.dmtf.org/standards/profiles/
- 1 WS-MAN リリースノートまたは Readme ファイル。

[目次ページに戻る](#)


[目次ページに戻る](#)

iDRAC6 Enterprise の使用 SM-CLP コマンドラインのインタフェース

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド


- [SM-CLP を使用したシステム管理](#)
- [iDRAC6 SM-CLP のサポート](#)
- [SM-CLP の機能](#)
- [MAP アドレス領域の移動](#)
- [show パープの使用](#)
- [iDRAC6 SM-CLP の例](#)

本項では、iDRAC6 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す。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。

iDRAC6 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 iDRAC6 内で実行され、RACADM は管理下サーバー上で実行されます。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。

 **メモ:** iDRAC6 SM-CLP プロパティデータベース、WS-MAN クラスと SM-CLP ターゲット間のマッピング、およびデルの実装の詳細については、www.delltechcenter.com のデルエンタープライズテクノロジーセンターで『iDRAC6 CIM Element Mapping』と『iDRAC6 SM-CLP Property Database』の文書を参照してください。『iDRAC6 CIM Element Mapping』の文書に含まれている情報は、DMTF プロファイルで指定されています。WSMAN の構成については、<http://www.dmtf.org/standards/profiles/> の DMTF プロファイルと MOF に記載されています。さらに、Dell 拡張は <http://www.delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions> で入手できます。

SM-CLP を使用したシステム管理


iDRAC6 SM-CLP を使用すると、以下のシステム機能をコマンドラインから管理できます。


- 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 iDRAC6 ユーザーアカウントの管理
- 1 Active Directory 設定
- 1 iDRAC6 LAN の設定
- 1 SSL 証明書署名要求(CSR)の生成
- 1 仮想メディア設定

iDRAC6 SM-CLP のサポート

SM-CLP は iDRAC6 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。iDRAC6 SM-CLP インタフェースは DMTF 組織が提供する SM-CLP 規格バージョン 1.0 に基づいています。

以下の項では、iDRAC6 からホストされる SM-CLP 機能の概要について説明します。

 **メモ:** SM-CLP セッションを Telnet/SSH を使用して確立し、ネットワークの切断によってセッションが正しく終了しなかった場合に、「最大接続数に達した」というメッセージが表示されることがあります。これを解決するには、新しい接続を試みる前に、ウェブ GUI の **システム → リモートアクセス → iDRAC6 → ネットワーク / セキュリティ → セッション** で SM-CLP セッションを終了してください。

 **メモ:** iDRAC6 は最大 4 つの Telnet セッションと 4 つの SSH セッションを同時にサポートします。ただし、それら 8 つのセッション中 1 つだけが SM-CLP を使用できます。つまり、iDRAC6 がサポートしているのは一度に 1 つの SM-CLP セッションのみです。

SM-CLP セッションの開始方法

- 1 SSH/Telnet を使用して iDRAC6 に接続すると、CLI(コンソール)が開きます。
- 1 ドル記号のプロンプトで「smclp」と入力して、SM-CLP コンソールを開始します。

構文:

```
telnet <iDRAC6 の IP アドレス>
```

```
%; (CLI プロンプトが表示されます)
```

\$smclp: (CLI プロンプトで smclp と入力します)

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 パーブの共通セットを提供しています。

SM-CLP はパーブ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。パーブは、実行する操作を示し、ターゲットは操作の実行対象となるエンティティ(またはオブジェクト)です。

以下は SM-CLP コマンドラインの構文です。

<パーブ> [<オプション>] [<ターゲット>] [<プロパティ>]

表 16-1 は、iDRAC6 CLI がサポートするパーブ、各コマンドの構文、およびパーブがサポートするオプションのリストです。

表 16-1 サポートされている SM-CLP CLI パーブ

パーブ	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。 構文: cd [オプション] [ターゲット]	-default, -examine, -help, -output, -version
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
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
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, -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 16-2 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 16-2 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 <番号 すべて>
-output、-o	出力のフォーマットを指定します。 構文: -output format=<テキスト clpcsv キーワード clpxml> または -output format=<テキスト clpcsv キーワード clpxml>
-version、-v	SM-CLP のバージョン番号を示します。

MAP アドレス領域の移動

 **メモ:** SM-CLP アドレスバスでスラッシュ(/)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。アドレスバスは、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、iDRAC6 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 /admin1/system1/logs1/log1/record3
```

ターゲットなしで cd パーブを入力し、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

SM-CLP で使用可能なターゲット一覧は、www.delltechcenter.com のデルエンタープライズテクノロジセンターで SM-CLP マッピングの文書を参照してください。

show パーブ の使用

ターゲットの詳細を理解するには、show パーブを使用します。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 オプションを使用すると、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、次のコマンドを使用します。

```
/admin1/system1/sp1/oemdcim_mfaaccount1 show -display properties,targets
```

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=(ユーザー ID、名前)/admin1/system1/sp1/oemdcim_mfaaccount1
```

1 つのプロパティのみを表示する場合、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。アドレス空間のターゲットとプロパティをすべて表示するには、-l all オプションを使用します。

-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(テキスト、clpcsv、キーワード、clpxml)の 1 つを指定します。

デフォルトのフォーマットは **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。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 /admin1/system1/logs1/log1
```

iDRAC6 SM-CLP の例

以下のサブセクションでは、SSH インタフェースを使用して iDRAC6 にログインし、SM-CLP セッションを開始して以下の操作を実行する方法の例を示します。

- 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

サーバーの電源管理

表 16-3 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。

「smclp」と入力して SM-CLP コンソールを開始します。

表 16-3 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 iDRAC6 にログインする	>ssh 192.168.0.120 >login: root >password: SM-CLP コンソールを開始するには、「smclp」と入力します。
サーバーの電源を切る	->stop /admin1/system1 system1 successfully stopped
電源オフの状態からサーバーの電源を入れる	->start /admin1/system1 system1 successfully started
サーバーを再起動する	->reset /admin1/system1 RESET successful for system1

SEL 管理

表 16-4 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。

MAP ターゲットのナビゲーション

表 16-4 SEL の管理操作

操作	構文
SEL の表示	->show -d targets,properties,verbs /admin1/system1/logs1/log1 Might return: Targets: record1/

	<pre> record2/... Properties: OverwritePolicy=7 LogState=4 CurrentNumberOfRecords=60 MaxNumberOfRecords=512 ElementName=Record Log 1 HealthState=5 EnabledState=2 RequestedState=12 EnabledDefault=2 TransitioningToState=12 InstanceID=DCIM: SEL Log OperationalStatus={2} Verbs: show exit version CD help </pre>
SEL レコ ード の 表 示	<pre> ->show /admin1/system1/logs1/log1/record4 Might return: ufip=/admin1/system1/logs1/log1/record4 Associations:LogManagesRecord=>/admin1/system1/logs1/log1 Properties: RecordData=*0.0.65*4 2*1245152621*65 65*4*31*0*true*111*1*255*255* RecordFormat=*IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*IPMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI_GeneratorID*IPMI_EvMRev*IPMI_Ser Description=:0:Assert:OEM specific ElementName=DCIM System Event Log Entry InstanceID=DCIM:SEL LOG:4 LogInstanceID=idrac:Unknown:Unknown SEL Log LogName=DCIM System Event Log Entry RecordID=DCIM:SEL LOG:4 CreationTimeStamp=20090616114341.000000+000 </pre>
	<pre> Verbs: show exit version CD help delete </pre>
SEL のク リア	<pre> ->delete /admin1/system1/logs1/log1/record* Returns: Records deleted successfully. </pre>

表 16-5 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 16-5 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	-->cd admin1/system1

	<pre>->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 admin1 ->cd system1 ->cd logs1 ->cd log1 ->show</pre> <p>is equivalent to</p> <pre>->cd admin1/system1/logs1/log1 ->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>

[目次ページに戻る](#)

[目次ページに戻る](#)

iVMCLI を使用したオペレーティングシステムの導入

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [作業を開始する前に](#)
- [ブータブル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](#)

統合仮想メディアコマンドラインインタフェース (iVMCLI) 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。iVMCLI 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 iVMCLI 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

iVMCLI 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 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 または CD/DVD ISO のイメージである必要があります。

ブータブルイメージファイルの作成

イメージファイルの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 のウェブインタ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>
```

例:

```
dd if=/dev/sdc0 of=mycd.img
```

Windows システム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ときには、イメージファイルと CD/DVD のブートセクターをコピーするユーティリティを選んでください。

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設定済みのブータブルな導入イメージファイルがある場合は、この手順をスキップしてください。

設定済みのブータブルな導入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 IPMI tool と仮想メディアコマンドラインインターフェイス (iVMCLI) 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。

 **メモ:** `ivmdeploy` は内部で `iVMCLI` と `ipmitool` を使用します。このツールを使用するには、IPMI オーバー > LAN 権限が必要です。また、`ivmdeploy` スクリプトを使用する場合は、仮想メディアが連結している状態であればなりません。

オペレーティングシステムの導入

iVMCLI ユーティリティとそのユーティリティに含まれている `ivmdeploy` 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、iVMCLI 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手順を詳しく説明しています。

以下は、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手順の概要です。

1. `ip.txt` テキストファイルに導入されるリモートシステムの iDRAC6 の IP アドレス (1 行に 1 個の IP アドレス) を一覧にします。
2. ブータブルなオペレーティングシステム CD または DVD をクライアントの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 iDRAC6 のユーザー名 (たとえば `root`) です。
- 1 <iDRAC パスワード> は iDRAC6 ユーザーのパスワード (たとえば `calvin`) です。
- 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 iDRAC6 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ファイル名でない場合は、単一の iDRAC6 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ーフェイ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ーフェイス (iVMCLI) 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ーフェイスです。

iVMCLI 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、複数のセッションで同じ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 つのセッションのみ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と互換性のある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を有効にした場合の自動終了
- 1 Secure Socket Layer (SSL)を使用した iDRAC6 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、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。

△ 注意: iVMCLI コマンドラインユーティリティを実行する際は、「-i」の対話フラグを利用することをお勧めします。多くの Windows および Linux オペレーティングシステムでは、他のユーザーがプロセスを確認する際、ユーザー名とパスワードが平文のまま表示されるため、上記を行うことで、ユーザー名とパスワードの秘密性が保たれ、セキュリティが強化されます。

オペレーティングシステムがシステム管理者権限、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、iVMCLI コマンドを実行するためにもシステム管理者権限が必要です。

クライアントシステムの管理者は、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、iVMCLI 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、システム管理者権限がなくても、sudo コマンドを使って iVMCLI ユーティリティにアクセスできます。このコマンドは、システム管理者以外のアクセス権を与える手段を集中化し、すべてのユーザーコマンドをログに記録します。iVMCLI グループにユーザーを追加または編集する場合、システム管理者は visudo コマンドを使用します。システム管理者権限がないユーザーは、sudo コマンド iVMCLI コマンドライン(または iVMCLI 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。

iVMCLI ユーティリティのインストール

iVMCLI 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。ユーティリティをインストールするには、DVD をシステムに挿入し、画面上の指示に従います。

『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、RACADM 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に関する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、iVMCLI と RACADM ユーティリティを使用し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サンプルスクリプト `ivmdeploy` も収録されています。

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、それと一緒にすべてのファイルをコピーしてください。

コマンドラインオプション

iVMCLI 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同じです。たとえば、iDRAC6 の IP アドレスを指定するオプションでは、RACADM ユーティリティと iVMCLI ユーティリティで同じ構文が必要です。

iVMCLI コマンド形式は次のとおりです。

```
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、「[iVMCLI 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、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 iVMCLI 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を手動で中止した。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。

iVMCLI パラメータ

iDRAC6 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 iDRAC6 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 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 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が終了します。

<iDRAC の IP アドレス> は有効な固有の IP アドレスまたは iDRAC6 の動的ドメイン命名システム (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 ポートを変更した場合を除いて、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。

- l 有効なユーザー名
- l 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 {<デバイス名> | <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は、仮想メディアが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禁止するように、オペレーティングシステムを設定してください。

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み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>}

この場合、<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がない場合を除いて、このコマンドで少なくとも 1 つメディアタイプ (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 iVMCLI 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 iVMCLI ユーティリティのパラメータの概要を表示します。スイッチ以外のオプションがほかに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 iVMCLI 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、iVMCLI 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 の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。

iVMCLI オペレーティングシステムのシェルオプション

iVMCLI 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、iVMCLI 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:** iVMCLI ユーティリティは標準入力 (stdin) からは読み取りません。したがって、stdin リダイレクトは不要です。

- 1 バックグラウンド実行 - iVMCLI 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の場合、コマンドの直後にアンバーサンド(&)を指定すると、プログラムが新しいバックグラウンドプロセスとして起動します。

後者はスクリプトプログラムの場合に便利です。この方法では、iVMCLI コマンドの新しいプロセスが開始した後もスクリプトを継続できます(これ以外の方法では、iVMCLI 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)。iVMCLI 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。

iVMCLI の戻りコード

0 = エラーなし

1 = 接続できない

2 = iVMCLI 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](#)

iDRAC6 設定ユーティリティの使用

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [概要](#)
- [iDRAC6 設定ユーティリティの起動](#)
- [iDRAC6 設定ユーティリティの使用](#)

概要

iDRAC6 設定ユーティリティは、iDRAC6 と管理下システムのパラメータを表示して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バー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(LAN)を設定して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 パラメータを設定する
- 1 システムサービスの有効 / 無効 / キャンセルを切り替える
- 1 自動検出を有効または無効にし、プロビジョニングサーバーを設定する
- 1 仮想メディアデバイスの取り付けまたは取り外しを行う。
- 1 VFlash を有効または無効にする
- 1 スマートカードログインとシングルサインオンを有効または無効にする
- 1 システムデバイスを設定する
- 1 システム管理者のユーザー名とパスワードを変更する
- 1 iDRAC6 の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)からメッセージを表示またはクリアする

iDRAC6 設定ユーティリティを使用して実行できるタスクは、iDRAC6 または Dell™ 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、ローカルおよびリモート RACADM コマンドラインインタフェース)を使用して実行することもできます。また、基本的なネットワーク設定は最初の iDRAC6 設定時に iDRAC6 LCD でも実行できます。

iDRAC6 設定ユーティリティの起動

初回、または iDRAC6 をデフォルト 設定にリセットした後で iDRAC6 設定ユーティリティにアクセスするには、iDRAC6 KVM に接続したコンソールを使用する必要があります。

1. iDRAC6 KVM コンソールに接続したキーボードで、<Print Screen> を押して **iDRAC6 KVM 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. リモートアクセス設定は <Ctrl-E> for Remote Access Setup within 5 sec..... (5 秒以内に <Ctrl><E> キーを押してください..... というメッセージが表示されたら)、すぐに <Ctrl> キーを押しながら <E> キーを押します。iDRAC6 設定ユーティリティが表示されます。

 **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。

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の決定に役立ちます。

iDRAC6 ファームウェアは、ウェブインタフェースや SM-CLP など、ファームウェアの外部インタフェースに関連する部分です。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。

iDRAC6 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 iDRAC6 設定ユーティリティの残りの部分は、上下の方向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 / いいえ、有効 / 無効** などの選択可能な値がある場合は、左右の方向キー、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場合があります。
- 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。

- iDRAC6 設定ユーティリティを使い終わったら、<Esc> キーを押して 終了 メニューを表示します。このメニューから、変更の保存または破棄を選択するか、ユーティリティに戻ることができます。

以下の項では、iDRAC6 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

左右の方向キーと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、iDRAC6 の機能を使用するには、LAN を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。

iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF. (LAN チャネルがオフの場合、iDRAC 帯域外インタフェースは無効になります。)

このメッセージは、LAN を無効にすると、iDRAC6 HTTP、HTTPS、Telnet、または SSH ポートに直接接続してアクセスする機能だけでなく、管理ステーションから iDRAC6 に送信された 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を通知します。ただし、ローカルの RACADM インタフェースは引き続き使用でき、iDRAC6 LAN の再設定に使用することもできます。

任意のキーを押してメッセージをクリアし、続行します。

IPMI オーバー LAN

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、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ません。

オフ を選択すると、警告メッセージが表示されます。

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ついては、「[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 19-1 LAN パラメータ

項目	説明
共通設定	
MAC アドレス	これは、iDRAC6 ネットワークインタフェースの編集不可の MAC アドレスです。
VLAN の有効化	オン / オフ を表示します。 オン を選択すると、iDRAC6 の仮想 LAN フィルタが有効になります。
VLAN ID	1 ~ 4094 の VLAN ID の値を表示します。
VLAN	0 ~ 7 の VLAN の優先順位を表示します。
iDRAC6 名の登録	iDRAC6 名を DNS サービスに登録するには、 オン を選択します。DNS でユーザーが iDRAC6 名を検索でき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。ドメイン名には、有効な DNS ドメイン(例:mycompany.com)を指定する必要があります。
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、最初の警告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 を オン に設定する場合は、PET LAN 警告の転送先となる IP アドレスを入力します。
IPv4 の設定	
IPv4 接続のサポート	IPv4 接続のサポートを 有効 または 無効 にします。
IPv4	IPv4 プロトコルのサポートを 有効 または 無効 に指定します。 デフォルトは 有効 です。
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 の拡張機能です。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 に設定する場合は、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 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。デフォルトは 192.168.0.1 です。
DHCP からの DNS サーバー	ネットワーク上の DHCP サービスから DNS サーバーアドレスを取得するには、 オン を選択します。下記の DNS サーバーアドレスを指定するには、 オフ を選択します。
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	IPv6 接続に対するサポートを有効または無効にします。
IPv6 アドレスソース	AutoConfig(自動設定) または 静的 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、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 に設定する場合は、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、iDRAC6 ネットワークインタフェースの編集不可の IPv6 リンクローカルアドレス です。
IPv6 アドレス 2 ~ 15	これは、iDRAC6 ネットワークインタフェースの編集不可の IPv6 アドレス 2...IPv6 アドレス 15 です。
DHCPv6 からの DNS サーバー	ネットワーク上の DHCP サービスから DNS サーバーアドレスを取得するには、 オン を選択します。下記の DNS サーバーアドレスを指定するには、 オフ を選択します。
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。

仮想メディアの設定

仮想メディア

左向き矢印キーと右向き矢印キーを使用して **自動連結**、**接続**、または **切断** を選択します。

- 1 **接続** を選択すると、仮想メディアデバイスが USB バスに連結され、**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。
- 1 **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。
- 1 **自動連結** を選択すると、仮想メディアセッションが開始されると、仮想メディアデバイスは自動的にサーバーに連結されます。


 **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。サーバー起動中に <F2> キーを押して、BIOS 設定ユーティリティへアクセスしてください。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

左向き矢印キーと右向き矢印キーを使用して **有効** または **無効** を選択します。


- 1 **有効 / 無効** にすると、すべての仮想メディアデバイスが USB バスから **切断 / 接続** されます。
- 1 **無効** にすると、VFlash が切断され、使用できなくなります。

 **メモ:** 256 MB より大きいサイズの SD カードが iDRAC6 Express カードスロットになければ、このフィールドは読み取り専用になります。

 **メモ:** VFlash パーティションには、デル製の VFlash メディアが必要です。

スマートカード /SSO

このオプションは、**スマートカードログオン** および **シングルサインオン** 機能を設定します。選択できるオプションは、**有効** と **無効** です。

 **メモ:** **シングルサインオン** 機能を有効にする場合、**スマートカードログオン** 機能は無効になります。

システムサービス

システムサービス

左向き矢印キーと右向き矢印キーを使用して **有効** または **無効** を選択します。有効にすると、一部の iDRAC6 機能を Lifecycle Controller から設定できます。詳細については、デルのサポートウェブサイト support.dell.com/manuals にある『Lifecycle Controller ユーザーガイド』を参照してください。

 **メモ:** このオプションを変更するには、**保存**、**終了**して新しい設定を適用し、サーバーを再起動します。

システムサービスのキャンセル

上矢印キーと下矢印キーを使用して **はい** または **いいえ** を選択します。

はい を選択した場合は、Lifecycle Controller の全セッションが終了し、**保存** と **終了** を選択して新しい設定を適用すると、サーバーが再起動します。

再起動時にシステムインベントリの収集

起動時にインベントリの収集を行う場合は、**有効** を選択します。詳細については、デルサポートウェブサイト support.dell.com/manuals にある『Dell Lifecycle Controller ユーザーガイド』を参照してください。

 **メモ:** このオプションを変更する場合、設定を保存し、iDRAC6 設定ユーティリティを終了すると、サーバーが再起動します。

LAN ユーザー設定

LAN ユーザーは iDRAC6 のシステム管理者アカウントで、デフォルトでは **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 19-2 LAN ユーザー設定画面

項目	説明
自動検出	<p>自動検出機能は、ネットワークでプロビジョニングされていないシステムの検出を有効にします。さらに、検出されたシステムを管理できるように、最初の資格情報をセキュアに確立します。この機能を使用すると、iDRAC6 がプロビジョニングサーバーを見つけることができます。iDRAC6 とプロビジョニングサービスのサーバーは相互認証を実行します。リモートプロビジョニングサーバーはユーザーの資格情報を送信して、iDRAC6 にユーザーアカウントを作成させます。ユーザーアカウントが作成されると、リモートコンソールは、検出プロセスで指定された資格情報を使用して iDRAC6 と WSMAN 通信を確立し、オペレーティングシステムをリモートから導入するためのセキュアな命令を iDRAC6 に送ります。</p> <p>リモートオペレーティングシステム導入の詳細については、デルのサポートウェブサイト support.dell.com/manuals にある『Dell Lifecycle Controller ユーザーガイド』を参照してください。</p> <p>自動検出を手動で有効にする前に、iDRAC6 設定ユーティリティの別のセッションで、以下の必要条件を満たしてください。</p> <ul style="list-style-type: none">1 NIC を有効にする(ブレードサーバー)1 IPv4 を有効にする(ブレードサーバー)1 DHCP 有効1 DHCP からドメイン名を取得する1 管理者アカウント(アカウント番号 2)を無効にする1 DHCP から DNS サーバーのアドレスを取得する1 DHCP から DNS ドメイン名を取得する <p>自動検出機能を有効にするには、有効 を選択します。このオプションはデフォルトでは 無効 になっています。自動検出機能を 有効 にしたデルシステムを注文した場合、デルシステムの iDRAC6 は リモートログインのデフォルトの資格情報なしに DHCP を有効にして出荷されます。</p>
自動検出 (続き...)	<p>デルシステムをネットワークに追加して自動検出機能を使用する前に、以下のことを確認してください。</p> <ul style="list-style-type: none">1 Dynamic Host Configuration Protocol(DHCP)サーバー / ドメイン名システム(DNS)が設定されている。1 プロビジョニングウェブサービスがインストール、設定、登録されている。
プロビジョ ニングサ ーバー	<p>このフィールドは、プロビジョニングサーバーの設定に使用されます。プロビジョニングサーバーのアドレスは、IPv4 アドレスまたはホスト名の組み合わせにできます。アドレスは、255 文字を超えてはなりません。各アドレスまたはホスト名は、カンマで区切ります。</p> <p>自動検出機能を有効にした場合、自動検出プロセスの完了後、将来のリモートプロビジョニングを可能にするため、設定されたプロビジョニングサーバーからユーザー資格情報が取得されます。</p> <p>詳細については、デルサポートウェブサイト support.dell.com/manuals にある『Dell Lifecycle Controller ユーザーガイド』を参照してください。</p>
アカウント アクセス	<p>有効 を選択すると、管理者アカウントが有効になります。管理者アカウントを無効にする場合、または自動検出が有効になっている場合は、無効 を選択します。</p>
IPMI LAN 権 限	<p>管理者、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。</p>
アカウント ユーザー 名	<p><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 ルート です。</p>
パスワード の入力	<p>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。</p>

パスワードの確認	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 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。

 **メモ:** デフォルト設定で iDRAC6 ネットワークは無効になっています。iDRAC6 設定ユーティリティで iDRAC6 ネットワークを有効にするまでは、ネットワーク上で iDRAC6 の設定を変更できません。

<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) >)

iDRAC6 をデフォルトにリセットするには、**はい** を選択して、<Enter> キーを押します。

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) 内のメッセージの表示とクリアができます。<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。ログのエントリがカウントされ、レコード総数と最新のメッセージが表示されます。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。移動方法:

- 1 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。
- 1 レコード番号を入力するとそのレコードに移動します。

<Esc> キーを押すと、システムイベントログ が終了します。

 **メモ:** iDRAC6 設定ユーティリティまたは iDRAC6 ウェブインタフェースでのみ SEL をクリアできます。

SEL 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。

iDRAC6 設定ユーティリティの終了

iDRAC6 設定の変更が終了し、<Esc> キーを押すと、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、変更が維持されます。

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。

セットアップへ戻る を選択して <Enter> キーを押すと、iDRAC6 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](#)

管理下システムの修復とトラブルシューティング

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 2.2 ユーザーガイド

- [ユーザーとシステムの安全優先](#)
- [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、iDRAC6 ユーティリティを使用して、リモート管理下システムの診断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について説明します。以下の項目が含まれています。

- 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 iDRAC6 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。

ユーザーとシステムの安全優先

本項に記載している特定の手順を実行するには、シャーシ、Dell PowerEdge™ システム、またはその他のハードウェアモジュールを操作する必要があります。このガイドおよびシステムの他のマニュアルで説明されている以外の方法でシステムハードウェアを修理しないでください。

△ 注意: 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™ で認可されていない修理によって生じた損傷は、保証の対象となりません。製品に付属しているマニュアルの「安全にお使いいただくために」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 は、通常、システム上の問題の初期兆候を示します。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 があります。

- 1 シャーシ LCD モニタ
- 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は、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は、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 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。

[表 20-1](#) に、Dell PowerEdge システムの LED が表す意味を説明します。

表 20-1 ブレードサーバーの LED インジケータ

LED インジケータ	意味
緑色に点灯(電源ボタンのみ)	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は、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	iDRAC6 は正常に動作しています。
黄色に点滅	iDRAC6 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

このような問題が発生した場合は、損傷の原因を調査し、以下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 20-2 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。
IDRAC6 ログのメッセージ	「IDRAC6 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 IDRAC6 ユーティリティ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 最近の起動順序の表示
- 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 IDRAC6 ログの表示
- 1 システム情報の表示
- 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

IDRAC6 ウェブインタフェースにログインすると、**システム概要** 画面にシステムコンポーネントの正常性の状態が表示されます。[表 20-3](#) に、システム正常性インジケータの意味を示します。

表 20-3 サーバー正常性のインジケータ

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。

サーバー正常性 画面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。iDRAC6 と CMC の情報画面には、現在の状態と設定に関する有用な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 画面には、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** 画面を表示します。

システムイベントログ 画面には、システム正常性インジケータ(「表 20-3」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. 適切な **システムイベントログ** ボタンをクリックして続行します(「表 20-4」を参照)。

表 20-4 SEL 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、保存中に問題が発生した場合は、Microsoft® サポートウェブサイト support.microsoft.com から Internet Explorer の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。
更新	SEL 画面を再ロードします。

POST コードの確認

POST コード 画面には、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 画面には、システム正常性のインジケータ(「表 20-3」を参照)、16 進コード、コードの説明が表示されます。

2. 適切な **POST コード** ボタンをクリックして続行します(「表 20-5」を参照)。

表 20-5 POST コードのボタン

ボタン	動作
印刷	POST コード 画面を印刷します。
更新	POST コード 画面を再ロードします。

前回のシステムクラッシュ画面の表示

 **メモ:** 前回クラッシュ画面機能は Server Administrator と iDRAC6 ウェブインタフェースで設定する必要があります。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、iDRAC6 の持続的なストアに保存され、リモートからアクセスできます。

前回クラッシュ画面を表示するには、次の手順を実行してください。

- 1 システム、ログ タブ、前回クラッシュ画面の順にクリックします。

前回クラッシュ画面には、表 20-6 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 20-6 前回のクラッシュ画面のボタン

ボタン	動作
印刷	前回のクラッシュ画面を印刷します。
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を保存できます。
削除	前回のクラッシュ画面を削除します。
更新	前回のクラッシュ画面を再ロードします。

 **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、起動キャプチャ画面で最後の 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。iDRAC6 は起動時に 50 フレームを記録します。

表 20-7 に、使用可能な制御処置を示します。


 **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 20-7 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。 <ul 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	起動キャプチャ画面を再ロードします。

サーバーステ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テ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 20-8 サーバーステータス画面

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 が見つからないか、不在です。
重要	システム基板ビデオライザー: 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に障害が発生しました。
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。	IDRAC6 ウォッチドッグタイマーが期限切れで、処置が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。	IDRAC6 ウォッチドッグが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。
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。	IDRAC6 ウォッチドッグが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、電源を切る処置が設定されています。
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、電源の入れ直しがアサートされました。	IDRAC6 ウォッチドッグが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、パワーサイクルが設定されています。
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 つしかエントリを追加できないことを検出しました。
警告	ECC 修正可能エラー: メモリセンサー、修正可能な 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: 重大イベントセンサー、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	メモリスペア: 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。	メモリスペ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 (<DIMM の場所>)から重要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の障害
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/iDRAC6 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/iDRAC6 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。

iDRAC6 ログの表示

iDRAC6 ログは持続的なログで、iDRAC6 ファームウェアで管理されています。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。ログは iDRAC6 ファームウェアのアップデート後に消去されます。

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保管され、iDRAC6 ログには iDRAC6 で発生するイベントのレコードが保管されます。

iDRAC6 ログにアクセスするには、以下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 → iDRAC6 をクリックしてから、ログ iDRAC6 ログ の順にクリックします。

iDRAC6 ログは表 20-9 で情報を提供します。

表 20-9 iDRAC6 ログ情報

フィールド	説明

日時	日付と時刻 (Dec 19 16:55:47 など)。 iDRAC6 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。iDRAC6 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 iDRAC6 にログインしたユーザー名。

iDRAC6 ログボタンの使用

iDRAC6 ログ 画面には以下のボタンがあります (「表 20-10」を参照)。

表 20-10 iDRAC6 ログボタン

ボタン	動作
印刷	iDRAC6 ログ 画面を印刷します。
ログのクリア	iDRAC6 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を開き、選択したディレクトリに iDRAC6 の 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	iDRAC6 ログ 画面を再ロードします。

システム情報の表示

システム詳細 画面には、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. Integrated Dell Remote Access Controller 6 (iDRAC6) -Enterprise

システム情報にアクセスするには、システム → プロパティ R システム詳細 の順にクリックします。

システム概要、メインシステムエンクロージャ、および iDRAC6 の詳細については、「[管理下システムの修復とトラブルシューティング](#)」を参照してください。

シャーシ内の管理下サーバーの識別

Dell 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には、iDRAC6 ウェブインタフェースを使用してサーバーの青色の点滅 LED をオンにします。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 → iDRAC6 → トラブルシューティング の順にクリックします。
2. 識別 画面で サーバーの識別 を選択します。
3. サーバertime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は、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 → iDRAC6 → トラブルシューティング の順にクリックします。
2. 識別 画面で サーバーの識別 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

iDRAC6 には、Microsoft® Windows® や Linux ベースの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 20-11](#)」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 画面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 P iDRAC6 P **トラブルシューティング** の順にクリックします。
2. **診断コンソール** タブを選択します。

[表 20-11](#) に、**診断コンソール** 画面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** 画面に表示されます。

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 画面を更新するには、**更新** をクリックします。

表 20-11 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 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側の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。
ping6 <IPv6 アドレス>	送信先の IPv6 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。送信先の IPv6 アドレスをこのオプションの右側のフィールドに入力する必要があります。ICMP(インターネットコントロールメッセージプロトコル)エコーパケットは、現在のルーティングテーブルの内容に基づいて宛先の IPv6 アドレスに送信されます。
tracert <IP アドレス>	IP ネットワークでパケットが通る経路を決定するために使用します。
tracert6 <IPv6 アドレス>	IPv6 ネットワークでパケットが通る経路を決定するために使用します。
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。

リモートシステムの電源管理

iDRAC6 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正しく実行するには、**電源管理** 画面を使用します。

 **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、「[iDRAC6 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** → **電源制御** 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 20-12](#) 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。

表 20-12 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。 メモ: サーバースoftwareが応答しなくなった場合やシステム管理者として Windows のローカルコンソールにログインしていない場合は、オペレーティングシステムの正常なシャットダウンができないことがあります。そのような場合には、Windows の正常なシャットダウンではなく強制再起動を指定する必要があります。また、Windows OS のバージョンによっては、iDRAC6 からトリガされた場合、シャットダウンの動作を変更するシャットダウンプロセスの前後にポリシーが設定されている場合があります。Microsoft のマニュアルで、ローカルコンピュータポリシー「シャットダウン: ログインなしでシステムのシャットダウンを許可する」を参照してください。
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なおす(コールドブート)	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)。

ブート)

詳細については、「[電源モニタおよび電源管理](#)」を参照してください。

トラブルシューティングとよくあるお問い合わせ(FAQ)

[表 20-13](#) 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 20-13 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。 iDRAC6 ウェブインタフェースを使用する場合： <ol style="list-style-type: none">「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">「SEL 管理」を参照してください。 iDRAC6 設定ユーティリティを使用する場合： <ol style="list-style-type: none">「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。シャー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、「 シャーシ内の管理下サーバーの識別 」を参照してください。
iDRAC6 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">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。導入 をクリックします。表示されるテーブルからサーバーの IP アドレスを読み取ります。 iKVM を使用する場合： <ol style="list-style-type: none">サーバーを再起動し、<Ctrl><E> キーを押して iDRAC6 設定ユーティリティ を開始します。BIOS POST 中に表示される IP アドレスを確認します。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 サブコマンドの完全なリストは、『Dell Chassis Management Controller システム管理者リファレンスガイド』を参照してください。iDRAC6 の IP アドレスを表示するには、ローカル RACADM <code>getsysinfo</code> コマンドを使用します。
	例： <pre>\$ racadm getniccfg -m server-1</pre> DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1 ローカル RACADM を使用する場合： 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> LCD を使用する場合： <ol style="list-style-type: none">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。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 アドレスを見つける方法を教えてください。	iDRAC6 ウェブインタフェースを使用する場合： <ol style="list-style-type: none">システム → リモートアクセス → CMC の順にクリックします。 CMC 概要 画面に CMC の IP アドレスが表示されます。 iKVM を使用する場合： <ol style="list-style-type: none">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 サブコマンドの完全なリストは、『Dell Chassis Management Controller システム管理者リファレンスガイド』を参照してください。 <pre>\$ racadm getniccfg -m chassis</pre> NIC Enabled = 1 DHCP Enabled = 1

	<p>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> <p>メモ: 上記の処置はリモート RACADM で実行することもできます。</p>
iDRAC6 ネットワーク接続が機能しません。	<ol style="list-style-type: none"> 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。 NIC の設定、IPv4 または IPv6 の設定、および静的または DHCP がネットワークで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"> サーバーがパワーアップするまで、iDRAC6 の初期化に最大 2 分かかります。 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。
iDRAC6 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>iDRAC6 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"> サーバーを再起動し、プロンプトが表示されたら <Ctrl><E> キーを押して iDRAC6 設定ユーティリティ を開始します。 iDRAC6 設定ユーティリティ メニューで、デフォルトにリセット をハイライトして <Enter> キーを押します。 <p>メモ: また、<code>racadm racresetofg</code> を発行してローカル RACADM から iDRAC6 をリセットすることもできます。</p> <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"> CMC ウェブインタフェースにログインします。 シャーシ ツリーを開き、サーバー をクリックします。 セットアップ タブをクリックします。 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。 適用 をクリックします。
iDRAC6 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開始すると、ActiveX セキュリティポップアップが表示されます。	<p>iDRAC6 が信用済みサイトでない可能性があります。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が表示されるのを防ぐには、クライアントのブラウザで次のように iDRAC6 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"> 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。 サイトをクリックして iDRAC6 の IP アドレスまたは DNS 名を入力します。 追加 をクリックします。 カスタムレベル をクリックします。 セキュリティ設定 ウィンドウで 署名なしの ActiveX Controls のダウンロード で プロンプト を選択します。
コンソールリダイレクトセッションを開始したとき、ビューアの画面は空白です。	<p>仮想メディア 権限があるが、コンソールリダイレクト 権限がない場合は、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。</p>
起動中 iDRAC6 が応答していません。	<p>サーバーを取り外し、挿入し直してください。</p> <p>iDRAC6 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 iDRAC6 ファームウェアのアップデート」の手順に従ってください。</p> <p>問題が解決されない場合は、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> <ol style="list-style-type: none"> 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。 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。 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、iDRAC6 ウェブインタフェースまたは LCD で iDRAC6 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](#)