Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

メモと注意

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

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

2009 年 6 月

目次ページに戻る

用語集

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

Active Directory

Active Directory は、ユーザーデータ、セキュリティ、分散リソースのネットワーク管理を自動化する標準化された集中管理システムで、他のディレクトリとの相互運用を可能にします。Active Directory は、分散ネットワーク環境用に特別設計されています。

ARP

アドレス解決プロトコル（Address Resolution Protocol）の略語。インターネットアドレスからホストの Ethernet アドレスを見つける手段。

ASCII

情報交換用アメリカ標準コード（American Standard Code for Information Interchange）の略語。文字、数字、その他の記号の表示と印刷に使用されるコード表現体系。

BIOS

Basic Input/Output System の略語。周辺デバイスに最下位レベルのインタフェースを提供し、オペレーティングシステムのメモリへのロードなど、システム起動処理の第一段階を制御するシステムソフトウェアの一部。

CA

認証局（CA）は、IT 業界で認知されたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を提供しています。CA には、Thawte や VeriSign などがあります。CA は CSR を受け取ると、CSR に含まれる情報を調べて有効性を確認します。申請者が CA のセキュリティ標準を満たしていると、CA はネットワークやインターネット上のトランザクションに対して、その申請者を一意に識別する証明書を発行します。

CD

コンパクトディスク（Compact Disc）の略語。

CHAP

Challenge-Handshake Authentication Protocol の略語。PPP サーバーが使用している認証方式で、接続元の ID を確認します。

CIM

Common Information Model の略語。ネットワーク上でシステムを管理するためのプロトコル。

CLI

コマンドラインインタフェース（Command Line Interface）の略語。

CLP

コマンドラインプロトコル（Command Line Protocol）の略語。

CSR

認証署名要求（Certificate signing request）の略語。

DDNS

Domain Name System（ドメイン名システム）

DHCP

ダイナミックホスト設定プロトコル(Dynamic Host Configuration Protocol)の略語。このプロトコルは IP アドレスをローカルエリアネットワーク(LAN)のコンピュータに動的に割り当てる手段を提供します。

DLL

Dynamic Link Library(ダイナミックリンクライブラリ) の略語。小さいプログラムで構成されたライブラリ。システムで実行中の大きいプログラムが必要時に呼び出すことができます。この小さいプログラムは、大きいプログラムがプリンタやスキャナなどの特定のデバイスと通信できるように、DLL プログラム(または DLL ファイル)としてパッケージ化されている場合があります。

DMTF

分散管理タスクフォース (Distributed Management Task Force) の略語。

DNS

ドメイン名システム (Domain Name System) の略語。

DSU

ディスクストレージユニット(Disk Storage Unit)の略語。

FQDN

完全修飾ドメイン名 (Fully Qualified Domain Names) の略語。Microsoft® Active Directory® は、64 バイト以下の FQDN のみをサポートしています。

FSMO

Flexible Single Master Operation の略語。Microsoft が拡張動作の一律性を保証する方法。

GMT

Greenwich Mean Time(グリニッジ標準時)の略語。世界各地に共通する標準時刻。GMT は一般的にイギリスのロンドン郊外にあるグリニッジ天文台を通過する子午線(経度 0°)に基づく平均太陽時を反映するものです。

GPIO

汎用入力 / 出力(General Purpose Input/Output)の略語。

GRUB

GRand Unified Bootloader の略語。一般的に使用される新しい Linux ローダー。

GUI

グラフィカルユーザーインタフェース(Graphical User Interface)の略語。ユーザーとの対話がすべてテキストによって表示または入力されるコマンド表示メッセージインタフェースとは対照的に、ウィンドウ、ダイアログボックス、ボタンなどの要素を使用したコンピュータ表示インタフェースを指します。

iAMT

Intel® Active Management Technology(アクティブマネジメントテクノロジ)- コンピュータの電源がオンかオフか、またオペレーティングシステムが応答しているかどうかに関わらず、よりセキュアなシステム管理機能を実現します。

ICMB

Intelligent Enclosure Management Bus(インテリジェントエンクロージャ管理バス)の略語。

ICMP

Internet Control Message Protocol の略語。

ID

識別子(Identifier)の略語。一般に、ユーザー識別子(ユーザー ID)またはオブジェクト識別子(オブジェクト ID)を参照するときに使用されます。

iDRAC6

integrated Dell Remote Access Controller の略語。Dell 11G PowerEdge サーバー用の総合的なシステムオンチップ監視 / 制御システム。

IP

インターネットプロトコル(Internet Protocol)の略語。TCP/IP のネットワーク層。IP はパケットの経路選択、断片化、再構成などを行います。

IPMB

intelligent platform management bus の略語。システム管理テクノロジで使用されるバス。

IPMI

Intelligent Platform Management Interface の略語。システム管理テクノロジの一部。

Kbps

1 秒あたりのキロビット数(Kilobits per second)の略語で、データ転送速度を表します。

LAN

構内通信網またはローカルエリアネットワーク(Local Area Network)の略語。

LDAP

軽量ディレクトリアクセスプロトコル(Lightweight Directory Access Protocol)の略語。

LED

発光ダイオード(light-emitting diode)の略語。

LOM

マザーボードに組み込まれた LAN 接続(Local area network On Motherboard)の略語。

LUN

logical unit の略語(論理装置)。

MAC

媒体アクセス制御(Media Access Control)の略語。ネットワークノードとネットワーク物理層の間のネットワークサブレイヤ。

MAC アドレス

媒体アクセス制御アドレス(Media Access Control address)の略語。NIC の物理コンポーネントに組み込まれる固有アドレス。

MAP

Manageability Access Point の略語。

Mbps

1 秒あたりのメガビット数(Megabits per second)の略語で、データ転送速度を表します。

MIB

管理情報ベース(Management Information Base)の略語。

MII

Media Independent Interface の略語。

NAS

ネットワーク接続ストレージ(Network Attached Storage)の略語。

NIC

Network Interface Card (ネットワークインタフェースカード)の略語。アダプタ回路基板。コンピュータに取り付けて、ネットワークへの物理的な接続を提供します。

OID

Object Identifiers(オブジェクト識別子)の略語。

PCI

Peripheral Component Interconnect(周辺機器コンポーネント相互接続)の略語。周辺機器をシステムに接続し、それらの周辺機器と通信するための標準インタフェースおよびバス技術です。

POST

電源投入時自己診断(power-on self-test)の略語。コンピュータの電源を入れると、システムで自動的に一連の診断テストが実行されます。

PPP

Point-to-Point Protocol の略語。ポイントツーポイントのシリアルリンクを通して、ネットワークレイヤデータグラム(IP パケットなど)の転送に使用されるうインターネット標準プロトコル。

RAC

Remote Access Controller の略語。

RAM

ランダムアクセスメモリ(Random-Access Memory)の略語。RAM は、システムおよび iDRAC6 上の の読み書き可能な汎用メモリです。

RAM ディスク

ハードディスクをエミュレートするメモリ常駐プログラム。iDRAC6 はメモリに RAM ディスクを保持しています。

ROM

読み取り専用メモリ(Read-Only Memory)の略語。データの読み取りはできますが、書き込みはできません。

RPM

Red Hat® Package Manager の略語。Red Hat Enterprise Linux® オペレーションシステム用のパッケージ管理システムで、ソフトウェアパッケージのインストールに使用します。インストールプログラムに似ています。

SAC

Microsoft? Special Administration Console の略語。

SAP

サービスアクセスポイント(Service Access Point)の略語。

SEL

システムイベントログ(system event log)の略語。

SM-CLP

Server Management-Command Line Protocol の略語(サーバー管理コマンドラインプロトコル)。SM-CLP は、複数のプラットフォームにわたるサーバー管理を円滑にする DMTF SMASH イニシアチブのサブコンポーネントです。SM-CLP 仕様書は、Managed Element Addressing Specification (管理下エレメントアドレス指定仕様書)や SM-CLP マッピング仕様に対する多数のプロファイルと共に、さまざまなタスク実行用の標準化バーブとターゲットについて説明しています。

SMI

システム管理割り込み(Systems Management Interrupt)の略語。

SMTP

簡易メール転送プロトコル(Simple Mail Transfer Protocol)の略語。システム間の電子メールの転送に使用するプロトコル。SMTP は通常、イーザネット上で使用されます。

SMWG

Systems Management Working Group(システム管理ワークグループ)の略語。

SNMP トラップ

iDRAC6 で生成される通知(イベント)で、管理下システムの状況の変化や、ハードウェアの潜在的な問題に関する情報が含まれています。

SSH

セキュアシェル(Secure Shell)の略語。

SSL

セキュアソケットレイヤ(Secure Sockets Layer)の略語。

TAP

Telelocator Alphanumeric Protocol の略語。ページャサービスに要求を送信するために使用するプロトコル。

TCP/IP

Transmission Control Protocol/Internet Protocol の略語。ネットワーク層とトランスポート層のプロトコルを含む標準 Ethernet プロトコル一式を指します。

TFTP

簡易ファイル転送プロトコル(Trivial File Transfer Protocol)の略語。デバイスやシステムに起動コードをダウンロードするために使用される簡易ファイル転送プロトコル。

UPS

無停電電源装置 (Uninterruptible power supply) の略語。

USB

Universal Serial Bus の略語。

USC

Unified Server Configurator の略語。

UTC

協定世界時(Universal Coordinated Time)の略語。「GMT」を*参照してください*。

VLAN

仮想構内通信網(Virtual Local Area Network)の略語。

VNC

仮想ネットワークコンピューティング(Virtual Network Computing)の略語。

VT-100

ビデオ端末(Video Terminal)100 の略語。多くの共通端末エミュレーションプログラムによって使用されています。

WAN

広域通信網(Wide Area Network)の略語。

WS-MAN

Web Services for Management (管理用ウェブサービス)(WS-MAN) プロトコルの略語。WS-MAN は、情報交換用のトランスポートメカニズムです。管理がしやすいように、WS-MAN はデバイスがデータを共有するための汎用言語を提供します。

拡張スキーマ

Active Directory と併用されるソリューションで iDRAC6 へのユーザーアクセスを特定します。Dell 定義の Active Directory オブジェクトを使用します。

管理ステーション

管理ステーションは、iDRAC6 を搭載した Dell システムをシステム管理者がリモートで管理するシステムです。

管理下サーバー

管理下サーバーは、iDRAC が組み込まれているシステムです。

管理下システム

管理ステーションによって監視されるシステムは、「管理下システム」と呼ばれています。

コンソールリダイレクト

コンソールリダイレクトは、管理下サーバーの表示画面、マウス機能、およびキーボード機能を管理ステーションの該当するデバイスに転送する機能です。これを使用して管理ステーションのシステムコンソールから管理下システムを制御できます。

統一されるサーバー設定

Dell Unified Server Configurator(USC)は組み込まれている設定ユーティリティで、サーバーのライフサイクル中、システムとストレージの管理タスクを組み込み環境から実行できるようにします。

ハードウェアログ

iDRAC6 が生成したイベントを記録します。

バス

コンピュータ内の各種の機能単位を接続する伝導体のセット。てバスは、伝送するデータの種類によって、データバス、アドレスバス、PCI バスなどと名付けられます。

標準スキーマ

Active Directory と併用されるソリューションで iDRAC6 へのユーザーアクセスを決定します。Active Directory グループオブジェクトのみを使用します。

ロールバック

ソフトウェアまたはファームウェアの以前のバージョンに戻すこと。

目次ページに戻る

目次ページに戻る

RACADM サブコマンドの概要

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

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: RACADM は、事前に機能の検証をせずにオブジェクトの値を設定します。たとえば、Active Directory® が有効な場合にのみ証明書の検証を実行できる場合でも、Active Directory オブジェクトを 0 に設定した状態で、証明書の検証オブジェクトを 1 に設定できます。同様に、cfgADSSOEnable オブジェクトは、cfgADEnable オブジェクトが 0 の場合でも 0 または 1 に設定できますが、この操作は Active Directory が有効な場合にのみ効力を発揮します。

---

help

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-1 に、**help** コマンドについて説明します。

表 A-1 Help コマンド

コマンド	定義
help	**RACADM** で使用できるすべてのサブコマンドを表示し、それぞれに短い説明を付けます。

概要

```
racadm help

racadm help <サブコマンド>
```

説明

help サブコマンドは **racadm** コマンドで使用できるサブコマンドすべてをすべて列挙し、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、指定したコマンドだけの情報を表示します。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

arp

メモ: このコマンドを使用するには、**診断コマンドの実行** パーミッションが必要です。

表 A-2 に**arp** コマンドを示します。

表 A-2 arp コマンド

コマンド	定義
arp	ARP テーブルの内容を表示します。ARP テーブル エントリの追加や削除はできません。

概要

```
racadm arp
```

対応インタフェース

- リモート RACADM
- telnet/ssh/シリアル RACADM

---

clearasrscreen

メモ: このサブコマンドを使用するには、**ログのクリア** 権限が必要です。

表 A-3 に、**clearasrscreen** サブコマンドについて説明します。

表 A-3 clearasrscreen

サブコマンド	定義
clearasrscreen	メモリにある最後のクラッシュ画面をクリアします。

概要

```
racadm clearasrscreen
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

config

メモ: **getconfig** コマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-4 に、**config** および **getconfig** サブコマンドについて説明します。

表 A-4 config/getconfig

サブコマンド	定義
config	iDRAC6 を設定します。
getconfig	iDRAC6 設定データを取得します。

概要

```
racadm config [-c|-p] -f <ファイル名>

racadm config -g <グループ名> -o <オブジェクト名> [-i <インデックス>] <値>
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル 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々に設定するか、設定ファイルの一部として一括設定できます。データが異なる場合は、その iDRAC6 オブジェクトが新しい値で書き込まれます。

入力

表 A-5 に、**config** サブコマンド オプションについて説明します。

メモ: **-f** と **-p** オプションは、シリアル/telnet/ssh コンソールではサポートされていません。

表 A-5 config サブコマンドオプションと説明

オプション	説明
-f	-f <**ファイル名**> オプションを使用すると、**config** は <**ファイル名**> で指定したファイルの内容を読み取り、iDRAC6 を設定します。ファイルの内容は 「構文解析規則」で指定した形式のデータでなければなりません。
-p	パスワード オプションの **-p** は、**config** に config ファイル **-f** <ファイル名> に含まれているパスワード エントリを設定完了後に削除させます。
-g	**-g** <**グループ名**>（グループオプション）は、**-o** オプションと一緒に使用する必要があります。 <**グループ名**> は、設定するオブジェクトを含むグループを指定します。
-o	**-o** <**オブジェクト名**> <**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**>（インデックスオプション）はインデックス付きのグループのみに有効で、固有のグループを指定できます。 <index> は 1～16 の 10 進整数です。この場合、索引は「名前付き」の値ではなく、索引値で指定されます。
-c	**-c**（チェックオプション）は **config** サブコマンドと一緒に使用し、ユーザーが **.cfg** ファイルの構文を解析して構文エラーを検出できるようにします。エラーが検出された場合は、その行番号とエラーの短い説明が表示されます。iDRAC6 には書き込まれません。このオプションはチェックのみです。

出力

このサブコマンドは、次のいずれかの場合にエラー出力を生成します。

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

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100`

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

- `racadm config -f myrac.cfg`

  iDRAC6 を設定または再設定します。**myrac.cfg** ファイルは **getconfig** コマンドから作成できます。**myrac.cfg** ファイルは、構文解析ルールに従って手動で編集することもできます。

  メモ: **myrac.cfg** ファイルにはパスワード情報は含まれていません。この情報をファイルに含めるには、手動で入力する必要があります。設定時に **myrac.cfg** ファイルからパスワード情報を削除する場合は、**-p** オプションを使用します。

---

getconfig

getconfig サブコマンドの説明

getconfig サブコマンドを使うと、ユーザーは iDRAC6 設定パラメータを個別に取得するか、すべての iDRAC6 設定グループを取得してファイルに保存できます。

入力

表 A-6 に、**getconfig** サブコマンド オプションについて説明します。

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

表 A-6 getconfig サブコマンドオプション

オプション	説明
-f	**-f** <**ファイル名**> オプションを getconfig に追加すると、iDRAC6 設定のすべてが設定ファイルに書き込まれます。このファイルは**config** サブコマンドを使った一括設定用に使用できます。 **メモ:** **-f** オプションでは **cfgIpmiPet** と **cfgIpmiPef** グループ用のエントリは作成されません。 **cfgIpmiPet** グループをファイルに取り込むためのトラップ先を少なくとも 1 つ設定する必要があります。
-g	**-g** <**グループ名**>、または **group** オプションを使用すると、1 つのグループの設定を表示できます。groupName **groupName** は **racadm.cfg** ファイルで使用され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すべてを表示します。このオプションは、正確なグループ名を覚えていない場合に便利です。
-i	**-i** <**インデックス**>（**インデックス** オプション）は、インデックス付きのグループのみに有効で、固有のグループを指定できます。<インデックス> は 1 ～ 16 の 10 進数です。**-i <インデックス>** を指定しなければ、グループに 1 の値が想定されます。これは複数のエントリを含んだテーブルです。この場合、索引は「名前付き」の値ではなく、索引値で指定されます。
-o	オブジェクトオプションの -o <**オブジェクト名**> は、クエリで使用するオブジェクト名を指定します。このオプションは省略可能で、-g オプションと一緒に使用できます。
-u	ユーザー名オプションの **-u** <**ユーザー名**>（**ユーザー名** オプション）を使用すると、指定したユーザーの設定を表示できます。**<ユーザー名>** オプションはユーザーのログインユーザー名です。
-v	**-v** オプションは、プロパティの表示で追加の詳細情報を表示するために、**-g** オプションと一緒に使用します。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

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

エラーが発生しなければ、指定した設定の内容が表示されます。

例

- `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。

- `racadm getconfig -f myfile.cfg`

  iDRAC6 のグループ設定オブジェクトすべてを **myrac.cfg** に保存します。

- `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。

- `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。

- `racadm getconfig -g cfgUserAdmin -i 2 -v`

  インデックス 2 でのユーザーグループインスタンスを、プロパティ値の詳細情報と一緒に表示します。

概要

```
racadm getconfig -f <ファイル名>

racadm getconfig -g <グループ名> [-i <索引>]

racadm getconfig -u <ユーザー名>

racadm getconfig -h
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

coredump

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

表 A-7 に、**coredump** サブコマンドについて説明します。

表 A-7 coredump

サブコマンド	定義
coredump	前回の iDRAC6 コア ダンプを表示します。

概要

```
racadm coredump
```

説明

coredump サブコマンドは、RAC で最近発生した重要な問題に関する詳細情報を表示します。coredump 情報はこれらの重要な問題の診断に使用できます。

使用可能な場合、coredump 情報は iDRAC6 の電源を切った後も、以下の状態が発生するまで保持されます。

- **coredumpdelete** サブコマンドで coredump 情報がクリアされた。
- RAC で別の重大な問題が発生した。この場合、coredump の情報は、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** を参照してください。

対応インタフェース

- リモート RACADM
- telnet/ssh/シリアル RACADM

---

coredumpdelete

メモ: このコマンドを使用するには、**ログのクリア** または **デバッグコマンドの実行** 権限が必要です。

表 A-8 に、**coredumpdelete** サブコマンドについて説明します。

表 A-8 coredumpdelete

サブコマンド	定義
coredumpdelete	iDRAC6 に保存されているコアダンプを削除します。

概要

```
racadm coredumpdelete
```

説明

coredumpdelete サブコマンドは、現在 RAC に保存されている **coredump** データをクリアするために使用できます。

メモ: **coredumpdelete** コマンドを発行したときに coredump が現在 RAC に保存されていない場合は、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。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

fwupdate

メモ: このコマンドを使うには、**iDRAC6 の設定** 権限が必要です。

メモ: ファームウェアのアップデートを開始する前に、「iDRAC6 の詳細設定」で詳細を確認してください。

表 A-9 に、**fwupdate** サブコマンドを示します。

表 A-9 fwupdate

サブコマンド	定義
fwupdate	iDRAC6 上のファームウェアをアップデートします。

概要

```
racadm fwupdate -s

racadm fwupdate -g -u -a <TFTP _サーバー_IP_ アドレス> [-d <パス>]

racadm fwupdate -p -u -d <パス>

racadm fwupdate -r
```

説明

fwupdate サブコマンドを使用する t p 、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。

- 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
- IP アドレスと オプションのパスを指定して TFTP サーバーから iDRAC6 ファームウェアをアップデートする
- ローカル RACADM を使ってローカル ファイル システムから iDRAC6 ファームウェアをアップデートする
- 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

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

入力

表 A-10 に **fwupdate** サブコマンドのオプションについて説明します。

メモ: **-p** オプションはローカル RACADM でのみサポートされています。リモートまたは serial/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-10 fwupdate サブコマンドオプション

オプション	説明
-u	**update** オプションはファームウェアアップデートファイルのチェックサムを実行して、実際のアップデートプロセスを開始します。このオプションは **-g** または **-p** オプションと一緒に使用できます。アップデートの最後に iDRAC6 はソフトリセットを実行します。
-s	**status** オプションはアップデートプロセスの現在の状態を返します。このオプションは、常に単独で使用します。
-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 **cfgRhostsFwUpdateIpAddr** と **cfgRhostsFwUpdatePath** を使用して、グループ **cfgRemoteHosts** に含まれているプロパティを読み込みます。
-a	**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 サーバー上または iDRAC6 のホストサーバー上のディレクトリを指定します。
-p	**-p**（**put**）オプションは、ファームウェアファイルを管理下システムから iDRAC6 にアップデートするために使用します。**-u** オプションは **-p** オプションと一緒に使用する必要があります。
-r	**ロールバック** オプションを使用すると、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

- `racadm fwupdate -g -u - a 143.166.154.143 -d <パス>`

  この例では、**-g** オプションは、（**-d** で指定した）特定の IP アドレスにある TFTP サーバー上の（**-a** オプションで指定した）場所からファームウェアアップデートファイルをダウンロードするように指示します。TFTP サーバーからイメージファイルをダウンロードした後、アップデートプロセスが開始します。完了時に iDRAC6 がリセットされます。

- `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。

- `racadm fwupdate -p -u -d <パス>`

  この例では、アップデートのファームウェアイメージがホストのファイルシステムによって提供されます。

メモ: **-p** オプションは、`fwupdate` サブコマンドのリモート RACADM インタフェースではサポートされていません。ローカルパスを使用したリモート RACADM ファームウェアのアップデートは、Linux オペレーティングシステムではサポートされていません。

---

getssninfo

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-11 に、**getssninfo** サブコマンドについて説明します。

表 A-11 getssninfo サブコマンド

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

概要

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

説明

getssninfo コマンドは、iDRAC6 に接続しているユーザーのリストを返します。概要情報では次の情報が表示されます。

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

入力

表 A-12 に、**getssninfo** サブコマンドオプションについて説明します。

表 A-12 getssninfo サブコマンドオプション

オプション	説明
-A	**-A** オプションを指定すると、データヘッダは印刷されません。
-u	**-u <ユーザー名 >** ユーザー名オプションは、印刷出力を特定のユーザー名の詳細セッション記録だけに限定します。ユーザー名として「*」記号を入力した場合は、すべてのユーザーが表示されます。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

- `racadm getssninfo`

表 A-13 に **racadm getssninfo** コマンドの出力例を示します。

表 A-13 getssninfo サブコマンド出力例

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

- `racadm getssninfo -A`

  `"root" "143.166.174.19" "Telnet" "NONE"`

- `racadm getssninfo -A -u *`

  `"root" "143.166.174.19" "Telnet" "NONE"`

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

---

getsysinfo

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-14 に、**racadm getsysinfo** サブコマンドについて説明します。

表 A-14 getsysinfo

コマンド	定義
getsysinfo	iDRAC6 情報、システム情報、ウォッチドッグステータス情報を表示します。

概要

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

説明

getsysinfo サブコマンドは、RAC 管理下システムに関する情報と、ウォッチドッグの設定を表示します。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

入力

表 A-15 に、**getsysinfo** サブコマンドオプションについて説明します。

表 A-15 getsysinfo サブコマンドオプション

オプション	説明
-4	IPv4 設定を表示します。
-6	IPv6 設定を表示します。
-c	共通設定を表示します。
-d	iDRAC6 情報を表示します。
-s	システム情報を表示します。
-w	ウォッチドッグ情報を表示します。
-A	ヘッダ / ラベルを印刷しません。

-w オプションを指定しないと、その他のオプションがデフォルトとして使用されます。

出力

getsysinfo サブコマンドは、RAC 管理下システムに関する情報と、ウォッチドッグの設定を表示します。

出力例

```
RAC Information:
RAC Date/Time = 10/01/2008 09:39:53
Firmware Version = 0.32
Firmware Build = 55729
```

```
Last Firmware Update = 09/25/2008 18:08:31
Firmware Version = 0.01
MAC Address = 00:1e:c9:b2:c7:1f

Common settings:
Register DNS RAC Name = 0
DNS RAC Name = iDRAC6
Current DNS Domain =
Domain Name from DHCP = 0

IPv4 settings:
Enabled = 1
Current IP Address = 192.168.0.120
Current IP Address = 192.168.0.1
Current IP Address = 255.255.255.0
DHCP Enabled = 0
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0

IPv6 settings:
Enabled = 0
Current IP Address 1 = 2002:0000:0000::0001
Current IP Gateway = ::
Prefix Length = 64
Autoconfig              = 1
DNS Servers from DHCPv6 = 0
Current DNS Server 1    = ::
Current DNS Server 2    = ::

System Information:
System Model = PowerEdge R610
System BIOS Version = 0.2.4
BMC Firmware Version     = 0.32
Service Tag = AC056
Host Name =
OS Name =
Power Status = ON

Watchdog Information:
Recovery Action          = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

例

- racadm getsysinfo -A -s

  "System Information:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"

  "Microsoft Windows 2000 version 5.0, Build Number 2195, Service Pack 2" "ON"

- racadm getsysinfo -w -s

```
System Information:
System Model             = PowerEdge 2900
System BIOS Version      = 0.2.3
BMC Firmware Version     = 0.17
Service Tag              = 48192
Host Name                = racdev103
OS Name                  = Microsoft Windows Server 2003
Power Status            = OFF


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

制限

Dell™ OpenManage™ システムが管理下システムにインストールされている場合にのみ、**getsysinfo** の出力のホスト名と OS 名フィールドに正確な情報が表示されます。管理下システムに OpenManage がインストールされていないと、これらのフィールドには空白または不正確な値が表示されます。

---

getractime

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

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

表 A-16 getractime

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

概要

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

説明

オプションを指定しないと、**getractime** 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、**getractime** は時刻を yyyymmddhhmmss.mmmmmms 形式で表示します。これは UNIX **date** コマンドで返されるのと同じ形式です。

出力

getractime サブコマンドは出力を 1 行で表示します。

出力例

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

ifconfig

メモ: このコマンドを使用するには、**診断コマンドの実行** または **iDRAC の設定** 権限が必要です。

表 A-17 に、**ifconfig** サブコマンドについて説明します。

表 A-17 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
```

---

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-18 に、**netstat** サブコマンドについて説明します。

表 A-18 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

- リモート RACADM
- telnet/ssh/シリアル 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 **iDRAC の設定** 権限が必要です。

表 A-19 に、**ping** サブコマンドについて説明します。

表 A-19 ping

サブコマンド	定義
ping	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。宛先 IP アドレスが必要です。ICMP（インターネットコントロールメッセージプロトコル）エコーパケットが現在のルーティングテーブルの内容に基づいて宛先 IP アドレスに送信されます。

概要

```
racadm ping <IP アドレス>
```

対応インタフェース

- リモート RACADM
- telnet/ssh/シリアル RACADM

---

setniccfg

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

表 A-20 に、**setniccfg** サブコマンドについて説明します。

表 A-20 setniccfg

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

メモ: NIC と Ethernet 管理ポートは同じ意味で使われる場合があります。

概要

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <IPv4アドレス> <ネットマスク> <IPv4 ゲートウェイ>

racadm setniccfg -s6 <IPv6 アドレス> <IPv6 プレフィクス長> <IPv6 ゲートウェイ>

racadm setniccfg -o
```

説明

setniccfg サブコマンドは、コントローラの IP アドレスを設定します。

- **-d** オプションは Ethernet 管理ポートの DHCP を有効にします（デフォルトでは DHCP は無効です）。
- **-d6** オプションは Ethernet 管理ポートの AutoConfig を有効にします。これはデフォルトで有効になっています。
- **-s** オプションは静的 IP 設定を有効にします。IPv4 アドレス、ネットマスク、ゲートウェイを指定できます。指定しなければ、既存の静的な設定が使用されます。<IPv4 アドレス>、<ネットマスク> と <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。
- **-s6** オプションは静的 IPv6 設定を有効にします。IPv6 アドレス、プレフィクス長、および IPv6 ゲートウェイを指定できます。
- **-o** オプションは Ethernet 管理ポートを完全に無効にします。

出力

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

getniccfg

メモ: **getniccfg** コマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-21 に **setniccfg** と **getniccfg** サブコマンドについて説明します。

表 A-21 setniccfg/getniccfg

サブコマンド	定義
getniccfg	コントローラの現在の IP 設定を表示します。

概要

```
racadm getniccfg
```

説明

getniccfg サブコマンドは、現在の Ethernet 管理ポートの設定を表示します。

出力例

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

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

getsvctag

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-22 に **getsvctag** サブコマンドについて説明します。

表 A-22 getsvctag

サブコマンド	定義
getsvctag	サービスタグを表示します。

概要

```
racadm getsvctag
```

説明

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

例

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

```
Y76TP0G
```

成功すると 0、エラーの場合はゼロ以外の値を返します。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル 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-23 に **racdump** サブコマンドについて説明します。

表 A-23 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、iDRAC 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。

- システム / RAC の一般情報
- コアダンプ
- セッション情報
- プロセス情報
- ファームウェアビルド情報

対応インタフェース

- リモート RACADM
- telnet/ssh/シリアル RACADM

---

racreset

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-24 **racreset** サブコマンドについて説明します。

表 A-24 racreset

サブコマンド	定義
racreset	iDRAC6 をリセットします。

メモ: racreset サブコマンドを発行すると、iDRAC6 が使用可能な状態に戻るまでに最大 1 分かかることがあります。

概要

```
racadm racreset [ハード | ソフト]
```

説明

racreset サブコマンドは iDRAC6 にリセットを発行します。リセットイベントは iDRAC6 ログに書き込まれます。

ハードリセットは RAC の深いリセットを行います。ハードリセットは、RAC を回復するための最終手段としてのみ実行してください。

メモ: iDRAC6 のハードリセットを行った後は、「表 A-25」の説明に従ってシステムを再起動する必要があります。

表 A-25 に、**racreset** サブコマンドのオプションについて説明します。

表 A-25 racreset サブコマンドオプション

オプション	説明
ハード	ハード リセットはリモートアクセスコントローラ（RAC）のディープリセットを行います。ハードリセットは、回復目的で の最終手段として iRAC6 コントローラをリセットするためにのみ使用してください。
ソフト	ソフト リセットは RAC の正常な再起動を行います。

例

- `racadm racreset`

  iDRAC6 のソフトリセットのシーケンスを開始します。

- `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

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

racresetcfg

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-26 に、**racresetcfg** サブコマンドについて説明します。

表 A-26 racresetcfg

サブコマンド	定義
racresetcfg	iDRAC6 設定全体を工場出荷時のデフォルト値に戻します。

概要

```
racadm racresetcfg
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

説明

racresetcfg サブコマンドは、ユーザーが設定したデータベースプロパティのエントリをすべて削除します。データベースの各エントリには、コントローラを初期設定に戻す場合に使用するデフォルトのプロパティがあります。データベースプロパティのリセット後、iDRAC6 は自動的にリセットされます。

メモ: このコマンドは iDRAC6 の現在の設定を削除し、iDRAC6 とシリアル設定を最初のデフォルト設定に戻します。リセット後のデフォルト名とパスワードはそれぞれ **root** と **calvin** で、IP アドレスは 192.168.0.120 です。ネットワーククライアント（対応ウェブブラウザ、telnet/ssh、リモート RACADM など）から **racresetcfg** を発行する場合は、デフォルトの IP アドレスを使う必要があります。

メモ: デフォルトへのリセットが完了するには、一部の iDRAC6 ファームウェア プロセスを終了して再起動する必要があります。この動作が完了するまで約 30 秒間、iDRAC6 は応答しなくなります。

---

serveraction

メモ: このコマンドを使用するには、**サーバー制御コマンドの実行** パーミッションが必要です。

表 A-27 に、**serveraction** サブコマンドについて説明します。

表 A-27 serveraction

サブコマンド	定義
serveraction	管理下システムのリセットまたは電源オン / オフ / サイクルを実行します。

概要

```
racadm serveraction <処置>
```

説明

serveraction サブコマンドを使用すると、ホストシステムの電源を管理できます。 表 A-28 で、**serveraction** 電源管理オプションについて説明します。

表 A-28 serveraction サブコマンドオプション

文字列	定義
<処置**>**	処置を指定します。<処置> の文字列のオプションは以下のとおりです。 • **powerdown** - 管理下システムの電源を切ります。 • **powerup** - 管理下システムの電源を入れます。 • **powercycle** -管理下システムの電源を入れ直します。この動作は、システムの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。 • **powerstatus** - サーバーの現在の電源状態を表示します（「オン」または「オフ」）。 • **hardreset** - 管理下システムをリセット（再起動）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

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

getraclog

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-29 で、**racadm getraclog** コマンドについて説明します。

表 A-29 getraclog

コマンド	定義
getraclog -i	iDRAC6 ログのエントリ数を表示します。
getraclog	iDRAC6 ログエントリを表示します。

概要

```
racadm getraclog -i
```

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

説明

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

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

- **-A** - ヘッダ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指定します。
- **-m** - 1 度に 1 画面分の情報を表示し、ユーザーに続行するように指示します（UNIX の **more** コマンドと同様）。
- **-o** - 出力を 1 行に表示します。
- **-s** - 表示する開始レコードを指定します。

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。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは 1 月 1 日の午前 0 時に始まり、システムが起動するまで進められます。システムが起動した後は、システムのタイムスタンプが使用されます。

出力例

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

clrraclog

メモ: このサブコマンドを使用するには、**ログのクリア** 権限が必要です。

概要

```
racadm clrraclog
```

説明

clrraclog サブコマンドは、iDRAC6 のログから既存のレコードをすべて削除します。ログがクリアされると、新しいレコードが 1 つ作成されてその日時が記録されます。

---

getsel

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-30 に、**getsel** コマンドについて説明します。

表 A-30 getsel

コマンド	定義

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。

-A - ヘッダとラベルなしで表示します。

-c - 返されるエントリの最大数を指定します。

-o - 出力を 1 行に表示します。

-s - 表示する開始レコードを指定します。

-E - 各行の終りに生の SEL を 16 バイトほど 16 進値で出力します。

-R - 生のデータのみ出力します。

-m - 1 度に 1 画面分を表示し、ユーザーに続行するように指示します（UNIX の **more** コマンドと同様）。

メモ: 引数を指定しなければ、すべてのログが表示されます。

出力

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

例:

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

clrsel

メモ: このサブコマンドを使用するには、**ログのクリア** 権限が必要です。

概要

```
racadm clrsel
```

説明

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

gettracelog

メモ: このコマンドを使用するには、**iDRAC へのログイン** 権限が必要です。

表 A-31 に、**gettracelog** サブコマンドについて説明します。

表 A-31 gettracelog

コマンド	定義
gettracelog -i	iDRAC6 トレースログのエントリ数を表示します。
gettracelog	iDRAC6 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。

-i - iDRAC6 トレースログのエントリの数を表示します。

-m - 1 度に 1 画面分を表示し、ユーザーに続行するように指示します（UNIX の **more** コマンドと同様）。

-o - 出力を 1 行に表示します。

-c - 表示するレコード数を指定します。

-s - 表示を開始するレコードを指定します。

-A - ヘッダとラベルを表示しません。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは 1 月 1 日の午前 0 時に始まり、システムが起動するまで増えていきます。システムが起動した後は、システムのタイムスタンプが使用されます。

例:

```
Record:      1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

sslcsrgen

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-32 に、**sslcsrgen** サブコマンドについて説明します。

表 A-32 sslcsrgen

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

概要

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

racadm sslcsrgen -s
```

説明

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

オプション

メモ: **-f** オプションは、シリアル/telnet/ssh コンソールではサポートされていません。

表 A-33 に、**sslcsrgen** サブコマンドオプションについて説明します。

表 A-33 sslcsrgen サブコマンドオプション

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

メモ: **-f** オプションを指定しなければ、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は使用できず、**-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。

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

制限

sslcsrgen サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できず、シリアル、telnet、SSH インタフェースでは使用できません。

メモ: CSR を生成する前に、CSR フィールドを RACADM **cfgRacSecurity** RACADM グループで設定する必要があります。例：racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany

例

```
racadm sslcsrgen -s
```

または

```
racadm sslcsrgen -g -f c:¥csr¥csrtest.txt
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

sslcertupload

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-34 に、**sslcertupload** サブコマンドについて説明します。

表 A-34 sslcertupload

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

概要

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

オプション

表 A-35 に、**sslccertupload** サブコマンドオプションについて説明します。

表 A-35 sslcertupload サブコマンドオプション

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

sslcertupload コマンドはアップロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

sslcertupload サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できません。**sslcsrgen** サブコマンドはシリアル、telnet、SSH インタフェースでは使用できません。

例

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

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

sslcertdownload

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-36 に、**sslcertdownload** サブコマンドについて説明します。

表 A-36 sslcertdownload

サブコマンド	説明
sslcertupload	SSL 証明書を iDRAC6 からクライアントのファイルシステムにダウンロードします。

概要

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

オプション

表 A-37 に、**sslccertdownload** サブコマンドオプションについて説明します。

表 A-37 sslcertdownload サブコマンドオプション

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

sslcertdownload コマンドはダウンロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

sslcertdownload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。**sslcsrgen** サブコマンドは、シリアル、telnet、SSH インタフェースでは使用できません。

例

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

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

sslcertview

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-38 に、**sslcertview** サブコマンドについて説明します。

表 A-38 sslcertview

サブコマンド	説明
sslcertview	RAC 上に存在する SSL サーバーまたは CA 証明書を表示します。

概要

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

オプション

表 A-39 に、**sslccertview** サブコマンドオプションについて説明します。

表 A-39 sslcertview サブコマンドオプション

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

出力例

```
racadm sslcertview -t 1

Serial Number             : 00

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

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

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

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 のデフォルト証明書
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 のデフォルト証明書
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

sslkeyupload

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、**sslkeyupload** サブコマンドについて説明します。

表 A-40 sslkeyupload

サブコマンド	説明
sslkeyupload	SSL キーをクライアントから iDRAC6 にアップロードします。

概要

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

オプション

表 A-41 に、**sslkeyupload** サブコマンドのオプションについて説明します。

表 A-41 sslkeyupload サブコマンドオプション

オプション	説明
-t	アップロードするキーを指定します。 1 = サーバー証明書の生成に使用する SSL キー
-f	アップロードする SSL キーのファイル名を指定します。

sslkeyupload コマンドはアップロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

sslkeyupload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。シリアル、SSH インタフェースでは使用できません。

例

```
racadm sslkeyupload -t 1 -f c:¥sslkey.txt
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

testemail

表 A-42 に、**testemail** サブコマンドについて説明します。

表 A-42 testemail の設定

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

概要

```
racadm testemail -i <索引>
```

説明

iDRAC6 から指定の宛先へテスト電子メールを送信します。

テスト電子メールコマンドを実行する前に、RACADM **cfgEmailAlert** グループ内の指定したインデックスが有効で、正しく設定されていることを確認してください。 表 A-43 に、**cfgEmailAlert** グループのリストと関連するコマンドを示します。

表 A-43 testemail の設定

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

オプション

表 A-44 に、**testemail** サブコマンドオプションについて説明します。

表 A-44 testemail サブコマンド

オプション	説明
-i	テストする電子メール警告の索引を指定します。

出力

なし。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

testtrap

メモ: このコマンドを使用するには、**警告のテスト** 権限が必要です。

表 A-45 に、**testtrap** サブコマンドについて説明します。

表 A-45 testtrap

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

概要

```
racadm testtrap -i <索引>
```

説明

testtrap サブコマンドは、iDRAC6 から、ネットワーク上の指定した宛先トラップリスナーにテストトラップを送信して RAC の SNMP トラップ警告機能をテストします。

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

表 A-46 に、 **cfgIpmiPet**グループに関するコマンドを示します。

表 A-46 cfgEmailAlert コマンド

動作	コマンド
警告を有効にします。	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable 0 -i 1 1
宛先の電子メールの IP アドレスを設定します。	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
現在のテストトラップ設定を表示します。	racadm getconfig -g cfgIpmiPet -i <索引> <索引> は 1 ～ 4 の数値です。

入力

表 A-47 に、**testtrap** サブコマンドオプションについて説明します。

表 A-47 testtrap サブコマンドオプション

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

vmdisconnect

メモ: このサブコマンドを使用するには、**仮想メディアのアクセス** 権限が必要です。

表 A-48 に、**vmdisconnect** サブコマンドについて説明します。

表 A-48 vmdisconnect

サブコマンド	説明
vmdisconnect	開いている iDRAC6 仮想メディア接続すべてをリモートクライアントから閉じます。

概要

```
racadm vmdisconnect
```

説明

vmdisconnect サブコマンドを使用すると、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。切断すると、そのウェブベースのインタフェースに正しい接続状態が表示されます。これは、ローカルまたはリモートの RACADM からのみ使用可能です。

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 ウェブインタフェースか、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

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

vmkey

メモ: このサブコマンドを使用するには、**仮想メディアのアクセス** 権限が必要です。

表 A-49 に、**vmkey** サブコマンドについて説明します。

表 A-49 vmkey

サブコマンド	説明
vmkey	仮想メディアキー関連の操作を行います。

概要

```
racadm vmkey <処置>
```

<処置> を リセット に設定すると、仮想フラッシュメモリはデフォルトサイズの 256 MB にリセットされます。

説明

カスタム仮想メディアキーイメージを RAC にアップロードすると、キーサイズがイメージサイズになります。vmkey サブコマンドを使用すると、キーを元のデフォルトサイズ（iDRAC6 では 256 MB）に戻すことができます。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

usercertupload

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-50 に、 **usercertupload** サブコマンドについて説明します。

表 A-50 usercertupload

サブコマンド	説明
usercertupload	ユーザー証明書またはユーザー CA 証明書をクライアントから iDRAC6 にアップロードします。

概要

```
racadm usercertupload -t <種類> [-f <ファイル名>] -i <索引>
```

オプション

表 A-51 に、**usercertupload** サブコマンドオプションについて説明します。

表 A-51 usercertupload サブコマンドオプション

オプション	説明
-t	アップロードする証明書の種類が CA 証明書かサーバー証明書かを指定します。 1 = ユーザー証明書 2 = ユーザー CA 証明書
-f	アップロードする証明書のファイル名を指定します。ファイルを指定しないと、現在のディレクトリ内の **sslcert** ファイルが選択されます。
-i	ユーザーの索引番号。有効な値は 1 ～ 16 です。

usercertupload コマンドはアップロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

usercertupload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。

例

```
racadm usercertupload -t 1 -f c:¥cert¥cert.txt -i 6
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

usercertview

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-52 に、**usercertview** サブコマンドを示します。

表 A-52 usercertview

サブコマンド	説明
usercertview	iDRAC6 上にあるユーザー証明書またはユーザー CA 証明書を表示します。

概要

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

オプション

表 A-53 に、**sslccertview** サブコマンドオプションについて説明します。

表 A-53 sslcertview サブコマンドオプション

オプション	説明
-t	表示する証明書の種類が ユーザー証明書かユーザー CA 証明書かを指定します。 1 = ユーザー証明書

	2 = ユーザー CA 証明書
-A	ヘッダー / ラベルを印刷しません。
-i	ユーザーの索引番号。有効な値は 1 ～ 16 です。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/シリアル RACADM

---

localConRedirDisable

メモ: このコマンドを実行できるのは、ローカルの RACADM ユーザーのみです。

表 A-54 に、**localConRedirDisable** サブコマンドについて説明します。

表 A-54 localConRedirDisable

サブコマンド	説明
localConRedirDisable	管理ステーションへのコンソールリダイレクトを無効にします。

概要

racadm localConRedirDisable <オプション>

<オプション> を 1 に設定すると、コンソールリダイレクトが無効になります。

<オプション> を 0 に設定すると、コンソールリダイレクトが有効になります。

対応インタフェース

- ローカル RACADM

---

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-55 に、**krbkeytabupload** サブコマンドについて説明します。

表 A-55 kerbkeytabupload

サブコマンド	説明
krbkeytabupload	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-56 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-56 kerbkeytabupload サブコマンドオプション

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。

制限

krbkeytabupload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。

例

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

対応インタフェース

- ローカル RACADM
- リモート RACADM

目次ページに戻る

目次ページに戻る

iDRAC6 プロパティデータベースグループとオブジェクト定義

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

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 を使用して iDRAC6 を設定します。以下の各項で、それぞれのオブジェクトについて説明し、オブジェクトが読み取り可能か、書き込み可能か、またはその両方が可能であるかを示します。

△ **注意: RACADM は、オブジェクトの値を機能検証せずに設定します。たとえば、Active Directory® が有効な場合にのみ証明書の検証を実行できる場合でも、Active Directory オブジェクトを 0 に設定した状態で証明書の検証オブジェクトを 1 に設定できます。同様に、cfgADSSOEnable オブジェクトは、cfgADEnable オブジェクトが 0 の場合でも 0 または 1 に設定できますが、この操作は Active Directory が有効な場合にのみ使用できます。**

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

表示可能な文字

表示可能文字には以下の文字セットが含まれます。

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

このグループには、クエリされた 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

iDRAC（Integrated Dell Remote Access Controller）

説明

製品を識別するテキスト文字列。

idRacDescriptionInfo（読み取り専用）

有効値

最大 255 文字の ASCII 文字列。

デフォルト

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

説明

iDRAC のタイプを説明するテキスト。

idRacVersionInfo（読み取り専用）

有効値

最大 63 文字の ASCII 文字列。

デフォルト

<現在のバージョン番号>

説明

現在の製品ファームウェアバージョンを示す文字列。

idRacBuildInfo（読み取り専用）

有効値

最大 16 文字の ASCII 文字列。

デフォルト

現在の iDRAC6 ファームウェアビルドバージョン。

説明

現在の製品ビルドバージョンを示す文字列。

idRacName（読み取り専用）

有効値

最大 15 文字の ASCII 文字列。

デフォルト

iDRAC

説明

このコントローラを識別するためにユーザーが割り当てた名前。

idRacType（読み取り専用）

有効値

プロダクト ID

デフォルト

10

説明

リモート アクセス コントローラーのタイプを iDRAC6 と識別します。

---

cfgLanNetworking

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

グループでは 1 つのインスタンスが許可されています。このグループの一部のオブジェクトで iDRAC6 NIC のリセットが必要になる場合があり、そのために接続が一時中断す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によって、すべてのアクティブなユーザーセッションが終了するので、ユーザーはアップデート後の IP アドレス設定を使って再接続する必要があります。

cfgNicIPv4Enable (読み取り / 書き込み)

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC6 IPv4 スタックを有効または無効にします。

cfgNicSelection（読み取り / 書き込み）

有効値

0 = 共有

1 = フェールオーバー LOM2 で共有

2 = 専用

3= すべてのフェールオーバー LOM で共有（iDRAC6 Enterprise のみ）

デフォルト

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

説明

RAC ネットワークインタフェースコントローラ （NIC）の現在の動作モードを指定します。 表 B-1 にサポートされているモードを示します。

表 B-1 cfgNicSelection でサポートされているモード

モード	説明
共有	ホストサーバーの組み込み NIC がホストサーバー上で RAC と共有されている場合に使用します。このモードでは、ホストサーバーと RAC に共通のネットワークアクセスができるように、同じ IP アドレスを使用できます。
フェールオーバーで共有： LOM 2	ホストサーバー LOM2 組み込みネットワークインタフェースコントローラー間でのチーム機能を有効にします。
専用	RAC NIC をリモートアクセス機能専用 NIC として使用するように指定します。
すべてのフェールオーバー LOM で共有	ホストサーバー統合ネットワークインタフェースコントローラ上のすべての LOM 間でチーム機能を有効にします。 リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムに NIC チーム機能が設定されている場合に完全に機能します。リモートアクセスデバイスは NIC 1 と NIC 2 を通してデータを受信しますが、データの送信は NIC 1 を通してのみ行います。 フェールオーバーは、NIC 2 から NIC 3 へ、次に NIC 4 へと発生します。NIC 4 が故障した場合、リモート アクセス デバイスはすべてのデータ伝送を NIC 1 に戻します。ただし、これは最初の NIC 1 の障害が修復済みである場合のみです。

cfgNicVLanEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC/BMC の VLAN 機能を有効または無効にします。

cfgNicVLanId（読み取り / 書き込み）

有効値

1～4094

デフォルト

1

説明

ネットワーク VLAN 設定用に VLAN ID を指定します。このプロパティは、**cfgNicVLanEnable** が **1** (有効) に設定されている場合にのみ有効です。

cfgNicVLanPriority（読み取り / 書き込み）

有効値

0～7

デフォルト

0

説明

ネットワーク VLAN 設定用に VLAN の優先順位を指定します。このプロパティは、cfgNicVLanEnable が 1 (有効) に設定されている場合にのみ有効です。

cfgDNSDomainNameFromDHCP （読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 DNS ドメイン名をネットワークの DHCP サーバーから割り当てる必要があると指定します。

cfgDNSDomainName（読み取り / 書き込み）

有効値

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

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

デフォルト

<空白>

説明

これは DNS ドメイン名です。

cfgDNSRacName（読み取り / 書き込み）

有効値

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

メモ: 一部の DNS サーバーは 31 文字以内の名前しか登録しません。

デフォルト

idrac-<サービスタグ>

説明

デフォルトの iDRAC6 名 rac-サービスタグ が表示されます。このパラメータは、**cfgDNSRegisterRac** が 1（TRUE） に設定されているときにのみ有効です。

cfgDNSRegisterRac（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバーに iDRAC6 の名前を登録します。

cfgTrapsSnmpFromDHCP（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバーの IPv4 アドレスをネットワーク上の DHCP サーバーから割り当てるかどうかを指定します。

cfgDNSServer1（読み取り / 書き込み）

有効値

有効な IPv4 アドレスを表す文字列。例：192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 1 の IPv4 アドレスを指定します。

cfgDNSServer2（読み取り / 書き込み）

有効値

有効な IPv4 アドレスを表す文字列。例：192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 2 の IPv4 アドレスを取得します。

cfgNicEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC6 ネットワークインタフェースコントローラを有効または無効にします。NIC を無効にした場合、iDRAC6 へのリモートネットワークインタフェースはアクセスできません。

cfgNicIpAddress（読み取り / 書き込み）

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

有効値

有効な IPv4 アドレスを表す文字列。例：192.168.0.20

デフォルト

192.168.0.120

説明

iDRAC6 に割り当てた IPv4 アドレスを指定します。

cfgNicNetmask（読み取り / 書き込み）

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

有効値

有効なサブネットマスクを表す文字列。例：255.255.255.0

デフォルト

255.255.255.0

説明

iDRAC6 IP アドレスに使用するサブネットマスク

cfgNicGateway（読み取り / 書き込み）

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

有効値

有効な ゲートウェイ IPv4 アドレスを表す文字列。例：192.168.0.1

デフォルト

192.168.0.1

説明

iDRAC6 ゲートウェイ IPv4 アドレス

cfgNicUseDhcp（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC の IPv4 アドレスの割り当てに DHCP を使用するかどうかを指定します。このプロパティを 1（TRUE）に設定すると、iDRAC の IPv4 アドレス、サブネットマスク、ゲートウェイがネットワーク上の DHCP サーバーから割り当てられます。このプロパティを **0**（FALSE）に設定すると、ユーザーは **cfgNicIpAddress**、**cfgNicNetmask**、および **cfgNicGateway** プロパティを設定できます。

cfgNicMacAddress（読み取り専用）

有効値

iDRAC6 NIC MAC アドレスを表す文字列。

デフォルト

iDRAC6 NIC の現在の MAC アドレス。例：00:12:67:52:51:A3

説明

iDRAC6 NIC の MAC アドレス。

---

cfgRemoteHosts

このグループは、電子メール警告用の SMTP サーバーの設定を可能にするプロパティを提供します。

cfgRhostsFwUpdateTftpEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

ネットワーク TFTP サーバーからの iDRAC6 ファームウェアのアップデートを有効または無効にします。

cfgRhostsFwUpdateIpAddr（読み取り / 書き込み）

有効値

有効な IPv4 アドレスを表す文字列。例：192.168.0.61

デフォルト

0.0.0.0

説明

TFTP iDRAC6 ファームウェアのアップデートに使うネットワーク TFTP サーバー IPv4 アドレスを指定します。

cfgRhostsFwUpdatePath（読み取り / 書き込み）

有効値

最大 255 文字の ASCII 文字列。

デフォルト

<空白>

説明

TFTP サーバー上の iDRAC6 ファームウェアイメージファイルの TFTP パスを指定します。TFTP パスは、TFTP サーバー上の TFTP ルートパスの相対パスです。

メモ: サーバーのドライブを指定しなければならない場合もあります（例：**C:**）。

cfgRhostsSmtpServerIpAddr（読み取り / 書き込み）

有効値

有効なSMTP サーバー IPv4 アドレスを表す文字列。例：192.168.0.55

デフォルト

0.0.0.0

説明

ネットワーク SMTP サーバーまたは TFTP サーバーの IPv4 アドレス。SMTP サーバーは、警告が設定されて有効になっていれば、iDRAC6 から電子メール警告を送信します。TFTP サーバーは iDRAC6 との間でファイルを送受信します。

---

cfgUserAdmin

このグループは、使用可能なリモートインタフェースから iDRAC6 へのアクセスが許可されているユーザーについての設定情報を提供します。

最大 16 のユーザーグループのインスタンスを使用できます。各インスタンスは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

1 ～ 16

デフォルト

<インスタンス>

説明

この数値はユーザーインスタンスを表します。

cfgUserAdminIpmiLanPrivilege（読み取り / 書き込み）

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

15（アクセスなし）

デフォルト

4（ユーザー 2）

15（その他すべて）

説明

IPMI LAN チャネルでの最大権限。

cfgUserAdminPrivilege（読み取り / 書き込み）

有効値

0x00000000 ～ 0x000001ff、および 0x0

デフォルト

0x00000000

説明

このプロパティは、ユーザーのロール（役割）ベースの権限を指定します。値は、権限の値を自由に組み合わせることのできるビットマスクとして表します。 表 B-2 に、組み合わせてビットマスクを作成できるユーザー権限ビット値について説明します。

表 B-2 ユーザー権限に応じたビットマスク

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

例

表 B-3に、1 つまたは複数の権限を持つユーザーの権限ビットマスクの例を示します。

表 B-3 ユーザー権限ビットマスクの例

ユーザー権限	権限ビットマスク
ユーザーは iDRAC にアクセスできません。	0x00000000
ユーザーは iDRAC へのログインと iDRAC とサーバーの設定情報の表示のみができます。	0x00000001
ユーザーは iDRAC へのログインと設定の変更ができます。	0x00000001 + 0x00000002 = 0x00000003

ユーザーは iDRAC へのログイン、仮想メディアへのアクセス、コンソールリダイレクトへのアクセスができます。	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName（読み取り / 書き込み）

メモ: このプロパティ値は、ユーザー名で固有の値でなくてはなりません。

有効値

最大 16 文字の ASCII 文字列。

デフォルト

root（ユーザー 2）

<空白>（他のすべてのユーザー）

説明

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

メモ: このプロパティ値は、ユーザー名で固有の値でなくてはなりません。

cfgUserAdminPassword（書き込み専用）

有効値

最大 20 文字の ASCII 文字列。

デフォルト

****

説明

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

cfgUserAdminEnable （読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1（ユーザー 2）

0（他のすべてのユーザー）

説明

ユーザーを個別に有効または無効にします。

cfgUserAdminSolEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

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

cfgUserAdminIpmiSerialPrivilege（読み取り / 書き込み）

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

15（アクセスなし）

デフォルト

4 (ユーザー 2)

15 (その他すべて)

説明

IPMI LAN チャネル上での最大権限。

---

cfgEmailAlert

このグループには、iDRAC6 電子メール警告機能を設定するためのパラメータが含まれています。

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。このグループは 4 つのインスタンスまで使用できます。

cfgEmailAlertIndex（読み取り専用）

有効値

1～4

デフォルト

<インスタンス>

説明

警告インスタンスの固有の索引。

cfgEmailAlertEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

警告インスタンスを有効または無効にします。

cfgEmailAlertAddress（読み取り/書き込み）

有効値

電子メールアドレス形式、最大 64 文字の ASCII 文字列。

デフォルト

<空白>

説明

電子メール用送信先電子メールアドレスを指定します。例：user1@company.com

cfgEmailAlertCustomMsg（読み取り/書き込み）

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

警告の件名を示すカスタムメッセージを指定します。

---

cfgSessionManagement

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

このグループでは 1 つのインスタンスが許可されています。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。

cfgSsnMgtRacadmTimeout（読み取り / 書き込み）

有効値

10～1920

デフォルト

60

説明

リモート RACADM インタフェースのアイドルタイムアウト（秒）を定義します。リモート RACADM セッションで指定した秒数以上、操作がない状態が続いた場合に、そのセッションは終了します。

cfgSsnMgtConsRedirMaxSessions（読み取り / 書き込み）

有効値

1～4

デフォルト

2

説明

iDRAC6 で許可されるコンソールリダイレクト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）。

cfgSsnMgtSshIdleTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60～1920

デフォルト

300

説明

セキュアシェルのアイドルタイムアウトを定義します。このプロパティでは、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）。

期限の切れたセキュアシェルセッションは、次のエラーメッセージを表示します。

Connection timed out（接続タイムアウト）

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

cfgSsnMgtTelnetTimeout（読み取り / 書き込み）

有効値

0（タイムアウトなし）

60～1920

デフォルト

300

説明

telnet アイドルタイムアウトを定義します。このプロパティでは、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）。

期限の切れたセキュアシェルセッションは、次のエラーメッセージを表示します。

Connection timed out（接続タイムアウト）

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

---

cfgSerial

このグループには、iDRAC6 サービスの設定パラメータが含まれます。

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

cfgSerialBaudRate（読み取り / 書き込み）

有効値

9600、28800、57600、115200

デフォルト

57600

説明

iDRAC6 シリアルポートのボーレートを設定します。

cfgSerialConsoleEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

B

説明

RAC シリアルコンソールインタフェースを有効または無効にします。

cfgSerialConsoleQuitKey（読み取り / 書き込み）

有効値

最大 4 文字の文字列。

デフォルト

^¥ (<Ctrl><¥>)

メモ: 「^」は <Ctrl> キーを示します。

説明

connect com2 コマンドを使用しているとき、このキーまたはキーの組み合わせによってテキストコンソールのリダイレクトを終了できます。**cfgSerialConsoleQuitKey** の値は、次のいずれかで表すことができます。

- 10 進数 - 例：95
- 16 進数 - 例：0x12
- 8 進数 - 例：007
- ASCII 値 - 例：^a

  ASCII 値は、次のエスケープキーコードを使って表すことができます。

  (a) ^ と任意の英字 (a-z, A-Z)

  (b) ^ と特殊文字 [ ] ¥ ^ _

cfgSerialConsoleIdleTimeout（読み取り / 書き込み）

有効値

0 = タイムアウトなし

60～1920

デフォルト

300

説明

アイドル状態が続いたときに、セッションが切断されるまでの最大待ち時間を秒で指定します。

cfgSerialConsoleNoAuth（読み取り / 書き込み）

有効値

0（シリアルログイン認証を有効にする）

1（シリアルログイン認証を無効にする）

デフォルト

0

説明

RAC シリアルコンソールログイン認証を有効または無効にします。

cfgSerialConsoleCommand（読み取り / 書き込み）

有効値

最大 128 文字の文字列。

デフォルト

<空白>

説明

ユーザーがシリアルコンソールインタフェースにログインした後で実行するシリアルコマンドを指定します。

cfgSerialHistorySize（読み取り / 書き込み）

有効値

0～8192

デフォルト

8192

説明

シリアル履歴バッファの最大サイズを指定します。

cfgSerialCom2RedirEnable（読み取り / 書き込み）

デフォルト

1

有効値

1 (TRUE)

0 (FALSE)

説明

COM 2 ポートリダイレクト用のコンソールを有効または無効にします。

cfgSerialSshEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC6 の セキュアシェル（SSH）インタフェースを有効または無効にします。

cfgSerialTelnetEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の Telnet コンソールインタフェースを有効または無効にします。

---

cfgOobSnmp

このグループには、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。

このグループでは 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。

cfgOobSnmpAgentCommunity（読み取り / 書き込み）

有効値

最大 31 文字の文字列。

デフォルト

public

説明

SNMP トラップに使用する SNMP コミュニティ名を指定します。

cfgOobSnmpAgentEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の SNMP エージェントを有効または無効にします。

---

cfgRacTuning

このグループは、有効なポートやセキュリティポート制限など、iDRAC6 の各種設定プロパティの設定に使用します。

cfgRacTuneConRedirPort（読み取り / 書き込み）

有効値

1～65535

デフォルト

5900

説明

RAC へのキーボード、マウス、ビデオ、および仮想メディアのトラフィックに使用するポートを指定します。

cfgRacTuneRemoteRacadmEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC のリモート RACADM インタフェースを有効または無効にします。

cfgRacTuneCtrlEConfigDisable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

ローカルユーザーが BIOS POST オプション ROM から iDRAC を設定できる機能を無効にする機能を有効または無効にします。

cfgRacTuneHttpPort（読み取り / 書き込み）

有効値

1～65535

デフォルト

80

説明

iDRAC6 との HTTP ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneHttpsPort（読み取り / 書き込み）

有効値

1～65535

デフォルト

443

説明

iDRAC6 との HTTPS ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneIpRangeEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の IPv4 アドレス範囲の検証機能を有効または無効にします。

cfgRacTuneIpRangeAddr（読み取り / 書き込み）

有効値

IPv4 アドレスフォーマット済み文字列、例：192.168.0.44

デフォルト

192.168.1.1

説明

範囲マスクプロパティ（**cfgRacTuneIpRangeMask**）で 1 で決定される IPv4 アドレスビットパターンの可能な位置を指定します。

cfgRacTuneIpRangeMask（読み取り / 書き込み）

有効値

IPv4 アドレスフォーマット済み文字列、例：255.255.255.0

デフォルト

255.255.255.0

説明

左寄せビットを使用した標準的な IP マスク値 例：255.255.255.0

cfgRacTuneIpBlkEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の IPv4 アドレスブロック機能を有効または無効にします。

cfgRacTuneIpBlkFailCount（読み取り / 書き込み）

有効値

2 ～16

デフォルト

5

説明

ウィンドウ（**cfgRacTuneIpBlkFailWindow**）内で何回ログインに失敗すると、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（読み取り / 書き込み）

有効値

10 ～ 65535

デフォルト

60

説明

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

cfgRacTuneIpBlkPenaltyTime（読み取り / 書き込み）

有効値

10 ～ 65535

デフォルト

300

説明

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

cfgRacTuneSshPort（読み取り / 書き込み）

有効値

1 ～ 65535

デフォルト

22

説明

iDRAC の SSH インタフェースに使用するポート番号を指定します。

cfgRacTuneTelnetPort（読み取り / 書き込み）

有効値

1 ～ 65535

デフォルト

23

説明

iDRAC6 の telnet インタフェースに使用するポート番号を指定します。

cfgRacTuneConRedirEnable（読み取り/書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

コンソールリダイレクトを有効にします。

cfgRacTuneConRedirEncryptEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

コンソールリダイレクトのセッションでビデオを暗号化します。

cfgRacTuneAsrEnable（読み取り / 書き込み）

メモ: このオブジェクトは、アクティブになる前に iDRAC6 をリセットする必要があります。

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の前回クラッシュ画面キャプチャ機能を有効または無効にします。

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)

cfgRacTuneLocalServerVideo（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

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

cfgRacTuneLocalConfigDisable（読み取り/書き込み）

有効値

0 (TRUE)

1 (FALSE)

デフォルト

0

説明

1 に設定すると、iDRAC6 設定データへの書き込み権限が無効になります。

cfgRacTuneWebserverEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

iDRAC6 ウェブサーバーを有効または無効にします。このプロパティを無効にすると、クライアントのウェブブラウザを使用して iDRAC6 にアクセスできなくなります。このプロパティは Telnet/SSH またはローカル RACADM インタフェースには影響しません。

---

ifcRacManagedNodeOs

このグループには、管理下サーバーのオペレーティングシステムを記述するプロパティが含まれます。

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。

ifcRacMnOsHostname (読み取り専用)

有効値

最大 255 文字の文字列。

デフォルト

<空白>

説明

管理下サーバーのホスト名。

ifcRacMnOsOsName (読み取り専用)

有効値

最大 255 文字の文字列。

デフォルト

<空白>

説明

管理下サーバーのオペレーティングシステム名。

---

cfgRacSecurity

このグループは、iDRAC6 SSL 証明書署名要求（CSR）機能に関連するオプションを設定するために使用します。このグループのプロパティは、iDRAC6 から CSR を生成する前に設定する必要があります。

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

cfgRacSecCsrCommonName（読み取り / 書き込み）

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 共通名（CN）を指定します。これは、証明書に記載された IP または iDRAC 名でなければなりません。

cfgRacSecCsrOrganizationName（読み取り / 書き込み）

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 組織名（O）を指定します。

cfgRacSecCsrOrganizationUnit（読み取り / 書き込み）

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 部門名（OU）を指定します。

cfgRacSecCsrLocalityName（読み取り / 書き込み）

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 地域（L）を指定します。

cfgRacSecCsrStateName（読み取り / 書き込み）

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR 都道府県名（S）を指定します。

cfgRacSecCsrCountryCode（読み取り / 書き込み）

有効値

最大 2 文字の文字列。

デフォルト

<空白>

説明

CSR 国番号（CC）を指定します。

cfgRacSecCsrEmailAddr（読み取り / 書き込み）

有効値

最大 254 文字の文字列。

デフォルト

<空白>

説明

CSR の電子メールアドレスを指定します。

cfgRacSecCsrKeySize（読み取り / 書き込み）

有効値

1024

2048

4096

デフォルト

1024

説明

CSR の非対称キーサイズを指定します。

---

cfgRacVirtual

このグループには iDRAC6 仮想メディア機能を設定するためのパラメータが含まれています。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。

cfgVirMediaAttached（読み取り / 書き込み）

有効値

0 = 分離

1 = 連結

2 = 自動連結

デフォルト

0

説明

このオブジェクトは、USB バスを介して仮想デバイスをシステムに接続するために使用されます。デバイスを接続すると、サーバーは、システムに接続している有効な USB 大容量記憶装置を認識します。これは、ローカル USB CD-ROM/ フロッピードライブをシステムの USB ポートに接続する場合と同じです。デバイスが接続されると、iDRAC6 の ウェブインタフェースまたは CLI を使用してこれらの仮想デバイスにリモート接続できるようになります。このオブジェクトを **0** に設定すると、デバイスは USB バスから切断されます。

cfgVirtualBootOnce（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 の仮想メディアのブートワンス機能を有効または無効にします。

cfgVirMediaFloppyEmulation（読み取り/書き込み）

メモ: この変更を有効にするには、（**cfgVirMediaAttached** を使用して）仮想メディアを再連結する必要があります。

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

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

cfgVirMediaKeyEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の仮想メディアキー機能を有効または無効にします。

---

cfgActiveDirectory

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

cfgADRacDomain（読み取り / 書き込み）

有効値

空白スペースなしの最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

iDRAC6 が置かれている Active Directory ドメイン。

cfgADRacName（読み取り / 書き込み）

有効値

空白スペースなしの最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

Active Directory フォレストに記録された iDRAC6 名。

cfgADEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

B

説明

iDRAC6 で Active Directory によるユーザー認証を有効または無効にします。このプロパティを無効にすると、ユーザーログインにローカルの iDRAC6 認証のみが使用されます。

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。

cfgADSmartCardLogonEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 でスマートカードによるログオンを有効または無効にします。

cfgADCRLEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

Active Directory ベースのスマートカードユーザー用の証明書失効リスト（CRL）を有効または無効にします。

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）を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDRAC6 は、指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADDomainController2（読み取り / 書き込み）

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDRAC6 は、指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADDomainController3（読み取り / 書き込み）

有効値

有効な IP アドレスまたは完全修飾ドメイン名（FQDN）を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDRAC6 は、指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADAuthTimeout（読み取り / 書き込み）

有効値

15 ～ 300 秒

デフォルト

120

説明

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

cfgADType（読み取り / 書き込み）

有効値

1（拡張スキーマ）

2（標準スキーマ）

デフォルト

1

説明

Active Directory と併用するスキーマタイプを指定します。

cfgADGlobalCatalog1（読み取り / 書き込み）

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDDRAC6 は、指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADGlobalCatalog2（読み取り / 書き込み）

有効値

有効な IP アドレスまたは完全修飾ドメイン名 (FQDN) を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDDRAC6 は、指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADGlobalCatalog3（読み取り / 書き込み）

有効値

有効な IP アドレスまたは完全修飾ドメイン名（FQDN）を表す最大 254 文字の ASCII 文字列。

デフォルト

<空白>

説明

iDDRAC6 は、指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADCertValidationEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

Active Directory 設定プロセスの一部として Active Directory 証明書検証を有効または無効にします。

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex（読み取り専用）

有効値

1 ～ 5 の整数。

デフォルト

<インスタンス>

説明

Active Directory で記録したロール（役割）グループの索引。

cfgSSADRoleGroupName（読み取り / 書き込み）

有効値

最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

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

cfgSSADRoleGroupDomain（読み取り / 書き込み）

有効値

空白スペースなしの最大 254 文字の印刷可能テキスト文字列。

デフォルト

<空白>

説明

ロール（役割）グループが常駐する Active Directory ドメイン。

cfgSSADRoleGroupPrivilege（読み取り / 書き込み）

有効値

0x00000000～0x000001ff

デフォルト

<空白>

説明

表 B-4 のビットマスク番号を使用して、ロール（役割）グループのロール（役割）ベースの権限を設定します。

表 B-4 ロール（役割）グループの権限のビットマスク

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

---

cfgIpmiSol

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

cfgIpmiSolEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

SOL を有効または無効にします。

cfgIpmiSolBaudRate（読み取り / 書き込み）

有効値

9600、19200、57600、115200

デフォルト

115200

説明

シリアルオーバー LAN 通信のボーレート。

cfgIpmiSolMinPrivilege（読み取り / 書き込み）

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

デフォルト

4

説明

SOL アクセスに必要な最小権限レベルを指定します。

cfgIpmiSolAccumulateInterval（読み取り / 書き込み）

有効値

1～255

デフォルト

10

説明

SOL 文字データパケットの一部を送信する前に通常 iDRAC6 が待機する時間を指定します。この値は 1 を基準に 5 ms 間隔で増分されます。

cfgIpmiSolSendThreshold（読み取り / 書き込み）

有効値

1 ～ 255

デフォルト

255

説明

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

---

cfgIpmiLan

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

cfgIpmiLanEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

IPMI オーバー LAN インタフェースを有効または無効にします。

cfgIpmiLanPrivilegeLimit（読み取り/書き込み）

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

デフォルト

4

説明

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

cfgIpmiLanAlertEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

グローバル電子メール警告を有効または無効にします。このプロパティは、個々の電子メール警告の有効 / 無効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 進数文字列。偶数の桁数のみが許可されます。

デフォルト

00000000000000000000

説明

IPMI 暗号化キー。

cfgIpmiPetCommunityName（読み取り / 書き込み）

有効値

最大 18 文字の文字列。

デフォルト

public

説明

トラップの SNMP コミュニティ名。

---

cfgIpmiPetIpv6

このグループは、管理下サーバーの IPv6 プラットフォームイベントトラップの設定に使用します。

cfgIpmiPetIPv6Index（読み取り専用）

有効値

1 ～ 4

デフォルト

<索引値>

説明

トラップに対応する索引の固有の識別子。

cfgIpmiPetIPv6AlertDestIpAddr

有効値

IPv6 アドレス

デフォルト

<空白>

説明

トラップの IPv6 警告送信先 IP アドレスを設定します。

cfgIpmiPetIPv6AlertEnable（読み取り/書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

トラップの IPv6 警告送信先を有効または無効にします。

---

cfgIpmiPef

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

イベントフィルタは、管理下サーバーで重大なイベントが発生したときにトリガされる処置に関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

索引フィルタの名前。

説明

プラットフォームイベントフィルタの名前を指定します。

cfgIpmiPefIndex（読み取り/書き込み）

有効値

1 ～ 19

デフォルト

プラットフォームイベントフィルタオブジェクトの索引値。

説明

特定のプラットフォームイベントフィルタの索引を指定します。

cfgIpmiPefAction（読み取り / 書き込み）

有効値

0（なし）

1（電源を切る）

2（リセット）

3（電源を入れ直す）

デフォルト

0

説明

警告がトリガされたときに管理下サーバーで実行される処置を指定します。

cfgIpmiPefEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

特定のプラットフォームイベントフィルタを有効または無効にします。

---

cfgIpmiPet

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

cfgIpmiPetIndex（読み取り専用）

有効値

1 ～ 4

デフォルト

特定のプラットフォームイベントトラップの索引値。

説明

トラップに対応する索引の固有の識別子。

cfgIpmiPetAlertDestIpAddr（読み取り / 書き込み）

有効値

有効な IPv4 アドレスを表す文字列。例：192.168.0.67

デフォルト

0.0.0.0

説明

ネットワーク上でのトラップレシーバの送信先 IPv4 アドレスを指定します。トラップレシーバは、管理下サーバーでイベントがトリガされたときに SNMP トラップを受信します。

cfgIpmiPetAlertEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

特定のトラップを有効または無効にします。

---

cfgUserDomain

このグループは、Active Directory のユーザードメイン名を設定するために使用されます。任意の時点で最大 40 個のドメイン名を指定できます。

cfgUserDomainIndex（読み取り専用）

有効値

1 ～ 40

デフォルト

索引値

説明

特定のドメインを表します。

cfgUserDomainName（読み取り専用）

有効値

最大 255 文字の ASCII 文字列。

デフォルト

<空白>

説明

Active Directory ユーザードメイン名を指定します。

---

cfgServerPower

このグループは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 (ON)

0 (OFF)

デフォルト

<現在のサーバー電源状態>

説明

サーバー電源状態を ON または OFF で表します。

cfgServerPowerAllocation（読み取り専用）

メモ: 複数の電源がある場合、このプロパティは最小容量の電源を表します。

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

サーバー要に割り当てられている電源を表します。

cfgServerActualPowerConsumption（読み取り専用）

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

現時点でサーバーが消費している電力を表します。

cfgServerMinPowerCapacity（読み取り専用）

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

サーバーの最小電力容量を表します。

cfgServerMaxPowerCapacity（読み取り専用）

有効値

最大 32 文字の文字列。

デフォルト

<空白>

説明

サーバーの最小電力容量を表します。

cfgServerPeakPowerConsumption（読み取り専用）

有効値

最大 32 文字の文字列。

デフォルト

<現在のサーバーのピーク電力消費>

説明

現在までにサーバーが消費した最大電力を表します。

cfgServerPeakPowerConsumptionTimestamp（読み取り専用）

有効値

最大 32 文字の文字列。

デフォルト

最大電力消費タイムスタンプ

説明

最大電力消費量が記録された時刻。

cfgServerPowerConsumptionClear（書き込み専用）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

****

説明

cfgServerPeakPowerConsumption（読み取り / 書き込み）プロパティを 0 に、 **cfgServerPeakPowerConsumptionTimestamp** プロパティを現在の iDRAC 時刻にリセットします。

cfgServerPowerCapWatts（読み取り / 書き込み）

有効値

最大 32 文字の文字列。

デフォルト

サーバー電源しきい値のワット数。

説明

サーバー電源しきい値のワット数を表します。

cfgServerPowerCapBtuhr（読み取り / 書き込み）

有効値

最大 32 文字の文字列。

デフォルト

サーバー電源しきい値（BTU/時）。

説明

サーバー電源しきい値（BTU/時）を表します。

cfgServerPowerCapPercent（読み取り / 書き込み）

有効値

最大 32 文字の文字列。

デフォルト

サーバー電源しきい値のワット数。

説明

サーバー電源しきい値のワット数を表します。

---

cfgIPv6LanNetworking

このグループは、IPv6 オーバー LAN ネットワーク接続機能の設定に使用します。

cfgIPv6Enable

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

iDRAC6 IPv6 スタックを有効または無効にします。

cfgIPv6Address1（読み取り / 書き込み）

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

iDRAC6 IPv6 アドレス。

cfgIPv6Gateway（読み取り / 書き込み）

有効値

有効な IPv6 エントリを表す文字列

デフォルト

::

説明

iDRAC6 ゲートウェイ IPv6 アドレス

cfgIPv6PrefixLength（読み取り / 書き込み）

有効値

1 ～ 128

デフォルト

64

説明

iDRAC6 IPv6 アドレス 1 のプレフィクスの長さ

cfgIPv6AutoConfig（読み取り/書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

IPv6 自動設定オプションを有効または無効にします。

cfgIPv6LinkLocalAddress（読み取り専用）

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

iDRAC6 IPv6 リンクのローカルアドレス

cfgIPv6Address2（読み取り専用）

有効値

有効な IPv6 エントリを表す文字列。

デフォルト

::

説明

iDRAC6 IPv6 アドレス

cfgIPv6DNSServersFromDHCP6（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

cfgIPv6DNSServer1 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 サーバーアドレス

cfgIPv6DNSServer2（読み取り/書き込み）

有効値

有効な IPv6 エントリを表す文字列

デフォルト

::

説明

IPv6 DNS サーバーアドレス

---

cfgIPv6URL

このグループは、iDRAC6 IPv6 URL の設定に使用するプロパティを指定します。

cfgIPv6URLstring（読み取り専用）

有効値

最大 80 文字の文字列

デフォルト

<空白>

説明

iDRAC6 IPv6 の URL アドレス

---

cfgIpmiSerial

このグループは、BMC の IPMI シリアルインタフェースの設定に使用されるプロパティを指定します。

cfgIpmiSerialConnectionMode（読み取り / 書き込み）

有効値

0（ターミナル）

1（基本）

デフォルト

1

説明

iDRAC6 **cfgSerialConsoleEnable** プロパティを 0（無効）に設定すると、iDRAC6 のシリアルポートが IPMI のシリアルポートになります。このプロパティによって、IPMI 定義のシリアルポートのモードが決まります。

基本モードの場合、ポートはシリアルクライアントのアプリケーションプログラムと通信するためにバイナリデータを使用します。ターミナルモードでは、ポートは非プログラム式 ASCII 端末が接続していると想定し、ごく単純なコマンドの入力を許可します。

cfgIpmiSerialBaudRate（読み取り / 書き込み）

有効値

9600、19200、57600、115200

デフォルト

57600

説明

IPMI を介したシリアル接続のボーレートを指定します。

cfgIpmiSerialChanPrivLimit（読み取り / 書き込み）

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

デフォルト

4

説明

IPMI シリアルチャネルで許可される最大権限レベルを指定します。

cfgIpmiSerialFlowControl（読み取り / 書き込み）

有効値

0 (なし)

1 (CTS/RTS)

2 (XON/XOFF)

デフォルト

1

説明

IPMI シリアルポートのフロー制御の設定を指定します。

cfgIpmiSerialHandshakeControl（読み取り / 書き込み）

有効値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI ターミナルモードのハンドシェイク制御を有効または無効にします。

cfgIpmiSerialLineEdit（読み取り / 書き込み）

有効値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI シリアルインタフェースのライン編集を有効または無効にします。

cfgIpmiSerialEchoControl（読み取り / 書き込み）

有効値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI シリアルインタフェースのエコー制御を有効または無効にします。

cfgIpmiSerialDeleteControl（読み取り / 書き込み）

有効値

0 (FALSE)

1 (TRUE)

デフォルト

0

説明

IPMI シリアルインタフェースの削除制御を有効または無効にします。

cfgIpmiSerialNewLineSequence（読み取り / 書き込み）

有効値

0 (なし)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

デフォルト

1

説明

IPMI シリアルインタフェースの改行シーケンスの仕様を指定します。

cfgIpmiSerialInputNewLineSequence（読み取り / 書き込み）

有効値

0 (<ENTER>)

1 (NULL)

デフォルト

1

説明

IPMI シリアルインタフェースの入力改行シーケンスの仕様を指定します。

---

cfgSmartCard

このグループは、スマートカードを使用した iDRAC6 へのアクセスのサポートに使用するプロパティを指定します。

cfgSmartCardLogonEnable（読み取り / 書き込み）

有効値

0（無効）

1（有効）

2（リモート RACADM で有効）

デフォルト

0

説明

スマートカードを使用した iDRAC6 へのアクセスのサポートを有効または無効にするか、リモート RACADM で有効にします。

cfgSmartCardCRLEnable（読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

証明書取り消しリスト（CRL）を有効または無効にします。

---

cfgNetTuning

このグループを使用して、RAC NIC のネットワークインタフェースの詳細パラメータを設定できます。新しい設定が有効になるまで、最大 1 分かかります。

△ **注意: このグループのプロパティを変更する場合には、特に注意が必要です。このグループのプロパティに不適切な変更を加えると、RAC NIC が動作しなくなることがあります。**

cfgNetTuningNicAutoneg （読み取り / 書き込み）

有効値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

物理リンクの速度とデュプレックスのオートネゴシエーションを有効にします。有効にした場合、オートネゴシエーションは、**cfgNetTuningNic100MB** オブジェクトと **cfgNetTuningNicFullDuplex** オブジェクトで設定した値をオーバーライドします。

cfgNetTuningNic100MB（読み取り / 書き込み）

有効値

0 (10 メガビット)

1 (100 メガビット)

デフォルト

1

説明

RAC NIC に使用する速度を指定します。このプロパティは、**cfgNetTuningNicAutoNeg** が **1**（有効）に設定されている場合には使用できません。

cfgNetTuningNicFullDuplex（読み取り / 書き込み）

有効値

0（半二重）

1（全二重）

デフォルト

1

説明

RAC NIC のデュプレックス設定を指定します。このプロパティは、**cfgNetTuningNicAutoNeg** が **1**（有効）に設定されている場合には使用できません。

cfgNetTuningNicMtu（読み取り / 書き込み）

有効値

576 ～ 1500

デフォルト

1500

説明

iDRAC6 NIC で使用する最大送信単位のバイトサイズ。

目次ページに戻る

目次ページに戻る

サポートされている RACADM インタフェース

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

以下の表に、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 C-1 RACADM サブコマンドのインタフェースサポート

サブコマンド	Telnet/SSH/シリアル	ローカル RACADM	リモート RACADM
arp	✓	✗	✓
clearasrscreen	✓	✓	✓
clrraclog	✓	✓	✓
clrsel	✓	✓	✓
coredump	✓	✗	✓
coredumpdelete	✓	✓	✓
fwupdate	✓	✓	✓
getconfig	✓	✓	✓
getniccfg	✓	✓	✓
getraclog	✓	✓	✓
getractime	✓	✓	✓
getsel	✓	✓	✓
getssninfo	✓	✓	✓
getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
netstat	✓	✗	✓
ping	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✗	✓	✓
sslkeyupload	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓
usercertupload	✗	✓	✓

usercertview	✔	✔	✔
localConRedirDisable	✖	✔	✖
✔ = サポートされている ✖ =サポートされていない			

目次ページに戻る

目次ページに戻る

iDRAC6 の概要

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

Integrated Dell™ Remote Access Controller（iDRAC6）はシステム管理ハードウェアおよびソフトウェアのソリューションで、Dell PowerEdge™ システムのリモート管理機能、クラッシュしたシステムのリカバリ機能、電源制御機能などを提供します。

iDRAC6 は、リモート監視 / 制御システムに、システムオンチップの内蔵マイクロプロセッサを採用しています。iDRAC6 は、管理下 PowerEdge サーバーとシステム基板上で共存します。サーバーオペレーティングシステムはアプリケーションの実行に関係し、iDRAC6 はサーバー環境およびオペレーティングシステム外の状態の監視と管理に関係します。

警告やエラーが発生したときに、電子メールまたは 簡易ネットワーク管理プロトコル（SNMP）のトラップ警告を送信するように iDRAC6 を設定できます。システムクラッシュの原因を診断する手助けとして、iDRAC6 はシステムクラッシュを検出すると、イベントデータをログに記録し、画面イメージをキャプチャできます。

iDRAC6 ネットワークインタフェースはデフォルトでは、静的 IP アドレス 192.168.0.120 で有効になります。これを設定しなければ、iDRAC6 にアクセスできません。iDRAC6 をネットワーク上で設定すると、iDRAC6 ウェブインタフェース、Telnet、Secure Shell (SSH) や、Intelligent Platform Management Interface（IPMI）などの対応するネットワーク管理プロトコルを使用して、割り当てられた IP アドレスにアクセスできるようになります。

---

iDRAC6 Express の管理機能

iDRAC6 には次の管理機能があります。

- ダイナミックドメイン名システム（DDNS）の登録
- ウェブインタフェース、およびシリアル、Telnet、または SSH 接続経由での SM-CLP コマンドラインを使用したリモートシステム管理と監視
- Microsoft® Active Directory® 認証のサポート - 標準スキーマまたは拡張スキーマを使用して iDRAC6 のユーザー ID とパスワードを Active Directory で一元管理
- 監視 - システム情報やコンポーネントのステータスにアクセス可能
- システムログへのアクセス - システムイベントログ、iDRAC6 のログ、およびオペレーティングシステムの状態とは関係なく、クラッシュしたシステムや応答しないシステムの前回クラッシュ画面にアクセス可能
- Dell OpenManage™ ソフトウェアの統合 - Dell OpenManage Server Administrator または IT Assistant から iDRAC6 ウェブインタフェースの起動が可能
- iDRAC6 警告 - 電子メールメッセージまたは SNMP トラップによって管理下ノードの不具合を警告
- リモート電源管理 - シャットダウンやリセットなどのリモート電源管理機能を管理コンソールから提供
- Intelligent Platform Management Interface（IPMI）のサポート
- Secure Sockets Layer（SSL）暗号化 - ウェブインタフェースからセキュアなリモートシステム管理を提供
- パスワードレベルのセキュリティ管理 - リモートシステムへの無許可のアクセスを防止
- 役割（ロール）ベースの権限 - さまざまなシステム管理タスクに応じて割り当て可能な権限
- IPv6 のサポート - IPv6 アドレスを使用して iDRAC6 ウェブインタフェースにアクセスできる IPv6 サポートの追加、iDRAC NIC IPv6 アドレスの指定、IPv6 SNMP 警告の宛先を設定するための 宛先番号の指定。
- WS-MAN のサポート - Web Services for Management（WS-MAN）プロトコルを使用したネットワークアクセス可能な管理を提供。
- SM-CLP のサポート - システム管理 CLI の実装標準を提供する Server Management-Command Line Protocol（SM-CLP）のサポートを追加。
- ファームウェアのロールバックとリカバリ - 選択したファームウェアイメージからの起動やファームウェアイメージへのロールバックが可能。

iDRAC6 Express 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。

---

iDRAC6 Enterprise および vFlash メディア

RACADM、仮想 KVM、仮想メディア機能、専用 NIC、および 仮想フラッシュ（オプションで Dell vFlash メディアカード装備）のサポートを追加。仮想フラッシュを使用すると、vFlash メディアに緊急用の起動イメージと診断ツールを保存できます。iDRAC6 Enterprise の詳細については、『ハードウェアオーナーズマニュアル』（**support.dell.com¥manuals**）を参照してください。

表 1-1 に、BMC、iDRAC6 Express、iDRAC6 Enterprise、および vFlash メディアの機能を示します。

表 1-1 iDRAC6 の機能リスト

機能	BMC	iDRAC6 Express	iDRAC6 Enterprise	VFlash メディア
インタフェースと標準サポート				
IPMI 2.0	✔	✔	✔	✔

ウェブベースの GUI	✗	✓	✓	✓
SNMP	✗	✓	✓	✓
WSMAN	✗	✓	✓	✓
SMASH-CLP	✗	✓	✓	✓
RACADM コマンドライン	✗	✗	✓	✓
伝導性				
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				
役割ベースの権限	✓	✓	✓	✓
ローカルユーザー	✓	✓	✓	✓
Active Directory	✗	✓	✓	✓
2 ファクタ認証	✗	✓	✓	✓
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	✓ [1]	✓	✓	✓
サーバーの電源制御	✓ [1]	✓	✓	✓
シリアルオーバーLAN （プロキシ使用）	✓	✓	✓	✓
シリアルオーバー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	✗	✗	✓	✓
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	✓ [1]	✓	✓	✓
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 ログからすべてのエントリをクリアします。	✗	✓	✓	✓
トレースログ	✗	✓	✓	✓

[1] - 機能はウェブインタフェースでなく IPMI からのみ使用可能

✓ = 対応 ✗ = 未対応

iDRAC6 には以下のようなセキュリティ機能があります。

- Microsoft Active Directory(オプション)またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証
- システム管理者が各ユーザーに特定の権限を設定できる役割(ロール)ベースの許可
- ウェブインタフェースまたは SM-CLP を使用したユーザー ID とパスワードの設定
- 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
- ウェブインターフェースまたは SM-CLP を使用したセッションタイムアウトの設定(秒単位)
- 設定可能な IP ポート(該当する場合)

  メモ: Telnet は SSL 暗号化をサポートしていません。

- 暗号化トランスポート層を使用してセキュリティを強化する SSH
- IP アドレスごとのログイン失敗回数の制限によって制限を越えた IP アドレスからのログインを阻止
- iDRAC6 に接続するクライアントの IP アドレス範囲を制限する機能
- スマートカード認証

対応プラットフォーム

対応プラットフォームの最新情報については、iDRAC6 Readme ファイルとデルサポートサイト **support.dell.com¥manuals** およびシステムに付属の『Dell Systems Management Tools and Documentation DVD』にある Dell Systems Software Support Matrix を参照してください。

対応 OS

最新情報については、iDRAC6 Readme ファイルとデルサポートサイト **support.dell.com¥manuals** およびシステムに付属の『Dell Systems Management Tools and Documentation DVD』にある Dell Systems Software Support Matrix を参照してください。

対応ウェブブラウザ

最新情報については、iDRAC6 Readme ファイルとデルサポートサイト **support.dell.com¥manuals** およびシステムに付属の『Dell Systems Management Tools and Documentation DVD』にある Dell Systems Software Support Matrix を参照してください。

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

サポートされる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	• 10Mbps/100Mbs/Ethernet • 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、シャットダウンコマンドなどの操作に使用する SM-CLP (Telnet または SSH)コマンドシェルのサポート • IPMItool や ipmishell 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。

表 1-3 iDRAC6 サーバーリスニングポート

ポート番号	機能

22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	コンソールリダイレクトキーボード/マウス、仮想メディアサービス、仮想メディアセキュアサービス、コンソールリダイレクトビデオ
*設定可能なポート	

表 1-4 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、以下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記載されています。これらのドキュメントは、デルサポートサイト **support.dell.com¥manuals** から入手可能です。

- iDRAC6 オンラインヘルプでは、ウェブインタフェースの使用法について詳しく説明しています。
- iDRAC ハードウェアとシステムサービスの設定の詳細については、『Dell Unified Server Configurator ユーザーズガイド』を参照してください。
- IT Assistant の使用法については、『Dell OpenManage IT Assistant ユーザーズガイド』を参照してください。
- iDRAC6 のインストールについては、『ハードウェアオーナーズマニュアル』を参照してください。
- Server Administrator のインストールと使用法については、『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。
- 最新の対応プラットフォーム、オペレーティングシステム、およびウェブブラウザについては、iDRAC6 Readme ファイルと Dell Systems Software Support Matrix を参照してください。
- システムアップデート対策としての Dell Update Packages の入手とその使用法については、『Dell Update Packages ユーザーズガイド』を参照してください。
- iDRAC6 と IPMI インタフェースについては、『Dell OpenManage Baseboard Management Controller ユーティリティユーザーズガイド』を参照してください。

以下のシステム文書にも、iDRAC6 をインストールするシステムについての詳細が記載されています。

- 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。保証情報については、このマニュアルに含まれている場合と、別のマニュアルが付属する場合があります。
- ラックソリューションに付属の『ラック取り付けガイド』では、システムをラックに取り付ける方法について説明しています。
- 『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。
- 『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。
- 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。
- 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。
- 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。
- 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。

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

目次ページに戻る

目次ページに戻る

WS-MAN インタフェースの使用

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

iDRAC6 ファームウェアは、Web Services for Management（WS-MAN）プロトコルを使用して ネットワークからアクセスできる管理を提供します。WS-MAN は、情報交換用のトランスポートメカニズムです。管理がしやすいように、WS-MAN はデバイスがデータを共有するための汎用言語を提供します。WS-MAN は、リモートシステム管理ソリューションの主要部分ですが、役割はこれだけではありません。

WS-MAN は HTTPS を使用して、管理トラフィックのセキュリティを保護しています。クライアントはローカルか Microsoft® Active Directory® ユーザ特権でログインして、セッションを認証する必要があります。HTTPS は IP ポート 443 のセキュアソケットレイヤー (SSL) を使用して、セキュリティを保護します。

WS-MAN で使用できるデータは、次の分散管理タスクフォース（DMTF）プロファイルと Dell の拡張子にマップされている iDRAC6 計装インタフェースによって提供されるデータのサブセットです。

WS-MAN を使用して DMTF CIM ベースの管理情報を伝えるには、WS-MAN を利用するのが最も一般的です。CIM は、管理下システムで操作される管理情報の種類を定義します。ここでは、ワイヤに関するクライアントとサービスの対話オブジェクトを提供します。WS-MAN は、管理オブジェクトで実行される標準的な処理をいくつか定義します。たとえば、WS-MAN を使用すると、クライアントシステムは管理オブジェクトのコレクションを検出し、管理オブジェクトのコンテンツを取得して、そのコンテンツを新しい値に設定できます。WS-MAN は、管理会話のバーブを提供します。CIM クラスおよびプロパティがナウンで、バーブによってオブジェクトが機能します。

クライアントとサービス間の相互運用性を維持するには、DMTF と Dell の CIM クラス、プロパティ、およびビヘイビアの標準的な最小限のボキャブラリを追加指定し、関係者全員が理解する必要があります。このような DMTF や Dell 固有のプロファイルは、規格準拠のサービスで実装される必要のアル表記規則を定義しています。したがって、すべてのクライアントがこれらの表記規則に依存して正しく機能することができます。

対応 CIM プロファイル

表 11-1 対応 CIM プロファイル

標準 DMTF
1. ベースサーバー ホストサーバーを表す CIM クラスを定義します。
2. サービスプロセッサ: iDRAC6 を表す CIM クラスの定義が記載されています。 **メモ:** ベースサーバープロファイル（上記）およびサービスプロセッサプロファイルは、ある意味では自律的なもので、コンポーネントプロファイルで定義されているその他すべての CIM オブジェクトを総合的に説明するオブジェクトです。
3. 物理的資産 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。
4. SM CLP 管理者ドメイン CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して独自の CLP を実装します
5. 電源状況管理 電源制御操作の CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーの電源制御操作を実行します。
6. 電源装置（バージョン 1.1） 電源装置を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーの電源装置を表し、消費電力の高低を示す電力消費量を説明します。
7. CLP サービス CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して独自の CLP を実行します
8. IP インタフェース
9. DHCP クライアント
10. DNS Client（DHCP クライアント）
11. Ethernet ポート 上記のプロファイルは、ネットワークを表す CIM クラスを定義します。iDRAC6 は、これらのプロファイルを使用して iDRAC6 NIC の構成を表します。
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. ソフトウェアインベントリ インストールしたソフトウェアや利用可能なソフトウェアのインベントリの 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、現在インストールしている iDRAC6 ファームウェアバージョンのインベントリを TFTP プロコルから実行します。

14. ロールベースの認証 ロールを表す CIM を定義します。iDRAC6 は、このプロファイルを使用して iDRAC6 のアカウント特権を定義します。
15. ソフトウェアのアップデート 利用可能なソフトウェアアップデートのインベントリの CIM クラスを定義します。iDRAC6 はこのプロファイルを使用して、 .TFTP プロコルからファームウェアアップデートのインベントリを実行します。
16. SMASH コレクション CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して独自の CLP を実行します
17. プロファイル登録 プロファイルの実行アドバタイズする 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ドバタイズします。
18. ベースメトリック メトリックを表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーのメトリックを表し、消費電力の高低を示す電力消費量を説明します。
19. 簡易 ID 管理 ID を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して iDRAC6 のアカウントを定義します。
20. USB リダイレクト ローカル USB ポートのリモートリダイレクトを表す CIM を定義します。iDRAC6 は、このプロファイルを仮想メディアプロファイルと併せて使用して、仮想メディアを定義します。
Dell 拡張
1. Dell™ Active Directory Client Version 2.0.0 iDRAC6 Active Directory クライアントおよび Active Directory グループのローカル権限を設定する CIM と Dell 拡張クラスを定義します。
2. Dell 仮想メディア iDRAC6 仮想メディアを設定する CIM と Dell 拡張クラスを定義します。USB リダイレクトプロファイルを拡張します。
3. Dell イーサネットポート iDRAC6 NIC 用 NIC サイドバンド(帯域)インターフェースを設定する CIM と Dell 拡張クラスを定義します。イーサネットポートプロファイルを拡張します。
4. Dell 電力使用制御 ホストサーバーの電力バジェットを表したり、ホストサーバーの電力を設定/監視したりするための CIM と Dell 拡張クラスを定義します。

詳細については、**www.dmtf.org/standards/profiles/** を参照してください。このプロファイル一覧の最新版や最新情報については、WS-MAN のリリースノートまたは readme ファイルを参照してください。

WS-MAN システムは、DMTF ウェブサービスの管理仕様バージョン 1.0.0 に準拠しています。WS-Management プロトコルに対応しているツールには、Microsoft Windows® Remote Management (WinRM) と open wsman、wsmancli ツールがありますが、これらに限定されません。

目次ページに戻る

目次ページに戻る

iDRAC6 SM-CLP コマンドラインインタフェースの使用

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

この項では、iDRAC6 に組み込まれている Distributed Management Task Force（DMTF）Server Management-Command Line Protocol（SM-CLP）について説明します。

メモ: ここでは、ユーザーが Systems Management Architecture for Server Hardware（SMASH）イニシアチブおよび SMWG SM-CLP 仕様に精通していることを前提としています。これらの仕様の詳細については、DMTF のウェブサイト **www.dmtf.org** を参照してください。

iDRAC6 SM-CLP は、システム管理 CLI 実装の標準となっているプロトコルです。SM-CLP は、複数のプラットフォームでサーバー管理を主導する DMTF SMASH イニシアチブのサブコンポーネントです。SM-CLP 規格は、Managed Element Addressing Specification（管理下エレメントアドレス指定規格）や SM-CLP マッピング規格に対する多くのプロファイルと共に、さまざまな管理タスクの実行に使用する標準化されたバーブとターゲットについて記述しています。

---

iDRAC6 SM-CLP のサポート

SM-CLP は iDRAC6 コントローラのファームウェアからホストされ、telnet、SSH、およびシリアルベースのインタフェースをサポートしています。iDRAC6 SM-CLP インタフェースは DMTF 組織が提供する SM-CLP 規格バージョン 1.0 に基づいています。iDRAC6 SM-CLP では、表 11-1「サポートされているCIM プロファイル」で説明したすべてのプロファイルがサポートされます。

以下の項では、iDRAC6 からホストされる SM-CLP 機能の概要を述べます。

SM-CLP の機能

SM-CLP はバーブとターゲットの概念を起用して、CLI によるシステム管理機能を提供しています。バーブは実行する処理を指し、ターゲットはその処理を実行するエンティティ（またはオブジェクト）を決定します。

下記は SM-CLP コマンドライン構文の例です。

<バーブ> [<オプション>] [<ターゲット>] [<プロパティ>]

標準的な SM-CLP セッション中は、表 12-1 のリストにあるバーブを使って操作を実行できます。

表 12-1 システムでサポートされている CLI バーブ

バーブ	定義
cd	シェルを使用して MAP を移動します。
set	特定の値に対してプロパティを設定します。
help	特定のターゲットのヘルプを表示します。
reset	ターゲットをリセットします。
show	ターゲットのプロパティ、バーブ、およびサブターゲットを表示します。
start	ターゲットをオンにします。
stop	ターゲットをシャットダウンします。
exit	SM-CLP シェルのセッションを終了します。
version	ターゲットのバージョン属性を表示します。
load	バイナリイメージを URL から指定されたターゲットアドレスに移動します。

SM-CLP の使用

正しい資格情報を使用して SSH（または telnet）で iDRAC6 に接続します。

SMCLP プロンプト（/admin1->）が表示されます。

SM-CLP のターゲット

表 12-2 は、上記の表 12-1 で説明した操作をサポートするために SM-CLP から提供されるターゲットのリストです。

表 12-2 SM-CLP のターゲット

ターゲット	定義
admin1	admin domain
admin1/profiles1	iDRAC6 の登録プロファイル
admin1/hdwr1	ハードウェア
admin1/system1	管理下システムターゲット
admin1/system1/redundancyset1	電源ユニット
admin1/system1/redundancyset1/pwrsupply*	管理下システムの電源ユニット
admin1/system1/sensors1	管理下システムセンサー
admin1/system1/capabilities1	管理下システム SMASH 収集機能
admin1/system1/capabilities1 pwrcap1	管理下システムの電力使用機能
admin1/system1/capabilities1 elecap1	管理下システムターゲット機能
admin1/system1/logs1	レコードログ収集ターゲット
admin1/system1/logs1/log1	システム イベント ログ(SEL)のレコードエントリ
admin1/system1/logs1/log1/ レコード*	管理下システムの SEL レコードの個々のインスタンス
admin1/system1/settings1	管理下システム SMASH 収集設定
admin1/system1/settings1 pwrmaxsetting1	管理下システム最大電源割り当て設定
admin1/system1/settings1 pwrminsetting1	管理下システム最小電源割り当て設定
admin1/system1/capacities1	管理下システム機能 SMASH 収集
admin1/system1/consoles1	管理下システムコンソール SMASH 収集
admin1/system1/usbredirectsap1	仮想メディア USB リダイレクト SAP
admin1/system1/usbredirectsap1/remotesap1	仮想メディア送信先 USB リダイレクト SAP
admin1/system1/sp1	サービスプロセッサ
admin1/system1/sp1/timesvc1	サービスプロセッサ時間サービス
admin1/system1/sp1/capabilities1	サービスプロセッサ機能 SMASH 収集
admin1/system1/sp1/capabilities1/clpcap1	CLP サービス機能
admin1/system1/sp1/capabilities1/pwrmgtcap1	システムの電源状態管理サービス機能
admin1/system1/sp1/capabilities1/ipcap1	IP インタフェース機能
admin1/system1/sp1/capabilities1/dhcpcap1	DHCP クライアント機能
admin1/system1/sp1/capabilities1/NetPortCfgcap1	ネットワークポート構成機能
admin1/system1/sp1/capabilities1/usbredirectcap1	仮想メディア機能 USB リダイレクト SAP
admin1/system1/sp1/capabilities1/vmsapcap1	仮想メディア SAP 機能
admin1/system1/sp1/capabilities1/swinstallsvccap1	ソフトウェアインストールサービス機能
admin1/system1/sp1/capabilities1/acctmgtcap*	アカウント管理サービス機能
admin1/system1/sp1/capabilities1/adcap1	Active Directory® 機能
admin1/system1/sp1/capabilities1/rolemgtcap*	ローカルロールベースの管理機能
admin1/system1/sp1/capabilities/PwrutilmgtCap1	電力使用管理機能
admin1/system1/sp1/capabilities/metriccap1	メトリックサービス機能
admin1/system1/sp1/capabilities1/elecap1	複数要素認証機能
admin1/system1/sp1/capabilities1/lanendptcap1	LAN(イーサネットポート) エンドポイント機能
admin1/system1/sp1/logs1	サービスプロセッサログ収集
admin1/system1/sp1/logs1/log1	システムレコードログ
admin1/system1/sp1/logs1/log1/record*	システムログエントリ
admin1/system1/sp1/settings1	サービスプロセッサ設定収集
admin1/system1/sp1/settings1 clpsetting1	CLP サービス設定データ
admin1/system1/sp1/settings1 ipsettings1	IP インタフェース割り当て設定データ(静的)
admin1/system1/sp1/settings1 ipsettings1/staticipsettings1	静的 IP インタフェース割り当て設定データ
admin1/system1/sp1/settings1 ipsettings1/dnssettings1	DNS クライアント設定データ
admin1/system1/sp1/settings1 ipsettings2	IP インタフェース割り当て設定データ(DHCP)
admin1/system1/sp1/settings1 ipsettings2/dhcpsettings1	DHCP クライアント設定データ
admin1/system1/sp1/clpsvc1	CLP サーバープロトコルサービス
admin1/system1/sp1/clpsvc1 clpendpt*	CLP サーバープロトコルエンドポイント

admin1/system1/sp1/clpsvc1 tcpendpt*	CLP サーバープロトコル TCP エンドポイント
admin1/system1/sp1/jobq1	CLP サーバープロトコルジョブキュー
admin1/system1/sp1/jobq1/job*	CLP サーバープロトコルジョブ
admin1/system1/sp1/pwrmgtsvc1	電源状況管理サービス
admin1/system1/sp1/ipcfgsvc1	IP インターフェース設定サービス
admin1/system1/sp1/ipendpt1	IP インタフェースプロトコルエンドポイント
admin1/system1/sp1 ipendpt1/gateway1	IP インタフェースゲートウェイ
admin1/system1/sp1 ipendpt1/dhcpendpt1	DHCP クライアントプロトコルエンドポイント
admin1/system1/sp1 ipendpt1/dnsendpt1	DNS クライアントプロトコルエンドポイント
admin1/system1/sp1/ipendpt1 dnsendpt1/dnsserver*	DNS クライアントサーバー
admin1/system1/sp1/NetPortCfgsvc1	ネットワークポート構成サービス
admin1/system1/sp1/lanendpt1	LAN エンドポイント
admin1/system1/sp1 lanendpt1/enetport1	Ethernet ポート
admin1/system1/sp1/VMediaSvc1	仮想メディアサービス
admin1/system1/sp1 VMediaSvc1/tcpendpt1	仮想メディア TCP プロトコルエンドポイント
admin1/system1/sp1/swid1	ソフトウェア識別
admin1/system1/sp1 swinstallsvc1	ソフトウェアインストールサービス
admin1/system1/sp1 account1-16	複数要素認証(MFA)アカウント
admin1/sysetm1/sp1/ account1-16/identity1	ローカルユーザー識別アカウント
admin1/sysetm1/sp1/ account1-16/identity2	IPMI 識別(LAN)アカウント
admin1/sysetm1/sp1/ account1-16/identity3	IPMI 識別(シリアル)アカウント
admin1/sysetm1/sp1/ account1-16/identity4	CLP 識別アカウント
admin1/system1/sp1/acctsvc1	MFA アカウント管理サービス
admin1/system1/sp1/acctsvc2	IPMI アカウント管理サービス
admin1/system1/sp1/acctsvc3	CLP アカウント管理サービス
admin1/system1/sp1/group1-5	Active Directory グループ
admin1/system1/sp1 group1-5/identity1	Active Directory 識別
admin1/system1/sp1/ADSvc1	Active Directory サービス
admin1/system1/sp1/rolesvc1	ローカルロールベース認証(RBA)サービス
admin1/system1/sp1/rolesvc1 Role1-16	ローカルロール
admin1/system1/sp1/rolesvc1 Role1-16/privilege1	ローカルロール権限
admin1/system1/sp1/rolesvc1 Role17-21/	Active Directory ロール
admin1/system1/sp1/rolesvc1 Role17-21/privilege1	Active Directory 権限
admin1/system1/sp1/rolesvc2	IPMI RBA サービス
admin1/system1/sp1/rolesvc2 Role1-3	IPMI ロール
admin1/system1/sp1/rolesvc2 Role4	IPMI シリアルオーバー LAN(SOL)ロール
admin1/system1/sp1/rolesvc3	CLP RBA サービス
admin1/system1/sp1/rolesvc3 Role1-3	CLP ロール
admin1/system1/sp1/rolesvc3 Role1-3/privilege1	CLP ロール権限
admin1/system1/sp1 pwrutilmgtsvc1	電源使用管理サービス
admin1/system1/sp1 pwrutilmgtsvc1/pwrcurr1	電源使用管理サービスの電力設定割り当て設定データ
admin1/system1/sp1/metricsvc1	メトリックサービス
/admin1/system1/sp1/metricsvc1/cumbmd1	累積ベースメトリック定義
/admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1	累積ベースメトリック値

/admin1/system1/sp1/metricsvc1/cumwattamd1	累積ワット集約メトリック定義
/admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1	累積ワット集約メトリック値
/admin1/system1/sp1/metricsvc1/cumampamd1	累積アンペア集約メトリック定義
/admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1	累積ワット集約メトリック値
/admin1/system1/sp1/metricsvc1/loamd1	低累積メトリック定義
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	低累積メトリック値
/admin1/system1/sp1/metricsvc1/hiamd1	高累積メトリック定義
/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*	高累積メトリック値
/admin1/system1/sp1/metricsvc1/avgamd1	平均累積メトリック定義
/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*	平均累積メトリック値

目次ページに戻る

目次ページに戻る

VMCLI を使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）バージョン 1.1 ユーザーズガイド

仮想メディアコマンドラインインタフェース（VMCLI）ユーティリティは、管理ステーションからリモートシステムの iDRAC6 に仮想メディアの機能を提供するコマンドラインインタフェースです。VMCLI とスクリプトメソッドの使用によって、オペレーティングシステムをネットワーク上の複数のリモートシステムに導入できます。

ここでは、VMCLI ユーティリティを企業のネットワークに組み込む方法について説明します。

作業を開始する前に

VMCLI ユーティリティを使用する前に、対象となるリモートシステムと企業のネットワークが以下の項に記載する要件を満たしていることを確認してください。

リモートシステム要件

各リモートシステムで iDRAC6 が設定されている。

ネットワーク要件

ネットワーク共有に以下のコンポーネントが含まれている。

- オペレーティングシステムファイル
- 必要なドライバ
- 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 のイメージであることが必要です。

ブータブルイメージファイルの作成

イメージファイルをリモートシステムに導入する前に、サポートされているシステムがそのファイルから起動できることを確認してください。イメージファイルをテストするには、iDRAC6 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 Microsoft® Windows® システム用のイメージファイルの作成方法について説明します。

Linux システム用のイメージファイルの作成

Linux システムの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定するときには、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、Windows オペレーティングシステムを導入する場合、イメージファイルには Microsoft Systems Management Server(SMS)で使用される導入方法と同様のプログラムを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。

   - 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
   - 対象システムのそれぞれが同じ導入プロシージャを起動して実行するように、導入イメージを「読み取り専用」とマークする

4. 次のいずれかの手順を実行してください。

   - 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 **IPMItool** と VMCLI を組み込みます。ユーティリティを使用する際の手引きとして **vm6deploy** サンプルスクリプトを使用します。
   - オペレーティングシステムの導入には、既存の **vm6deploy** スクリプトを使用します。

オペレーティングシステムの導入

VMCLI ユーティリティと、そのユーティリティに含まれている **vm6deploy** スクリプトを使用して、リモートシステムにオペレーティングシステムを導入します。

始める前に、VMCLI ユーティリティに含まれているサンプル **vm6deploy** スクリプトを確認してください。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、導入するリモートシステムの iDRAC6 IPv4 アドレス(1 行に 1 つの IPv4 アドレス)を入力します。
2. ブータブル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 **vm6deploy** を実行します。

vm6deploy スクリプトを実行するには、コマンドプロンプトで次のコマンドを入力します。

```
vm6deploy -r ip.txt -u <idrac-user> -p <idrac-passwd> -c {<iso9660-img> | <path>} -f {<111128899.590floppy-img>|<path>}
```

この場合、

- <iDRAC6 ユーザー> は iDRAC ユーザー名です(例:**root**)。
- <idrac-passwd> は iDRAC 6 ユーザーのパスワードです(たとえば **calvin**)。
- <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。
- <path> は、オペレーティングシステムのインストール CD、DVD、またはフロッピー があるデバイスのパスです。
- <floppy-img> は有効なフロッピーイメージのパスです。

vm6deploy スクリプトは、コマンドラインオプションを **VMCLI** ユーティリティに渡します。これらのオプションの詳細については、「コマンドラインオプション」を参照してください。このスクリプトは **-r** オプションを処理する方法は、**vmcli -r** オプションとは若干異なります。**-r** オプションの引数が既存のファイル名である場合、スクリプトは指定したファイルから iDRAC6 IPv4 アドレスを読み取り、各行で **VMCLI** ユーティリティを一度実行します。**-r** オプションの引数が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**VMCLI** ユーティリティの説明どおりに機能します。

VMCLI ユーティリティの使用

VMCLI ユーティリティは、管理ステーションから iDRAC6 に仮想メディアの機能を提供するスクリプト可能なコマンドラインインタフェースです。

VMCLI ユーティリティには以下の機能があります。

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。

- 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
- 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

- セキュアソケットレイヤ(SSL)を使用した iDRAC6 へのセキュアな通信

ユーティリティを実行する前に、iDRAC6 に対する仮想メディアユーザー権限があることを確認してください。

オペレーティングシステムが管理者権限、オペレーティングシステム固有の権限、またはグループメンバーシップをサポートしている場合、VMCLI コマンドを実行するためには管理者権限も必要です。

クライアントシステムの管理者は、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、VMCLI ユーティリティを実行するにはパワーユーザーの権限が必要です。

Linux システムの場合は、**sudo** コマンドを使うと管理者権限なしで VMCLI コマンドにアクセスできます。このコマンドは、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。システム管理者は VMCLI グループのユーザーを追加または編集する場合に、**visudo** コマンドを使用します。管理者権限のないユーザーは、VMCLI コマンドライン(または VMCLI スクリプト)のプレフィックスとして **sudo** コマンドを追加すると、リモートシステムの iDRAC6 へのアクセス権を得て、このユーティリティを実行できます。

VMCLI ユーティリティのインストール

VMCLI ユーティリティは、Dell OpenManage システム管理ソフトウェアキットに含まれている『Dell Systems Management Tools and Documentation DVD』に収録されています。このユーティリティをインストールするには、『Dell Systems Management Tools and Documentation DVD』をシステムの DVD ドライブに挿入して画面に表示される指示に従ってください。

『Dell Systems Management Tools and Documentation DVD』には、診断、ストレージ管理、リモートアクセスサービス、IPMItool 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、VMCLI および IPMItool 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説明するサンプルスクリプト **vm6deploy** が含まれています。

メモ: **vm6deploy** スクリプトは、インストール時にディレクトリに存在する他のファイルに依存しています。別のディレクトリからスクリプトを使用する場合は、それと一緒にすべてのファイルをコピーする必要があります。IPMItool ユーティリティがインストールされていない場合は、これもコピーする必要があります。

コマンドラインオプション

VMCLI インタフェースは Windows と Linux システムで全く同じです。

VMCLI コマンド形式は次のとおりです。

```
VMCLI [parameter] [operating_system_shell_options]
```

コマンドライン構文では、大文字と小文字が区別されます。詳細については、「VMCLI パラメータ」を参照してください。

リモートシステムでコマンドが受け入れられ、iDRAC6 が接続を許可した場合は、次のどちらかが発生するまでコマンドの実行が続行します。

- 何らかの理由で VMCLI の接続が切れた。
- 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 ではタスク マネージャを使用して処理を中止できます。

VMCLI 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 IPv4 アドレスと SSL ポートを提供します。これらは、ユーティリティがターゲット iDRAC6 と仮想メディア接続を確立するために必要です。無効な IPv4 アドレスまたは DDNS 名を入力すると、エラーメッセージが表示されてコマンドが終了します。

<iDRAC-IP-address> は有効な固有の IPv4 アドレスまたは iDRAC6 動的ドメインネームシステム(DDNS)名です(サポートしている場合)。<iDRAC-SSL-port> を省くと、デフォルトのポート 443 が使用されます。iDRAC6 のデフォルト SSL ポートを変更する場合を除いて、オプションの SSL ポートは不要です。

iDRAC6 ユーザー名

```
-u <iDRAC-user-name>
```

このパラメーター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-user-name> には、次の属性が必要です。

- 有効なユーザー名
- 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-user-password>
```

このパラメータは、指定した iDRAC6 ユーザーのパスワードを提供します。

iDRAC6 の認証に失敗した場合は、エラーメッセージが表示されてコマンドが終了します。

フロッピー / ディスクデバイスまたはイメージファイル

```
-f {<device-name> | <イメージファイル>}
```

この場合、<device-name> は有効なドライブ文字（Windows システム）または有効なデバイスファイル名（Linux システム）で、<image-file> は有効なイメージファイルの名前とパスです。

メモ: VMCLI ユーティリティでは、マウントポイントはサポートされていません。

このパラメータは、仮想フロッピー / ディスクメディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

```
-f c:¥temp¥myfloppy.img（Windows システム）

-f /tmp/myfloppy.img（Linux システム）
```

イメージファイルが書き込み保護されていない場合は、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）
```

メモ: Red Hat® Enterprise Linux® バージョン 4 では、複数の LUN はサポートされておらず、サポートされる予定もありません。カーネルはこの機能をサポートしていますが、以下の手順に従って、Red Hat Enterprise Linux バージョン 4 で複数の LUN を搭載した SCSI デバイスの認識を有効にする必要があります。

1. **/etc/modprobe.conf** を編集して、次の行を追加します。
   options scsi_mod max_luns=8
   （LUN の数は 8 のほかにも、2 以上の任意の数を指定できます。）

2. コマンドラインで次のコマンドを入力して、カーネルイメージの名前を取得します。

   ```
   uname -r
   ```

3. **/boot** ディレクトリに移動し、手順 2 で決定した名前のカーネルイメージファイルを削除します。

   ```
   mkinitrd /boot/initrd-'uname -r'.img `uname -r'
   ```

4. サーバーを再起動します。

5. 次のコマンドを実行して、手順 1 で指定した 数の LUN のサポートが追加されたことを確認します。

   ```
   cat /sys/modules/scsi_mod/max_luns
   ```

デバイスに書き込み保護機能がある場合は、その機能を使用して、仮想メディアがメディアに書き込めないようにしてください。

フロッピーメディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出されたら、エラーメッセージが表示されてコマンドが終了します。

CD/DVD デバイスまたはイメージファイル

```
-c {<device-name> | <image-file>}
```

この場合、<device-name> 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、<image-file> は有効な ISO-9660 イメージファイルのファイル名とパスです。

このパラメータは、仮想 CD/DVD-ROM メディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

```
-c c:¥temp¥mydvd.img（Windows システム）

-c /tmp/mydvd.img (Linux システム)
```

たとえば、デバイスは次のように指定します。

```
-c d:¥（Microsoft® Windows® システム）
```

-c /dev/cdrom（Linux システム）

CD/DVD メディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出されたら、エラーメッセージが表示されてコマンドが終了します。

スイッチオプションしかない場合を除いて、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、VMCLI ユーティリティのバージョンを表示するために使用します。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、コマンドはエラーメッセージなしで終了します。

ヘルプの表示

-h

このパラメータは、VMCLI ユーティリティパラメータの概要を示します。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。

暗号化データ

-e

このパラメータがコマンドラインに含まれていると、VMCLI は SSL で暗号化されたチャネルを使用して、管理ステーションとリモートシステムの iDRAC6 間でデータを転送します。このパラメータがコマンドラインに含まれていない場合は、データ転送が暗号化されません。

メモ: このオプションを使用しても、RACADM やウェブインタフェースなど、他の iDRAC6 設定インタフェースに表示される仮想メディアの暗号化状態を 有効 に変更することはできません。

VMCLI オペレーティングシステムシェルオプション

VMCLI コマンドラインでは、以下のオペレーティングシステム機能を使用できます。

- stderr/stdout redirection - 印刷されたユーティリティの出力をファイルにリダイレクトします。

  たとえば、「より大」の不等号（>）の後にファイル名を入力すると、指定したファイルが VMCLI ユーティリティの印刷出力で上書きされます。

  メモ: VMCLI ユーティリティは標準入力（**stdin**）からは読み取りません。したがって、**stdin** リダイレクトは不要です。

- バックグラウンドでの実行 - デフォルトで VMCLI ユーティリティはフォアグラウンドで実行されます。オペレーティングシステムのコマンドシェル機能を使用すると、ユーティリティをバックグラウンドで実行できます。たとえば、Linux オペレーティングシステムの場合、コマンドの直後にアンパーサンド（&）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。

後者の方法はスクリプトプログラムの場合に便利です。VMCLI コマンドの新しいプロセスが開始した後、スクリプトを継続できます（そうでない場合は、VMCLI プログラムが終了するまでスクリプトがブロックされます）。VMCLI の複数のインスタンスがこの方法で開始し、コマンドインスタンスの 1 つ以上を手動で終了しなければならない場合は、オペレーティングシステムに固有の機能を使用して、プロセスをリストにして終了します。

VMCLI 戻りコード

エラーが発生した場合は、標準エラー出力に英語のみのテキストメッセージも表示されます。

目次ページに戻る

目次ページに戻る

Intelligent Platform Management Interface (IPMI) の設定

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

IPMI の設定

ここでは、iDRAC6 IPMI インタフェースの設定と使用について説明します。インタフェースには以下が含まれます。

- LAN 上の IPMI
- IPMI オーバーシリアル
- シリアルオーバー LAN

iDRAC6 は完全に IPMI 2.0 対応です。以下を使用して iDRAC6 IPMI を設定できます。

- お使いのブラウザからの iDRAC6 GUI
- IPMItool などのオープンソースユーティリティ
- Dell™ OpenManage™ IPMI シェル、ipmish
- RACADM

IPMI シェル、ipmish の使用法の詳細については、、**support.dell.com¥manuals** で『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

RACADM の使い方の詳細については、「RACADM のリモート使用」を参照してください。

ウェブベースインタフェースを使った IPMI の設定

詳細については、「IPMI の設定」を参照してください。

RACADM CLI を使った IPMI の設定

1. RACADM インタフェースを使ったリモートシステムへのログイン「RACADM のリモート使用を参照してください。
2. IPMI オーバー LAN を設定します。

   コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

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

   a. IPMI チャネル権限を更新します。

      コマンドプロンプトに次の内容を入力し、<Enter> を押します。

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <レベル>
      ```

      <レベル> は次のいずれかです。

      - 2 (ユーザー)
      - 3 (オペレータ)
      - 4 (管理者)

      たとえば、IPMI LAN チャネル権限を 2（ユーザー）に設定するには、次のコマンドを入力します。

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

   b. 必要なら IPMI LAN チャネルの暗号キーを設定します。

   メモ: iDRAC6 IPMI は RMCP+ プロトコルに対応しています。詳細については、IPMI 2.0 規格を参照してください。

      コマンドプロンプトに次の内容を入力し、<Enter> を押します。

racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <キー>

<キー> は有効な 16 進数 形式の 20 文字からなる暗号キーです。

3. IPMI シリアルオーバー LAN (SOL)を設定します。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1

a. IPMI SOL の最小権限レベルを更新します。

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。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <レベル>

<レベル> は次のいずれかです。

- 2 (ユーザー)
- 3 (オペレータ)
- 4 (管理者)

たとえば、IPMI 権限を 2 (ユーザー) に設定するには、次のコマンドを入力します。

racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2

b. IPMI SOL ボーレートを更新します。

メモ: シリアルコンソールを LAN 経由でリダイレクトするには、SOL ボーレートが管理下システムのボーレートと同じであること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して <Enter> を押します。

racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <ボーレート>

ここで、<ボーレート> は 9600、19200、57600、または 115200 bps です。

例:

racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600

c. 個々のユーザーに対して SOL 有効にします。

メモ: SOL は個々のユーザーに対して有効または無効にできます。

コマンドプロンプトに次の内容を入力し、<Enter> を押します。

racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2

<id> はユーザーの固有の ID です。

4. IPMI シリアルを設定します。

a. IPMI シリアル接続モードを適切な設定に変更します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

racadm config -g cfgSerial -o cfgSerialConsoleEnable 0

b. IPMI シリアルボーレートを設定します。

コマンドプロンプトを開いて次のコマンドを入力し、<Enter> を押します。

racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <ボーレート>

<ボーレート> は 9600、19200、57600、115200 bps のいずれかを指定します。

例:

racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600

c. IPMI シリアルハードウェアフロー制御を有効にします。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1

d. IPMI シリアルチャネルの最低権限レベルを設定します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <レベル>
```

<レベル> は次のいずれかです。

- 2(ユーザー)
- 3(オペレータ)
- 4(管理者)

たとえば、IPMI シリアルチャネル権限を 2(ユーザー) に設定するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. BIOS セットアッププログラムでシリアル MUX が正しく設定されていることを確認します。

- システムを再起動します。
- POST 中に F2 を押して BIOS セットアッププログラムを起動します。
- **シリアル通信** をクリックします。
- **シリアル接続** メニューで **外部シリアルコネクタ** が **リモートアクセスデバイス** に設定されていることを確認します。
- 保存して BIOS セットアッププログラムを終了します。
- システムを再起動します。

IPMI の設定が完了しました。

IPMI シリアルが端末モードの場合は、**racadm config cfgIpmiSerial** コマンドを使って次の設定を追加できます。

- 削除制御
- エコー制御
- ライン編集
- 新しいラインシーケンス
- 新しいラインシーケンスの入力

これらのプロパティの詳細については、IPMI 2.0 規格を参照してください。

IPMI リモートアクセスシリアルインタフェースの使用

IPMI シリアルインタフェースでは、次のモードを使用できます。

- **IPMI 端末モード** - シリアル端末から送信された ASCII コマンドをサポートします。コマンドセット内のコマンド(電源制御を含む)の数は限られていますが、16 進数の ASCII 文字で入力された未処理の IPMI コマンドをサポートしています。
- **IPMI 基本モード** - プログラムへのアクセス用に、Baseboard Management Utility(BMU)に含まれている IPMI シェル(IPMISH)など、バイナリインタフェースをサポートしています。

RACADM を試用して IPMI モードを設定するには、以下の手順を実行します。

1. RAC シリアルインタフェースを無効にします。

   コマンドプロンプトで、次のコマンドを入力します。

   ```
   racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
   ```

2. 適切な IPMI モードを有効にします。

   たとえば、コマンドプロンプトで次のコマンドを入力します。

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 or 1>
   ```

詳細については、「iDRAC6 プロパティデータベースグループとオブジェクト定義」を参照してください。

ウェブベースのインタフェースによる Serial Over LAN の設定

詳細については、「IPMI の設定」を参照してください。

メモ: Serial Over LAN は、次の Dell OpenManage ツールで使用することができます: SOLProxy および IPMItool。詳細については、**support.dell.com¥manuals** で『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

目次ページに戻る

目次ページに戻る

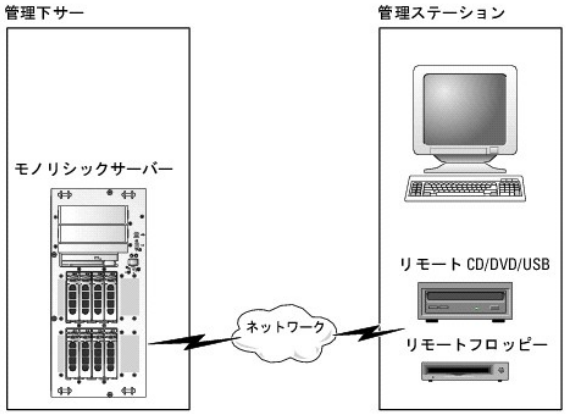
仮想メディアの設定と使用法

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

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 15-1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 15-1 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 およびディスケ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** が連結または自動連結している場合、管理下サーバーからのすべての仮想 CD / フロッピードライブのアクセス要求がネットワーク経由で管理ステーションに転送されます。**仮想メディア** の接続は、メディアを管理下システム上の物理デバイスに挿入することと同じです。**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 15-1 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 15-1 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 フロッピーディスケット）	CD-ROM、DVD、CDRW、CD-ROM メディアとのコンボドライブ
USB フロッピードライブ（1.44 フロッピーディスケット）	ISO9660 フォーマットの CD-ROM/DVD イメージファイル
1.44 フロッピーイメージ	CD-ROM メディアのある USB CD-ROM ドライブ
USB リムーバブルディスク	

Windows ベースの管理ステーション

Microsoft® Windows® オペレーティングシステムが稼動する管理ステーションで **仮想メディア** 機能を実行するには、対応バージョンの Internet Explorer または Firefox と Java ランタイム環境（JRE）をインストールします。詳細については、「対応ウェブブラウザ」を参照してください。

Linux ベースの管理ステーション

Linux オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Firefox の対応バージョンをインストールします。詳細については、「対応ウェブブラウザ」を参照してください。

コンソールリダイレクトプラグインを実行するには、Java ランタイム環境（JRE）が必要です。JRE は、**java.sun.com** からダウンロードできます。JRE バージョン 1.6 以降が推奨されます。

仮想メディアの設定

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** の順に選択します。
3. **設定**→ **仮想メディア** の順にクリックして仮想メディアを設定します。

   表 15-2 は **仮想メディア** の設定値の説明です。
4. 設定が終了したら、**適用** をクリックします。
5. 適切なボタンをクリックして続行します。「表 15-3」を参照してください 。

表 15-2 仮想メディアの設定プロパティ

属性	値
リモートメディアの連結状態	**連結** - 瞬時に **仮想メディア** をサーバーに連結します。 **分離** -瞬時に **仮想メディア** からサーバーを分離します。 **自動連結** - 仮想メディアセッションが開始している場合のみ、**仮想メディア** をサーバーに連結します。
最大セッション数	最大**仮想メディア**セッション数が表示されます。これは、常に 1 です。
アクティブセッション数	仮想メディアの現在のセッション数を表示します。
仮想メディア暗号化の有効	チェックボックスを選択または選択解除して、**仮想メディア** 接続の暗号化を有効または無効にします。選択すると暗号化は有効になり、選択解除すると暗号化は無効になります。
フロッピーのエミュレーション	**仮想メディア** がサーバーにフロッピードライブとして表示されるか USB キーとして表示されるかを示します。**フロッピーのエミュレーション** のチェックボックスがオンの場合、**仮想メディア** デバイスはサーバーでフロッピーデバイスとして表示されます。オフの場合は、USB キードライブとして表示されます。
ブートワンスを有効にする	このチェックボックスをオンにして、**ブートワンス**オプションを有効にします。この属性は、次回の起動時に仮想メディアから起動する場合に使用します。システムは起動順序の次のエントリから起動します。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** セッションを自動的に終了します。

表 15-3 設定ページのボタン

ボタン	説明
印刷	画面に表示されている **設定** ページの値を印刷します。
更新	**設定** ページを再ロードします。
変更の適用	**設定** ページ上の新しい設定を保存します。

仮想メディアの実行

△ **注意: 仮想メディアセッションの実行中は、racreset コマンドを使用しないでください。使用すると、データ損失などの不測の結果が生じます。**

メモ: 仮想メディアにアクセス中、[コンソールビューア] ウィンドウアプリケーションはアクティブな状態であることが必要です。

メモ: Red Hat® Enterprise Linux®（バージョン 4）がマルチ論理ユニット（LUN）の SCSI デバイスを認識できるようにするには、次の手順を実行します。

1. **/ect/modprobe** に次の行を追加します。

   options scsi_mod max_luns=256

   cd /boot

   mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
2. サーバーを再起動します。

3. 仮想 CD/DVD または仮想フロッピーを表示するには、次のコマンドを実行します。

   cat /proc/scsi/scsi

メモ: 仮想メディアを使用する場合、管理下サーバー上の(仮想)ドライブとして仮想化できるのは、管理ステーションのフロッピー /USB ドライブ / イメージ / キー 1 つと、オプティカルドライブ 1 台のみです。

サポートされている仮想メディア設定

フロッピードライブと光ドライブ 1 台ずつの仮想メディアを有効にできます。1 度に仮想化できるのは各メディアタイプのドライブ 1 台のみです。

サポートされているフロッピードライブには 1 つのフロッピーイメージまたは 1 つの空きフロッピードライブがあります。サポートされている光ドライブには、最大 1 台の空き光ドライブまたは 1 つの ISO イメージファイルがあります。

仮想メディアの接続

仮想メディアを実行するには、次の手順を実施します。

1. 管理ステーションで対応ウェブブラウザを開きます。詳細については、「対応ウェブブラウザ」を参照してください。

2. iDRAC6 ウェブインタフェースを開始します。詳細については、「ウェブインタフェースへのアクセス」を参照してください。

3. **システム** → **コンソール/メディア** の順に選択します。

   コンソールリダイレクトおよび仮想メディア ページが表示されます。表示されている属性値を変更する場合は、「仮想メディアの設定」を参照してください。

   メモ: このデバイスは仮想フロッピーとして仮想化できるので、**フロッピーイメージファイル** が **フロッピードライブ** (該当する場合)の下に表示されることがあります。同時に選択できるのは、オプティカルドライブ 1 台と、フロッピー/USB フラッシュドライブ 1 台の仮想化です。

   メモ: 管理下サーバー上の仮想デバイスドライブ文字は、管理ステーション上の物理ドライブ文字とは一致しません。

   メモ: Internet Explorer の 拡張セキュリティが設定されている Windows オペレーティングシステムクライアントでは、**仮想メディア** が正しく機能しないことがあります。この問題を解決するには、Microsoft オペレーティングシステムのマニュアルを参照するか、システム管理者にお問い合わせください。

4. **ビューアの起動** をクリックします。

   メモ: Linux では、ファイル **jviewer.jnlp** がデスクトップにダウンロードされ、ファイルの処置について尋ねるダイアログボックスが表示されます。**プログラムを指定して開く** オプションを選択し、JRE インストールディレクトリの **bin** サブディレクトリにある **javaws** アプリケーションを選択します。

   iDRAC KVM エージェント アプリケーションが別のウィンドウで起動します。

5. **ツール** → **仮想メディアの起動** の順にクリックします。

   メディアリダイレクト ウィザードが表示されます。

   メモ: 仮想メディアセッションを終了する場合を除いて、このウィザードを閉じないでください。

6. メディアが接続している場合は、別のメディアソースに接続する前に切断してください。切断する場合は、メディアの左のチェックボックスをオフにします。

7. 接続するメディアタイプのチェックボックスをオンにします。

   フロッピーイメージまたは ISO イメージを接続する場合は、(ローカルコンピュータ上の)イメージのパスを入力するか、**イメージの追加...** ボタンでイメージを参照します。

   メディアが接続され、**ステータス** ウィンドウが更新します。

仮想メディアの切断

1. **ツール** → **仮想メディアの起動** の順にクリックします。

2. 切断する**メ**ディアのチェックボックスをオフにします。

   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. メディアリダイレクト ウィザードを終了するには、**終了** をクリックします。

仮想メディアからの起動

システム BIOS を使用すると、仮想オプティカルドライブまたは仮想フロッピードライブから起動できるようになります。POST 中、BIOS セットアップウィンドウを開き、仮想ドライブが有効になっており、正しい順序で表示されていることを確認します。

BIOS 設定を変更するには、次の手順を実行してください。

1. 管理下サーバーを起動します。
2. <F2> を押して BIOS 設定ウィンドウを開きます。
3. 起動順序をスクロールして、<Enter> キーを押します。

   ポップアップウィンドウに、仮想オプティカルデバイス と仮想フロッピードライブのリストがその他の標準起動デバイスと共に表示されます。
4. 仮想ドライブが有効で、ブータブルメディア(起動メディア)の最初のデバイスとして表示されていることを確認してください。必要に応じて、画面の指示に従って起動順序を変更します。
5. 変更を保存して終了します。

   管理下サーバーが再起動します。

   管理下サーバーは起動順序に従って、ブータブル(起動)デバイスからの起動を試みます。仮想デバイスが接続済みでブータブルメディアが存在している場合、システムはこの仮想デバイスで起動します。起動メディアがない場合は、ブータブルメディアのない物理デバイスの場合と同様にデバイスを無視します。

仮想メディアを使用したオペレーティングシステムのインストール

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では 15 分以内で完了します。詳細については、「オペレーティングシステムの導入」を参照してください。

1. 次の点を確認します。
   - 管理ステーションの CD ドライブにオペレーティングシステムのインストール CD が挿入されている。
   - ローカルの CD ドライブが選択されている。
   - 仮想ドライブに接続している。
2. 「仮想メディアからの起動」の仮想メディアからの起動手順に従って、BIOS がインストール元の CD ドライブから起動するように設定されていることを確認してください。
3. 画面の説明に従ってセットアップを完了します。

マルチディスクのインストールの場合は、必ず次の手順に従ってください。

1. 仮想メディアコンソールから仮想化(リダイレクトされた) CD/DVD をマップ解除します。
2. リモートオプティカルドライブに次の CD/DVD を挿入します。
3. 仮想メディアコンソールからこの CD/DVD をマッピング(リダイレクト)します。

   再マッピングすることなく、リモートオプティカルドライブに新しい CD/DVD を挿入しても、正常に動作しない可能性があります。

ブートワンス機能

ブートワンス機能は、リモートの仮想メディアデバイスから起動できるように、一時的に起動順序を変更できるようにします。この機能は、一般的にオペレーティングシステムのインストール時に仮想メディアと併用されます。

メモ: この機能を使用するには、**iDRAC6 の設定** 権限が必要です。

メモ: リモートデバイスでこの機能を使用するには、仮想メディアでリダイレクトする必要があります。

ブートワンス機能の使用

1. サーバーに電源を投入し、BIOS 起動マネージャを立ち上げます。
2. リモートの仮想メディアデバイスから起動するように、起動順序を変更します。
3. ウェブインタフェースを介して iDRAC6 にログインし、**システム** → **コンソール/メディア** → **設定** の順にクリックします。
4. 仮想メディアの下の **ブートワンス**を**有効にする** オプションを選択します。
5. サーバーの電源をオフにしてから、再びオンにします。

サーバーは、リモートの仮想メディアデバイスから起動します。次回のサーバーの起動時には、リモートの仮想メディア接続は分離された状態になります。

メモ: 仮想ドライブが起動順序に表示されるには、仮想メディアが **連結** 状態であることが必要です。**ブートワンス** を有効にするには、仮想化されたドライブ内にブータブルメディアがあることを確認します。

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。

仮想メディアについてのよくあるお問い合わせ(FAQ)

表 15-4 は、よくあるお問い合わせとその回答です。

表 15-4 仮想メディアの使い方 :よくあるお問い合わせ(FAQ)

質問	回答
仮想メディアのクライアントの接続が時々切断されます。 どうしてでしょうか。	ネットワークのタイムアウトが発生した場合、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。 仮想メディアの設定を iDRAC6 ウェブインタフェースまたはローカル RACADM コマンドで変更した場合、設定変更が適用されると、接続しているすべてのメディアが切断されます。 仮想ドライブに再接続するには、仮想メディアウィザードを使用します。
どのオペレーティングシステムが iDRAC6 をサポートしていますか。	対応オペレーティングシステムについては、「対応 OS」のリストを参照してください。
どのウェブブラウザが iDRAC6 をサポートしていますか。	対応ウェブブラウザのリストは、「対応ウェブブラウザ」を参照してください。
時々クライアントの接続が切れるのはなぜですか。	• 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。 • ネットワークのタイムアウトが発生した場合、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。また、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。
仮想メディアからの Windows オペレーティングシステムのインストールは時間がかかりすぎるようです。どうしてでしょうか。	『Dell Systems Management Tools and Documentation DVD 』を使用して Windows オペレーティングシステムをインストールするときにネットワーク接続が低速な場合は、ネットワークの遅延により iDRAC6 ウェブベースインタフェースへのアクセスに時間が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。
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。	管理下サーバーで、BIOS セットアップ にアクセスして起動メニューをクリックします。仮想 CD、仮想フロッピー、または仮想フラッシュを見つけて、必要に応じてデバイスの起動順序を変更します。また、CMOS 設定の起動順序で「スペースバー」キーを押すと、仮想デバイスをブータブルにできます。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。 • CDROM/DVD データメディア • ISO 9660 イメージ • 1.44 フロッピーディスクまたはフロッピーイメージ • 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 • 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。 `sys a: x: /s` x: は、ブータブルにする USB キーです。
Red Hat Enterprise Linux または SUSE® Linux オペレーティングシステムが稼動するシステム上で仮想フロッピーデバイスを見つけることができません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。	一部の Linux バージョンは仮想フロッピードライブと仮想 CD ドライブを同じ方法で自動マウントしません。仮想フロッピードライブをマウントするには、Linux が仮想フロッピードライブに割り当てたデバイスノードを検索します。仮想フロッピードライブを正しく見つけてマウントするには、次の手順を実行してください。 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。

	grep "Virtual Floppy" /var/log/messages 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。 grep "hh:mm:ss" /var/log/messages このコマンドで、 hh:mm:ss は、手順 1 で grep から返されたメッセージのタイムスタンプです。 4. 手順 3 で、grep コマンドの結果を読み、DELL 仮想フロッピー のデバイス名を探します。 5. 仮想フロッピードライブに連結し接続していることを確認します。 6. Linux のプロンプトで次のコマンドを入力します。 mount /dev/sdx /mnt/floppy このコマンドで、 /dev/sdx は、ステップ 4 で見つけたデバイス名です。 /mnt/floppy はマウントポイントです。
Red Hat Enterprise Linux または SUSE Linux オペレーティングシステムが稼動するシステム上で仮想フロッピー / 仮想 CD デバイスを見つけることができません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。	(回答の続き) 仮想 CD ドライブをマウントするには、Linux が仮想 CD ドライブに割り当てるデバイスノードを検索します。仮想 CD ドライブを見つけ、マウントするには、次の手順に従います。 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。 grep "Virtual CD" /var/log/messages 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。 grep "hh:mm:ss" /var/log/messages パラメータ hh:mm:ss は、ステップ 1 で grep から返されたメッセージのタイムスタンプです。 4. ステップ 3 で、grep コマンドの結果を読み込んで、「Dell Virtual CD」に与えられたデバイス名を検索します。 5. 仮想 CD ドライブに連結し、接続していることを確認します。 6. Linux のプロンプトで次のコマンドを入力します。 mount /dev/sdx /mnt/CD このコマンドで、 /dev/sdxはステップ 4 で見つけたデバイス名です。 /mnt/floppy はマウントポイントです。
iDRAC6 ウェブインタフェースを使用してファームウェアのアップデートをリモートで実行すると、サーバーで仮想ドライブが削除されました。どうしてでしょうか。	ファームウェアのアップデートによって iDRAC6 がリセットされ、リモート接続が切断して仮想ドライブがアンマウントされます。
USB デバイスを接続すると、すべての USB デバイスが分離されるのはなぜですか。	仮想メディアデバイスおよび仮想フラッシュデバイスは、複合 USB デバイスとしてホスト USB バスに接続しているため、共通の USB ポートを共有しています。仮想メディアまたは仮想フラッシュ USB デバイスがホスト USB バスに接続したり切断されたりすると、すべての仮想メディアと仮想フラッシュデバイスが一時的にホスト USB バスから切断されてから、再接続します。仮想メディアデバイスがホストオペレーティングシステムで使用されている場合は、仮想メディアデバイスや仮想フラッシュデバイスの連結や分離を避ける必要があります。使用する前に、必要な USB デバイスをすべて接続することをお勧めします。
USB リセットボタンの機能は何ですか。	サーバーに接続されたリモートおよびローカル USB デバイスをリセットします。

目次ページに戻る

目次ページに戻る

iDRAC 設定ユーティリティの使用

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

概要

iDRAC 設定ユーティリティは、iDRAC6 と管理下サーバーのパラメータを表示および設定できる起動前の設定環境です。具体的には、以下のことが可能です。

- iDRAC6 および一次バックプレーンのファームウェアリビジョン番号を表示する
- iDRAC6 ローカルエリアネットワークを有効または無効にする
- IPMI オーバー LAN を有効または無効にする
- LAN パラメータを設定する
- 仮想メディアを設定する
- スマートカードを設定する
- システム管理者のユーザー名とパスワードを変更する
- iDRAC 設定を出荷時のデフォルトに戻す
- 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。
- LCD を設定する
- システムデバイスを設定する

iDRAC 設定ユーティリティを使用して実行できるタスクは、SM-CLP コマンドラインインタフェースやローカル RACADM コマンドラインインタフェースなどの iDRAC または Dell™ OpenManage™ ソフトウェアで提供されるその他のユーティリティを使用して実行することも可能です。

---

iDRAC 設定ユーティリティの起動

1. サーバーの前面にある電源ボタンを押してサーバーの電源を入れるか、再起動します。
2. **<Ctrl-E> を押して 5 秒 以内にリモートアクセスのセットアップを .....**というメッセージが表示されたら、すぐに <Ctrl><E> を押します。

メモ: <Ctrl><E> キーを押す前にオペレーティングシステムがロードを開始した場合は、起動が完了するのを待ってからシステムを再起動して、もう一度やり直してください。

iDRAC 設定ユーティリティが表示されます。最初の 2 行に、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、ウェブベースのインタフェース、SM-CLP、ウェブインタフェースなど、外部インタフェースに関連する情報の一部です。一次バックプレーンファームのファームウェアは、サーバーのハードウェア環境とインタフェースし、それを監視するファームウェアの一部です。

---

iDRAC 設定ユーティリティの使用

ファームウェアのリビジョンメッセージの下の iDRAC 設定ユーティリティの残りの部分は、上方向キーと下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。

- 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。
- 項目に [はい / いいえ]、[有効 / 無効] など選択可能な値がある場合は、左方向キー、右方向キー、またはスペース キーを押して値を選択します。
- 編集不可の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。
- 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。
- iDRAC 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。ここで、変更内容の保存または破棄を選択したり、ユーティリティに戻ったりできます。

次の項では、iDRAC 設定ユーティリティのメニュー項目について説明します。

iDRAC6 LAN

<左方向>、<右方向>、およびスペースキー使用して **オン** または **オフ** を選択します。

iDRAC6 LAN は、デフォルト設定では有効になっています。ウェブベースのインタフェース、telnet/SSH、コンソールリダイレクト、仮想メディアなどの iDRAC6 装置を使用できるようにするには、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。

`iDRAC6 Out-of-Band interface will be disabled if the LAN Channel is OFF. (LAN チャネルがオフの場合、iDRAC6 帯域外インタフェースは無効になります。)`

`Press any key to clear the message and continue. (いずれかのキーを押してメッセージをクリアし、続行します。)`

このメッセージは、LAN が無効になっていると、iDRAC6 HTTP、HTTPS、Telnet、または SSH ポートに直接接続している装置にアクセスできないだけでなく、管理ステーションから iDRAC6 に送信される IPMI メッセージなどの帯域外管理ネットワークトラフィックも受信できないことを知らせます。ただし、ローカル RACADM インタフェースは引き続き使用可能で、iDRAC6 LAN の再設定に使用できます。

IPMI オーバー LAN

<左方向>、<右方向>、およびスペースキーを押して **オン** または **オフ** を選択します。**オフ** を選択すると、iDRAC6 は LAN インタフェース経由の IPMI メッセージを受け入れません。

オフ を選択すると、次の警告が表示されます。

`iDRAC IPMI Over LAN 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 IPMI オーバー LAN 帯域外インタフェースは無効になります。)`

任意のキーを押してメッセージをクリアし、続行します。メッセージの説明は、「iDRAC6 LAN」を参照してください。

LAN パラメータ

LAN パラメータのサブメニューを表示するには、Enter キーを押します。LAN パラメータの設定を終えた後、Esc キーを押すと、前のメニューに戻ります。

表 18-1 LAN パラメータ

項目	説明
共通設定	
NIC の選択	<右方向>、<左方向>、およびスペースキーを押して、モードを切り替えます。 **専用**、**共有**、**フェールオーバーで共有 (LOM2)**、**フェールオーバーで共有 (すべてのLOM)** のモードがあります。 これらのモードは、iDRAC が対応するインタフェースを外部との通信に使用できるようにします。
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能な MAC アドレスです。
VLAN の有効化	iDRAC6 の仮想 LAN フィルタを有効にするには、**オン** を選択します。
VLAN Id	**VLAN を有効にする** を **オン** に設定する場合は、VLAN ID を 1 ～ 4094 の範囲で入力します。
VLAN	**VLAN を有効にする** を **オン** に設定する場合は、VLAN の優先度を 0 ～ 7 の範囲で選択します。
iDRAC6 名の登録	**オン** を選択すると、DNS サービスに iDRAC6 名を登録できます。DNS でユーザーが iDRAC6 の名前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。ドメイン名は、有効な DNS ドメイン (例:mycompany.com) でなければなりません。
ホスト名文字列	Enter キーを押して編集します。プラットフォームイベントトラップ (PET) 警告を有効にするホスト名を入力します。
LAN 警告有効	PET LAN 警告を有効にするには、**オン** を選択します。
警告ポリシーエントリ 1	**有効** または **無効** を選択すると、最初の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 設定	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。
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、iDRAC6 に割り当てる IP アドレスを入力します。 デフォルトは **192.168.0.120** です。
サブネットマスク	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得したサブネットマスクアドレスが表示されます。

	IP アドレスソース を **静的** に設定する場合は、iDRAC6 のサブネットマスクを入力します。デフォルトは **255.255.255.0** です。
デフォルトゲートウェイ	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイのアドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。デフォルトは **192.168.0.1** です。
DHCP からの DNS サーバー	**オン** を選択すると、ネットワーク上の DHCP サービスから DNS サーバーアドレスが取得されます。**オフ** を選択すると、下記の DNS サーバーアドレスを指定できます。
DNS サーバー 1	**DHCP からの DNS サーバー** が **オフ** の場合、最初の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	**DHCP からの DNS サーバー** が **オフ** の場合、2 番目の DNS サーバーの IP アドレスを入力します。
IPv6 の設定	IPv6 接続に対するサポートを有効または無効にします。
IP アドレスソース	**AutoConfig（自動設定）** または **静的** 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、iDRAC6 に割り当てる IP アドレスを入力します。
プレフィックス長	IPv6 アドレスのプレフィックス長を設定します。この値は、1 ～ 128 です。
デフォルトゲートウェイ	**IP アドレスソース** を **AutoConfig（自動設定）** に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイの IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。
IPv6 リンクローカルアドレス	これは、iDRAC ネットワークインタフェースの編集不可の **IPv6 リンクローカルアドレス** です。
IPv6 アドレス 2	これは、iDRAC ネットワークインタフェースの編集不可の **IPv6 アドレス 2** です。
DHCP からの DNS サーバー	**オン** を選択すると、ネットワーク上の DHCP サービスから DNS サーバーアドレスが取得されます。**オフ** を選択すると、下記の DNS サーバーアドレスを指定できます。
DNS サーバー 1	**DHCP からの DNS サーバー** が **オフ** の場合、最初の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	**DHCP からの DNS サーバー** が **オフ** の場合、最初の DNS サーバーの IP アドレスを入力します。
LAN 詳細設定	
オートネゴシエート	**NIC の選択** を **専用** に設定する場合は、**有効** か **無効** かを選択します。 **有効** を選択した場合は、**LAN スピード設定** と **LAN デュプレックス設定** が自動的に設定されます。
LAN の速度設定	**オートネゴシエート** を **無効** に設定する場合は、10Mbps または 100Mbps を選択します。
LAN の二重設定	**オートネゴシエート** を **無効** に設定する場合は、**半二重 または 全二重** を選択します。

仮想メディアの設定

仮想メディア

<Enter> キーを押して、**分離**、**連結**、または**自動連結**を選択します。**連結** を選択すると、仮想メディアデバイスが USB バスに接続され、**コンソールリダイレクト** セッション中に使用可能になります。

分離 を選択すると、ユーザーは **コンソールリダイレクト** セッション中に仮想メディアデバイスにアクセスできません。

メモ: **仮想メディア** 機能で USB フラッシュドライブを使用するには、BIOS 設定ユーティリティで **USB フラッシュドライブのエミュレーションタイプ** を **ハードディスク** に設定してください。BIOS 設定ユーティリティへは、サーバー起動中に< F2> キーを押すとアクセスできます。**USB フラッシュドライブのエミュレーションタイプ** が **自動** に設定されていると、フラッシュドライブはシステムでフロッピードライブとして表示されます。

仮想フラッシュ

<Enter> キーを押して、**無効** または **有効** を選択します。

有効 / **無効** に選択することにより、すべての仮想メディアデバイスが USB バスから **分離** または **連結** されます。

無効 にすると、仮想フラッシュが取り外され使用できなくなります。

メモ: 256 MB 以上の容量を持つ SD カードが iDRAC6 Express カードスロットに存在しない場合は、このフィールドは読み取り専用になります。

スマートカードのログオン

<Enter> キーを押して、**無効** または **有効** を選択します。このオプションは、スマートカードログイン機能を設定します。**有効**、**無効**、**RACADM で有効** のオプションがあります。

メモ: **有効** を選択した場合は、**IPMI オーバー LAN** がオフになり、編集不可になります。

システムサービス設定

システムサービス

<Enter> キーを押して、**無効** または **有効** を選択します。詳細については、デルサポートサイト **support.dell.com¥manuals** にある『Dell Unified Server Configurator ユーザーズガイド』を参照してください。

メモ: このオプションを変更し、**保存** し、**終了** して新しい設定を適用すると、サーバーが再起動します。

システムサービスのキャンセル

<Enter> キーを押して、**いいえ** または **はい** を選択します。

はい を選択した場合は、**保存** し、**終了** して新しい設定を適用すると、すべての Unified Server Configurator セッションが閉じてサーバーが再起動します。

LCD の設定

LCD 設定 サブメニューを表示するには、<Enter> キーを押します。LCD パラメータの設定を終えた後、<Esc> キーを押すと、前のメニューに戻ります。

表 18-2 LCD ユーザー設定

LCD ライン 1	<右方向>、<左方向>、およびスペースキーを押して、オプションを切り替えます。 この機能は、LCD の **ホーム** 表示を次のいずれかのオプションに設定します。 **周辺温度**、**管理タグ**、**ホスト名**、**iDRAC6 IPv4 アドレス**、**iDRAC6 IPv6 アドレス**、**iDRAC6 MAC アドレス**、**モデル番号**、**なし**、**サービスタグ**、**システム電源**、**ユーザー定義の文字列**。
LCD ユーザー定義の文字列	**LCD ライン 1** を **ユーザー定義の文字列** に設定した場合は、LCD に表示する文字列を入力します。 文字列は最大 62 文字まで入力できます。
LCD システム電力単位	**LCD ライン 1** を **システム電源** に設定した場合は、LCD に表示する単位を **ワット** または **BTU/時** から選択します。
LCD 周辺温度単位	**LCD ライン 1** を **周辺温度** に設定した場合は、LCD に表示する単位を **摂氏** または **華氏** から選択します。
LCD エラー表示	**Simple(簡易)** または **SEL**(システムイベントログ) を選択します。 この機能を使用すると、次のいずれかの形式で LCD にエラーメッセージを表示できます。 簡易フォーマットは、イベントの説明を英語で表示します。 SEL フォーマットは、システムイベントログのテキスト文字列を表示します。
LCD のリモート KVM 表示	装置で仮想 KVM がアクティブの間、テキスト KVM を表示するには、**有効** を選択します。
LCD フロントパネルアクセス	<右方向>、<左方向>、およびスペースキーを押して、**無効**、**表示 / 変更**、**表示のみ** のオプション間を切り替えます。 この設定は、LCD に対するユーザーのアクセスレベルを決定します。

LAN ユーザー設定

LAN ユーザーは iDRAC の Administrator(システム管理者)アカウント(デフォルトで **root[ルート]**)です。LAN ユーザー設定のサブメニューを表示するには、Enter キーを押します。LAN ユーザーの設定を終えて、Esc キーを押すと、前のメニューに戻ります。

表 18-3 LAN ユーザー設定

項目	説明
アカウントアクセス	**有効** を選択すると Administrator(システム管理者)アカウントが有効になります。**無効** を選択すると 管理者アカウントが無効になります。
アカウント権限	**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。
アカウントユーザー名	Enter キーを押してユーザー名を編集し、終了したら Esc キーを押します。デフォルトのユーザー名は **ルート** です。
パスワードの入力	Administrator(システム管理者)アカウントの新しいパスワードを入力します。入力時に文字は表示されません。
パスワードの確認	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 **パスワードの入力** 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、パスワードの再入力が必要になります。

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になる可能性があります。

Enter キーを押して項目を選択します。次の警告メッセージが表示されます。

Resetting to factory defaults will restore remote Non-Volatile user settings. Continue? (出荷時のデフォルト設定に戻すと、リモートの非揮発性ユーザー設定が復元されます。続行しますか ?)

< NO (Cancel) > (<いいえ（キャンセル） >)

< YES (Continue) > (<はい（続行）>)

はい を選択し、Enter キーを押すと iDRAC はデフォルト設定に戻ります。

システムイベントログメニュー

システムイベントログ メニューでは、システムイベントログ（SEL）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。左方向キーを使用すると、前の（古い）メッセージに移動し、右方向キー を押すと次の（新しい）メッセージに移動します。レコード番号を入力すると、そのレコードに移動します。SEL メッセージの表示を終了するには、Esc キーを押します。

SEL メッセージをクリアするには、**システムイベントログのクリア** を選択して Enter キーを押します。

SEL メニューの使用を終えて、Esc キーを押すと、前のメニューに戻ります。

iDRAC 設定ユーティリティの終了

iDRAC 設定の変更を完了して 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、変更が保存されます。

変更を保存せずに終了 を選択して Enter キーを押すと、変更は保存されません。

セットアップに戻る を選択して Enter キーを押すと、iDRAC 設定ユーティリティに戻ります。

目次ページに戻る

目次ページに戻る

監視と警告管理

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

ここでは、iDRAC6 の監視方法と、システムと iDRAC6 が警告を受け取るように設定する手順を説明します。

管理下システムに前回クラッシュ画面の取り込みを設定する方法

iDRAC6 が前回クラッシュ画面を取り込めるようにするには、管理下システムの次の必須項目を設定する必要があります。

1. 管理下システムソフトウェアをインストールします。管理下システムソフトウェアのインストールについては、『Server Administrator ユーザーズガイド』を参照してください。
2. **Windows の起動とリカバリ設定** で Windous の「自動再起動」機能をオフにした状態で、サポートされている Microsoft® Windows® オペレーティングシステムを実行します。
3. 前回クラッシュ画面を有効にする（デフォルト=無効）。

   ローカル RACADM を使って前回クラッシュ画面機能を有効にするには、コマンドプロンプトで次のコマンドを入力します。

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

4. 自動リカバリタイマーを有効にして、**自動リカバリの**処置を**リセット**、**電源を切る**、または **電源を入れ直す** に設定します。**自動リカバリ** タイマーを設定するには、Server Administrator または IT Assistant を使用する必要があります。

   自動リカバリ の設定手順については、『 Server Administrator ユーザーズガイド』を参照してください。前回のクラッシュ画面を取り込めるように、**自動リカバリ** タイマーを 60 秒以上に設定してください。デフォルト設定は 480 秒です。

   自動リカバリの処置が **シャットダウン** または **電源の入れ直し** に設定されている場合は、管理下システムがクラッシュしたときに前回のクラッシュ画面は使用できません。

Windows の 自動再起動オプションを無効にする

iDRAC6 のウェブインタフェースの前回クラッシュ画面機能が正しく機能するように、Microsoft Windows Server? 2008 および Windows Server 2003 オペレーティングシステムを実行している管理下システムで、**自動再起動** オプションを無効にします。

Windows 2008 Server の自動再起動オプションを無効にする

1. Windows **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. 左側の **タスク** の下にある **詳細システム設定** をクリックします。
3. **詳細** タブをクリックします。
4. **起動と回復** で **設定** をクリックします。
5. **自動再起動** チェックボックスをオフにします。
6. **OK** を 2 度クリックします。

Windows Server 2003 の自動再起動オプションを無効にする

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

4. **自動再起動** チェックボックスをオフにします。

5. **OK** を 2 度クリックします。

プラットフォームイベントの設定

プラットフォームイベントの設定では、リモートアクセスデバイスが特定のイベントメッセージに応答して、選択した処置を実行するように指定できます。これらの処置には、再起動、電源の入れ直し、電源オフ、警告のトリガ(プラットフォームイベントトラップ [PET] または電子メール)などがあります。

フィルタ可能なプラットフォームイベントには、以下のようなイベントがあります。

- ファン重要アサートフィルタ
- バッテリー警告アサートフィルタ
- バッテリー重要アサートフィルタ
- 低電圧重要アサートフィルタ
- 温度警告アサートフィルタ
- 温度重要アサートフィルタ
- イントルージョン重要アサートフィルタ
- 冗長性低下フィルタ
- 冗長性喪失フィルタ
- プロセッサ警告アサートフィルタ
- プロセッサ重要アサートフィルタ
- プロセッサ不在フィルタ
- プロセッサ供給警告アサートフィルタ
- プロセッサ供給重要アサートフィルタ
- プロセッサ供給不在アサートフィルタ
- イベントログ重要アサートフィルタ
- ウォッチドッグ重要アサートフィルタ
- システム電源警告アサートフィルタ
- システム電源重要アサートフィルタ

プラットフォームイベントが発生すると(ファンプローブエラーなど)、システムイベントが生成されてシステムイベントログ(SEL)に記録されます。このイベントがウェブベースインタフェースのプラットフォームイベントフィルタリストにあるプラットフォームイベントフィルタ(PEF)と一致し、このフィルタが警告(PET または 電子メール)を生成するように設定されていると、PET または電子メール警告が 1 つまたは複数の宛先に送信されます。

同じプラットフォームイベントフィルタで別の処置(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

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、プラットフォームのイベントフィルタを設定します。

ウェブベースインタフェースを使用した PEF の設定

詳細については、「プラットフォームイベントフィルタ(PEF) の設定」を参照してください。

RACADM CLI を使った PEF の設定

1. PEF を有効にします。

   コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
   ```

   1 と 1 は、それぞれ PEF のインデックスと、有効 / 無効の選択です。

   PEF インデックス値は 1 ～ 19 です。有効 / 無効の選択は、1(有効)または 0(無効)です。

   たとえば、PEF をインデックス 5 で有効にするには、次のコマンドを入力します。

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
   ```

2. PEF の処置を設定します。

   コマンドプロンプトに次の内容を入力し、<Enter> を押します。

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <処置>
   ```

   <処置> の値ビットは次のとおりです。

   - 0 = 警告処置なし
   - 1 = サーバーの電源を切る
   - 2 = サーバーを再起動する
   - 3 = サーバーの電源を入れ直す

   たとえば、PEF でサーバーを再起動するには次のコマンドを入力します。

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
   ```

   1 は PEF インデックス、2 は PEF 処置を再起動に設定します。

PET の設定

ウェブインタフェースを使用した PET の設定

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。

RACADM CLI を使用した PET の設定

1. グローバル警告を有効にします。

   コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. PET を有効にします。

   コマンドプロンプトで以下のコマンドを入力し、各コマンドの後で <Enter> を押します。

   ```
   IPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
   ```

   ```
   IPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 1 1
   ```

   1 と 1 は、それぞれ PET の送信先インデックスと、有効 / 無効の選択です。

   PET の送信先インデックスは 1 ～ 4 です。有効 / 無効の選択は 1(有効)または 0(無効)に設定できます。

   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。

   ```
   iPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
   ```

   ```
   iPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 4 1
   ```

3. PET ポリシーを設定します。

   コマンドプロンプトで次のコマンドを入力して <Enter> を押します。

   ```
   iPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IPv4_address>
   ```

   ```
   iPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6_address>
   ```

   1 は PET の送信先インデックスで、<IPv4_address> と <IPv6_address> はプラットフォームイベント警告の送信先 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>
   ```

電子メール警告の設定

ウェブインタフェースを使用した電子メール警告の設定

詳細については、「電子メール警告の設定」を参照してください。

RACADM CLI を使用した電子メール警告の設定

1. グローバル警告を有効にします。

   コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. 電子メール警告を有効にします。

   コマンドプロンプトで次のコマンドを入力し、各コマンドの後で <Enter> を押します。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
   ```

   1 と 1 は、それぞれ電子メール送信先のインデックスと、有効 / 無効の選択です。

   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。有効 / 無効の選択は、1(有効)または 0(無効)を設定できます。

   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 cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. 電子メール設定を指定します。

   コマンドプロンプトで次のコマンドを入力して <Enter> を押します。

   ```
   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の送信先の電子メールアドレスです。

   カスタムメッセージを設定するには、コマンドプロンプトに次の内容を入力し、Enter を押します。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <カスタムメッセージ>
   ```

   1 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> は電子メール警告に表示されるメッセージです。

電子メール警告のテスト

RAC 電子メール警告機能を使用すると、ユーザーは管理下システムで重大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、RAC がネットワークで正しく電子メール警告を送信できるかどうかを確認するために、電子メール警告機能をテストする方法を示しています。

```
racadm testemail -i 2
```

メモ: 電子メール警告機能のテストを行う前に、**SMTP** と**電子メール警告** 設定が指定されていることを確認してください。詳細については、「電子メール警告の設定」を参照してください。

RAC SNMP トラップ警告機能のテスト

RAC SNMP トラップ警告機能を使用すると、管理下システム上で発生したシステムイベントのトラップを SNMP トラップリスナー設定で受信できます。

次の例で、ユーザーが RAC の トラップ警告機能をテストする例を示します。

```
racadm testtrap -i 2
```

RAC SNMP トラップ警告機能をテストする前に、SNMP とトラップの設定が正しく設定されていることを確認してください。これらの設定の指定方法については、「**testtrap**」と「**sslkeyupload**」のサブコマンドの説明を参照してください。

SNMP 認証についてよくあるお問い合わせ(FAQ)

どうして次のメッセージが表示されるのでしょうか?

```
Remote Access: SNMP Authentication Failure (リモートアクセス : SNMP 認証エラー)
```

検出作業の一部として、IT Assistant はデバイスの get と set コミュニティ名の確認を試みます。IT Assistantには、get **community name = public** と set **community name =**

private があります。iDRAC6 エージェントのデフォルトコミュニティ名は **public** です。IT Assistant が set リクエストを送信すると、iDRAC6 エージェントは**コミュニティ = public**からのリクエストしか受け入れないため、SNMP 認証エラーが生成されます。

メモ: これは、検出に使う SNMP エージェントコミュニティです。

RACADM を使用して、iDRAC6 のコミュニティ名を変更できます。

iDRAC6 コミュニティ名を表示するには、次のコマンドを使用します。

```
racadm getconfig -g cfgOobSnmp
```

iDRAC6 コミュニティ名を設定するには、次のコマンドを使用します。

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <コミュニティ名>
```

ウェブインタフェースを使って iDRAC6 SNMP エージェントコミュニティ名にアクセス/設定するには、リモートアクセス → **設定** → **サービス** に進み、**SNMP エージェント** を クリックします。

SNMP 認証エラーが生成されないように、エージェントに受け入れられるコミュニティ名を入力する必要があります。iDRAC6 では 1 つしかコミュニティ名を許可しないので、同じ **get** と **set** コミュニティ名をIT Assistant の検出設定用に使用しなければなりません。

目次ページに戻る

目次ページに戻る

管理下システムの修復とトラブルシューティング

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

ここでは、iDRAC6 ウェブベースのインタフェースを使用して、クラッシュしたリモートシステムの修復とトラブルシューティングに関連するタスクを実行する方法について説明します。

- 「リモートシステムのトラブルシューティングの第一歩」
- 「リモートシステムの電源管理」
- 「IPv6 情報」
- 「前回システムクラッシュ画面の表示」

リモートシステムのトラブルシューティングの第一歩

以下は、管理下システムで発生する複雑な問題をトラブルシューティングする際に確認すべき事項です。

1. システムの電源はオンになっていますか、オフになっていますか?
2. 電源がオンの場合は、オペレーティングシステムが正しく機能していますか、それともクラッシュまたはフリーズしていますか?
3. 電源がオフの場合は、突然オフになりましたか?

システムがクラッシュした場合は、前回のクラッシュ画面を確認し（「前回システムクラッシュ画面の表示」を参照）、コンソールリダイレクトとリモート電源管理（「リモートシステムの電源管理」を参照）を使用してシステムを再起動し、その過程を見てください。

リモートシステムの電源管理

iDRAC6 では、管理下システムでシステムクラッシュ、またはその他のシステムイベントが発生した後、リモートで電源管理処置を実行して修復できます。

iDRAC6 ウェブインタフェースからの電源制御処置の選択

ウェブインタフェースを使用して電源管理処置を実施するには、「サーバーに対する電源制御操作の実行」を参照してください。

iDRAC6 CLI からの電源制御処置の選択

`racadm serveraction` サブコマンドを使用すると、ホストシステムの電源を管理できます。

```
racadm serveraction <処置>
```

<処置> の文字列のオプションは以下のとおりです。

- **powerdown** - 管理下システムの電源を切ります。
- **powerup** - 管理下システムの電源を入れます。
- **powercycle** - 管理下システムの電源を入れ直します。これは、システムのフロントパネルの電源ボタンを押してシステムの電源を切ってから入れ直す操作に似ています。
- **powerstatus** - サーバーの現在の電源状態を表示します（「オン」または「オフ」）。
- **hardreset** - 管理下システムのリセット（再起動）を行います。

システム情報の表示

システム概要 ページには、次のシステムコンポーネントに関する情報が表示されます。

- メインシステムシャーシ

- Integrated Dell Remote Access Controller 6 - Enterprise

システム情報にアクセスするには、**システム** ツリーを展開して **プロパティ** をクリックします。

メインシステムシャーシ

表 20-1 と 表 20-2 に、システムシャーシのプロパティを示します。

メモ: ホスト名 と **OS 名** の情報を受け取るには、管理下システムに iDRAC6 サービスをインストールしておく必要があります。

表 20-1 システム情報フィールド

フィールド	説明
説明	システムの説明
BIOS バージョン	システム BIOS バージョン
サービスタグ	システムのサービスタグナンバー
ホスト名	ホストシステム名
OS 名	システムで実行しているオペレーティングシステム

表 20-2 自動リカバリのフィールド

フィールド	説明
リカバリ処置	「システムハング」が検知されたときに、iDRAC6 に次の処置を行うように設定できます：処置なし、ハードリセット、電源を切る、電源を入れ直す。
初期カウントダウン	「システムハング」が検知されてから iDRAC6 が修復処置を実行するまでの秒数。
現在のカウントダウン	カウントダウンタイマーの現在の値（秒）。

Integrated Dell Remote Access Controller 6 Enterprise

表 20-3 では、iDRAC6 Enterprise のプロパティを説明しています。

表 20-3 iDRAC6 Enterprise の情報フィールド

フィールド	説明
日時	現在の時刻（以下の形式で表記）： 日 月 DD HH:MM:SS:YYYY
ファームウェアバージョン	iDRAC ファームウェアバージョン。
ファームウェアアップデート	ファームウェアが最後にフラッシュされた日付（以下のフォーマットで表記）： 日 月 DD HH:MM:SS:YYYY
ハードウェアバージョン	リモートアクセスコントローラのバージョン。
MAC 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

IPv4 情報

表 20-4 は、IPv4 プロパティについて説明しています。

表 20-4 IPv4 の情報フィールド

フィールド	説明
有効	はい または いいえ
IP アドレス	ホストへのネットワークインタフェースカード（NIC）を識別する 32 ビットアドレス。値は、143.166.154.127 のようなドット区切りの形式で表示されます。
サブネットマスク	サブネットマスクは、IP アドレスを構成する拡張ネットワークプレフィックスとホスト番号の部分を示します。値は、255.255.0.0 のようなドット区切りの形式で表示されます。
ゲートウェイ	ルーターまたはスイッチのアドレス。値は、143.166.154.1 のようなドット区切りの形式で表示されます。
DHCP 有効	[はい] または [いいえ] 動的ホスト構成プロトコル（DHCP）が有効かどうかを示します。

IPv6 情報

表 20-5 は、IPv6 プロパティについて説明しています。

表 20-5 IPv6 の情報フィールド

フィールド	説明
有効	Ipv6 スタックが有効であるかを示します。
IP アドレス 1	iDRAC6 の NIC IPv6 アドレスを指定します。
プレフィックス長	IPv6 アドレスのプレフィックス長を指定する整数。この値は 1 ～ 128 です。
IP ゲートウェイ	iDRAC6 の NIC ゲートウェイを指定します。
リンクのローカルアドレス	iDRAC6 の NIC IPv6 アドレスを指定します。
IP アドレス 2	iDRAC6 の追加のIC IPv6 アドレスがある場合は指定します。
Auto Config（自動設定）	AutoConfig（自動設定）は、Server Administrator が動的ホスト構成プロトコル（DHCPv6）サーバーから iDRAC NIC の IPv6 アドレスを取得できるようにします。また、静的 IP アドレス、プレフィックス長および静的ゲートウェイの値を無効にし、フラッシュします。

システムイベントログ（SEL）の使用

SEL ログ ページには、管理下システムで発生するシステムの重要イベントが表示されます。

システムイベントログを表示するには、次の手順を実行してください。

1. **システム** ツリーの **システム** をクリックします。
2. **ログ** タブをクリックしてから **システムイベントログ** をクリックします

   システムイベントログ ページには、イベントの重大度と、「表 20-6」に示すようなその他の情報が表示されます。
3. **システムイベントログ** ページの適切なボタンをクリックして続行します（「表 20-6」を参照）。

表 20-6 状態インジケータのアイコン

アイコン / カテゴリ	説明
	緑のチェックマークは、正常（平常）ステータスを示します。
	感嘆符の入った黄色の三角形は、警告（非重要）ステータスを示します。
	赤い X は、重要（エラー）ステータスを示します。
	疑問符のアイコンは、不明なステータスを示します。
日時	イベントが発生した日時。日付が空白の場合は、システム起動時にイベントが実行されます。24 時間制 mm/dd/yyyy hh:mm:ss の形式です。
説明	イベントの短い説明

表 20-7 SEL ページのボタン

ボタン	動作
印刷	**ウィンドウに表示される**並び順に SEL を**印刷します**。
更新	**SEL** ページを再ロードします。
ログのクリア	**SEL** をクリアします。 **メモ:** **ログのクリア** ボタンは、**ログのクリア** 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、選択したディレクトリに **SEL** を保存できます。 **メモ:** Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト **support.microsoft.com** から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。

コマンドラインを使ってシステムログを表示する

```
racadm getsel -i
```

getsel -i コマンドは SEL 内のエントリ数を表示します。

```
racadm getsel <オプション>
```

メモ: 引数を何も指定しないと、ログ全体が表示されます。

メモ: 使用できるオプションの詳細については、「getsel」を参照してください。

clrsel コマンドは SEL から既存のレコードをすべて削除します。

```
racadm clrsel
```

POST 起動ログの使用

メモ: iDRAC6 を再起動すると、すべてのログはクリアされます。

iDRAC6 のこの機能を使用すると、BIOS POST 起動の最後の 3 つのインスタンスとオペレーティングシステム起動のストップモーションビデオを再生できます。

POST 起動のキャプチャログを表示するには、以下の手順を実行します。

1. **システム** ツリーの **システム** をクリックします。
2. **ログ** タブをクリックしてから、**起動キャプチャ** タブをクリックします。
3. POST 起動キャプチャログのログ番号を選択し、**再生** をクリックします。

   新しい画面にログのビデオが再生されます。

   メモ: 他のビデオを再生するには、開いている POST 起動ログのビデオを閉じる必要があります。2 つのログを同時に再生することはできません。
4. POST キャプチャログのビデオを再生するには、**再生** → **開始** の順にクリックします。
5. ビデオを停止するには、**終了** をクリックします。

起動中に **F10** を押すと、USC(Unified Server Configurator)アプリケーションの開始時に iDRAC6 Express Card が iDRAC6 に接続します。接続に成功すると、SEL と LCD に`iDRAC6 Upgrade Failed` (`iDRAC6` のアップグレードに成功しました)というメッセージが記録されます。接続に失敗すると、SEL と LCD に「`iDRAC6` のアップグレードに失敗しました」というメッセージが記録されます。さらに、特定のプラットフォームをサポートしていない古いファームウェア iDRAC6 ファームウェアが含まれている iDRAC6 Express Card をマザーボードに挿入してシステムを起動すると、`iDRAC firmware is out-of-date` (iDRAC ファームウェアが最新ものではありません)というログが `POST` 画面に生成されます。最新のファームウェアにアップデートしてください。指定のプラットフォームに対しては最新の iDRAC6 ファームウェアで iDRAC6 Express Card をアップデートします。詳細については、『Dell Unified Server Configurator ユーザーズガイド』と『Dell Unified Server Configurator- Lifecycle Controller Enabled ユーザーズガイド』を参照してください。

前回システムクラッシュ画面の表示

メモ: 前回クラッシュ画面の機能を使用するには、管理下システムの Server Administrator に **自動リカバリ** 機能が設定されている必要があります。また、iDRAC6 を使用した **自動システム修復** 機能が有効になっていることを確認します。この機能は、**リモートアクセス** セクションの **設定** タブにある **サービス** ページで有効にします。

前回クラッシュ画面 ページには最新のクラッシュ画面が表示されます。前回システムクラッシュ情報は、iDRAC6 メモリに保存され、リモートからアクセスが可能です。

前回のクラッシュ画面 ページを表示するには、次の手順を実行してください。

1. **システム** ツリーの **システム** をクリックします。
2. **ログ** タブをクリックして、**前回のクラッシュ 画面**を クリックします。

前回のクラッシュ画面 ページの右上に以下のボタンがあります(「表 20-8」を参照)。

表 20-8 前回のクラッシュ画面ページのボタン

ボタン	動作
印刷	**前回のクラッシュ画面** ページを印刷します。
更新	**前回のクラッシュ画面** ページを再ロードします。

メモ: 自動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 30 秒未満に設定されている場合は、**前回のクラッシュ画面** を取り込めないことがあります。Server Administrator と IT Assistant でシステムリセットタイマーを 30 秒以上に設定して、**前回クラッシュ画面** が正しく機能することを確認します。詳細については、「管理下システムに前回クラッシュ画面の取り込みを設定する方法」を参照してください。

目次ページに戻る

目次ページに戻る

iDRAC6 の修復とトラブルシューティング

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

ここでは、クラッシュした iDRAC6 の修復とトラブルシューティングに関連するタスクを実行する方法を説明します。

iDRAC6 のトラブルシューティングには、以下のいずれかのツールを使用できます。

- RAC ログからすべてのエントリをクリアします。
- 診断コンソール
- トレースログ
- racdump
- coredump

RAC ログの使用

RAC ログ は持続的なログで、iDRAC6 ファームウェアに保管されています。ログにはユーザーの処置（ログイン、ログアウト、セキュリティポリシーの変更など）と iDRAC6 が発行する警告のリストが格納されています。ログが満杯になると、最も古いエントリから上書きされます。

iDRAC6 ユーザーインタフェース (UI) から RAC ログにアクセスするには、次の手順を実行します。

1. **システム** ツリーの **リモートアクセス** をクリックします。
2. **ログ** タブをクリックして、**RAC ログ** をクリックします。

RAC ログ には、表 21-1 に示す情報が記録されています。

表 21-1 RAC ログページ情報

フィールド	説明
日時	日付と時刻（Dec 19 16:55:47など）。 iDRAC6 を最初に起動したときにまだ管理下システムと通信 できない間は、時刻にはシステムの起動 と表示されます。
ソース	イベントを引き起こしたインタフェース
説明	イベントの概要と iDRAC6 にログインしたユーザー名。

RAC ログページのボタンの使用

RAC ログ ページには、表 21-2 に示すボタンがあります。

表 21-2 RAC ログのボタン

ボタン	動作
印刷	**RAC ログ** ページを印刷します。
ログのクリア	**RAC ログ** のエントリを消去します。 **メモ: ログのクリア** ボタンは、**ログのクリア** 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、選択したディレクトリに **RAC ログ** を保存できます。 **メモ:** Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト **support.microsoft.com** から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。

更新	**RAC ログ** ページを再ロードします。

コマンドラインの使用

RAC ログのエントリを表示するには、`getraclog` コマンドを使用します。

```
racadm getraclog -i
```

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

```
racadm getraclog [オプション]
```

メモ: 詳細については、「getraclog」を参照してください。

RAC ログからすべてのエントリをクリアするには、`clrraclog` コマンドを使用します。

```
racadm clrraclog
```

診断コンソールの使用

iDRAC6 には、Microsoft® Windows® や Linux システムに含まれている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 21-3」 を参照)。iDRAC6 ウェブインタフェースを使用して、ネットワークのデバッグツールにアクセスできます。

診断コンソール ページにアクセスするには、次の手順を行います。

1. **システム** ツリーの **リモートアクセス** をクリックします。
2. **診断** タブをクリックします。

表 21-3 に、**診断コンソール** ページで使用できるオプションを示します。コマンドを入力して **送信** をクリックします。デバッグの結果が **診断コンソール** ページに表示されます。

診断コンソール ページを更新するには、**更新** をクリックします。別のコマンドを実行するには、**診断ページに戻る** をクリックします。

表 21-3 診断コマンド

コマンド	説明
arp	ARP (Address Resolution Protocol) テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を印刷します。**netstat** オプションの右のテキストフィールドにインタフェース番号をオプションで入力すると、インタフェース、バッファの使用率、その他のネットワークインタフェースに関する情報が印刷されます。
ping <IP アドレス>	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。送信先の 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。
gettracelog	iDRAC6 トレースログ を表示します。 詳細については、「gettracelog」を参照してください。

トレースログの使用

iDRAC6 の内部トレースログは、システム管理者が iDRAC6 の警告およびネットワークに関する問題をデバッグするために使用します。

iDRAC6 のウェブベースインタフェースからトレースログにアクセスするには、次の手順を実行してください。

1. **システム** ツリーの **リモートアクセス** をクリックします。
2. **診断** タブをクリックします。
3. **gettracelog** コマンドまたは **racadm gettracelog** コマンドを **コマンド** フィールドに入力します。

   メモ: このコマンドはコマンドラインインタフェースからも使用できます。詳細については、「gettracelog」を参照してください。

トレースログは次の情報を追跡します。

- DHCP - DHCP サーバーから送受信したパケットを追跡します。
- IP - 送受信した IP パケットを追跡します。

トレースログには、管理下システムのオペレーティングシステムではなく、iDRAC6 の内部ファームウェアに関連する iDRAC6 ファームウェア固有のエラーコードが含まれている場合もあります。

メモ: iDRAC6 は、1500 バイトより大きいパケットサイズの ICMP(Ping)には応答しません。

---

racdump の使用

racadm racdump コマンドは単一コマンドで、ダンプ、状態、iDRAC6 ボードの一般情報を取得します。

メモ: このコマンドは Telnet と SSH のインタフェースでのみ使用できます。詳細については、racdump コマンドを参照してください。

---

coredump の使用

racadm coredump コマンドは、RAC で最近発生した重要な問題に関する詳細情報を表示します。coredump 情報はこれらの重要な問題の診断に使用できます。

使用可能な場合、coredump 情報は RAC の電源を切った後も、以下のどちらかの状態が発生するまで保持されます。

- **coredumpdelete** サブコマンドを使用して coredump 情報がクリアされた
- RAC で別の重要な問題が発生した 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。

racadm coredumpdelete コマンドを使用すると、現在 RAC に保存されている **coredump** データを消去できます。

詳細については、「coredump」および「coredumpdelete」サブコマンドを参照してください。

目次ページに戻る

目次ページに戻る

センサー

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

ハードウェアセンサーまたはプローブを使用すると、不安定なシステムや損傷などの障害に対して適切な処置を講じることができるため、ネットワーク上のシステムをさらに効率的に監視できます。

iDRAC6 を使用すると、ハードウェアセンサーのバッテリー、ファンプローブ、シャーシイントルージョン、電源装置、消費電力、温度、電圧などを監視できます。

バッテリープローブ

バッテリープローブは、システム基板 CMOS とストレージ ROMB（RAM on Motherboard）のバッテリーに関する情報を提供します。

メモ: ストレージ ROMB のバッテリー設定は、システムに ROMB がある場合にのみ使用可能です。

ファンプローブ

ファンプローブセンサーは以下についての情報を提供します。

- ファンの冗長性 - プライマリファンが事前に設定された速度で熱を放散しなくなると、セカンダリファンが取って代わる機能。
- ファンプローブリスト - システムのすべてのファンのファン速度についての情報を提供します。

シャーシイントルージョンプローブ

シャーシイントルージョンプローブは、シャーシが開いているか閉じているかというシャーシの状態を表示します。

電源装置プローブ

電源装置プローブは以下についての情報を提供します。

- 電源装置の状態
- 電源装置の冗長性（主電源が故障した場合に冗長電源が取って代わる機能）。

メモ: システムに電源装置が 1 個しかない場合、電源の冗長性は **無効** に設定されます。

電力監視プローブ

電力監視プローブは、リアルタイムの消費電力に関する情報をワットとアンペアで表示します。

iDRAC6 で設定した現在の日時から数えて最後の 1 分、1 時間、1 日、または 1 週間の消費電力をグラフで表示することもできます。

温度プローブ

温度センサーは、システム基板の周辺温度についての情報を提供します。温度プローブは、プローブの状態が事前に設定された警告値と重要なしきい値の範囲内にあるかどうかを示します。

電圧プローブ

以下は一般的な電圧プローブです。ご使用のシステムにこれら以外も付いている可能性があります。

- CPU [n] VCORE

- システム基板 0.9V PG
- システム基板 1.5V ESB2
- システム基板 1.5V PG
- システム基板 1.8V PG
- システム基板 3.3V PG
- システム基板 1.5V PG
- システム基板バックプレーン PG
- システム基板 CPU VTT
- システム基板リニア PG

電圧プローブは、プローブの状態が事前に設定された警告値と重要なしきい値の範囲内にあるかどうかを示します。

目次ページに戻る

目次ページに戻る

iDRAC6 を始めるにあたって

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

iDRAC6 を使用すると、システムがダウンしているときでも Dell システムのリモート監視、トラブルシューティング、修復ができます。iDRAC6 には、コンソールリダイレクト、仮想メディア、仮想 KVM、スマートカード認証、シングルサインオンを始め、豊富な機能が揃っています。

管理ステーション とは、システム管理者がリモートから iDRAC6 を備えた Dell システムを管理するシステムを指します。この方法で監視されるシステムのことを、管理下システム と呼んでいます。

また、管理ステーションに加え、オプションで管理下システムにも Dell™ OpenManage™ ソフトウェアをインストールできます。管理下システムソフトウェアなしでは RACADM をローカルで使用できず、iDRAC6 は前回のクラッシュ画面をキャプチャできません。

iDRAC6 をセットアップするには、次の一般的な手順に従います。

メモ: この手順はシステムによって異なります。お使いのシステムに固有の手順については、デルサポートサイト **support.dell.com¥manuals** で該当する『ハードウェア取扱説明書 』を参照してください。

1. iDRAC6 のプロパティ、ネットワーク、ユーザーを設定します。iDRAC6 の設定には、iDRAC6 設定ユーティリティ、ウェブインタフェース、または RACADM を使用できます。
2. Windows システムを使用している場合は、Microsoft® Active Directory® に iDRAC6 へのアクセスを設定し、Active Directory のソフトウェアで既存のユーザーに iDRAC6 ユーザー権限を追加して制御できるように します。
3. スマートカード認証を設定します。スマートカードは企業のセキュリティを強化します。
4. コンソールリダイレクトや仮想メディアなどのリモートアクセスポイントを設定します。
5. セキュリティの設定を指定します。
6. システム管理機能を効率化するための警告を設定します。
7. 標準ベースの IPMI ツールを使用してネットワーク上のシステムを管理するには、iDRAC6 Intelligent Platform Management Interface（IPMI）を設定します。

目次ページに戻る

目次ページに戻る

Kerberos 認証を有効にする方法

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

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。これは、ローカルのスマートカード認証の追加機能です。

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

- iDRAC6 に Active Directory ログイン を設定します。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。
- 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. **リモートアクセス** → **設定** タブ → **ネットワーク** サブタブをクリックします。
  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 iDRAC 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。

  詳細については、**iDRAC6 のオンラインヘルプ**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の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 ファイルには暗号鍵が含まれており、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、Kerberos 対応サービスとしてネットワーク上で有効になります。

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 -princ HOST/dracname.domainname.com@DOMAINNAME.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out
c:¥krbkeytab
```

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がマッピングされている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。

- このアカウントに DES 暗号化を使用する
- Kerberos 事前認証が不要

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。

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 ウェブサイトを参照してください。**http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**

- iDRAC6 の時刻を Active Directory ドメインコントローラと同期する必要があります。

---

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. **リモートアクセス** → **設定** タブ→ **Active Directory** サブタブ → **Active Directory の設定** をクリックします。
2. **Kerberos Keytab のアップロード** を選択し、**次へ** 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。RACADM コマンドはローカルとリモートの両方の RACADM でサポートされています。

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オ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 のログオン設定を有効にしていることも確認してください。Active Directory ユーザーの設定方法については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。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 対応サービスとして有効にする必要があります。

GUI および CLI を使用してシングルサインオンを有効にする方法については、「iDRAC6 にシングルサインオンの使用を設定する方法」を参照してください。

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 iDRAC6 のウェブアドレスを入力します。

   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に、シングルサインオン ActiveX 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。

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

   - Microsoft Active Directory のユーザーである。
   - iDRAC6 で Active Directory ログインが設定されている。
   - iDRAC6 で Kerberos Active Directory 認証が有効になっている

Active Directory ユーザーへの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され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 のログオン設定を有効にしていることも確認してください。Active Directory ユーザーの設定方法については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。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 対応サービスとして有効にする必要があります。

目次ページに戻る

目次ページに戻る

iDRAC6 で使用する vFlash メディアカードの設定

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

vFlash メディアカードは、SD カードの一種で、システム背面にあるオプションの iDRAC6 Enterprise カードスロットに差し込みます。記憶領域を提供し、通常の USB フラッシュキーのように動作します。vFlash メディアカードの挿入および取り外し方法については、『ハードウェアオーナーズマニュアル』（**support.dell.com¥manuals**）を参照してください。

---

iDRAC6 ウェブインタフェースを使用した vFlash メディアカードの設定

vFlash メディアカードの有効と無効

メモ: **仮想フラッシュの有効** オプションは、vFlash メディアカードが搭載されている場合にのみアクティブになります。カードが搭載されていない場合には、次のメッセージが表示されます。

```
SD Card not inserted. Please insert an SD card of size greater than 256MB. (SD カードが挿入されていません。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。
2. 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、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 **サーバー** を選択します。
4. **仮想フラッシュ** タブをクリックします。

   仮想フラッシュ 画面が表示されます。
5. **仮想フラッシュの有効** オプションを選択し、vFlash メディアカードを有効にします。仮想フラッシュを有効にすると、選択したサイズの USB キーとして SD カードで作成されたイメージファイル **ManagedStore.IMG** が表示されます。仮想フラッシュは、有効な **ManagedStore.IMG** イメージが SD カードにある場合にのみ有効にできます。無効にするには、オプションをオフにします。

   メモ: 仮想フラッシュ GUI ページにある 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でなく SD カードで表示できます。
6. **変更の適用** をクリックします。

vFlash メディアカードのフォーマット

メモ: **フォーマット** オプションは、vFlash メディアカードがある場合にのみアクティブになります。また、SD カードは、仮想フラッシュが無効の場合にのみフォーマットできます。

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 **サーバー** を選択します。
3. **仮想フラッシュ** タブをクリックします。

   仮想フラッシュ 画面が表示されます。
4. **仮想フラッシュの有効** オプションをオフにします。
5. **フォーマット** をクリックして、仮想フラッシュイメージファイル **ManagedStore.IMG** を SD カードに作成します。テキストファイル **ManagedStore.ID** も SD カードに作成され、仮想フラッシュイメージに関する情報を提供します。

   警告ボックスが表示され、カードにある既存のイメージがフォーマット中に消去されることに対する確認が要求されます。**OK** をクリックして続行します。

   フォーマットの進行状況を示すステータスバーが表示されます。

ディスクイメージをアップロードする

1. イメージファイルサイズが 256 MB 以下であることを確認します。

   メモ: vFlash カードの容量が 256 MB を超える場合、現時点では 256 MB のみにアクセスできます。

   メモ: 仮想フラッシュを使用すると、緊急用起動イメージと診断ツールを直接 vFlash メディアに保存できます。イメージファイルは、Windows の場合は ***.img** ファイルとして DOS のブータブルフロッピーイメージ、Linux の場合は Red Hat® Enterprise Linux® メディアの **diskboot.img** ファイルです。**diskboot.img** を使用すると、修復ディスクの作成や、ネットワークインストールを実行するディスクの作成ができます。仮想フラッシュを使用すると、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。

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 **サーバー** を選択します。

4. **仮想フラッシュ** タブをクリックします。

   仮想フラッシュ 画面が表示されます。

5. **仮想フラッシュの有効** オプションをオフにします。

6. **「仮想フラッシュドライブ」** の項で、イメージファイルのパスを入力するか、**[参照]** をクリックしてシステム内のその場所に移動します。

   アップロード をクリックします。

   アップロードの進行状況を示すステータスバーが表示されます。

メモ: ブータブルな ISO イメージを仮想フラッシュパーティションにアップロードできますが、ブータブルでなくなります。ISO イメージを IMG イメージに変換し、IMG イメージをブータブルにします。

仮想フラッシュキーサイズの表示

Virtual フラッシュキーサイズ のドロップダウンメニューには、現在設定されているサイズが表示されます。

RACADM を使用した vFlash メディアカードの設定

vFlash メディアカードの有効または無効

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。

メモ: 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。書き込み保護された SD カードが挿入されていることを確認します。

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

電源モニタと電源管理

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

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。

基本的なハードウェア設計は、電源の観点から最適化されました。

- 高効率電源装置と電圧レギュレータが組み込まれました。
- 該当する場合は、最低電力のコンポーネントが選択されました。
- ファンの電力消費量が最小化するため、シャーシ設計のシステムのエアフローが最適化されました。

PowerEdge システムは電源を制御、管理する多数の機能を提供します。

- **電力バジェット:** 起動時に、システムインベントリにって、現在の設定のシステム電力バジェットが算出されます。
- **電力制限:** 指定した電力制限を維持するように、システムを制御できます。
- **電源モニタ:** iDRAC6 は電源装置をポーリングして電力測定値を収集します。iDRAC6 は電力測定の履歴を収集して、移動平均とピーク値を計算します。iDRAC6 のウェブベースのインタフェースを使用して、**電源モニタ** ページでこれら情報を確認できます。

電力インベントリ、電力バジェット、電力制限

使用上、ラックレベルでの冷却量が制限されることがあります。ユーザー定義の電力制限を使用して、パフォーマンスの要件を満たすために必要に応じて電力を割り当てることができます。

iDRAC6 は電力消費量を監視し、指定された電力制限レベルに合わせて動的にプロセッサを減速することで、電源要件に適合しながらパフォーマンスを最大化できます。

電源モニター

iDRAC6 は、PowerEdge サーバーの消費電力を継続的に監視します。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 で情報を提供します。

- 累積電力
- 平均、最小、最大電力
- 電力ヘッドルーム値
- 電力消費量（ウェブインタフェースでグラフとしても表示）

電源の設定と管理

iDRAC6 ウェブインタフェースと RACADM コマンドラインインタフェース（CLI）を使用して、PowerEdge システム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。

- サーバーの電源状態を表示できます。
- サーバーの電源制御操作（例：電源オン、電源オフ、システムリセット、電源サイクル）を実行できます。
- サーバーとインストールされている電源装置の電力バジェット情報（設定可能な最大および最小電力消費量）を表示します。
- サーバーの電力バジェットのしきい値を表示、設定できます。

電源装置の正常性状態の表示

電源装置 ページに、インストールされているサーバー内の電源装置の状態と定格が表示されます。

ウェブインタフェースの使用

ファン装置の正常性状態を表示するには、以下の手順を実行します。

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. システムツリーで **電源装置** を選択します。**電源装置** ページには、以下の情報が表示されます。
   - **電源装置冗長性の状態**:次のような値があります。
     - **完全**:電源装置 PS1 と PS2 は同じタイプで、正しく機能しています。
     - **喪失**: 電源装置 PS1 と PS2 は異なるタイプで、どちらか一方が正しく機能していません。冗長性なし。
     - **無効**: 2 台の電源装置のうち 1 台しか使用できません。冗長性なし。
   - **個々の電源装置**: 次のような値があります。
   - **状態** には以下が表示されます。
     - **OK** は、電源装置があり、サーバーと通信していることを示します。
     - **警告**は、警告アラートのみが発行され、システム管理者が対応処置を取る必要があることを示します。システム管理者が対応処置を取らなかった場合は、サーバーの保全性に影響するような重要または重大な電源エラーを引き起こす可能性があります。
     - **重大**は、少なくとも 1 つのエラー警告が発行されたことを示します。エラーステータスは、シャーシの電源エラーを示し、直ちに対応処置を取る必要があります。
   - **場所** : 電源装置ユニットの名前 PS-n を表示します。n は電源装置番号です。
   - **タイプ**:AD、DC など電源装置のタイプを表示します(AC-DC または DC-DC 電圧変換)。
   - **入力ワット数** : 電源装置の入力ワット数。これは、システムがデータセンターにかけることのできる最大 AC 電力負荷です。
   - **最大ワット数**: 電源装置の最大ワット数。これは、システムで使用できる DC 電力です。この値は、システム構成に対して十分な電源容量があることを示すために使用されます。
   - **オンライン状態**:電源装置の電源状況(存在し OK、入力の喪失、不在、予測エラー)を示します。
   - **ファームウェアバージョン**:電源装置のファームウェアバージョンを表示します。

   メモ: 電源装置の効率性が関わるため、最大ワット数は入力ワット数とは異なります。たとえば、電源装置の効率が 89% の場合に最大ワット数が 717W であれば、入力ワット数は 797W と推定されます。

RACADM の使用

iDRAC への Telnet/SSH テキストコンソールを開いて、ログインし、次のように入力します。

```
racadm getconfig -g cfgServerPower
```

電力バジェットの表示

サーバーは、**電力バジェット情報** ページに電源サブシステムの電力バジェット状態の概要を提供します。

ウェブインタフェースの使用

メモ: 電源管理操作を行うには、**システム管理者** 権限が必要となります。

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. **Power Management**(電力の管理)タブをクリックします。
3. **電力バジェット** オプションを選択します。
4. **電力バジェット状態** ページが表示されます。

最初のテーブルには、現在のシステム構成でのユーザー指定の最大と最小の電源制限しきい値が表示されます。これらは、システム制限として設定できる AC 電力消費量の範囲を表します。選択されたシステム制限は、システムがデータセンターにかけることのできる最大 AC 電力負荷となります。

設定可能な最小電力消費量 には、指定できる電力バジェット下限のしきい値が表示されます。

設定可能な最大電力消費量 には、指定できる電力バジェット上限のしきい値が表示されます。この値は、現在のシステム設定の絶対的な最大電力消費量でもあります。

RACADM の使用

CMC への Telnet/SSH テキストコンソールを開いて、ログイン後、以下を入力します。

```
racadm getconfig -g cfgServerPower
```

メモ: 出力の詳細を含む cfgServerPower の詳細については、「cfgServerPower」を参照してください。

電力バジェットのしきい値

電力バジェットのしきい値を有効にすると、システムの電力制限の範囲を設定できます。指定したしきい値近く消費電力を維持するために、システムパフォーマンスが動的に調整されます。低負荷環境においては、実際の電力消費量は少なくなり、パフォーマンスの調整が完了するまで、一時的にしきい値を下回る場合もあります。

電力バジェットのしきい値の **有効** を選択すると、システムはユーザー指定のしきい値を強制的に適用します。電力バジェットのしきい値**の選択を解除すると**、電力制限は適用されません。たとえば、あるシステム構成での設定可能な最大電力消費量が 700W で、設定可能な最小電力消費量が 500W であるとします。電力バジェットのしきい値を現在の 650W から 525W に下げて有効にすることができます。以降、システムのパフォーマンスはユーザー指定のしきい値 525W を超えないように電力消費量を維持すべく動的に調整されます。

ウェブインタフェースの使用

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. **Power Management**(電力の管理)タブをクリックします。
3. **電力バジェット** オプションを選択します。**電力バジェット情報** ページが表示されます。
4. **電力バジェットのしきい値** テーブルに値をワット、BTU/時、またはパーセント単位で入力します。ワットまたは BTU/時 単位は、電力バジェットのしきい値の上限値の入力に使用します。パーセント単位は、設定可能な最大と最小電力消費量範囲内のパーセントで指定する場合に使用します。たとえば、100% しきい値は設定可能な最大電力消費量を示し、0% は最小電力消費量を示します。

   メモ: 電力バジェットのしきい値は設定可能な最大電力消費量を上回ったり、設定可能な最小電力消費量を下回ることはできません。

5. しきい値を有効にする場合は **有効** を選択し、有効にしない場合は選択しないままにします。**有効**を選択すると、システムはユーザー指定のしきい値を強制的に適用します。**を選択しないと**、システムは電力制限されません。
6. **変更の適用** をクリックします。

RACADM の使用

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts <ワット単位の電力制限値>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr <BTU/時の電力制限値>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent <電力制限値のパーセント>
```

メモ: 電力バジェットのしきい値を BTU/時で設定するときは、ワットに変換すると、近似の整数値に丸められます。電力バジェットのしきい値をワットから BTU/時に読み戻すときにも、同様に近似の整数値に丸められます。このため、書き込まれた値が読み取り値と若干異なる場合があります。たとえば、600 BTU/時に設定されたしきい値は 601 BTU/時として読み込まれます。

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**ページが表示されます。

電源モニタ ページに表示される情報は次のとおりです。

電源モニター

- **状態**:**OK** は、電源装置ユニットがあり、現在サーバーと通信していることを示し、**警告** は警告が発行されたこと、**重大** はエラーアラートが発行されたことを示します。
- **プローブ名**: システム基板のシステムレベル この説明は、システムにおける場所に基づいて、プローブが監視されていることを示します。
- **読み取り値**:ワット単位または BTU/時の現在の消費電力量。

アンペア数

- **場所** :電源装置ユニットの名前 PS-n を表示します。n は電源装置番号です。
- **読み取り値**:現在の消費電力量(アンペア)。

電源 トラッキング統計

メモ: 現在の時間とピーク時間のリストに未解決のエラーがあります。現在時間の下に表示されている値は実際はピーク時間の値で、ピーク時間の下の値は現在時間の値です。

- **累積** 電源装置の入力側から測定したサーバーの現在の累積エネルギー消費量を示します。値は KWh で表示される累積値で、システムによって使用された総エネルギー量です。この値は、**累積のリセット** ボタンを使ってリセットできます。
- **最大ピーク アンペア数** は、開始 と現在時間ので指定された間隔内のピーク現在値です。この値は、**最大ピークのリセット** ボタンを使ってリセットできます。
- **最大ピーク ワット数** は、開始 と現在時間ので指定された間隔内のピーク現在値です。この値は、**最大ピークのリセット** ボタンを使ってリセットできます。
- **測定開始時間** はシステムエネルギー消費量の値が最後にクリアされ、新しい測定サイクルが開始された日時を表示します。**累積** の場合、この値は **累積のリセット** ボタンを使ってリセットできますが、システムリセットまたはフェールオーバー時まで持続します。**最大ピーク アンペア数** と **最大ピーク ワット数** では、この値は **最大ピークのリセット** ボタンを使ってリセットできますが、システムリセットまたはフェールオーバー時まで持続します。
- **累積** の **測定終了時刻** は、システムエネルギー消費量が算出された現在の日時を表示します。**最大ピーク アンペア数** と **最大ピーク ワット数** では、**測定終了時刻** イールドにはこれらのピークが発生した時刻が表示されます。

メモ: 電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、指定された測定開始から終了までのすべてのアクティビティを反映します。**最大ピークのリセット** ボタンは、個々のフィールドをゼロにリセットします。次の表の電力消費量のデータは、システムのリセット後に失われるため、ゼロにリセットされます。表示される電力値は、特定の時間間隔(過去 1 分、1 時間、1 日 および 1 週間)にわたって測定された累積平均値です。開始から終了までの間隔が電源追跡統計値と異なる場合もあるため、ピーク電力値(最大ピークワット数 対 最大電力消費量)も異なる可能性があります。

電力消費

- 過去 1 分、1 時間、1 日、1 週間の平均、最大、および最小電力消費量が表示されます。
- 平均電力消費量:過去 1 分、過去 1 時間、過去 1 日、および過去 1 週間の平均値。
- 最大 および 最小の電力消費量:特定の時間間隔で測定された最大および最小電力消費量。
- 最大および 最小の電力消費時間:電力消費量が最大であった時間と 最小であった時間。

ヘッドルーム

システムの即時ヘッドルーム には、電源装置ユニットで使用可能な電力とシステムの現在の電力消費量間の差が表示されます。

システムのピークヘッドルーム には、電源装置ユニットで使用可能な電力とシステムのピーク電力消費量間の差が表示されます。

グラフの表示

このボタンをクリックすると、過去 1 時間の iDRAC6 の電力消費量と電流消費量がそれぞれワットとアンペアで表示されます。これらの統計値は、グラフの上方にあるドロップダウンメニューを使って 1 週間前まで表示できます。

メモ: グラフに描かれた各データポイントは、読み取り値の 5 分間平均を表します。このため、電力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。

サーバーに対する電源制御操作の実行

メモ: 電源管理の操作を行うには、**シャーシ制御システム管理者** 権限が必要です。

iDRAC6 では、正常なシャットダウンなど、複数の電源管理処置をリモートで実行できます。

ウェブインタフェースの使用

1. iDRAC6 ウェブインタフェースにログインします。
2. **Power Management**(電力の管理)タブをクリックします。**電力制御** ページが表示されます。
3. ラジオボタンをクリックして、**電源制御操作** のいずれかを選択します。
   - **システムの電源を入れる** は、サーバーの電源をオンにします(サーバーの電源がオフのときに電源ボタンを押す操作と同じ)。サーバーの電源がすでにオンの場合は、このオプションが無効になっています。
   - **システムの電源を切る** は、サーバーの電源をオフにします。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
   - **NMI(マスク不能な割り込み)**は、NMI を生成し、システム動作を一時停止させます。

- **正常なシャットダウン** は、システムをシャットダウンします。
- **システムをリセットする**（ウォームブート）は、電源をオフにすることなく、システムをリセットします。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
- **システムの電源サイクル**（コールドブート）はサーバーの電源を切ってから再起動します。サーバーの電源がすでにオフの場合、このオプションは無効になっています。

4. **適用** をクリックします。確認ダイアログボックスが表示されます。
5. **OK** をクリックして、電力管理の操作（システムのリセットなど）を行います。

RACADM の使用

サーバーへの Telnet/SSH テキストコンソールを開いて、ログイン後、以下を入力します。

```
racadm serveraction <動作>
```

ここで、<操作> は、powerup（電源投入）、powerdown（電源切断）、powercycle（電源サイクル）、hardreset（ハードリセット）または powerstatus（電源状態）を指します。

目次ページに戻る

目次ページに戻る

セキュリティ機能の設定

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

iDRAC6 には次のセキュリティ機能があります。

- iDRAC6 管理者用の高度なセキュリティオプション
  - コンソールリダイレクトの無効オプションをオンにすると、ローカルシステムユーザーが iDRAC6 コンソールリダイレクト機能を使用してコンソールリダイレクトを無効にできます。
  - ローカル設定の無効オプションをオンにすると、リモート iDRAC6 管理者が iDRAC6 の設定機能を以下から選択的に無効にできます。
    - BIOS POST オプション ROM
    - ローカル RACADM と Dell™ OpenManage™ Server Administrator ユーティリティを使用してオペレーティングシステムから
- 128 ビット SSL 暗号化と 40 ビット SSL 暗号化（128 ビットが許可されていない国）をサポートする RACADM CLI とウェブベースインタフェース操作から

  メモ: Telnet は SSL 暗号化をサポートしていません。

- ウェブインタフェースまたは RACADM CLI を使用したセッションタイムアウトの設定（分単位）
- 設定可能な IP ポート（該当する場合）
- 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）
- IP アドレスごとのログイン失敗数の制限により制限を超えた IP アドレスのログインを阻止
- iDRAC6 に接続するクライアントの IP アドレス範囲を制限

---

iDRAC6 システム管理者用のセキュリティオプション

iDRAC6 ローカル設定を無効にする

システム管理者は、**リモートアクセス** → **設定** → **サービス** を選択して、iDRAC6 グラフィカルユーザーインタフェース（GUI）をからたローカル設定を無効にできます。オプションの **ROM を使用した iDRAC のローカル設定を無効にする** チェックボックスをオンにすると、iDRAC6 ローカル設定ユーティリティ（システム起動時に <Ctrl+E> を押してアクセス）は読み取り専用モードで起動し、ローカルユーザーがデバイスを設定できなくなります。システム管理者が **RACADM を使用した iDRAC のローカル設定を無効にする** チェックボックスをオンにすると、ローカルユーザーは iDRAC6 の設定を読み取ることはできますが、RACADM ユーティリティや Dell OpenManage Server Administrator を使用して設定することができません。

システム管理者はこれらのオプションのいずれか一方、または両方を同時に有効にできます。ウェブインタフェースを介して有効にするほかに、ローカル RACADM コマンドを使って有効にすることもできます。

システム再起動中のローカル設定を無効にする

この機能は、システムの再起動中に管理下システムのユーザーが iDRAC6 を設定できないようにします。

```
racadm config -g cfgRacTuning -o

cfgRacTuneCtrlEConfigDisable 1
```

メモ: このオプションは、iDRAC6 設定ユーティリティでのみサポートされています。このバージョンにアップグレードするには、デルサポートサイト **support.dell.com** から BIOS アップデートパッケージを使用して BIOS をアップグレードしてください。

ローカル RACADM からローカル設定を無効にする

この機能は、管理下システムのユーザーがローカル RACADM または Dell OpenManage Server 管理ユーティリティを使って iDRAC6 を設定する機能を無効にします。

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

注意: これらの機能は、ローカルユーザーがローカルシステムから iDRAC6 を設定する機能（デフォルト設定に戻す機能も含む）を著しく制限します。これらの機能を慎重に使用し、一度に 1 つのインターフェイスのみを無効にして、ログイン権限を完全に失うことを避けることをお勧めします。

メモ: 詳細については、デルサポートサイト **support.dell.com** にあるホワイトペーパー「DRAC 上のローカル設定とリモート仮想 KVM を無効にする」をお読みください。

システム管理者はローカル RACADM コマンドを使ってローカル設定オプションを設定できますが、セキュリティ上の理由から、リセットは帯域外の iDRAC6 ウェブインタフェース またはコマンドラインイ

ンターフェイスからしかできません。システムの電源投入時自己診断テストが完了し、オペレーティングシステムが起動したら、cfgRacTuneLocalConfigDisable オプションが適用されます。オペレーティングシステムとしては、ローカル RACADM コマンドを実行できる Microsoft® Windows Server® または Enterprise Linux 、あるいは Dell OpenManage Deployment Toolkit のローカル RACADM コマンド を実行するために限定的に使用される Microsoft Windows ® Preinstallation Environment や vmlinux などが挙げられます。

次のような場合には、システム管理者がローカル設定を無効にする必要があります。たとえば、サーバーやリモートアクセスデバイスの管理者が複数人いるデータセンターでは、サーバーのソフトウェアスタックの保守担当者はリモートアクセスデバイスへの管理者権限を必要としない場合があります。同様に、技術者はシステムの定期保守作業中、サーバーへの物理的なアクセス権限を持ち、この間、システムを再起動し、パスワード保護されている BIOS にもアクセスできますが、リモートアクセスデバイスの設定はできないようにする必要があります。このような状況では、リモートアクセスデバイスの管理者がローカル設定を無効にすることができます。

ただし、ローカル設定を無効にすると、iDRAC6 をデフォルト設定に戻す能力を含め、ローカル設定権限が著しく制限されるため、これらのオプションは必要なときのみ使用し、通常は一度に 1 つだけのインターフェイスを無効にし、ログイン権限を完全に失わないように注意してください。たとえば、管理者がローカル iDRAC6 ユーザー全員を無効にし、Microsoft Active Directory® ディレクトリサービスのユーザーだけが iDRAC6 にログインできるようにした後、Active Directory の認証インフラストラクチャにエラーが発生すると、管理者がログインできなくなる可能性があります。同様に、管理者がすべてのローカル設定を無効にし、動的ホスト構成プロトコル(DHCP)サーバーを含むネットワークに静的 IP アドレスを使って iDRAC6 を配置した後、DHCP サーバーが iDRAC6 の IP アドレスをネットワーク上の別のデバイスに割り当てた場合、その競合によって DRAC の帯域外の接続が無効になり、管理者がシリアル接続を通してファームウェアをデフォルト設定に戻すことが必要になります。

iDRAC6 リモート仮想 KVM を無効にする

管理者は iDRAC6 リモート KVM を選択的に無効にすることで、コンソールリダイレクトを通して他のユーザーから見られることなくローカルユーザーがシステムを操作するための柔軟でセキュアなメカニズムを提供できます。この機能を使用するには、サーバーに iDRAC 管理下ノードソフトウェアをインストールする必要があります。管理者は次のコマンドを使用して、リモート vKVM を無効にできます。

```
racadm LocalConRedirDisable 1
```

LocalConRedirDisable コマンドは、引数 1 を使って実行すると既存のリモート vKVM セッションウィンドウを無効にします。

リモートユーザーがローカルユーザーの設定を上書きするのを防ぐために、このコマンドはローカル RACADM でのみ使用可能です。管理者は、Microsoft Windows Server 2003 および SUSE Linux Enterprise Server 10 など、ローカル RACADM 対応のオペレーティングシステムでこのコマンドを使用できます。このコマンドはシステム再起動後も有効であるため、リモート vKVM を再度有効にするには、管理者がこのコマンドを無効にする必要があります。これには、次のように引数 0 を使用します。

```
racadm LocalConRedirDisable 0
```

状況によっては、iDRAC6 リモート vKVM を無効にする必要が生じます。たとえば、管理者は自分が設定した BIOS 設定をリモート iDRAC6 ユーザーに見られたくない場合、LocalConRedirDisable コマンドを使ってシステム POST 中にリモート vKVM を無効にできます。また、管理者がシステムにログインするたびにリモート vKVM を自動的に無効にすることでセキュリティを強化できます。これには、ユーザーログオンスクリプトから LocalConRedirDisable コマンドを実行します。

メモ: 詳細については、デルサポートサイト **support.dell.com** にあるホワイトペーパー「DRAC 上のローカル設定とリモート仮想 KVM を無効にする」をお読みください。

ログオンスクリプトの詳細については、**technet2.microsoft.com / windowsserver / en / library / 31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx** を参照してください。

SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保

ここでは、iDRAC6 に組み込まれているデータセキュリティの機能について説明します。

- 「SSL (Secure Sockets Layer)」
- 「証明書署名要求(CSR)」
- 「SSL メインメニューへのアクセス」
- 「証明書署名要求の生成」

SSL (Secure Sockets Layer)

iDRAC6 には、業界標準の SSL セキュリティプロトコルを使用してインターネットで暗号化データを送信するように構成されたウェブサーバーが含まれています。公開鍵と秘密鍵の暗号技術に基づく SSL は、クライアントとサーバー間で認証済みの暗号化通信を使用して、ネットワーク上の盗聴を防止するために広く受け入れられているセキュリティ方式です。

SSL に対応したシステムの特徴

- SSL 対応のクライアントに対して自己認証する
- クライアントがサーバーに対して認証できるようにする
- 両方のシステムが暗号化された接続を確立できる

この暗号処理は高度なデータ保護を提供します。iDRAC6 では、北米のインターネットブラウザで一般的に使用されている最も安全な暗号化方式である 128 ビットの SSL 暗号化標準を採用しています。

iDRAC6 ウェブサーバーには、デルが署名をした SSL デジタル証明書(サーバー ID)が含まれています。インターネットで高度なセキュリティを確保するには、新しい証明書署名要求(CSR)を生成する要求を iDRAC6 に送信して、ウェブサーバー SSL 証明書を置き換えてください。

証明書署名要求(CSR)

CSR は、認証局(CA)に対してセキュアサーバー証明書の発行を求めるデジタル要求です。セキュアサーバー証明書は、リモートシステムの身元を保護して、リモートシステムとやり取りする情報を他のユーザーが表示したり変更したりできないようにします。DRAC のセキュリティを確保するため、CSR を生成して CSR を CA に送信し、CA から返された証明書をアップロードすることをお勧めしま

す。

CA は、信頼性の高いスクリーニング、身分証明、その他の重要なセキュリティ条件を満たすことが IT 業界で認められた事業体です。CA には、Thawte や VeriSign などがあります。CA は CSR を受け取ると、CSR に含まれている情報を確認します。申請者が CA のセキュリティ標準を満たしていると、CA はネットワークおよびインターネットを介したトランザクションに対して、申請者を一意に識別する証明書を発行します。

CA が CSR を承認して証明書を送信したら、証明書を iDRAC6 ファームウェアにアップロードする必要があります。iDRAC6 ファームウェアに保管されている CSR 情報は、証明書に記載されている情報と一致する必要があります。

SSL メインメニューへのアクセス

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**SSL** をクリックします。

CSR を生成、既存サーバー証明書をアップロード、または既存サーバー証明書を表示するには、**SSL メインメニュー**(「表 23-1」を参照)を使用します。CSR の情報は iDRAC6 ファームウェアに保存されています。表 23-2 は、**SSL メインメニュー** ページに表示されるボタンについて説明しています。

表 23-1 SSL メインメニュー

フィールド	説明
証明書署名要求(CSR)の生成	**次へ** をクリックしてページを開くと、CA に送信する CSR を生成して、セキュアなウェブ証明書を申請できます。
サーバー証明書のアップロード	**次へ** をクリックし、iDRAC6 へのアクセス制御に使用する会社の既存の証明書をアップロードします。 **メモ:** iDRAC6 で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER によって符号化された証明書は受け入れられません。新しい証明書をアップロードすると、iDRAC6 で受信したデフォルトの証明書が置き換えられます。
サーバー証明書の表示	**次へ** をクリックして、既存のサーバー証明書を表示します。

表 23-2 SSL メインメニューボタン

ボタン	説明
印刷	**SSL メインメニュー** ページを印刷します。
更新	**SSL メインメニュー** ページを再ロードします。
次へ	次のページに移動します。

証明書署名要求の生成

メモ: 新しい CSR は、ファームウェアにある古い CSR を上書きします。iDRAC が署名付き CSR を受け入れる前に、ファームウェアの CSR が CA から返された証明書と一致する必要があります。

1. **SSL メインメニュー** ページで、**証明書署名要求(CSR)の生成** を選択して、**次へ** をクリックします。
2. **証明書署名要求(CSR)の生成** ページで、各 CSR 属性の値を入力します。

   表 23-3 に、**証明書署名要求 (CSR) の生成** ページのオプションを示します。
3. CSR を開くまたは保存するには、**生成** をクリックします。
4. **証明書署名要求(CSR)の生成** ページで適切なボタンをクリックして続行します。表 23-4 は、**証明書署名要求(CSR)の生成** ページに表示されるボタンについて説明しています。

表 23-3 証明書署名要求(CSR)の生成 ページのオプション

フィールド	説明
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、ハイフン、アンダースコア、スペース、およびピリオドが有効です。
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られた名前(たとえば「エンタープライズグループ」)。英数字、ハイフン、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都市や地域(たとえば「神戸」)。英数字とスペースのみが有効です。アンダースコアやその他の文字で単語を区切らないでください。
都道府県名	証明書を申請している組織の所在地(たとえば「東京」)。英数字とスペースのみが有効です。略語は使用しないでください。
国番号	証明書を申請している組織が所在する国の名前。国を選択するには、ドロップダウンメニューを使用します。

電子メール	CSR に関連付けられている電子メールアドレス。会社の電子メールアドレスや、CSR に関連付けたいその他の電子メールアドレスを入力できます。このフィールドは省略可能です。

表 23-4 証明書署名要求(CSR)の生成 ページのボタン

ボタン	説明
印刷	**証明書署名要求(CSR)の生成** ページを印刷します。
更新	**証明書署名要求(CSR)の生成** ページを再ロードします。
SSL メインメニューに戻る	**SSL メインメニュー** ページに戻ります。
生成	CSR を生成します。

サーバー証明書の表示

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

   表 23-5 に、**証明書** ウィンドウに表示されるフィールドと説明を示します。

2. **サーバー証明書の表示** ページの適切なボタンを押して続行します。

表 23-5 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	証明書の失効日

Secure Shell(SSH)の使用

SSH の使用方法の詳細については、「Secure Shell (SSH) の使用」を参照してください。

サービスの設定

メモ: これらの設定を変更するには、**iDRAC の設定** 権限が必要です。また、リモート RACADM コマンドラインユーティリティは、ユーザーが **root** としてログインしているときにのみ有効にできます。

1. **システム** ツリーを展開し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**サービス** をクリックします。
3. 必要に応じて次のサービスを設定します。
   - ローカル設定(表 23-6)
   - ウェブサーバー(表 23-7)
   - SSH(表 23-8)
   - Telnet(表 23-9)
   - リモート RACADM(表 23-10)
   - SNMP エージェント(表 23-11)
   - 自動システムリカバリエージェント(表 23-12)

   自動システムリカバリエージェント を使用して、iDRAC6 の **前回のクラッシュ画面** 機能を有効にします。

   メモ: iDRAC6 で **前回クラッシュ画面** が機能するためには、**Server Administrator** をインストールするときに **処置** を **システムの再起動**、**システムの電源を切る**、または **システムの電源を入れ直す** に設定して **自動回復** 機能をアクティブにする必要があります。

4. **変更の適用** をクリックします。

5. **サービス** ページの適切なボタンをクリックして続行します。表 23-13を参照してください 。

表 23-6 ローカル設定

設定	説明
オプション ROM を使って iDRAC ローカル設定を無効にする	オプション ROM を使って iDRAC のローカル設定を無効にします。システム再起動中に <Ctrl+E> を押してセットアップモジュールを開始するようにプロンプトが表示されます。
RACADM を使って iDRAC ローカル設定を無効にする	ローカル RACADM を使って iDRAC のローカル設定を無効にします。

表 23-7 ウェブサーバーの設定

設定	説明
有効	ウェブサーバーを有効または無効にします。オン=有効、オフ=無効
最大セッション数	システムで許可される同時セッションの最大数。
アクティブなセッション数	システムの現在のセッション数(**最大セッション数** 以下)。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更はすぐに適用され、現在のウェブインタフェースセッションが終了します。ウェブサーバーもリセットされます。新しいウェブインタフェースセッションが始まるまで数分お待ちください。タイムアウト範囲は 60 ～ 10800 秒です。デフォルト値は 1800 秒です。
HTTP ポート番号	iDRAC がサーバー接続に使用するポート。デフォルト設定は **80** 秒です。
HTTPS ポート番号	iDRAC がサーバー接続に使用するポート。デフォルト設定は **443** 秒です。

表 23-8 SSH の設定

設定	説明
有効	SSH を有効または無効にします。チェックボックスが選択されている場合、SSH は有効であることを示します。
タイムアウト	セキュアシェルのアイドルタイムアウト(秒)。タイムアウト範囲は 60 ～ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **300** です。
ポート番号	SSH 接続で iDRAC6 が通信するポート。デフォルトは **22** です。

表 23-9 Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。選択されている場合、Telnet は有効です。
タイムアウト	telnet のアイドルタイムアウト(秒)。タイムアウト時間の範囲は 60 ～ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **300** です。
ポート番号	iDRAC6 が Telnet 接続を待ち受けるポート。デフォルトは **23** です。

表 23-10 リモート RACADM の設定

設定	説明
有効	リモート RACADM を有効または無効にします。チェックボックスをオンにすると、リモート RACADM が有効になります。
アクティブなセッション数	システムの現在のセッション数。
アクティブなセッション数	システムの現在のセッション数(**最大セッション数** 以下)。

表 23-11 SNMP エージェントの設定

設定	説明
有効	SNMPエージェントを有効または無効にします。オン=有効、オフ=無効
コミュニティ名	SNMP 警告の送信先 IP アドレスを含むコミュニティ名。コミュニティ名は、空白文字を含まずに最大 31 文字まで使用できます。デフォルト設定は **public** です。

表 23-12 自動システムリカバリエージェントの設定

設定	説明
有効	自動システムリカバリエージェントを有効にします。

表 23-13 サービスページのボタン

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

---

iDRAC6 の追加のセキュリティオプションを有効にする

リモートシステムへの不正アクセスを防ぐため、iDRAC6 では次の機能を提供しています。

- IP アドレスフィルタ(IPRange)- iDRAC6 にアクセスできる特定の IP アドレス範囲を定義します。
- IP アドレスのブロック - 特定の IP アドレスからのログイン試行の失敗回数を制限します。

これらの機能は iDRAC6 のデフォルト設定では無効になっています。次のサブコマンドまたはウェブインタフェースを使用して、これらの機能を有効にしてください。

```
racadm config -g cfgRacTuning -o <オブジェクト名> <値>
```

これらの機能はまた、セッションのアイドルタイムアウト値や、ネットワークに定義済みのセキュリティプランと一緒にも使用できます。

以下の項で、これらの機能について詳しく説明します。

IP フィルタ(IpRange)

IP アドレスフィルタ(または IP 範囲チェック)を使用すると、ユーザーが特定した範囲内にある IP アドレスのクライアントワークステーションや管理ワークステーションからのみ iDRAC6 へのアクセスを許可します。その他のログインはすべて拒否されます。

IP フィルタは着信ログインの IP アドレスを、次の **cfgRacTuning** プロパティで指定する IP アドレス範囲と比較します。

- `cfgRacTuneIpRangeAddr`
- `cfgRacTuneIpRangeMask`

cfgRacTuneIpRangeMask プロパティは着信 IP アドレスと **cfgRacTuneIpRangeAddr** プロパティの両方に適用されます。両方のプロパティの結果が同じであれば、受信ログイン要求の iDRAC6 へのアクセスが許可されます。この範囲外の IP アドレスからのログイン要求にはエラーが返されます。

次の式の値がゼロに等しい場合は、ログインに進みます。

```
cfgRacTuneIpRangeMask & (<着信 IP アドレス> ^ cfgRacTuneIpRangeAddr)
```

& は数量のビットワイズ AND で ^ はビットワイズ XOR です。

cfgRacTuning プロパティの完全なリストは、「iDRAC6 プロパティデータベースグループとオブジェクト定義」に掲載されています。

表 23-14 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。 このプロパティと **cfgRacTuneIpRangeMask** とのビットワイズ ANDによって、許可する IP アドレスの上位部分が決定されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0～192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
cfgRacTuneIpRangeMask	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。

IP フィルタを有効にする

以下に、IP フィルタ設定のコマンド例を示します。

RACADM と RACADM コマンドの詳細については、「RACADM のリモート使用」を参照してください。

メモ: 次の RACADM コマンドは 192.168.0.57 以外のすべての IP アドレスをブロックします。

ログインを 1 つの IP アドレスに限定するには(たとえば 192.168.0.57)、次のようにフルマスクを使用してください。

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

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

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
```

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。

- **cfgRacTuneIpRangeMask** は必ずネットマスク形式で設定します。最上位ビットがすべて 1 で(これがマスクのサブネットを定義)、下位ビットはすべてゼロにします。
- 必要な範囲の基底アドレスを **cfgRacTuneIpRangeAddr** の値として使用します。このアドレスの 32 ビットのバイナリ値は、マスクにゼロがある下位ビットがすべてゼロになります。

IP ブロック

IP ブロックは、事前に選択した時間枠で、特定の IP アドレスからの過剰なログイン失敗を動的に判別して、そのアドレスが iDRAC6 にログインできないようにブロックします。

IP ブロックのパラメータは、次のような **cfgRacTuning** グループ機能を使用します。

- 許可するログイン失敗回数
- これらの失敗を数える時間枠(秒)
- ログイン失敗回数が所定の合計数を超えた IP アドレスからのセッション確立を防止する時間(秒)

特定の IP アドレスからのログイン失敗が累積すると、それらは内部カウンタによって計数されます。ユーザーがログインに成功すると、失敗履歴がクリアされて、内部カウンタがリセットされます。

メモ: クライアント IP アドレスからのログイン試行が拒否されると、SSH クライアントに「ssh exchange identification: Connection closed by remote host(SSH ID: リモートホストが接続を閉じました)」というメッセージが表示される場合があります。

cfgRacTuning プロパティの完全なリストは、「iDRAC6 プロパティデータベースグループとオブジェクト定義」に掲載されています。

表 23-15 に、ユーザー定義のパラメータを示します。

表 23-15 ログイン再試行制限のプロパティ

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(**cfgRacTuneIpBlkFailCount**)1 つの IP アドレスからの失敗が連続すると(**cfgRacTuneIpBlkFailWindow**)、以降そのアドレスからのセッション確立試行が一定の時間(**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	失敗回数を数える時間枠を秒で指定します。失敗回数がこの制限値を超えると、カウンタはリセットされます。
cfgRacTuneIpBlkPenaltyTime	失敗回数が制限値を超えた IP アドレスからのセッションをすべて拒否する時間枠を秒で定義します。

IP ブロックを有効にする

次の例では、クライアントが 1 分間に 5 回ログイン試行に失敗した場合に、5 分間このクライアント IP アドレスのセッション確立を防止します。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

次の例は、1 分以内に失敗が 3 回を超えた場合に、1 時間ログイン試行を阻止します。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

iDRAC6 GUI を使ったネットワークセキュリティの設定

メモ: 次の手順を実行するには、**iDRAC6 の設定** 権限が必要です。

1. **システム** ツリーの **リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**ネットワーク** をクリックします。
3. **ネットワークの設定** ページで **詳細設定** をクリックします。
4. **ネットワークセキュリティ** ページで属性値を設定してから **変更の適用** をクリックします。

   表 23-16 に、**ネットワークセキュリティ** ページの設定を示します。
5. **ネットワークセキュリティ** ページの適切なボタンをクリックして続行します。**ネットワークセキュリティ** ページのボタンについては、表 23-17 を参照してください。

表 23-16 ネットワークセキュリティページの設定

設定	説明
IP 範囲を有効にする	IP 範囲のチェック機能を有効にします。この設定により、iDRAC6 にアクセスできる IP アドレスの範囲を定義できます。
IP 範囲のアドレス	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。可能な IP アドレスの上位部分を決定するため、この値は IP 範囲サブネットマスクとビット単位で AND されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0～192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。 例:**255.255.255.0**
IP ブロックを有効にする	事前に選択した時間枠で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。
IP ブロックエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。
IP ブロックエラー時間枠	ここで指定した時間枠(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。
IP ブロックペナルティ時間	失敗回数が制限値を超えた IP アドレスからのセッションをすべて拒否する時間を秒で指定します。

表 23-17 ネットワークセキュリティページのボタン

ボタン	説明
印刷	**ネットワークセキュリティ** ページを印刷します。
更新	**ネットワークセキュリティ** ページを再ロードします。
変更の適用	**ネットワークセキュリティ** ページに加えた変更を保存します。
ネットオワーク設定ページに戻る	**ネットワーク設定** ページに戻ります。

目次ページに戻る

目次ページに戻る

iDRAC6 の基本インストール

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

この項では、iDRAC6 のハードウェアとソフトウェアのインストールと設定方法について説明します。

作業を開始する前に

iDRAC6 ソフトウェアをインストールして設定する前に、システムに含まれている以下のアイテムを用意してください。

- iDRAC6 ハードウェア（組み込みかまたはオプションキットに同梱）
- iDRAC6 インストール手順（本章で記載）
- 『Dell Systems Management Tools and Documentation DVD』

---

iDRAC6 Express/Enterprise ハードウェアの取り付け

メモ: iDRAC6 接続は USB キーボード接続をエミュレートします。そのため、システムを再起動したとき、キーボードが接続していなくても通知されません。

iDRAC6 Express/Enterprise は、事前にシステムに取り付けられているか、個別に取り付けることができます。システムに取り付けられている iDRAC6 の利用を開始するには、「ソフトウェアのインストールと設定の概要」を参照してください。

iDRAC6 Express/Enterprise がシステムに取り付けられていない場合は、使用しているプラットフォームの『ハードウェアオーナーズマニュアル』でハードウェアの取り付け方法を参照してください。

---

iDRAC 6 を使用するためのシステムの設定

iDRAC6 を使用するようにシステムを設定するには、iDRAC6 設定ユーティリティを使用します。

iDRAC6 設定ユーティリティを実行するには、以下の手順を実行します。

1. システムの電源を入れるか、再起動します。
2. POST 中に、画面の説明に従って <Ctrl><E> を押します。

   <Ctrl><E> キーを押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、もう一度システムを再起動し、この手順を実行してください。
3. LOM を設定します。
   a. 方向キーを使用して LAN パラメータ を選択し、<Enter> を押します。NIC の選択 が表示されます。
   b. 方向キーを使用して、次のいずれかのNIC モードを選択します。
      - **専用** - このオプションは、リモートアクセスデバイスから iDRAC Enterprise 上で使用可能な専用ネットワークインタフェースを使用できるようにする場合に選択します。このインタフェースは、ホストオペレーティングシステムと共有されず、管理トラフィックを別の物理ネットワークに転送することでアプリケーションのトラフィックから分離できます。このオプションは、システムに iDRAC6 Enterprise が搭載されている場合にのみ、利用可能です。
      - **共有** - このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムが NIC チーミング用に設定されている場合に完全に機能します。リモートアクセスデバイスは、データの受信は NIC 1 と NIC 2 で行いますが、送信は NIC 1 からのみ行います。NIC 1 が故障すると、リモートアクセスデバイスにアクセスできなくなります。
      - **フェールオーバーで共有（LOM2）** - このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムが NIC チーミング用に設定されている場合に完全に機能します。リモートアクセスデバイスは、データの受信は NIC 1 と NIC 2 で行いますが、データの送信は NIC 1 からのみ行います。NIC 1 が故障した場合、リモートアクセスデバイスはすべてのデータ送信を NIC 2 にフェールオーバーします。リモートアクセスデバイスはデータの送信に引き続き NIC 2 を使用します。NIC 2 が故障した場合、リモート アクセス デバイスはすべての送受信を再び NIC 1 にフェールオーバーします。ただし、これは最初の NIC 1 の障害が修復されている場合に限ります。
      - **フェールオーバーで共有（すべての LOM）**）- このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスネットワークインタフェースは、ホストオペレーティングシステムが NIC チーミング用に設定されている場合に完全に機能します。リモートアクセスデバイスは、データの受信は NIC 1、NIC 2、NIC 3、NIC 4 で行いますが、データの送信は NIC 1 からのみ行います。NIC 1 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 2 にフェールオーバーします。NIC 2 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 3 にフェールオーバーします。NIC 3 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 4 にフェールオーバーします。NIC 4 が故障した場合、リモート アクセス デバイスはすべての送受信を再び NIC 1 にフェールオーバーします。ただし、これは最初の NIC 1 の障害が修復されている場合に限ります。このオプションは、iDRAC6 Enterprise では使用できない場合があります。

4. DHCP または静的 IP アドレスソースを使用するようにネットワークコントローラ LAN パラメータを設定します。
    a. 下方向キーを使って、**LAN パラメータ** を選択し、<Enter> を押します。
    b. 上下の方向キーを使って、**IP アドレスソース** を選択します。
    c. 左右の方向キーを使って、**DHCP、Auto Config（自動設定）** または **静的** を選択します。
    d. **静的** を選択した場合は、**イーサネット IP アドレス、サブネットマスク、デフォルトゲートウェイ** 設定を選択します。
    e. <Esc> を押します。
5. <**Esc**> を押します。
6. **変更を保存して終了** を選択します。

ソフトウェアのインストールと設定の概要

この項では、iDRAC6 ソフトウェアのインストールと設定について概説します。iDRAC6 のソフトウェアコンポーネントの詳細については、「管理下システムへのソフトウェアのインストール」を参照してください。

iDRAC6 ソフトウェアのインストール

iDRAC6 ソフトウェアをインストールするには:

1. ソフトウェアを管理下システムにインストールします。「管理下システムへのソフトウェアのインストールを参照してください。
2. ソフトウェアを管理ステーションにインストールします。「管理下システムへのソフトウェアのインストールを参照してください。

iDRAC6 の設定

iDRAC6 を設定するには:

1. 次のいずれかの設定ツールを選択します。
    - ウェブインタフェース（「ウェブインタフェースを使用した iDRAC6 の設定」を参照）
    - RACADM CLI（「iDRAC6 SM-CLP コマンドラインインタフェースの使用」を参照）
    - Telnet コンソール（「Telnet コンソールの使用」を参照）

    メモ: 複数の iDRAC6 設定ツールを同時に使用すると、不測の結果が生じることがあります。
2. iDRAC6 ネットワークを設定します。「iDRAC6 のネットワーク設定」を参照してください。
3. iDRAC6 ユーザーを追加して設定します。「iDRAC6 ユーザーの追加と設定」を参照してください。
4. ウェブインタフェースにアクセスするために、ウェブブラウザを設定します。「対応ウェブブラウザの設定」を参照してください。
5. Microsoft® Windows® の自動再起動オプションを無効にします。「Windows の 自動再起動オプションを無効にする」を参照してください。
6. iDRAC6 ファームウェアをアップデートします。「iDRAC6 ファームウェアのアップデートを参照してください。

管理下システムへのソフトウェアのインストール

管理下システムへのソフトウェアのインストールは省略可能です。管理下システムソフトウェアがない場合は、RACADM をローカルで使用できず、iDRAC6 は前回のクラッシュ画面をキャプチャできません。

管理下システムソフトウェアをインストールするには、『Dell Systems Management Tools and Documentation DVD』で管理下システムにソフトウェアをインストールします。このソフトウェアのインストール手順については、デルサポートサイト **support.dell.com¥manuals** でダウンロード可能な『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。

管理下システムソフトウェアは、Dell™ OpenManage™ Server Administrator の適切なバージョンから、選択したコンポーネントを管理下システムにインストールします。

メモ: iDRAC6 管理ステーションソフトウェアと iDRAC6 管理下システムソフトウェアを同じシステムにインストールしないでください。

管理下システムに Server Administrator がインストールされていない場合は、システムの前回クラッシュ画面の表示 や**自動リカバリ** 機能は使用できません。

前回クラッシュ画面の詳細については、「前回システムクラッシュ画面の表示」を参照してください。

管理ステーションへの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。

- 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。
- 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。
- Docs - システム管理ソフトウェア製品、周辺機器および RAID コントローラのマニュアルが入っています。
- SERVICE - システムを設定するために必要なツールやシステムの最新の診断および Dell 最適化ドライバが含まれます。

Server Administrator、IT Assistant および Unified Server Configurator の詳細については、デルサポートサイト **support.dell.com¥manuals** で『Server Administrator ユーザーズガイド』、『IT Assistant ユーザーズガイド』および『Unified Server Configurator ユーザーズガイド』を参照してください。

Linux 管理ステーションでの RACADM のインストールと削除

リモート RACADM 機能を使用するには、Linux を実行している管理ステーションに RACADM をインストールします。

メモ: 『Dell Systems Management Tools and Documentation DVD』で **Setup(セットアップ)** を実行すると、サポートされているすべてのオペレーティングシステム用の RACADM ユーティリティが管理ステーションにインストールされます。

RACADM のインストール

1. 管理ステーションコンポーネントをインストールするシステムに、ルート権限でログオンします。
2. 必要に応じて、次のコマンドまたは同等のコマンド を使って、『Dell Systems Management Tools and Documentation DVD』をマウントします。

   ```
   mount /media/cdrom
   ```

3. **/linux/rac** ディレクトリに移動して、次のコマンドを実行します。

   ```
   rpm -ivh *.rpm
   ```

RACADM コマンドに関するヘルプは、コマンドを入力した後「**racadm help** 」と入力してください。

RACADM のアンインストール

RACADM をアンインストールするには、コマンドプロンプトを開いて次のように入力します。

```
rpm -e <racadm パッケージ名>
```

<racadmパッケージ名> は RAC ソフトウェアのインストールに使用する rpm パッケージです。

たとえば、rpm パッケージ名が **srvadmin-racadm5** であれば、次のように入力します。

```
rpm -e srvadmin-racadm5
```

---

iDRAC6 ファームウェアのアップデート

iDRAC6 ファームウェアをアップデートするには、次のいずれかの方法を使用します。

- ウェブインタフェース(「ウェブベースのインタフェースを使用した iDRAC6 ファームウェアのアップデート」を参照)
- RACADM CLI(「RACADM を使用した iDRAC6 ファームウェアのアップデート」を参照)
- Dell Update Packages(「Windows および Linux 対応オペレーティングシステム用の Dell Update Packages を使用した iDRAC6 ファームウェアのアップデート」を参照)

作業を開始する前に

ローカル RACADM またはDell Update Packages を使用して iDRAC6 ファームウェアをアップデートする前に、次の手順を実行してください。この手順を実行しないと、アップデートに失敗することがあります。

1. 適切な IPMI と管理下ノードのドライバをインストールして有効にします。

2. システムで Windows オペレーティングシステムが実行されている場合は、**Windows Management Instrumentation** (WMI) サービスを有効にして起動します。

3. iDRAC6 Enterprise を使用し、システムで SUSE® Linux Enterprise Server（バージョン 10）for Intel® EM64T を実行している場合は、**Raw** サービス を開始します。

4. 仮想メディアを切断してマウント解除します。

   メモ: iDRAC6 ファームウェアのアップデートが何らかの理由で中断されると、ファームウェアのアップデートを再び実行できるまでに最大 30 分間待たなければならない場合があります。

5. USB が有効になっていることを確認してください。

iDRAC6 ファームウェアのダウンロード

iDRAC6 ファームウェアをアップデートするには、デルサポートサイト **support.dell.com** から最新ファームウェアをダウンロードしてローカルシステムに保存します。

iDRAC6 ファームウェアパッケージには、次のソフトウェアコンポーネントが含まれています。

- コンパイルされた iDRAC6 ファームウェアコードとデータ
- ウェブベースのインタフェース、JPEG、およびその他のユーザーインタフェースのデータファイル
- デフォルト構成ファイル

ウェブベースのインタフェースを使用した iDRAC6 ファームウェアのアップデート

詳細については、「iDRAC6 ファームウェア/システムサービスリカバリイメージのアップデート」を参照してください。

RACADM を使用した iDRAC6 ファームウェアのアップデート

CLI ベースの RACADM ツールを使用して、iDRAC6 ファームウェアをアップデートできます。管理下システムに Server Administrator をインストールしている場合は、ローカル RACADM を使用してファームウェアをアップデートしてください。

1. デルのサポートサイト **support.dell.com** から iDRAC6 のファームウェアイメージを管理下システムにダウンロードします。

   例:

   ```
   C:¥downloads¥firmimg.d6
   ```

2. 次の RACADM コマンドを実行します。

   ```
   racadm fwupdate -pud c:¥downloads¥
   ```

   リモート RACADM および TFTP サーバーを使用して、ファームウェアをアップデートすることも可能です。

   例:

   ```
   racadm -r <iDRAC6 IP アドレス> -u <ユーザー名> -p <パスワード> fwupdate -g -u -a <パス>
   ```

   この場合、パス は、**firmimg.d6** が保存されている **TFTP** サーバー上の場所です。

Windows および Linux 対応オペレーティングシステム用の Dell Update Packages を使用した iDRAC6 ファームウェアのアップデート

Windows および Linux の対応オペレーティングシステム用の Dell Update Package をデルのサポートサイト **support.dell.com** からダウンロードして実行します。詳細については、デルサポートサイト **support.dell.com¥manuals** の『Dell Update Package ユーザーズガイド』を参照してください。

メモ: Linux で Dell Update Package ユーティリティを使用して iDRAC6 ファームウェアをアップデートする際は、コンソール上に次のメッセージが表示される場合があります。

```
usb 5-2: device descriptor read/64, error -71
usb 5-2: device descriptor not accepting address 2, error -71
```

これらのエラーは表面的なものであり、無視しても構いません。これらのメッセージは、ファームウェアのアップデートプロセス中に USB デバイスがリセットされたためで、無害です。

ブラウザキャッシュのクリア

ファームウェアアップグレード後、ウェブベースブラウザのキャッシュをクリアします。

詳細については、ウェブブラウザのオンラインヘルプを参照してください。

対応ウェブブラウザの設定

次に、対応ウェブブラウザの設定手順を説明します。

iDRAC6 ウェブインタフェースに接続するためのウェブブラウザの設定

プロキシサーバー経由でインターネットに接続している管理ステーションから iDRAC6 のウェブインタフェースに接続する場合は、このサーバーからインターネットにアクセスするようにウェブブラウザを設定する必要があります。

Internet Explorer ウェブブラウザをプロキシサーバーにアクセスするように設定するには、以下の手順を実行します。

1. ウェブブラウザのウィンドウを開きます。
2. **ツール** をクリックして、**インターネットオプション** をクリックします。
3. **インターネットオプション** ウィンドウで **接続** タブをクリックします。
4. **ローカルエリアネットワーク(LAN)設定** で **LAN 設定** をクリックします。
5. **プロキシサーバーを使用** ボックスが選択されている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** ボックスを選択します。
6. **OK** を 2 度クリックします。

信頼されているドメインのリスト

ウェブブラウザから iDRAC6 ウェブインタフェースにアクセスするとき、信頼されたドメインのリストに iDRAC6 の IP アドレスがない場合は、この IP アドレスをリストに加えるように要求されることがあります。追加したら、更新 をクリックするかウェブブラウザを再起動して、iDRAC6 ウェブインタフェースへの接続を再確立します。

32 ビットと 64 ビットのウェブブラウザ

iDRAC6 ウェブインタフェースは、64 ビットウェブブラウザではサポートされていません。64 ビットブラウザを開いた後、コンソールリダイレクトページにアクセスしてプラグインをインストールすると、インストールに失敗します。このエラーを確認しないでこの手順を繰り返すと、最初の試みでプラグインのインストールに失敗したにも関わらず、コンソールリダイレクトページがロードされます。これは、プラグインのインストールに失敗しても、ウェブブラウザがプロファイルディレクトリにプラグイン情報を保存するからです。この不具合を修正するには、32 ビットの対応ウェブブラウザをインストールして起動し、iDRAC6 にログインしてください。

ウェブインタフェースの日本語版の表示

Windows

iDRAC6 ウェブインタフェースは、次の Windows オペレーティングシステム言語でサポートされています。

- 英語
- フランス語
- ドイツ語
- スペイン語
- 日本語
- 簡体字中国語

Internet Explorer で iDRAC6 ウェブインタフェースのローカライズバージョンを表示するには、次の手順に従います。

1. **ツール** をクリックして、**インターネットオプション** を選択します。
2. **インターネットオプション** ウィンドウで **言語** をクリックします。
3. **言語設定 ウィンドウで 追加** をクリックします。

4. **言語の追加** ウィンドウでサポートされている言語を選択します。

   複数の言語を選択するには、<Ctrl> を押しながら選択します。

5. 優先言語を選択して **上に移動** をクリックし、その言語をリストの先頭に移動します。

6. **OK** をクリックします。

7. **言語設定** ウィンドウで **OK** をクリックします。

Linux

Red Hat® Enterprise Linux®（バージョン 4）クライアントで簡体字中国語の GUI を使ってコンソールリダイレクトを実行している場合は、ビューアのメニューとタイトルが文字化けすることがあります。この問題は、Red Hat Enterprise Linux (バージョン 4) 簡体字中国語オペレーティングシステムでのエンコードエラーによるものです。この問題を解決するには、次の手順で現在のエンコード設定にアクセスして変更してください。

1. コマンド端末を開きます。

2. 「locale」と入力して、<Enter> を押します。次の出力が表示されます。

```
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」が含まれている場合は、変更する必要はありません。値に「zh_CN.UTF-8」が含まれていない場合は、ステップ 4 に進んでください。

4. **/etc/sysconfig/i18n** ファイルに移動します。

5. ファイルに次の変更を加えます。

   現在のエントリ：

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

6. ログアウトしてから、オペレーティングシステムにログインします。

7. iDRAC6 を再起動します。

他の言語から簡体字中国語に切り替える場合は、この修正がまだ有効であることを確認してください。有効でない場合は、この手順を繰り返します。

iDRAC6 の詳細設定については、「iDRAC6 の詳細設定」を参照してください。

目次ページに戻る

目次ページに戻る

ウェブインタフェースを使用した iDRAC6 の設定

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

iDRAC6 には、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）システムのリモート管理タスクとトラブルシューティングを可能にするウェブ インタフェースが備わっています。日常のシステム管理に、iDRAC6 ウェブインタフェースを使用してください。この章では、iDRAC6 のウェブインタフェースを使って一般的なシステム管理タスクを実行する方法について説明し、関連情報へのリンクも掲載しています。

ほとんどのウェブインタフェースの設定タスクは、RACADM コマンドまたは SM-CLP（サーバー管理コマンドラインプロトコル）を使用して実施することも可能です。

ローカル RACADM コマンドは、管理下サーバーから実行できます。

SM-CLP および SSH/Telnet RACADM コマンドは、Telnet または SSH 接続によってリモートアクセス可能なシェルにて実行されます。SM-CLP の詳細については、「iDRAC6 SM-CLP コマンドラインインタフェースの使用」を参照してください。RACADM コマンドの詳細については、「RACADM サブコマンドの概要」および「iDRAC6 プロパティデータベースグループとオブジェクト定義」を参照してください。

ウェブインタフェースへのアクセス

iDRAC6 ウェブインタフェースにアクセスするには、次の手順を実行します。

1. サポートされているウェブブラウザのウィンドウを開きます。

   詳細については、「対応ウェブブラウザ」を参照してください。

   IPv4 アドレスを使用してウェブインタフェースにアクセスする場合は、ステップ 2 へ進みます。

   IPv6 アドレスを使用してウェブインタフェースにアクセスする場合は、ステップ 3 へ進んでください。

2. IPv4 アドレスを使用してウェブインタフェースにアクセスするには、IPv4 が有効になっている必要があります。

   ブラウザの **アドレス** バーに、次のように入力します。

   https://<iDRAC IPv4 アドレス>

   次に、<Enter> キーを押します。

3. IPv6 アドレスを使用してウェブインタフェースにアクセスするには、IPv6 が有効になっている必要があります。

   ブラウザの **アドレス** バーに、次のように入力します。

   https://[<iDRAC IPv6 アドレス>]

   次に、<Enter> キーを押します。

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

   https://<iDRAC IP アドレス>:<ポート番号>

   iDRAC IP アドレス は iDRAC6 用の IPアドレスで、ポート番号 は HTTPS ポート番号です。

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

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

   https://<iDRAC IP アドレス>:<ポート番号>

   iDRAC IP アドレス は iDRAC6 用の IPアドレスで、ポート番号 は HTTPS ポート番号です。

iDRAC6 **ログイン** ウィンドウが表示されます。

ログイン

iDRAC6 ユーザーまたは Microsoft® Active Directory® ユーザーとして ログインできます。iDRAC6 ユーザーのデフォルトのユーザー名とパスワードは、それぞれ **root** および **calvin** です。

iDRAC6 にログインするには、システム管理者から **iDRAC へのログイン** 権限が与えられている必要があります。

ログインするには、次の手順に従ってください。

1. **ユーザー名** フィールドに、次のいずれかを入力します。

   - iDRAC6 ユーザー名。

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

   - Active Directory ユーザー名。

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

2. **パスワード** フィールドに、iDRAC6 のユーザーパスワードまたは Active Directory のユーザーパスワードを入力します。パスワードでは大文字と小文字が区別されます。

3. **ドメイン**ドロップダウンボックスから、This iDRAC を選択して iDRAC6 ユーザーとしてログインするか、利用可能ないずれかのドメインを選択して Active Directory ユーザーとしてログインします。

   メモ: Active Directory ユーザーの場合、ユーザー名の一部としてドメイン名を指定した場合は、ドロップダウンメニューから This iDRAC を選択します。

4. **OK** をクリックするか、Enter キーを押します。

ログアウト

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

2. ブラウザウィンドウを閉じます。

メモ: ログインするまで **ログアウト** ボタンは表示されません。

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

メモ: Microsoft Internet Explorer で、ウィンドウの右上隅の閉じるボタン("x")を使用して iDRAC6 ウェブインタフェースを閉じると、アプリケーションエラーが発生する可能性があります。この不具合を修正するには、Microsoft サポートウェブサイト **support.microsoft.com** から、最新の Internet Explorer 用累積セキュリティアップデートをダウンロードしてください。

---

iDRAC6 NIC の設定

ここでは、iDRAC6 が設定済みで、ネットワーク上でアクセス可能であると想定しています。iDRAC6 ネットワークの初期設定については、「iDRAC6 の設定」を参照してください。

ネットワークと IPMI LAN の設定

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

メモ: ほとんどの DHCP サーバーは、予約テーブルにクライアントの ID トークンを保存するためのサーバーを必要とします。このトークンは、クライアント(たとえば iDRAC)が DHCP ネゴシエーション中に提供します。iDRAC6 は、1 バイトのインタフェース 番号(0)とそれに続く 6 バイトの MAC アドレスを使用して、クライアント ID オプションを提供します。

メモ: スパニングツリープロトコル (STP) を有効にして実行している場合は、PortFast または同様のテクノロジも、次のとおり有効になっていることを確認してください。

- iDRAC6 に接続しているスイッチのポート上
- iDRAC KVM セッションを実行中の管理ステーションに接続しているポート上

メモ: POST 中にシステムが停止した場合は、「続行するには F1 キー、システムセットアッププログラムを実行するには F2 を押してください」というメッセージが表示される可能性があります。このエラーの原因としては、iDRAC6 との通信喪失を引き起こすネットワークストームイベントが考えられます。ネットワークストームが収まった後、システムを再起動します。

1. **リモートアクセス** → **設定** → **ネットワーク** の順にクリックします。

2. **ネットワーク** ページでは、ネットワークインタフェースカードの設定、共通 iDRAC 設定、IPv4 設定、IPv6 設定、IPMI 設定、および VLAN 設定を入力できます。これらの設定については、「表 4-1」、「表 4-2」、「表 4-3」、表 4-4、「表 4-5」、および「表 4-6」を参照してください。

3. 必要な設定を入力したら、**変更の適用** をクリックします。

4. 適切なボタンをクリックして続行します。「表 4-7」を参照してください 。

表 4-1 ネットワークインタフェースカードの設定

設定	説明
NIC の選択	次の 4 つのモードから現在のモードを設定します。 · 専用(iDRAC NIC) **メモ:** このオプションは iDRAC6 Enterprise でのみ使用可能です。 · 共有(LOM1) · フェールオーバーで共有(LOM2) · フェールオーバーで共有(すべての LOM) **メモ:** このオプションは、iDRAC6 Enterprise では使用できない場合があります。 **メモ:** **NIC の選択** が **共有** または **フェールオーバーで共有** モードの場合、iDRAC6 は同じ物理ポート経由でローカル通信を行いません。これは、ネットワークスイッチがパケットを受信したポートと同じポートからパケットを送信しないからです。
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。
NIC を有効にする	選択すると、NIC が有効になり、このグループの残りのコントロールがアクティブになることを示します。NIC が無効になっている場合は、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、**オン** です。
オートネゴシエーション	**オン** に設定した場合は、最も近いルーターまたはハブと通信してネットワーク速度とモードを表示します。**オフ** に設定した場合は、ネットワーク速度とデュプレックスモードを手動で設定できます(オフ)。 **NIC の選択** が **専用** に設定されていない場合は、オートネゴシエーションは常に有効になります**(オン)**。
ネットワーク速度	ネットワーク環境に合わせて、ネットワーク速度を 100 Mb または 10 Mb に設定することができます。このオプションは、オートネゴシエーションが **オン** に設定されているときは使用できません。
デュプレックスモード	ネットワーク環境に合わせて、デュプレックスモードを全二重または半二重に設定することができます。**オートネゴシエーション** が **オン** の場合、このオプションは使用できません。

表 4-2 共通 iDRAC 設定

設定	説明
DNS に iDRAC を登録	DNS サーバーに iDRAC6 の名前を登録します。 デフォルトは **無効** です。
DNS iDRAC 名	**DNS に iDRAC を登録** が選択されている場合にのみ、iDRAC6 名を表示します。デフォルト名は idrac-サービス_タグで、サービス_タグは Dell サーバーのサービスタグ番号を示します。例:idrac-00002
DNS ドメイン名に DHCP を使用	デフォルトの DNS ドメイン名を使用します。このチェックボックスがオフで、**DNS に iDRAC を登録** オプションがオンの場合は、**DNS ドメイン名** フィールドで DNS ドメイン名を変更します。 デフォルトは **無効** です。 **メモ:** **DNS ドメイン名に DHCP を使用** チェックボックスをオンにするには、**DHCP の使用(NIC IP アドレス用)**チェックボックスもオンにする必要があります。
DNS ドメイン名	デフォルトの **DNS ドメイン名** は空白です。**DNS ドメイン名に DHCP を使用** チェックボックスがオンの場合は、このオプションがグレー表示になり、フィールドを変更できません。

表 4-3 IPv4 の設定

設定	説明
有効	NIC を有効にすると、IPv4 プロトコルサポートが選択され、このセクションの他のフィールドが有効に設定されます。
NIC IP アドレスに DHCP を使用	iDRAC6 に動的ホスト構成プロトコル(DHCP)サーバーから NIC 用の IP アドレスを取得するように指示します。デフォルトは **オフ** です。
IP アドレス	iDRAC6 の IC IP アドレスを指定します。
サブネットマスク	iDRAC6 NIC の静的 IP アドレスを入力または編集できます。この設定を変更するには、[DHCP を使用(NIC IP アドレス用)] チェックボックスをオフにします。
ゲートウェイ	ルーターまたはスイッチのアドレス この値は「ドット区切り」の形式です。例:192.168.0.1
DHCP を使用して DNS サーバーアドレスを取得する	**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオンにし、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、**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。 デフォルトは **オフ** です。 **メモ:** **DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスがオンの場合は、**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	DNS サーバーの IP アドレス
代替 DNS サーバー	代替 IP アドレス

表 4-4 IPv6 の設定

設定	説明
有効	チェックボックスをオンにした場合は、IPv6 が有効になります。チェックボックスをオフにした場合は、IPv6 が無効になります。デフォルトは無効です。
Auto Config（自動設定）	このチェックボックスをオンにすると、iDRAC6 は動的ホスト設定（DHCPv6）サーバーから iDRAC6 NIC の IPv6 アドレスを取得できます。**Auto Config（自動設定）** を有効にすると、IP アドレス、プレフィックス長、および IP ゲートウェイの静的な値を非アクティブにして削除します。
IP アドレス 1	iDRAC NIC の IPv6 アドレスを設定します。この設定を変更するには、まず関連するチェックボックスをオフにして **AutoConfig** を無効にする必要があります。
プレフィックス長	IPv6 アドレスのプレフィ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、まず関連するチェックボックスをオフにして **AutoConfig** を無効にする必要があります。
IP ゲートウェイ	iDRAC NIC の静的ゲートウェイを設定します。この設定を変更するには、まず関連するチェックボックスをオフにして **AutoConfig** を無効にする必要があります。
リンクのローカルアドレス	iDRAC6 の NC IPv6 アドレスを指定します。
IP アドレス 2	追加の iDRAC6 NIC IPv6 アドレスがある場合は、それも指定します。
DHCP を使用して DNS サーバーアドレスを取得する	**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオンにし、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、**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。 デフォルトはオフです。見直しコピーを確認します。 メモ: **DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスがオンの場合は、IP アドレスを **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、まず**DHCP を使用して DNS サーバーアドレスを取得する** を選択解除する必要があります。
代替 DNS サーバー	代替 DNS サーバーの静的 IPv6 アドレスを設定します。この設定を変更するには、まず **DHCP を使用して DNS サーバーアドレスを取得する** をオフにする必要があります。

表 4-5 IPMI 設定

設定	説明
IPMI オーバー LAN を有効にする	このチェックボックスがオンになっていると、IPMI LAN チャネルが有効であることを示します。デフォルトは **オフ** です。
チャネル権限レベルの制限	LAN チャネル上で許可されるユーザーの最小権限レベルを設定します。**システム管理者（Administrator）**、**オペレータ**、**ユーザー** のオプションから 1 つを選択します。デフォルトは **システム管理者（Administrator）** です。
暗号キー	暗号キーの文字形式の設定では、0 ～ 20 の 16 進数の文字を使用します（空白は使用できません）。デフォルトは空白です。

表 4-6 VLAN の設定

設定	説明
VLAN ID を有効にする	有効である場合、一致する仮想 LAN (VLAN) ID トラフィックのみが受け入れられます。
VLAN ID	802.1g フィールドの VLAN ID フィールド。VLAN ID の有効値を入力します (1 ～ 4094 の値を指定する必要があります)。
優先度	802.1g フィールドの [優先度] フィールド。0 ～ 7 の値を入力して、VLAN ID の優先度を設定します。

表 4-7 ネットワーク設定ページのボタン

ボタン	説明
印刷	画面に表示されている **ネットワーク設定** ページの値を印刷します。
更新	**ネットワーク設定** ページを再ロードします。
詳細設定	**ネットワークセキュリティ** ページを開いて、IP 範囲と IP ブロックの属性を入力できます。
変更の適用	ネットワーク設定ページに追加された新規設定を保存します。 **メモ:** NIC の IP アドレス設定を変更すると、すべてのユーザーセッションが終了します。ユーザーは、更新後の IP アドレス設定を使って iDRAC6 ウェブインタフェースに再接続する必要があります。その他の変更では NIC をリセットする必要があり、このため接続が一時的に途絶える場合があります。

IP フィルタおよびIP ブロックの設定

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

1. **リモートアクセス** → **設定** をクリックし、次に **ネットワーク** タブをクリックして **ネットワーク** ページを開きます。
2. **詳細設定** をクリックして、ネットワークセキュリティ設定を行います。

   表 4-8で、**ネットワークセキュリティ ページの設定** について説明します。設定が完了したら、**適用** をクリックします。
3. 適切な ボタンをクリックして続行します。表 4-9を参照してください 。

表 4-8 ネットワークセキュリティページの設定

設定	説明
IP 範囲を有効にする	IP 範囲のチェック機能を有効します。これにより、iDRAC にアクセスできる IP アドレスの範囲を定義できます。デフォルトは **オフ** です。
IP 範囲のアドレス	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。可能な IP アドレスの上位部分を決定するため、この値は IP 範囲サブネットマスクとビット単位で AND されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインには失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0～192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。デフォルトは **255.255.255.0** です。
IP ブロックを有効にする	事前に選択した時間枠で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。デフォルトは **オフ** です。
IP ブロックエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。デフォルトは **10** です。
IP ブロックエラー時間枠	IP ブロックペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間枠を秒で指定します。デフォルトは **3600** です。
IP ブロックペナルティ時間	ログイン失敗回数が制限値を超えた IP アドレスからのログインを拒否する時間を秒で指定します。デフォルトは **3600** です。

表 4-9 ネットワークセキュリティページのボタン

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

プラットフォームイベントの設定

プラットフォームイベントの設定では、特定のイベントメッセージに対して iDRAC6 が選択した処置を実行するように設定します。処置には、処置の必要なし、システムの再起動、システムの電源を入れ直す、システムの電源を切る、警告の生成（プラットフォームイベントトラップ [PET] 、電子メール）があります。

表 4-10 に、フィルタ可能なプラットフォームイベントを示します。

表 4-10 プラットフォームイベントフィルタ

索引	プラットフォームイベント
1	ファン重要アサート
2	バッテリー警告アサート
3	バッテリー重要アサート
4	低電圧重要アサート
5	温度警告アサート
6	温度重要アサート
7	侵入重要アサート
8	ファン冗長性低下
9	ファン冗長性喪失
10	プロセッサ警告アサート
11	プロセッサ重要アサート

12	プロセッサがありません
13	電源供給警告アサート
14	電源供給重要アサート
15	電源装置がありません
16	イベントログ重要アサート
17	ウォッチドッグ重要アサート
18	システム電源警告アサート
19	システム電源重要アサート

。

プラットフォームイベント（たとえば、バッテリー警告アサート）が発生すると、システムイベントが生成され、システムイベントログ（SEL）に記録されます。このイベントが、有効に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動作（システムの再起動など）を実行するように設定すると、その動作が行われます。

プラットフォームイベントフィルタ（PEF）の設定

メモ: プラットフォームイベントトラップまたは電子メール警告を設定する前に、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. 対応ウェブブラウザを使ってリモートシステムにログインします。「ウェブインタフェースへのアクセス」を参照してください。
2. **システム** → **警告管理** → **プラットフォームイベント** の順にクリックします。
3. 最初のテーブルで、**プラットフォームイベントフィルタ警告を有効にする** チェックボックスをオンにし、**変更の適用** をクリックします。

   メモ: 設定されている有効な送信先（PET または電子メール）に警告を送信するためには、**プラットフォームイベントフィルタ警告を有効にする** を有効にする必要があります。
4. 次の表の **プラットフォームイベントフィルタリスト** で、設定するフィルタをクリックします。
5. **プラットフォームイベント設定** ページで、適切な **シャットダウン動作** または **なし** を選択します。
6. **警告の生成** をオンまたはオフにして、この処置を有効または無効にします。

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

   プラットフォームイベント ページが再表示され、実行した変更が **プラットフォームイベントフィルタリスト** に表示されます。
8. ステップ 4 ～ 7 を繰り返して追加のプラットフォームイベントフィルタを設定します。

プラットフォームイベントトラップ（PET）の設定

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

1. 対応ウェブブラウザを使ってリモートシステムにログインします。「ウェブインタフェースへのアクセス」を参照してください。
2. 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。
3. **システム** → **警告管理** → **トラップ設定** の順にクリックします。
4. IPv4 送信先リスト または **IPv6 送信先リスト** で、送信先番号**をクリック**して IPv4 または IPv6 SNMP 警告送信先を設定します。
5. **プラットフォームイベント警告送信先の設定** ページで、**送信先を有効にする** をオンまたはオフにします。チェックボックスがオンになっていると、警告受信用の IP アドレスが有効になっていることを示しています。チェックボックスがオフの場合は、警告受信用の IP アドレスが無効になっていることを示しています。
6. 有効なプラットフォームイベントトラップ送信先 IP アドレスを入力し、**変更の適用** をクリックします。
7. **テストトラップを送信** をクリックして設定済み警告をテストするか、**プラットフォームイベント送信先ページへ戻る** をクリックします。

   メモ: テストトラップを送信するには、ユーザーアカウントに **テスト警告** 権限が必要です。詳細については、表 6-6 の「iDRAC グループ権限」を参照してください。

プラットフォームイベント警告送信先 ページで、適用された変更が IPv4 または IPv6 **送信先リスト** に表示されます。

8. **コミュニティ文字列**フィールドで、適切な iDRAC SNMP コミュニティ名を入力します。**変更の適用** をクリックします。

   メモ: 送信先コミュニティ文字列は iDRAC6 コミュニティ文字列と同じである必要があります。

9. ステップ 4 ～ 7 を繰り返して、追加の IPv4 または IPv6 送信先番号を設定します。

電子メール警告の設定

メモ: 電子メール警告は IPv4 および IPv6 の両方のアドレスをサポートしています。

1. 対応ウェブブラウザを使ってリモートシステムにログインします。
2. 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。
3. **システム** → **警告管理** → **電子メール警告の設定** の順にクリックします。
4. **送信先電子メールアドレス** の表で、送信先アドレスを設定する対象の **電子メール警告番号** をクリックします。
5. **電子メール警告の設定** ページで、**電子メール警告を有効にする** をオンまたはオフにします。チェックボックスがオンの場合は、警告受信用の電子メールアドレスが有効になっていることを示しています。チェックボックスがオフの場合は、警告受信用の電子メール アドレスが無効になっていることを示しています。
6. **送信先電子メールアドレス** フィールドに有効な電子メールアドレスを入力します。
7. **電子メールの説明** フィールドに、電子メールに表示する短い説明を入力します。
8. **変更の適用** をクリックします。
9. 設定済みの電子メール警告をテストする場合、**テスト電子メールの送信** をクリックします。テストしない場合、**電子メール警告送信先ページへ戻る** をクリックします。
10. **電子メール警告送信先ページへ戻る** をクリックし、**SMTP（電子メール）サーバー IP アドレス** フィールドに有効な SMTP IP アドレスを入力します。

    メモ: テスト電子メールの送信に成功するには、**電子メール警告設定**ページで **SMTP（電子メール）サーバー IP アドレス** を設定する必要があります。SMTP サーバーは設定した IP アドレスを使用して iDRAC6 と通信し、プラットフォームイベントが発生したときに電子メール警告を送信します。

11. **変更の適用** をクリックします。
12. ステップ 4 ～ 9 を繰り返して、追加の電子メール警告送信先を設定します。

IPMI の設定

1. 対応ウェブブラウザを使ってリモートシステムにログインします。
2. IPMI オーバー LAN を設定します。
   a. **システム** ツリーの **リモートアクセス** をクリックします。
   b. **設定** タブをクリックし、**ネットワーク** をクリックします。
   c. **ネットワーク設定** ページの **IPMI LAN 設定** で **IPMI オーバー LAN を有効にする** を選択して **変更の適用** をクリックします。
   d. 必要に応じて IPMI LAN チャネル権限を更新します。

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

   IPMI LAN 設定で **チャネル権限レベルの制限** ドロップダウンメニューをクリックし、**管理者**、**オペレータ**、または **ユーザー** を選択して、**変更の適用** をクリックします。

   e. 必要に応じて IPMI LAN チャネルの暗号キーを設定します。

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

   暗号鍵 フィールドの **IPMI LAN 設定** に暗号鍵を入力して、**変更の適用** をクリックします。

メモ: 暗号鍵は 40 文字までの偶数の 16 進数で指定します。

3. IPMI シリアルオーバー LAN (SOL)を設定します。
   a. **システム** ツリーの **リモートアクセス** をクリックします。
   b. **設定** タブで **シリアルオーバー LAN** をクリックします。
   c. **シリアルオーバー LAN の設定** ページで **シリアルオーバー LAN を有効にする** を選択します。
   d. IPMI SOL ボーレートを更新します。

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 ボーレートが管理下システムのボーレートと同じであることを確認してください。

   e. **ボーレート**ドロップダウンメニューで、適切なボーレートを選択して **変更の適用** をクリックします。
   f. **最低限必要な権限 を更新します。**このプロパティは、**シリアルオーバー LAN** 機能を使うために最低限必要なユーザー権限を定義します。

      チャネル権限レベルの制限 ドロップダウンメニューで、**ユーザー**、**オペレータ**、または **管理者** を選択します。

   g. **変更の適用** をクリックします。

4. IPMI シリアルを設定します。
   a. **設定** タブで **シリアル** をクリックします。
   b. **シリアルの設定** メニューで、IPMI シリアル接続モードを適切な設定に変更します。

      IPMI シリアル の **接続モードの設定** ドロップダウンメニューで適切なモードを選択します。

   c. IPMI シリアルボーレートを設定します。

      ボーレートドロップダウンメニューをクリックして、適切なボーレートを選択し、**変更の適用** をクリックします。

   d. チャネル権限レベルの制限を設定します。

      チャネル権限レベルの制限 ドロップダウンメニューで **管理者**、**オペレータ**、または **ユーザー** を選択します。

   e. **変更の適用** をクリックします。
   f. 管理下システムの BIOS セットアッププログラムでシリアル MUX が正しく設定されていることを確認します。
      - システムを再起動します。
      - POST 中に F2 を押して BIOS セットアッププログラムを起動します。
      - **シリアル通信** に移動します。
      - **シリアル接続** メニューで **外部シリアルコネクタ** が **リモートアクセスデバイス** に設定されていることを確認します。
      - 保存して BIOS セットアッププログラムを終了します。
      - システムを再起動します。

IPMI シリアルが端末モードの場合は、次の設定を追加できます。

- 削除制御
- エコー制御
- Line edit
- New line sequences
- Input new line sequences

For more information about these properties, see the IPMI 2.0 specification.ターミナルモードコマンドの詳細については、**support.dell.com¥manuals¥** の『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

---

iDRAC6 ユーザーの設定

詳細については、「iDRAC6 ユーザーの追加と設定」を参照してください。

SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保

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

- SSL (Secure Sockets Layer)

- 証明書署名要求 (CSR)
- ウェブインタフェースを介した SSL へのアクセス
- CSR の生成
- サーバー証明書のアップロード
- 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。

- SSL 対応クライアントに自らを認証する
- 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
- 両システムが暗号化接続を確立できるようにする

暗号化プロセスは高度なデータ保護を提供します。iDRAC6 では、北米のインターネットブラウザで一般的に使用されている最も安全な暗号化方式である 128 ビットの SSL 暗号化標準を採用しています。

iDRAC6 のウェブサーバーは、デフォルトでDell の署名入り SSL デジタル証明書(サーバー ID)を提供します。インターネット上で高いセキュリティを確保するには、ウェブサーバーの SSL 証明書を、著名な認証局によって署名された証明書で置き換えてください。署名された証明書を取得するには、まず、iDRAC6 ウェブインタフェースを使用して企業情報を掲載した証明書署名要求(CSR)を生成します。生成した CSR を VeriSign や Thawte などの 認証局(CA) に送信します。

証明書署名要求 (CSR)

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

認証局(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 には、Thawte や VeriSign などがあります。CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ基準を満たしていれば、ネットワークやインターネット上でトランザクションを行う申請者を個別に識別するデジタル署名付き証明書を発行します。

CA が CSR を承認して証明書を送信したら、それを iDRAC6 ファームウェアにアップロードします。iDRAC6 ファームウェアに保管されている CSR 情報は、証明書に記載されている情報と一致する必要があります。

ウェブインタフェースを介した SSL へのアクセス

1. **リモートアクセス**→ **設定**をクリックします。
2. **SSL** をクリックして **SSL** ページを開きます。

SSL ページを使用して次のいずれかのオプションを実行します。

- CA に送信する証明書署名要求(CSR)を生成する。CSR 情報は iDRAC6 ファームウェアに保存されています。
- サーバー証明書をアップロードする。
- サーバー証明書を表示する

表 4-11では、上記の **SSL** ページのオプションについて説明しています。

表 4-11 SSL ページのオプション

フィールド	説明
証明書署名要求 (CSR) の生成	このオプションにより、CA に送信する安全なウェブ証明書を要求するための CSR を生成できます。 **メモ:** 新しい CSR は、ファームウェアにある古い CSR を上書きします。CA が CSR を受け入れるためには、ファームウェアにある CSR が CA から返された証明書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	このオプションにより、会社が保有する既存の証明書をアップロードし、iDRAC6 へのアクセス制御に利用できます。 **メモ:** iDRAC6 で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER でエンコードされた証明書は受け入れられません。新しい証明書をアップロードすると、iDRAC6 を使って受信したデフォルトの証明書と置き換えられます。
サーバー証明書の表示	このオプションにより、既存のサーバー証明書を表示できます。

証明書署名要求の生成

メモ: 新しい CSR はファームウェアに保存されている古い CSR データを上書きします。iDRAC が署名済み CSR を受け入れる前に、CA から返された証明書とファームウェアの CSR が一致する必要があります。

1. **SSL** ページで、**証明書署名要求(CSR)の生成** を選択し、**次へ** をクリックします。
2. **証明書署名要求(CSR)の生成** ページで、各 CSR 属性の値を入力します。表 4-12 では、CSR 属性について説明しています。
3. **生成** をクリックして CSR を生成し、ローカルコンピュータへダウンロードします。
4. 適切な ボタンをクリックして続行します。表 4-13 を参照してください 。

表 4-12 証明書署名要求(CSR)属性の生成

フィールド	説明
コモンネーム	証明する名前(通常は **www.xyzcompany.com** のような iDRAC のドメイン名)。英数字、ハイフン、アンダースコア、スペース、ピリオドが有効です。
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 Tokyo)。英数字とスペースのみが有効です。略語は使用しないでください。
国番号	証明書を申請している組織が所在する国の名前。
電子メール	CSR に関連付けられている電子メールアドレス。組織の電子メールアドレスまたは CSR に関連付ける電子メールアドレスを入力します。このフィールドは任意選択です。

表 4-13 証明書署名要求(CSR)生成 ページのボタン

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

サーバー証明書のアップロード

1. **SSL** ページで **サーバー証明書のアップロード** を選択して **次へ** をクリックします。

   サーバー証明書のアップロード ページが表示されます。
2. **ファイルパス** フィールドの **値** フィールドに証明書のパスを入力するか、**参照** をクリックして証明書ファイルに移動します。

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

3. **適用** をクリックします。
4. 適切なボタンをクリックして続行します。表 4-14を参照してください 。

表 4-14 証明書のアップロードページのボタン

ボタン	説明
印刷	**証明書のアップロード** ページを印刷します。
SSL メインメニューに戻る	**SSL メインメニュー** ページに戻ります。
適用	証明書を iDRAC6 ファームウェアに適用します。

サーバー証明書の表示

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

   サーバー証明書の表示 ページは、iDRAC へアップロードしたサーバー証明書を表示します。

   表 4-15に、**証明書** テーブルに表示されるフィールドと関連する説明を記載してします。

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

表 4-15 証明書情報

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

表 4-16 サーバー証明書の表示ページのボタン

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

Active Directory 証明書の設定と管理

このページでは、Active Directory 設定の設定と管理ができます。

メモ: Active Directory を使用または設定するには、**iDRAC の設定**権限が必要です。

メモ: Active Directory の機能を設定または使用する前に、Active Directory サーバーと iDRAC6 が通信できるように設定されていることを確認してください。

メモ: Active Directory 設定の詳細および拡張スキーマまたは標準スキーマによる Active Directory の設定方法については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。

Active Directory の設定と管理 ページにアクセスするには、次の手順を実行してください。

1. **リモートアクセス** → **設定** の順にクリックします。

2. **Active Directory** をクリックして **Active Directory の設定と管理** ページを開きます。

   表 4-17 に、**Active Directory の設定と管理** ページのオプションを示します。

3. 適切な ボタンをクリックして続行します。表 4-18を参照してください 。

表 4-17 Active Directory の設定と管理 ページのオプション

Attribute(属性)	説明
共通設定	
Active Directory が有効	Active Directory が有効か無効かを指定します。
シングルサインオンが有効	シングルサインオンが有効か無効かを指定します。有効の場合は、ユーザー名やパスワードなどのドメインユーザー資格情報を入力せずに、iDRAC6 にログインできます。値は **はい** と **いいえ** です。
スキーマの選択	Active Directory で標準スキーマが使用されているか拡張スキーマが使用されているかを指定します。 **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。
ユーザードメイン名	この値は最大 40 個のユーザードメインエントリを保持します。設定した場合、ログインユーザーが選択できるユーザードメイン名のリストがログインページのプルダウンメニューに表示されます。設定しなかった場合でも、Active Directory ユーザーは ユーザー名@ドメイン名、ドメイン名/ユーザー名、または ドメイン名¥ユーザー名 の形式でユーザー名を入力すると、ログインできます。
タイムアウト	Active Directory クエリが完了するまで待つ時間(秒)を指定します。デフォルト値は 120 秒です。

ドメインコントローラーサーバーアドレス 1-3 (FQDN または IP)	ドメインコントローラーの完全修飾ドメイン名(FQDN)または IP アドレスを指定します。3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC は、接続が確立されるまで、設定されたアドレスに一つずつ接続を試みます。拡張スキーマを選択した場合、これらは iDRAC デバイスオブジェクトと関連オブジェクトが存在するドメインコントローラーのアドレスです。標準スキーマを選択した場合、これらはユーザーアカウントとロールグループが存在するドメインコントローラのアドレスです。
証明書検証が有効	iDRAC は Active Directory への接続時に、SSL(セキュリティソケットレイヤ)経由で LDAP(Lightweight Directory Access Protocol) を使用します。デフォルト設定では、iDRAC は SSL(セキュリティソケットレイヤ)のハンドシェーク中、iDRAC にロードされた CA 証明書を使用してドメインコントローラーの SSL(セキュリティソケットレイヤ)サーバー証明書を検証し、強力なセキュリティを提供します。テスト目的の場合や、システム管理者が SSL(セキュリティソケットレイヤ)証明書を検証せずにセキュリティ境界内のドメインコントローラーを信頼することにした場合は、証明書の検証を無効にできます。このオプションは、証明書の検証を有効にするか無効にするかを指定します。
Active Directory CA 証明書	
証明書	すべてのドメインコントローラーのSSL(セキュリティソケットレイヤ)サーバー証明書に署名する認証局の証明書。
拡張スキーマの設定	**iDRAC 名**:Active Directory 内の iDRAC を一意に識別する名前を指定します。この値はデフォルトでは NULL になっています。 **iDRAC ドメイン名**:Active Directory iDRAC オブジェクトが存在するドメインの DNS 名(文字列)。この値はデフォルトでは NULL になっています。 これらの設定は、拡張 Active Directory スキーマで iDRAC 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。
標準スキーマ設定	**グローバルカタログサーバーアドレス 1-3(FQDN または IP)**:グローバルカタログサーバーの完全修飾ドメイン名(FQDN)または IP アドレスを指定します。3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC は、接続が確立されるまで、設定されたアドレスに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。 **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。 **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。 **グループドメイン**: グループドメインを指定します。 **グループ権限**: グループ権限レベルを指定します。 これらの設定は、標準 Active Directory スキーマで iDRAC 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。

表 4-18 Active Directory の設定と管理 ページのボタン

ボタン	定義
印刷	Active Directory の設定と管理 ページに表示される値を印刷します。
更新	Active Directory の設定と管理 ページを再ロードします。
Active Directory の設定	Active Directory を設定できます。設定情報の詳細については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。
設定のテスト	指定した設定を使用して Active Directory の設定をテストできます。**設定のテスト** オプションの使用方法については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。

---

iDRAC6 サービスの設定

メモ: これらの設定を変更するには、**iDRAC の設定** 権限が必要です。

1. リ**モートアクセス** → **設定** の順にクリックします。次に、**サービス** タブをクリックして **サービス**設定 ページを表示します。
2. 必要に応じて、次のサービスを設定します。
   - ローカル設定 -表 4-19を参照
   - ウェブサーバー - ウェブサーバーの設定については表 4-20を参照
   - SSH - SSH 設定については表 4-21を参照
   - Telnet - Telnet 設定については表 4-22を参照
   - リモート RACADM - リモート RACADM 設定については表 4-23を参照
   - SNMP - SNMP 設定については表 4-24を参照
   - 自動システムリカバリ(ASR)エージェント - ASR エージェント設定については表 4-25を参照
3. **適用** をクリックします。
4. 適切なボタンをクリックして続行します。表 4-26を参照してください 。

表 4-19 ローカル設定

設定	説明

オプション ROM を使用して iDRAC ローカル設定を無効にする	オプションの ROM を使用して iDRAC のローカル設定を無効にします。オプションの ROM は BIOS 内にあり、BMC および iDRAC の設定を可能にするユーザーインタフェースエンジンを提供します。オプションの ROM は、<Ctrl+E> を押してセットアップモジュールを開始するよう指示します。
RACADM を使用して iDRAC ローカル設定を無効にする	ローカル RACADM を使用した iDRAC のローカル設定を無効にします。

表 4-20 ウェブサーバーの設定

設定	**説明**
有効	iDRAC ウェブサーバーを有効または無効にします。チェックボックスがオンの場合は、ウェブサーバーが有効であることを示します。デフォルトは **有効** です。
最大セッション数	システムで許可される同時セッションの最大数。このフィールドは編集できません。最大同時セッション数は 5 です。
アクティブセッション数	システムの現在のセッション数(**最大セッション数** 以下)。このフィールドは編集できません。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更はすぐに適用され、現在のウェブインタフェースセッションが終了します。ウェブサーバーもリセットされます。新しいウェブインタフェースセッションが始まるまで数分お待ちください。タイムアウト範囲は 60 ～ 10800 秒です。デフォルト値は 1800 秒です。
HTTP ポート番号	ブラウザ接続で iDRAC6 が通信するポート。デフォルトは **80** です。
HTTPS ポート番号	セキュアなブラウザ接続で iDRAC6 が通信するポート。デフォルトは **443** です。

表 4-21 SSH の設定

設定	**説明**
有効	SSH を有効または無効にします。チェックボックスが選択されている場合、SSH は有効であることを示します。
タイムアウト	セキュアシェルのアイドルタイムアウト(秒)。タイムアウト範囲は 60 ～ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **300** です。
ポート番号	SSH 接続で iDRAC6 が通信するポート。デフォルトは **22** です。

表 4-22 Telnet の設定

設定	**説明**
有効	Telnet を有効または無効にします。選択すると、Telnet が有効になります。
タイムアウト	telnet のアイドルタイムアウト(秒)。タイムアウト時間の範囲は 60～1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **300** です。
ポート番号	Telnet 接続で iDRAC6 が通信するポート。デフォルトは **23** です。

表 4-23 リモート RACADM の設定

設定	**説明**
有効	リモート RACADM を有効または無効にします。チェックボックスをオンにすると、リモート RACADM が有効になります。
アクティブセッション数	システムの現在のセッション数。

表 4-24 SNMP 設定

設定	**説明**
有効	SNMP を有効または無効にします。選択した場合、SNMP が有効になります。
SNMP コミュニティ名	SNMP コミュニティ名を有効または無効にします。選択した場合、SNMP コミュニティ名が有効になります。SNMP 警告の送信先 IP アドレスを含むコミュニティ名。コミュニティ名は最大 31 文字まで指定できます。デフォルトは **public** です。

表 4-25 自動システムリカバリエージェントの設定

設定	**説明**
有効	自動システムリカバリエージェントを有効または無効にします。選択した場合、自動システムリカバリエージェントが有効になります。

表 4-26 サービスページのボタン

ボタン	**説明**

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

---

iDRAC6 ファームウェア/システムサービスリカバリイメージのアップデート

メモ: iDRAC6 ファームウェアのアップデートが完了する前に中断されるなどにより、iDRAC6 のファームウェアが破損した場合は、iDRAC6 ウェブインタフェースを使用して iDRAC6 を修復できます。

メモ: ファームウェアアップデートは、デフォルトで現在の iDRAC6 設定を保持します。アップデートプロセス中、iDRAC6 設定を工場出荷時のデフォルト設定にリセットできるオプションが用意されています。設定を工場出荷時のデフォルト設定に設定する場合は、iDRAC6 設定ユーティリティを使用してネットワークを設定する必要があります。

1. iDRAC6 ウェブインタフェースを開いてリモートシステムにログインします。
2. **リモートアクセス** をクリックし、次に **アップデート** タブをクリックします。
3. **アップロード/ロールバック(ステップ 1 / 3)** ページで **参照** をクリックするか、support.dell.com からダウンロードしたファームウェアイメージまたはシステムサービスリカバリイメージへのパスを入力します。

   メモ: Firefox を実行している場合は、**ファームウェアイメージ** フィールドにテキストカーソルは表示されません。

   例:

   `C:¥Updates¥V1.0¥<イメージ名>.`

   または

   `¥¥192.168.1.10¥Updates¥V1.0¥<イメージ名>`

   デフォルトのファームウェアイメージ名は **firmimg. d6** です。
4. **アップロード** をクリックします。

   ファイルは iDRAC6 にアップロードされます。この処理に数分かかる場合があります。

   プロセスが完了するまで次のメッセージが表示されます。

   `File upload in progress...`(ファイルアップロード中)
5. **ステータス(ページ** 2/3)ページで、アップロードしたイメージファイルに対する検証結果が表示されます。
   - イメージファイルのアップロードに成功し、すべての検証チェックに合格すると、イメージファイル名が表示されます。ファームウェアイメージをアップロードした場合は、現在のファームウェアと新しいファームウェアバージョンが表示されます。

     または

   - イメージのアップロードに失敗した場合や、検証チェックに合格しなかった場合は、該当するエラーメッセージが表示され、アップデートが **アップロード/ロールバック(ステップ 1 / 3)** ページに戻ります。iDRAC6 のアップグレードを再試行するか、**キャンセル** をクリックして iDRAC を通常の動作モードにリセットします。

- ファームウェアイメージの場合、**設定の保存** は既存の iDRAC6 設定を保存または消去するオプションを提供します。このオプションは、デフォルトでは選択されています。

  メモ: 設定の保存 チェックボックスをオフにすると、iDRAC6 はデフォルト設定にリセットされます。デフォルト設定では LAN は無効になっています。iDRAC6 ウェブインタフェースにログインできない場合もあります。BIOS POST 時に iDRAC6 設定ユーティリティを使用して LAN 設定を再設定する必要があります。

7. **アップデート** をクリックして、アップデートプロセスを開始します。
8. **アップデート中 (ステップ 3 / 3)** ページに、アップデートの状況が表示されます。アップグレードの進行状況は、**進行状況** 列にパーセントで表示されます。

   メモ: アップデートモードでは、このページから移動してもアップデートプロセスはバックグラウンドで継続されます。

   ファームウェアのアップデートに成功すると、iDRAC6 は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC6 に再接続する必要があります。エラーが発生した場合、該当するエラーメッセージが表示されます。

   システムサービスリカバリのアップデートに成功または失敗した場合は、該当するステータスメッセージが表示されます。

iDRAC6 ファームウェアのロールバック

iDRAC6 は、2 つの同時ファームウェアイメージを保持できます。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** をクリックしてから、**アップデート** タブをクリックします。

2. **アップロード/ロールバック(ステップ 1/3)** ページで、**ロールバック** をクリックします。現在およびロールバックのファームウェアバージョンが **ステータス(ステップ 2/3)**ページに表示されます。

   設定の保存 で、iDRAC6 の既存の設定を保存するか消去するかを指定できます。このオプションは、デフォルトでは選択されています。

   メモ: **設定の保存** チェックボックスをオフにすると、iDRAC6 はデフォルト設定にリセットされます。デフォルト設定では LAN は無効になっています。iDRAC6 ウェブインタフェースにログインできない場合もあります。BIOS POST 時に iDRAC6 設定ユーティリティを使用するか、racadm コマンド(ローカルサーバー上で利用可能)を使用して LAN 設定を再設定する必要があります。

3. **アップデート** をクリックして、ファームウェアアップデートプロセスを開始します。

   アップデート中(ステップ 3/3)ページに、ロールバック処理の状況が表示されます。進行度が **進行状況** 列にパーセントで表示されます。

   メモ: アップデートモードでは、このページから移動してもアップデートプロセスはバックグラウンドで継続されます。

   ファームウェアアップデートが成功した場合、iDRAC6 は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC6 に再接続する必要があります。エラーが発生した場合、該当するエラーメッセージが表示されます。

目次ページに戻る

目次ページに戻る

iDRAC6 の詳細設定

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

ここでは、iDRAC6 の詳細設定について説明します。システム管理の知識が豊富なユーザーや、特定のニーズに応じて iDRAC6 環境をカスタマイズしたいユーザーにお勧めします。

作業を開始する前に

DRAC6 ハードウェアとソフトウェアの基本インストールと設定が完了していることを前提とします。詳細については、「iDRAC6 の基本インストール」を参照してください。

リモート SSH / Telnet 経由でシリアル出力を表示するための iDRAC6 設定

以下の手順を実行して、iDRAC6 にリモートシリアルコンソールリダイレクトを設定できます。

まず、BIOS を設定して、シリアルコンソールリダイレクトを有効にします。

1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に <F2> を押します。

   ```
   <F2> = System Setup
   ```

3. スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。
4. **シリアル通信** 画面のオプションを次のように設定します。

   ```
   serial communication....On with serial redirection via com2
   ```

   メモ: シリアルポートアドレス フィールドのシリアル device2 も com1 に設定されている限り、シリアル通信を **com1 のシリアルリダイレクトでオン** に設定できます

   ```
   serial port address....Serial device1 = com1, serial device2 = com2

   external serial connector....Serial device 1

   failsafe baud rate....115200

   remote terminal type....vt100/vt220

   redirection after boot....Enabled
   ```

   次に、**変更を保存** を選択します。

5. **セットアップユーティリティ** を終了してシステムセットアップ プログラムの設定を完了するには、<Esc> を押してください。

iDRAC6 で SSH / Telnet を有効にする設定

次に、iDRAC6 を設定して ssh/telnet を有効にします。これは RACADM または iDRAC6 ウェブインタフェースからできます。

RACADM を使用して iDRAC6 で ssh/telnet を有効にするには、次のコマンドを実行します。

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

リモートでも RACADM コマンドを実行できます。「RACADM のリモート使用」を参照してください。

iDRAC6 のウェブインタフェース を使用して issh/telnet を有効にするには、次の手順を実行します。

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**サービス** をクリックします。
3. **SSH** または **Telnet** セクションの下にある **有効** を選択します。
4. **変更の適用** をクリックします。

次に、Telnet または SSH 経由で iDRAC6 に接続します。

Telnet または SSH を使用したテキストコンソールの起動

管理ステーションの端末ソフトウェアから telnet または SSH で iDRAC6 にログインした後、telnet/SSH コマンドの **console com2** を使用して、管理下システムのテキストコンソールをリダイレクトできます。1 度に 1 つの **console com2** クライアントのみサポートされています。

管理下システムのテキストコンソールに接続するには、iDRAC6 コマンドプロンプトを開いて(telnet または SSH セッションを通して表示)、次のように入力します。

```
console com2
```

`console -h com2` コマンドは、キーボードからの入力またはシリアルポートからの新しい文字を待つ前にシリアル履歴バッファの内容を表示します。

履歴バッファのデフォルト(最大)サイズは 8192 文字です。この値は、次のコマンドを使って小さくすることができます。

```
racadm config -g cfgSerial -o cfgSerialHistorySize <数値>
```

起動中に Linux にコンソールダイレクトを設定するには、「起動中に Linux にシリアルコンソールリダイレクトを設定する方法」を参照してください。

Telnet コンソールの使用

Microsoft® Windows® XP または Windows 2003 での Telnet の実行

管理ステーションで Windows XP または Windows 2003 を実行している場合は、iDRAC6 Telnet セッションで文字の問題が発生する可能性があります。この問題はログインのフリーズとして表れ、Return キーが応答せず、パスワードプロンプトが表示されません。

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。

Windows 2000 での Telnet の実行

管理ステーションで Windows 2000 を実行している場合は、<F2> キーを押して BIOS セットアップにアクセスすることができません。この問題は、Microsoft から無料でダウンロードできる UNIX® 3.5 の Windows サービスに同梱されている telnet クライアントを使用すると解決できます。**www.microsoft.com/downloads/** にアクセスして「Windows Services for UNIX 3.5」を検索してください。

Microsoft Telnet で Telnet コンソールリダイレクトを有効にする方法

メモ: Microsoft オペレーティングシステム上の一部の telnet クライアントでは、BIOS コンソールリダイレクトを VT100/VT220 エミュレーションに設定した場合に BIOS セットアップ画面が正しく表示されないことがあります。この問題が発生した場合は、GIOS コンソールリダイレクトを ANSI モードに変更して表示を更新します。BIOS セットアップメニューでこの手順を実行するには、**Console Redirection** → **リモート端末タイプ** → **ANSI** を選択します。

メモ: クライアント VT100 エミュレーションウィンドウを設定するときにテキストを正しく表示するには、リダイレクトコンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定してください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

1. **Windows コンポーネントサービス** で **Telnet** を有効にします。
2. 管理ステーションの iDRAC6 に接続します。

   コマンドプロンプトを開いて次のテキストを入力し、<Enter> を押します。

   ```
   telnet <IP アドレス>:<ポート番号>
   ```

   IP アドレス は iDRAC6 の IP アドレスで、ポート番号は telnet ポート番号です(新しいポートを使用している場合)。

Telnet セッション用の 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、予期しない結果が生じることがあります。たとえば、セッションが ^h をエコーすることがあります。Microsoft と Linux の telnet クライアントではほとんどの場合、<Backspace> キーの使用を設定できます。

Microsoft telnet クライアントで <Backspace> キーを使用できるように設定するには、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 セッションをまだ実行していない場合は、次のように入力します。

   ```
   telnet
   ```

   telnet セッションを実行している場合は、<Ctrl><]> を押します。
3. コマンドプロンプトで、次のコマンドを入力します。

   ```
   set bsasdel
   ```

   次のメッセージが表示されます。

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

Linux telnet セッションで <Backspace> キーを使用できるように設定するには、以下の手順を実行してください。

1. コマンドプロンプトを開いて、次のように入力します。

   ```
   stty erase ^h
   ```
2. コマンドプロンプトで、次のように入力します。

   ```
   telnet
   ```

Secure Shell (SSH) の使用

システムのデバイスとデバイス管理がセキュアであることは不可欠です。組み込み接続デバイスは多くのビジネスプロセスの中核となっています。これらのデバイスが危険に曝されると、ビジネスリスクが生じる可能性があるため、コマンドラインインタフェース(CLI)のデバイス管理ソフトウェアに新しいセキュリティ要件が求められます。

Secure Shell(SSH)は telnet セッションと同じ機能を持つコマンドラインセッションですが、セキュリティ面で telnet より優れています。iDRAC6 は、パスワード認証付きの SSH バージョン 2 をサポートしています。iDRAC6 ファームウェアをインストールまたはアップデートすると、iDRAC6 上の SSH が有効になります。

管理ステーション上では、PuTTY または OpenSSH を使用して、管理下システムの iDRAC6 に接続できます。ログイン中にエラーが発生すると、セキュアシェルクライアントでエラーメッセージが表示されます。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、グラフィックが表示されません)。

一度に最大 4 つの SSH セッションのみがサポートされます。セッションタイムアウトは、「iDRAC6 プロパティデータベースグループとオブジェクト定義」に示した cfgSsnMgtSshIdleTimeout プロパティによって制御されます。

iDRAC6 で SSH を有効にするには、次を入力します。

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

SSH ポートを変更するには、次のように入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <ポート番号>
```

cfgSerialSshEnable と cfgRacTuneSshPort のプロパティについては、「iDRAC6 プロパティデータベースグループとオブジェクト定義」を参照してください。

iDRAC6 SSH の実装では、表 5-1 に示すように複数の暗号化スキームがサポートされています。

表 5-1 暗号化スキーム

スキーマの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024(ランダム)ビット(NIST 仕様)
対称暗号	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128

メッセージの整合性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	• パスワード

メモ: SSHv1 はサポートされていません。

起動中に Linux にシリアルコンソールリダイレクトを設定する方法

以下は、Linux GRand Unified Bootloader(GRUB)に固有の手順です。別のブートローダを使用する場合も、同様の変更が必要になる可能性があります。

メモ: クライアント VT100 エミュレーションウィンドウを設定するとき、リダイレクトコンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定し、テキストが正しく表示されるようにしてください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

/etc/grub.conf ファイルを次のように編集します。

1. ファイルの 全般設定 セクションを見つけて、次の 2 行を追加します。

   ```
   serial --unit=1 --speed=57600
   terminal --timeout=10 serial
   ```

2. カーネル行に次の 2 つにオプションを追加します。

   ```
   kernel .............console=ttyS1,115200n8r console=tty1
   ```

3. **/etc/grub.conf** に splashimage ディレクティブがある場合は、コメントアウトします。

表 5-2 に、この手順で説明する変更を示したサンプル **/etc/grub.conf** ファイルがあります。

表 5-2 サンプルファイル: /etc/grub.conf

```
# grub.conf generated by anaconda (grub.conf （作成者： anaconda）)
#
#Note that you do not have to rerun grub after making changes (このファイルに変更を加えた後 grub を再実行する)
# to this file (必要はありません)
# NOTICE:  You do not have a /boot partition.  This means that (通知：/boot パーティションがありません。  これは)
#          all kernel and initrd paths are relative to /, e.g. (すべてのカーネルと initrd パスが / に相対パスであることを意味します。例：)
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

/etc/grub.conf ファイルを編集するとき、次のガイドラインに従ってください。

1. GRUB のグラフィカルインタフェースを無効にして、テキストベースのインタフェースを使用します。そしないと、RAC コンソールリダイレクトで GRUB 画面が表示されません。グラフィカルインタフェースを無効にするには、splashimage で始まる行をコメントアウトします。

2. RAC シリアル接続を介してコンソールセッションを開始する GRUB オプションを複数有効にするには、すべてのオプションに次の行を追加します。

   ```
   console=ttyS1,115200n8r console=tty1
   ```

   表 5-2 に、console=ttyS1,57600 を最初のオプションにのみ追加した例を示します。

ブート後のコンソールへのログインを有効にする

/etc/inittab ファイルを次のように編集します。

COM2 シリアルポートに agetty を設定する新しい行を追加します。

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

表 5-3 に、新しい行を追加したサンプルファイルを示します。

表 5-3 サンプルファイル: /etc/innitab

```
#
# inittab  This file describes how the INIT process should set up (inittab  このファイルは INIT プロセスで特定ランレベルのシステムを)
#         the system in a certain run-level. (セットアップする方法を記述します。)
#
# Author:(作成者：)  Miquel van Smoorenburg
#         Modified for RHS Linux by Marc Ewing and Donnie Barnes (RHS Linux 用に修正：Marc Ewing、Donnie Barnes)
#
# Default runlevel. The runlevels used by RHS are: (デフォルトランレベル。RHS が使用するランレベル：)
#   0 - halt (Do NOT set initdefault to this) (停止 (initdefault はこの値に設定しないでください))
#   1 - Single user mode (シングルユーザーモード)
#   2 - Multiuser, without NFS (The same as 3, if you do not have (マルチユーザー、NFS なし（ネットワークがない場合は
#       3 と同じ）)
#   3 - Full multiuser mode (フルマルチユーザーモード)
#   4 - unused (未使用)
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this) (再起動(initdefault はこの値に設定しないでください))
#
id:3:initdefault:

# System initialization. (システムの初期化。)
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

(# 各ランレベルで実行するもの。
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# UPS から停電が知らされたら、数分間分の
# 電源が残っていることを仮定します。シャットダウンを 2 分間後にスケジュールします。
# 電源が取り付けられており UPS が接続して
# 正しく動作していることを前提とします。
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# シャットダウンの前に電源が復元した場合は、割り込んでキャンセルします。
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled")
```

```
# Run gettys in standard runlevels (gettys を標準ランレベルで実行します。)
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5 (xdm をランレベル 5 で実行します)
# xdm is now a separate service (xdm が別のサービスになりました。)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

/etc/securetty ファイルを下記のように編集します。

COM2 用のシリアル tty の名前の新しい行を追加します。

```
ttyS1
```

表 5-4 に、新しい行を追加したサンプルファイルを示します。

表 5-4 サンプルファイル: /etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

シリアル接続のための iDRAC6 の設定

シリアル接続経由での iDRAC6 への接続には、次のいずれかのインタフェースを使用できます。

- iDRAC6 CLI
- 直接接続基本モード
- 直接接続端末モード

このいずれかのインタフェースを使用するようにシステムを設定するには、以下の手順を実行してください。

BIOS を設定して、シリアル接続を有効にします。

1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に <F2> を押します。

   ```
   <F2> = System Setup
   ```

3. スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。
4. **シリアル通信** 画面を次のように設定します。

   external serial connector....remote access device

   次に、**変更を保存** を選択します。

5. **セットアップユーティリティ** を終了してシステムセットアップ プログラムの設定を完了するには、<Esc> を押します。

次に、DB-9 またはヌルモデムケーブルを管理ステーションから管理下ノードサーバーに接続します。「シリアルコンソールの DB-9 またはヌルモデムケーブルの接続」を参照してください。

次に、管理ステーションのターミナルエミュレーションソフトウェアにシリアル接続が設定されていることを確認します。「管理ステーションのターミナルエミュレーションソフトウェアの設定を参照してください。

最後に、シリアル接続が有効になるように iDRAC6 を設定します。これは RACADM または iDRAC6 のウェブインタフェースからできます。

RACADM を使用して iDRAC6 でシリアル接続を有効にするには、以下のコマンドを実行します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

iDRAC6 のウェブインタフェースを使用して iDRAC6 でシリアル接続を有効にするには、次の手順を実行します。

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. **RAC シリアル** セクションの下にある **有効** を選択します。
4. **変更の適用** をクリックします。

元の設定でシリアルに接続した場合は、ログインプロンプトが表示されます。iDRAC6 ユーザー名とパスワードを入力します（デフォルト値は、それぞれ root と calvin です）。

このインタフェースから、RACADM などの機能を実行できます。たとえば、システムイベントログ を表示するには、次の RACADM コマンドを入力します。

```
racadm getsel
```

直接接続基本モードと直接接続端末モードの iDRAC の設定

RACADM を使用して次のコマンドを実行し、iDRAC6 コマンドラインインタフェースを無効にします。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

次に、以下の RACADM コマンドを実行し、直接接続基本モード を有効にします。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 1
```

または、以下の RACADM コマンドを実行し、直接接続端末モード を有効にします。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 0
```

iDRAC6 ウェブインタフェースを使用して同じ処置を実行できます。

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. **RAC シリアル** セクションの下にある **有効** を選択解除します。

   直接接続基本モードの設定

   IPMI シリアル セクションの下にある **接続モード設定** ドロップダウンメニューを **直接接続基本モード** に変更します。

   直接接続端末モードの設定

   IPMI シリアル セクションの下にある **接続モード設定** ドロップダウンメニューを **直接接続端末モード** に変更します。
4. **変更の適用** をクリックします。
   直接接続基本モードと直接接続端末モードの詳細については、「シリアルと端末モードの設定」を参照してください。

直接接続基本モードでは、シリアル接続から直接 ipmish などのツールを使用できます。たとえば、IPMI 基本モードから ipmish を使用してシステムイベントログを印刷するには、次のコマンドを実行します。

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```

直接接続端末モードでは、iDRAC6 に ASCII コマンドを発行できます。たとえば、直接接続端末モードでサーバーの電源をオンまたはオフにするには、

1. ターミナルエミュレーションソフトウェアから iDRAC6 に接続します
2. 次のコマンドを入力し、ログインします。

   ```
   [SYS PWD -U root calvin]
   ```

   次の応答が表示されます。

   ```
   [SYS]

   [OK]
   ```
3. 次のコマンドを入力し、ログインが成功したことを確認します。

   ```
   [SYS TMODE]
   ```

   次の応答が表示されます。

   ```
   [OK TMODE]
   ```
4. サーバーの電源をオフにするには（サーバーの電源はすぐに切れます）、次のコマンドを入力します。

   ```
   [SYS POWER OFF]
   ```
5. サーバーの電源をオンにするには（サーバーの電源はすぐに入ります）、次のコマンドを入力します。

   ```
   [SYS POWER ON]
   ```

RAC シリアルインタフェース通信モードとシリアルコンソールリダイレクトの間の切り替え

iDRAC6 では、RAC シリアルインタフェース通信モードとシリアルコンソールリダイレクトの切り替えができる Esc キーシーケンスがサポートされています。

この動作を使用できるようにシステムを設定するには、次の手順を実行します。

1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に <F2> を押します。

   ```
   <F2> = System Setup
   ```

3. スクロールダウンし、**シリアル通信** を選択して <Enter>. を押します。
4. **シリアル通信** 画面を次のように設定します。

   serial communication -- On with serial redirection via com2

   メモ: **シリアルポートアドレス** フィールドの**serial device2** も com1 に設定されている限り、**シリアル通信** フィールドを **com1 のシリアルリダイレクトでオン** に設定できます。

   ```
   serial port address -- Serial device1 = com1, serial device2 = com2

   external serial connector -- Serial device 2

   failsafe baud rate....115200

   remote terminal type ...vt100/vt220

   redirection after boot ... Enabled
   ```

   次に、**変更を保存** を選択します。

5. **セットアップユーティリティ** を終了してシステムセットアップ プログラムの設定を完了するには、<Esc> を押します。

管理下システムの外部シリアルコネクタと管理ステーションのシリアルポートをヌルモデムケーブルで接続します。

管理ステーション上のターミナルエミュレーションプログラム（ハイパーターミナルまたは teraterm）を使用すると、管理下サーバーの起動シーケンスの進行状態によって、POST 画面またはオペレーティングシステムの画面が表示されます。これは設定によって異なり、Windows では SAC、Linux では Linux テキストモード画面がそれぞれ表示されます。管理ステーションのターミナル設定をボーレート-115200、データ-8 ビット、パリティ-なし、ストップ-1 ビット、およびフロー制御-なしに設定します。

シリアルコンソールリダイレクトモードのときに RAC シリアルインタフェース通信モードに切り替えるには、以下のキーシーケンスを使用してください。

```
<Esc> +<Shift> <9>
```

上述のキーシーケンスを使用すると、「iDRAC ログイン」プロンプト（RAC が「RAC シリアル」モードに設定されている場合）、またはターミナルコマンドを発行できる「シリアル接続」モード（RAC が「IPMI シリアル直接接続端末モード」に設定されている場合）に移動します。

RAC シリアルインタフェース通信モードのときにシリアルコンソールリダイレクトモードに切り替えるには、以下のキーシーケンスを使用してください。

```
<Esc> +<Shift> <q>
```

シリアルコンソールの DB-9 またはヌルモデムケーブルの接続

シリアルテキストコンソールを使って DRAC/MC にアクセスするには、管理下システム上の COM ポートに DB-9 ヌルモデムケーブルを接続します。ヌルモデムケーブルで接続が機能するには、対応するシリアル通信設定を CMOS セットアップで行う必要があります。DB-9 ケーブルのすべてが、この接続に必要なピン割り当て / 信号を持っているわけではありません。この接続に使用する DB-9 ケーブルは、表 5-5の仕様に従っている必要があります。

メモ: DB-9 ケーブルは BIOS テキストコンソールリダイレクトにも使用できます。

表 5-5 DB-9 ヌルモデムケーブルに必要なピン割り当て

信号名	DB-9 ピン (7 ピン)	DB-9 ピン (ワークスステーションピン)
FG (Frame Ground)	-	-
TD (Transmit data)	3	2
RD (Receive Data)	2	3
RTS（Request To Send）	7	8
CTS（Clear To Send）	8	7
SG（Signal Ground）	5	5
DSR（Data Set Ready）	6	4

CD (Data Carrier Detect)	1	4
DTR(Data Terminal Ready)	4	1 と 6

管理ステーションのターミナルエミュレーションソフトウェアの設定

iDRAC6 は、次のいずれかの種類のターミナルエミュレーションソフトウェアを実行している管理ステーションからシリアルまたは telnet テキストコンソールをサポートしています。

- Xterm の Linux Minicom
- Hilgraeve の HyperTerminal Private Edition(バージョン 6.3)
- Xterm の Linux Telnet
- Microsoft Telnet

使用するターミナルソフトウェアを設定するには、以下の項の手順に従ってください。Microsoft Telnet を使用する場合、設定は不要です。

Linux Minicom にシリアルコンソールエミュレーションを設定する方法

Minicom は Linux 用のシリアルポートアクセスユーティリティです。次の手順は、Minicom のバージョン 2.0 に有効です。他のバージョンでは若干異なる場合がありますが、必要な基本設定は同じです。他のバージョンの Minicom の設定については、「シリアルコンソールエミュレーションに必要な Minicom の設定」を参照してください。

Minicom バージョン 2.0 にシリアルコンソールエミュレーションを設定する方法

メモ: telnet コンソールを表示する場合は、テキストが正しく表示されるように、Linux のインストールによるデフォルトウィンドウでなく、Xterm ウィンドウの使用をお勧めします。

1. 新しい Xterm セッションを開始するには、コマンドプロンプトで `xterm &` と入力します。
2. Xterm ウィンドウで、矢印キーをウィンドウの右下隅に移動してウィンドウのサイズを 80 x 25 に変更します。
3. Minicom の設定ファイルがない場合には、次のステップに進んでください。

   Minicom の設定ファイルがある場合は、`minicom <Minicom config file name>` と入力し、手順 17に進んでください。
4. Xterm コマンドプロンプトで、`minicom -s` と入力します。
5. **Serial Port Setup**(シリアルポートのセットアップ)を選択し、 <Enter> を押します。
6. <a> を押して、該当するシリアルデバイスを選択します(例: **/dev/ttyS0**)。
7. <e> を押して、**Bps/Par/Bits** オプションを **57600 8N1** に設定します。
8. <f> を押して、**ハードウェアフロー制御** を **はい** に設定し、**ソフトウェアフロー制御** を **いいえ** に設定します。
9. **シリアルポートの設定** メニューを終了するには、<Enter> を押します。
10. **モデムとダイヤル** を選択して、<Enter> を押します。
11. **モデムダイヤルとパラメータのセットアップ** メニューで、 <Backspace>を押して **初期化、リセット、接続、切断** 設定をクリアすると、設定が空白になります。
12. <Enter> を押して、それぞれの空白値を保存します。
13. 指定のフィールドをすべてクリアする場合は、<Enter > を押して **モデムダイヤルとパラメータのセットアップ** メニューを終了します。
14. **セットアップを config_name として保存** を選択して、<Enter> を押します。
15. **Minicom から終了** を選択して、<Enter> を押します。
16. コマンドシェルプロンプトで、`minicom <Minicom config file name>` と入力します。
17. Minicom ウィンドウを 80 x 25 に拡大するには、ウィンドウの隅をドラッグします。
18. <Ctrl+a>、<z>、<x> を押して、Minicom を終了します。

メモ: シリアルテキストコンソールのリダイレクトに Minicom を使用して管理下システムの BIOS を設定する場合は、Minicom で色をオンにすると便利です。色をオンにするには、 `minicom -c on` コマンドを入力します。

Minicom ウィンドウにコマンドプロンプトが表示されることを確認します。コマンドプロンプトが表示されたら、接続が確立され、**connect** シリアルコマンドを使用して管理下システムのコンソールに接続できます。

シリアルコンソールエミュレーションに必要な Minicom の設定

表 5-6に従って Minicom を設定します。

表 5-6 シリアルコンソールエミュレーションに必要な Minicom の設定

設定の説明	必要な設定
Bps/Par/Bits	57600 8N1
ハードウェアフロー制御	○
ソフトウェアフロー制御	×
ターミナルエミュレーション	ANSI
モデムダイヤルとパラメータの設定	**初期化、リセット、接続、切断** 設定をクリアして空白にします。
ウィンドウのサイズ	80 x 25(サイズ変更するには、ウィンドウの隅をドラッグする)

シリアルコンソールリダイレクト用ハイパーターミナルの設定

HyperTerminal は、Microsoft Windows のシリアルポートアクセスユーティリティです。コンソール画面のサイズを正しく設定するには、Hilgraeve の HyperTerminal Private Edition バージョン 6.3 を使用します。

注意: Microsoft Windows オペレーティングシステムのすべてのバージョンに Hilgraeve の 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。システムの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例として、Hilgraeve の HyperTerminal Private Edition 6.3 があります。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。

HyperTerminal にシリアル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。

1. HyperTerminal プログラムを起動します。
2. 新しい接続名を入力して、**OK** をクリックします。
3. **使用する接続方法:**の隣で、DB-9 ヌルモデムケーブルを接続した管理ステーション上の COM ポート(たとえば COM2)を選択し、**OK** をクリックします。
4. 表 5-7 に示した COM ポート設定を指定します。
5. **OK** をクリックします。
6. [**ファイル** → **プロパティ** をクリックして、**設定** タブをクリックします。
7. **Telnet ターミナル ID:** を **ANSI** に設定します。
8. **ターミナル設定** をクリックして、**画面の行数** を **26** に設定します。
9. **列数** を **80** に設定して、**OK** をクリックします。

表 5-7 管理ステーション COM ポート設定

設定の説明	必要な設定
Bps	57600
データビット	8
パリティ	なし
終了ビット	1
フロー制御	ハードウェア

シリアルと端末モードの設定

IPMI と iDRAC6 シリアルの設定

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. IPMI のシリアル設定を指定します。

   IPMI シリアル設定については、表 5-8 を参照してください。
4. iDRAC6 のシリアル設定

   iDRAC6 シリアル設定については、表 5-9 を参照してください。
5. **変更の適用** をクリックします。
6. **シリアル設定** ページの適切なボタンをクリックして続行します。シリアル設定ページの設定については、表 5-10 を参照してください。

表 5-8 IPMI シリアル設定

設定	説明
接続モードの設定	• 直接接続基本モード - IPMI シリアル基本モード • 直接接続端末モード - IPMI シリアル端末モード
ボーレート	• データ速度を設定します。**9600 bps**、**19.2 kbps**、**57.6 kbps**、または **115.2 kbps** を選択します。
フロー制御	• なし - ハードウェアフロー制御オフ • RTS/CTS - ハードウェアフロー制御オン
チャネル権限レベルの制限	• 管理者 • オペレータ • ユーザー

表 5-9 iDRAC6 シリアル設定

設定	説明
有効	iDRAC6 シリアルコンソールを有効または無効にします。オン=有効、オフ=無効
タイムアウト	回線が切断される前の最大アイドル時間(秒)。範囲は 60 ～ 1920 秒です。デフォルトは 300 秒です。タイムアウト機能を無効にするには、0 秒を使用します。
リダイレクト有効	コンソールリダイレクトを有効または無効にします。オン=有効、オフ=無効
ボーレート	外部シリアルポート上のデータ速度。値は **9600 bps**、**19.2 kbps**、**57.6 kbps**、および **115.2 kbps** です。デフォルトは **57.6 kbps** です。
Esc キー	<Esc> キーを指定します。デフォルトは ^¥ です。
履歴バッファサイズ	コンソールに書き込まれた最後の文字を保持するシリアル履歴バッファのサイズ。最大値およびデフォルト値 = 8192 文字
ログインコマンド	有効なログイン後に実行する iDRAC6 コマンドライン。

表 5-10 シリアル設定ページの設定

ボタン	説明
印刷	**シリアル設定** ページを印刷します。
更新	**シリアル設定** ページを更新します。
変更の適用	IPMI と iDRAC6 シリアルの変更を適用します。
端末モードの設定	**端末モード設定** ページを開きます。

端末モードの設定

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**シリアル** をクリックします。
3. **シリアル設定** ページで **端末モードの設定** をクリックします。
4. 端末モード設定を指定します。

   端末モードの設定の説明は、表 5-11 を参照してください。
5. **変更の適用** をクリックします。
6. **端末モードの設定** ページの適切なボタンをクリックして続行します。端末モードの設定 ページのボタンの説明は、表 5-12 を参照してください。

表 5-11 端末モードの設定

設定	説明
ライン編集	ライン編集を有効または無効にします。
削除制御	次のいずれかを選択します。 • **iDRAC は、<bksp> または <del> を受け取ると、<bksp><sp><bksp> 文字を出力します** - • **iDRAC は、<bksp> または <del>を受け取ると、<del> 文字を出力します** -
エコー制御	エコーを有効または無効にします。
ハンドシェイク制御	ハンドシェークを有効または無効にします。
新しいラインシーケンス	**None**、**<CR-LF>**、**<NULL>**、**<CR>**、**<LF-CR>**、または **<LF>** を選択します。
新しいラインシーケンスの入力	**<CR>** または**<NULL>** を選択します。

表 5-12 端末モード設定ページのボタン

ボタン	説明
印刷	**端末モード設定** ページを印刷します。
更新	**端末モード設定** ページを更新します。
シリアルポート設定 に戻ります。	**シリアルポート設定** ページに戻ります。
変更の適用	端末モード設定の変更を適用します。

---

iDRAC6 のネットワーク設定

注意: iDRAC6 のネットワーク設定を変更すると、現在のネットワーク接続が切断される可能性があります。

iDRAC6 のネットワーク設定には、次のいずれかのツールを使用します。

- ウェブベースのインタフェース - 「iDRAC6 NIC の設定」を参照してください。
- RACADM CLI - 「cfgLanNetworking」を参照してください。
- iDRAC6 設定ユーティリティ - 「iDRAC 6 を使用するためのシステムの設定」を参照してください。

メモ: Linux 環境で iDRAC6 を展開する場合は、「RACADM のインストール」を参照してください。

ネットワーク経由による iDRAC6 へのアクセス

iDRAC6 を設定した後、以下のいずれかのインタフェースを使って管理下システムにリモートアクセスできます。

- ウェブインタフェース
- RACADM
- Telnet コンソール
- SSH
- IPMI

表 5-13 に、各 iDRAC6 インタフェースを示します。。

表 5-13 iDRAC6 インタフェース

インタフェース	説明
ウェブインタフェース	グラフィカルユーザーインタフェースを使って iDRAC6 へのリモートアクセスを提供します。ウェブインタフェースは iDRAC6 ファームウェアに組み込まれており、管理ステーション上の対応ウェブブラウザから NIC インタフェースを通してアクセスします。 対応ウェブブラウザについては、「対応ウェブブラウザ」のリストを参照してください。
RACADM	コマンドラインインタフェースを使って iDRAC6 にリモートアクセスできます。RACADM は iDRAC6 IP アドレスを使って RACADM コマンドを実行します **メモ:** racadm リモート機能オプションは、管理ステーションでのみサポートされています。詳細については、「RACADM のリモート使用」を参照してください。 **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 sslcertupload -t 1 -f c:¥cert¥cert.txt` サブコマンド
Telnet コンソール	iDRAC6 へアクセスを提供し、**電源オフ**、**電源オン**、**パワーサイクル**、**ハードリセット**などのコマンドを含んだシリアルおよび RACADM コマンドをサポートしています。 **メモ:** Telnet は、すべてのデータ(パスワードも含めて)をテキスト形式で送信するプロトコルです。機密情報を送信する場合は、SSH インタフェースを使用してください。
SSH インタフェース	高度なセキュリティ用の暗号化トランスポート層を使った telnet コンソールと同じ機能を提供します。
IPMI インタフェース	iDRAC6 を通してリモートシステムの基本管理機能にアクセスできます。このインタフェースには IPMI オーバー LAN、IPMI オーバーシリアル、シリアルオーバー LAN が含まれます。詳細については、**support.dell.com¥manuals** で『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

メモ: iDRAC6 のデフォルトユーザー名は root、デフォルトパスワードは calvin です。

iDRAC6 NIC 経由で iDRAC6 のウェブインタフェースにアクセスするには、対応するウェブブラウザか、Server Administrator または IT Assistant を使用します。

Server Administrator を使用して iDRAC6 リモートアクセスインタフェースにアクセスするには、次の手順を実行します。

- Server Administrator を起動します。
- Server Administrator ホームページの左ペインにあるシステムツリーで、**システム** → **メインシステムシャーシ** → **リモートアクセスコントローラ** の順にクリックします。

詳細については、『Server Administrator ユーザーズガイド』を参照してください。

RACADM のリモート使用

メモ: RACADM のリモート機能を使用する前に、iDRAC6 の IP アドレスを設定します。iDRAC6 の設定方法の詳細と関連文書については、「iDRAC6 の基本インストール」を参照してください。

RACADM には、管理下システムに接続し、リモートコンソールまたは管理ステーションから RACADM サブコマンドを実行できるリモート機能オプション(-**r**)があります。リモート機能を使用するには、有効なユーザー名(-**u** オプション)、パスワード(-**p** オプション)、および iDRAC6 IP アドレスが必要です。

メモ: リモートシステムにアクセスしているシステムのデフォルト証明書ストアに iDRAC6 証明書がない場合は、RACADM コマンドを入力したときにメッセージが表示されます。iDRAC6 証明書の詳細については、「SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保」を参照してください。

```
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. (実行を継続します。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 IP address (エラー:指定した IP アドレスで iDRAC6 に接続できません。)

メモ: RACADM リモート機能は、管理ステーションでのみサポートされています。詳細については、デルサポートサイト **support.dell.com¥manuals** の **Dell OpenManage ソフトウェア** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

メモ: RACADM リモート機能を使用する場合は、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 sslcertupload -t 1 -f c:¥cert¥cert.txt サブコマンド
```

RACADM 構文概要

```
racadm -r <iDRAC6 IP アドレス> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <iDRAC6 IP アドレス> <サブコマンド> <サブコマンドオプション>
```

例:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

iDRAC6 の HTTPS ポート番号をデフォルトポート(443)以外のカスタムポートに変更した場合は、次の構文を使用します。

```
racadm -r <iDRAC6 IP アドレス>:<ポート> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <iDRAC6 IP アドレス>:<ポート> <サブコマンド> <サブコマンドオプション>
```

RACADM オプション

表 5-14 に、RACADM コマンドのオプションを示します。

表 5-14 racadm コマンドオプション

オプション	説明
-r <**racIpAddr**> **-r**<**racIpAddr**>:<ポート番号>	コントローラのリモート IP アドレスを指定します。 iDRAC6 のポート番号がデフォルトポート(443)と異なる場合は、<ポート番号> を使用します。
-**i**	インタラクティブにユーザーのユーザー名とパスワードを問い合わせるように RACADM に指示します。
-**u <ユーザー名>**	コマンドのトランザクションの認証に使用するユーザー名を指定します。-**u** オプションを使用すると、-**p**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。

RACADM リモート機能の有効 / 無効化

メモ: これらのコマンドはローカルシステムで実行することをお勧めします。

RACADM リモート機能はデフォルトでは有効になっています。無効になっている場合は、次の RACADM コマンドを入力して有効にします。

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

リモート機能を無効にするには、次のように入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

RACADM サブコマンド

表 5-15 は、RACADM で実行できる各 RACADM サブコマンドについて説明しています。構文と有効なエントリを含む RACADM サブコマンドの詳細については、「RACADM サブコマンドの概要」のリストを参照してください。

RACADM サブコマンドを入力するときは、コマンドに racadm のプレフィックスを付けてください。

```
racadm help
```

表 5-15 RACADM サブコマンド

コマンド	説明
help	iDRAC6 サブコマンドを一覧にします。
help <サブコマンド>	指定したサブコマンドの使用ステートメントを一覧にします。
arp	ARP テーブルの内容を表示します。ARP エントリの追加や削除はできません。
clearasrscreen	前回の ASR (クラッシュ) 画面をクリアします(前回の青色画面)。
clrraclog	iDRAC6 のログをクリアします。ログがクリアされたときのユーザーと時間を示すエントリが 1 つ作成されます。
config	iDRAC6 を設定します。
getconfig	現在の iDRAC6 設定のプロパティを表示します。
coredump	前回の iDRAC6 コア ダンプを表示します。
coredumpdelete	iDRAC6 に保存されているコアダンプを削除します。
fwupdate	iDRAC6 ファームウェアアップデートを実行、または状態を表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsysinfo	iDRAC6 とシステムの一般情報を表示します。
getractime	iDRAC6 の時刻を表示します。
ifconfig	現在の iDRAC6 の IP 設定を表示します。
netstat	ルーティングテーブルと現在の接続を表示します。
ping	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。
setniccfg	コントローラの IP 設定を指定します。
getniccfg	コントローラの現在の IP 設定を表示します。
getsvctag	サービスタグを表示します。
racdump	iDRAC6 のステータスと状態情報をデバッグ用にダンプします。
racreset	iDRAC6 をリセットします。
racresetcfg	iDRAC6 をデフォルト設定にリセットします。
serveraction	管理下システムの電源管理を行います。
getraclog	iDRAC6 のログを表示します。
clrsel	システムイベントログのエントリをクリアします。
gettracelog	iDRAC6 トレースログ を表示します。-i と一緒に使用した場合は、iDRAC6 のトレースログ内のエントリ数を表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
sslcertupload	CA 証明書またはサーバー証明書を iDRAC6 にアップロードします。
sslcertdownload	CA 証明書をダウンロードします。
sslcertview	iDRAC6 で CA 証明書またはサーバー証明書を表示します。
sslkeyupload	電子メールの設定をチェックするには、iDRAC6 に iDRAC6 NIC 経由でテスト電子メールを送信させます。
testtrap	トラップの設定をチェックするには、iDRAC6 に iDRAC6 NIC 経由でテスト SNMP トラップを送信させます。
vmdisconnect	仮想メディア接続を強制終了します。
vmkey	仮想フラッシュサイズをデフォルトサイズ(256 MB)に戻します。

RACADM エラーメッセージについてよくあるお問い合わせ

(racadm racreset コマンドを使用して)iDRAC6 リセットを実行した後、コマンドを発行すると次のメッセージが表示されます。

ERROR: Unable to connect to RAC at specified IP address (エラー:指定した IP アドレスで RAC に接続できません)

このメッセージは何を意味しますか?

iDRAC6 のリセットが完了してから、別のコマンドを発行してください。

racadm コマンドやサブコマンドを使用すると、原因不明のエラーが発生します。

RACADM コマンドやサブコマンドを使用するとき、次のようなエラーが 1 つまたは複数発生することがあります。

- ローカル RACADM エラーメッセージ - 構文、入力ミス、名前の誤りなどの問題。
- リモート RACADM エラーメッセージ - IP アドレスの誤り、ユーザー名の誤り、パスワードの誤りなどの問題。

システムから iDRAC6 IP アドレスを ping した後で、iDRAC6 を専用モードと共有モードを切り替えると、応答がありません。

システムの ARP テーブルをクリアしてください。

複数の iDRAC6 コントローラの設定

RACADM を使用すると、同じプロパティで 1 つまたは複数の iDRAC6 コントローラを設定できます。グループ ID と オブジェクト ID を使って特定の iDRAC6 コントローラをクエリすると、RACADM

は取得した情報から **racadm.cfg** 設定ファイルを作成します。ファイルを 1 つまたは複数の iDRAC6 にエクスポートすると、同じプロパティを使用してコントローラを最短時間で設定できます。

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が必要な固有の iDRAC6 情報(静的 IP アドレスなど)が含まれています。

複数の iDRAC6 コントローラを設定するには、次の手順を実行してください。

1. RACADM を使用して、適切な設定が含まれているターゲット iDRAC6 にクエリします。

   メモ: 生成された **.cfg** ファイルにはユーザーパスワードは含まれていません。

   コマンドプロンプトを開いて、次のように入力します。

   ```
   racadm getconfig -f myfile.cfg
   ```

   メモ: **getconfig -f** を使った iDRAC6 設定のファイルへのリダイレクトは、ローカルまたはリモート RACADM インタフェースでのみサポートされています。

2. テキストエディタを使用して、設定ファイルに変更を加えます(省略可能)。

3. 新しい設定ファイルを使用して、ターゲット iDRAC6 を変更します。

   コマンドプロンプトで、次のように入力します。

   ```
   racadm getconfig -f myfile.cfg
   ```

4. 設定されたターゲット iDRAC6 をリセットします。

   コマンドプロンプトで、次のように入力します。

   ```
   racadm racreset
   ```

getconfig -f racadm.cfg サブコマンドは iDRAC6 の設定を要求し、**racadm.cfg** ファイルを生成します。必要に応じて、ファイルに別の名前を付けることもできます。

getconfig コマンドを使用すると、次のような操作ができます。

- グループのすべての設定プロパティを表示する(グループ名とインデックスで指定)
- ユーザーのすべての設定プロパティをユーザー名別に表示する

config サブコマンドは、この情報を他の iDRAC6 にロードします。ユーザーとパスワードのデータベースを Server Administrator と同期するには、**config** を 使用します。

初期設定ファイルの **racadm.cfg**, はユーザーが命名します。次の例では、設定ファイルの名前は **myfile.cfg** です。このファイルを作成するには、コマンドプロンプトで次のように入力します。

```
racadm getconfig -f myfile.cfg
```

注意: このファイルはテキストエディタで編集することをお勧めします。RACADM ユーティリティは ASCII テキストの構文解析を使用します。フォーマットすると、パーサーが混乱して RACADM データベースが破損する可能性があります。

iDRAC6 設定ファイルの作成

iDRAC6 設定ファイル <ファイル名>.cfg は、racadm racadm config -f <ファイル名>**.cfg** コマンドで使用されます。この設定ファイルを使用して設定ファイルを作成し(**.ini** ファイルと同様)、このファイルから iDRAC6 を設定できます。ファイル名は自由に指定でき、最後に **.cfg** を付ける必要もありません(ただし、この項ではその命名法を使用しています)。

.cfg ファイルの扱いは次のとおりです。

- 作成する
- racadm getconfig -f <ファイル名>.cfg コマンドで取得する
- racadm getconfig -f <filename>.cfg コマンドで取得してから編集する

メモ: **getconfig** コマンドの詳細については、「getconfig」を参照してください。

.cfg ファイルは、最初に解析が行われ、有効なグループとオブジェクト名があるかどうか、いくつかの単純な構文規則が守られているかどうかが検証されます。エラーはエラーが検出された行番号でフラグ指定され、その問題を説明した簡単なメッセージがあります。ファイル全体の正確性について解析され、すべてのエラーが表示されます。**.cfg** ファイルにエラーが見つかった場合は、iDRAC6 に書き込みコマンドは送信されません。設定する前に、すべてのエラーを訂正する必要があります。-c オプションは **config** サブコマンドで使用できます。これは構文のみを検証し、iDRAC6 への書き込みを行いません。

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

- パーサーが索引付けされたグループを見つけた場合、これはさまざまな索引との差を表すアンカー付きオブジェクトの値です。

  パーサーは、iDRAC6 からそのグループのすべてのインデックスを読み取ります。グループ内のオブジェクトはすべて iDRAC6 が設定されたときに簡単な変更が加えられたものです。変更されたオブジェクトが新しいインデックスを表す場合、設定中にその iDRAC6 のインデックスが作成されます。

- **.cfg** ファイルでは、インデックスを選択して指定することはできません。

索引は作成と削除が繰り返されるため、グループは次第に使用と未使用の索引で断片化してくる可能性があります。索引が存在する場合は、変更されます。索引が存在しない場合は、最初に使用できる索引が使用されます。この方法では、索引付きエントリを追加するときに、管理下のすべての RAC 間で索引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、最初に使用可能な索引に追加されます。すべてのインデックスが一杯のときに新しいユーザーを追加しなければならない場合は、1 つの iDRAC6 で正しく解析および実行される **.cfg** ファイルが別の iDRAC6 でも正しく実行されるとは限りません。

- 同じプロパティを持つ複数の iDRAC6 を設定するには、**racresetcfg** サブコマンドを使用します。

  racresetcfg サブコマンドを使って iDRAC6 を元のデフォルトに戻し、`racadm config -f <ファイル名>.cfg` コマンドを実行します。**.cfg** ファイルにすべての必要オブジェクト、ユーザー、インデックス、およびその他のパラメータが入っていることを確認します。

注意: racresetcfg サブコマンドを使用すると、データベースと C iDRAC6 NIC は元のデフォルトの設定にリセットされ、ユーザーとユーザー設定はすべて削除されます。root（ルート）ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。

構文解析規則

- 「#」で始まる行はすべてコメントとして扱われます。

  コメント行は一列目から記述する必要があります。その他の列にある「#」の文字は単に # という文字として扱われます。

  一部のモデムパラメータでは # をその文字列内に含むことができます。エスケープ文字は必要ありません。`racadm getconfig -f <ファイル名>.cfg` コマンドで **.cfg** を生成し、エスケープ文字を追加せずに、`racadm config -f <ファイル名>.cfg` コマンドを異なる iDRAC6 上で実行します。

  例:

  ```
  #

  # This is a comment (これはコメントです)

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # not a comment>
  ```

- 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「**[**」文字は一列目になければなりません。このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。設定データは「iDRAC6 プロパティデータベースグループとオブジェクト定義」で定義されているようにグループに分類されます。

  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=143.154.133.121 {オブジェクト名}
  ```

- すべてのパラメータは、「`object`（オブジェクト）」、「=」、または「`value`（値）」の間に空白を入れずに「`object=value`」のペアとして指定されます。

  値の後にあるスペースは無視されます。値の文字列内にあるスペースは変更されません。'=' の右側の文字はそのまま使用されます（例：2 番目の '='、または '#'、'[',']' など）。これらの文字は、有効なモデムチャットスクリプト文字です。

  上記の例を参照してください。

- **.cfg** パーサーはインデックスオブジェクトエントリを無視します。

  ユーザーは、使用する索引を指定できません。索引が既に存在する場合は、それが使用されます。索引がない場合は、そのグループで最初に使用可能な索引に新しいエントリが作成されます。

  `racadm getconfig -f <ファイル名>.cfg` コマンドは、インデックスオブジェクトの前にコメントを配置するため、ユーザーは使用されているコメントをここで参照できます。

メモ: 次のコマンドを使用すると、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 <アンカーオブジェクト> -i <インデックス 1 ～ 16> <固有のアンカー名>`

- インデックスグループの行は、**.cfg** ファイルからは削除できません。

  次のコマンドを使用して、手動で索引オブジェクトを削除する必要があります。

  ```
  racadm config -g <グループ名> -o <オブジェクト名> -i <インデックス 1 ～ 16> ""
  ```

メモ: NULL 文字列（2 つの "" 文字）は、指定したグループのインデックスを削除するように iDRAC6 に命令します。

索引付きグループの内容を表示するには、次のコマンドを使用します。

```
racadm getconfig -g <グループ名> -i <インデックス 1 ～ 16>
```

- インデックスグループの場合、オブジェクトアンカーは "[ ]" の組み合わせの後に出現する最初のオブジェクトでなければなりません。次は、現在の索引付きグループの例です。

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<ユーザー名>
  ```

`racadm getconfig -f <myexample>.cfg`と入力すると、現在の iDRAC6 設定用の **.cfg** ファイルが構築されます。この設定ファイルは、固有の **.cfg** ファイルの使用例または開始点として利用できます。

iDRAC6 IP アドレスの変更

設定ファイルの iDRAC6 IP アドレスを変更する場合は、不要な **<**変数**>**=<**値** > のエントリをすべて削除します。IP アドレスの変更に関する **<**値**>**=**値** エントリを含む実際の変数グループのラベルと "[" と "]" だけが残ります。

例:

```
#

# Object Group (オブジェクトグループ)"cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

This file will be updated as follows: (このファイルは次のようにアップデートされます。)

```
#

# Object Group (オブジェクトグループ)"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
```

racadm config -f myfile.cfg コマンドは、このファイルを解析して、行番号ごとにエラーを特定します。ファイルが正しければ、該当するエントリがその内容で更新されます。さらに、前の例の **getconfig** コマンドを使用して、更新を確認できます。

このファイルを使用して会社全体の変更をダウンロードしたり、ネットワーク上で新しいシステムを設定したりできます。

メモ: "Anchor" は内部用語です。ファイルには使用しないでください。

iDRAC6 ネットワークプロパティの設定

使用可能なネットワークプロパティのリストを生成するには、次のように入力します。

```
racadm getconfig -g cfgLanNetworking
```

DHCP を使用して IP アドレスを取得するには、次のコマンドを使って **cfgNicUseDhcp** オブジェクトを記述し、この機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

このコマンドは、起動時に <Ctrl><E> の入力を求められたときの iDRAC6 設定ユーティリティと同じ設定機能を提供します。iDRAC6 設定ユーティリティを使用したネットワークプロパティ設定の詳細については、「iDRAC 6 を使用するためのシステムの設定」を参照してください。

次に、LAN ネットワークプロパティ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。

iDRAC6 モード

iDRAC6 は、次の 4 つのモードのいずれかに設定できます。

- 専用
- 共有
- フェールオーバーで共有(LOM2)
- フェールオーバーで共有(すべてのLOM)

表 5-16 に、各モードについて説明します。

表 5-16 iDRAC6 NIC の設定

モード	説明
専用	iDRAC6 は、ネットワークトラフィックに対して独自の NIC(RJ-45 コネクタ)と iDRAC MAC アドレスを使用します。
共有	iDRAC6 はプレーナで LOM1 を使用します。
フェールオーバーで共有(LOM2)	iDRAC6 は LOM1 と LOM2 をフェールオーバー用のチームとして使用します。このチームは iDRAC6 MAC アドレスを使用します。
フェールオーバーで共有(すべての LOM)	iDRAC6 は LOM1、LOM2、LOM3、および LOM4 をフェールオーバー用のチームとして使用します。このチームは iDRAC6 MAC アドレスを使用します。

ネットワークセキュリティについてよくあるお問い合わせ(FAQ)

iDRAC6 ウェブインタフェースにアクセスするときに、SSL 証明書のホスト名が iDRAC6 のホスト名と一致しないというセキュリティ警告が表示されます。

iDRAC6 にはデフォルトの iDRAC6 サーバー証明書が含まれており、ウェブインタフェースのネットワークセキュリティとリモート RACADM 機能を確保します。この証明書を使用する場合には、ウェブブラウザにはセキュリティ警告が表示されます。これは、デフォルトの証明書が iDRAC6 のホスト名(たとえば IP アドレス)と一致しない **iDRAC6 デフォルト証明書** に対して発行されたためです。

このセキュリティ問題に対処するには、iDRAC6 の IP アドレスまたは iDRAC 名に発行された iDRAC6 サーバー証明書をアップロードします。証明書の発行に使用する証明書署名要求(CSR)を生成する場合には、CSR の共通名(CN)が(**証明書を IP に発行する場合**) iDRAC6 の IP アドレス(例:192.168.0.120)、または登録されている DNS iDRAC6 名(**証明書が登録済み iDRAC 名に発行された場合**)と一致することを確認してください。

CSR が登録されている DNS iDRAC6 名と一致することを確認するには、以下の手順を実行します。

1. **システム** ツリーの **リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**ネットワーク** をクリックします。
3. **共通設定** テーブルで以下の操作を行います。
   a. **DNS に iDRAC を登録** チェックボックスを選択します。
   b. **DNS iDRAC 名** フィールドに iDRAC6 名を入力します。
4. **変更の適用** をクリックします。

CSR の生成と証明書の発行については、「SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保」を参照してください。

プロパティを変更すると、リモート RACADMとウエブベースのサービスを使用できなくなるのはなぜですか?

iDRAC6 ウェブサーバーがリセットした後、リモート RACADM サービスとウェブベースのインタフェースが使用できるようになるまでに時間がかかることがあります。

iDRAC6 ウェブサーバーは次のような場合にリセットします。

- iDRAC6 ウェブユーザーインタフェースを使ってネットワーク設定またはネットワークセキュリティのプロパティが変更された
- **cfgRacTuneHttpsPort** プロパティが変更された(config -f <設定ファイル> によって変更された場合を含む)
- **racresetcfg** が使われた
- iDRAC6 がリセットされた
- 新しい SSL サーバー証明書がアップロードされた

DNS サーバーで iDRAC6 を登録できない理由は何ですか?

一部の DNS サーバーは 31 文字以内の名前しか登録しません。

iDRAC6 ウェブインタフェースにアクセスすると、SSL 証明書が信頼できない認証局 (CA) から発行されたというセキュリティ警告が表示されます。

iDRAC6 にはデフォルトの iDRAC6 サーバー証明書が含まれており、ウェブインタフェースのネットワークセキュリティとリモート RACADM 機能を確保します。この証明書は信頼できる CA によって発行されませんでした。このセキュリティ問題に対処するには、信頼できる CA (たとえば Microsoft 認証局、Thawte または Verisign) から発行された iDRAC6 サーバー証明書をアップロードしてください。証明書の発行の詳細については、を参照してください。「SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保」

目次ページに戻る

目次ページに戻る

iDRAC6 ユーザーの追加と設定

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

iDRAC6 を使用してシステムを管理し、システムのセキュリティを維持するには、特定の管理者権限（または役割ベースの権限）を持つ固有のユーザーを作成します。セキュリティを強化するため、特定のシステムイベントが発生したときに、特定のユーザーに電子メールで警告を送るように設定することもできます。

ウェブインタフェースを使用した iDRAC6 ユーザーの設定

iDRAC6 ユーザーの追加と設定

iDRAC6 を使用してシステムを管理し、システムのセキュリティを確保するには、特定の管理者権限（役割ベースの権限）を持つ固有のユーザーを作成します。

iDRAC6 のユーザーを追加して設定するには、次の手順を実行してください。

メモ: iDRAC ユーザーを設定するには、**ユーザーの設定** 権限が必要です。

1. **リモートアクセス** → **設定** → **ユーザー** の順にクリックします。

   ユーザー ページには、iDRAC ユーザーの **ユーザー ID**、**状態（有効 / 無効）**、**ユーザー名**、**RAC 権限**、**IPMI LAN 権限**、**IPMI シリアル権限**、および **シリアルオーバー LAN 状態（有効 / 無効）** が表示されます。表 6-1は、iDRAC ユーザー設定用のユーザーの状態と権限について説明しています。

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

2. **ユーザー ID** 列で、ユーザー ID をクリックします。

   ユーザーメインメニュー ページで、ユーザーの設定、ユーザー証明書の表示、信頼される認証局 (CA) 証明書のアップロード、信頼された CA 証明書の表示などができます。

   ユーザーの設定 を選択して **次へ** をクリックすると、**ユーザー設定** ページが表示されます。ステップ 4 へ進みます。

   スマートカードの設定 でオプションを選択した場合は、表 6-2を参照してください。

3. **ユーザー設定** ページで、以下の項目を設定します。
   - 新規または既存の iDRAC ユーザーのユーザー名、パスワード、およびアクセス権限。では、**一般ユーザー設定** について 表 6-3説明しています。
   - ユーザーの IPMI 権限。表 6-4 では、ユーザーの LAN 権限を設定するための **IPMI ユーザー権限** について説明しています。
   - iDRAC ユーザー権限 表 6-5 では、**iDRAC のユーザー権限** について説明しています。
   - iDRAC のグループアクセス権限。表 6-6 では、**iDRAC グループ権限** について説明しています。

4. 完了したら、**変更の適用** をクリックします。

5. 適切なボタンをクリックして続行します。表 6-7を参照してください 。

表 6-1 ユーザーの状態とアクセス権

設定	説明
ユーザー ID	ユーザー ID 番号の連番リストを表示します。**ユーザー ID** の各フィールドには、事前設定された 16 個のユーザー ID 番号の 1 つが含まれています。このフィールドは編集できません。
都道府県	ユーザーのログイン状態（有効または無効）を表示します。（デフォルトでは無効になっています。） **メモ:** ユーザー 2 はデフォルトで有効になっています。
ユーザー名	ユーザーのログイン名を表示します。iDRAC6 ユーザー名は、最大 16 文字で指定できます。各ユーザーは固有のユーザー名を持つ必要があります。 **メモ:** iDRAC6 のユーザー名に **/**（フォワードスラッシュ）や **.**（ピリオド）を含めることはできません。 **メモ:** ユーザー名を変更した場合は、新しい名前は次回のユーザーログイン時までユーザーインタフェースに表示されません。

RAC 権限	ユーザー(管理者、オペレーター、読み取り専用、またはなし)を割り当てたグループ(権限レベル)を表示します。
IPMI LAN 権限	ユーザー(管理者、オペレーター、読み取り専用、なし)を割り当てた IPMI LAN の権限レベルを表示します。
IPMI シリアル権限	ユーザー(管理者、オペレーター、読み取り専用、なし)を割り当てた IPMI シリアルポートの権限レベルを表示します。
シリアルオーバー LAN.	IPMI シリアルオーバー LAN の使用を許可または拒否します。

表 6-2 スマートカード設定オプション

オプション	**説明**
ユーザー証明書の表示	iDRAC にアップロードされたユーザー証明書ページを表示します。
信頼された CA 証明書のアップロード	信頼された CA 証明書を iDRAC にアップロードして、ユーザープロファイルにインポートできます。
信頼された CA 証明書の表示	iDRAC にアップロード済みの信頼された CA 証明書を表示します。信頼された CA 証明書は、ユーザーに証明書を発行することを許可されている CA が発行します。

表 6-3 一般ユーザー設定

ユーザー ID	16 個ある設定済みユーザー ID 番号の 1 つです。
ユーザーを有効にする	オンの場合は、iDRAC6 へのユーザーアクセスが有効であることを示します。オフの場合は、ユーザーアクセスが無効であることを示します。
ユーザー名	最大 16 文字のユーザー名。
パスワードの変更	**新しいパスワード** と**新しいパスワードの確認** フィールドを有効にします。オフの場合は、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	20 文字以内で **パスワード** を入力します。文字は表示されません。
新しいパスワードの確認	確認のために iDRAC ユーザーのパスワードを再入力します。

表 6-4 IPMI のユーザー権限

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として、**システム管理者**、**オペレータ**、**ユーザー**、**または なし** のユーザーグループからいずれかを指定します。
シリアルポートに許可する最大ユーザー権限	IPMI シリアルチャネルでのユーザーの最大権限として、**システム管理者**、**オペレータ**、**ユーザー**、**または なし** のユーザーグループからいずれかを指定します。
シリアルオーバー LAN を有効にする	IPMI シリアルオーバー LAN を使用できます。選択すると、権限が有効になります。

表 6-5 iDRAC ユーザー権限

プロパティ	**説明**
役割	iDRAC ユーザーの最大権限として、**システム管理者**、**オペレータ**、**読み取り専用**、または **なし** のいずれかを指定します。**iDRAC グループ 権限**については、表 6-6を参照してください。
iDRAC へのログイン	iDRAC にログインできます。
iDRAC の設定	iDRAC を設定できます。
ユーザーの設定	特定ユーザーのシステムアクセスを許可できるようにします。
ログのクリア	iDRAC のログをクリアできます。
サーバーコントロールコマンドの実行	サーバー制御のコマンドを実行できるようにします。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告(電子メールと PET)を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

表 6-6 iDRAC グループのアクセス権

ユーザーグループ	**許可する権限**
管理者	**iDRAC へのログイン**、**iDRAC の設定**、**ユーザー設定**、**ログのクリア**、**サーバーコントロールコマンドの実行**、**コンソールリダイレクトへのアクセス**、**仮想メディアへのアクセス**、**テスト警告**、**診断コマンドの実行**。
オペレータ	次の権限を組み合わせて選択します。**iDRAC へのログイン**、**iDRAC の設定**、**ユーザーの設定**、**ログのクリア**、**サーバー処置コマンドの実行**、**コンソールリダイレクトへのアクセス**、**仮想メディアへのアクセス**、**テスト警告**、**診断コマンドの実行**。
読み取り専用。	**iDRAC へのログイン**
なし	権限の割り当てなし

表 6-7 ユーザー設定ページのボタン

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

RACADM ユーティリティを使用した iDRAC6 ユーザーの設定

メモ: リモート Linux システム上で RACADM コマンドを実行するには、ユーザー **root** としてログインする必要があります。

管理下システムに iDRAC6 エージェントと一緒にインストールされている RACADM コマンドラインを使用すると、単一または複数の iDRAC6 ユーザーを設定できます。

同じ設定を複数の iDRAC6 に対して指定する場合は、次のいずれかの手順を実行します。

- この項の RACADM の例を参考にして、RACADM コマンドのバッチファイルを作成し、各管理下システム上でこのバッチファイルを実行します。
- 「RACADM サブコマンドの概要」の説明に従って、iDRAC6 設定ファイルを作成し、各管理下システムで同じ設定ファイルを使用して **racadm config** サブコマンドを実行します。

作業を開始する前に

iDRAC6 のプロパティデータベースには、最大 16 のユーザーを設定できます。iDRAC6 ユーザーを手動で有効にする前に、現在のユーザーが存在するかどうかを確認します。新しい iDRAC6 を設定している場合や、**racadm racresetcfg** コマンドを実行した場合、現在のユーザーは `root` のみで、パスワードは `calvin` になります。**racresetcfg** サブコマンドは iDRAC6 をデフォルト値にリセットします。

注意: racresetcfg コマンドを使用する場合は、注意が必要です。すべての 設定パラメータがデフォルト値に戻ります。それまでに行った変更がすべて失われます。

メモ: ユーザーは経時的に有効にしたり、無効にしたりできます。その結果、ユーザーが各 iDRAC6 に異なる索引番号を持つ場合があります。

コマンドプロンプトで次のコマンドを入力すると、ユーザーが存在するかどうかがわかります。

```
racadm getconfig -u <ユーザー名>
```

または

1 ～ 16 までの各索引に、次のコマンドを 1 回ずつ入力することもできます。

```
racadm getconfig -g cfgUserAdmin -i <索引>
```

メモ: `racadm getconfig -f <myfile.cfg>` と入力して、iDRAC6 設定パラメータが含まれる **myfile.cfg** ファイルの表示や集もできます。

複数のパラメータとオブジェクト ID が現在値と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=XX

cfgUserAdminUserName=
```

cfgUserAdminUserName オブジェクトに値がない場合は、**cfgUserAdminIndex** オブジェクトで示されるその索引番号は使用可能です。"=" の後に名前が表示される場合は、そのインデックスがそのユーザー名で使用されています。

メモ: **rracadm config** サブコマンドを使用してユーザーを手動で追加または削除する場合は、**-i** オプションでインデックスを指定する必要があります。前の例で示した **cfgUserAdminIndex** オブジェクトに '#' 文字が含まれていることに注目してください。**racadm config -f racadm.cfg** コマンドを使用して、書き込むグループ / オブジェクトの数を指定する場合、インデックスは指定できません。最初に 使用可能な索引に新しいユーザーが追加されます。この動作により、設定が同じ持つ複数の iDRAC6 を設定する柔 軟性が得られます。

iDRAC6 ユーザーの追加

新しいユーザーを RAC 設定に追加するには、基本的なコマンドをいくつか使用できます。通常は、次の手順を実行してください。

1. ユーザー名を設定します。
2. パスワードを設定します。
3. 次のユーザー権限を設定します。
   - iDRAC 権限
   - IPMI LAN 権限

- IPMI シリアル権限
- シリアルオーバー LAN 権限

4. ユーザーを有効にします。

例

次の例では、パスワード "123456" と LOGIN 権限を持つ新しいユーザー名 "John" を RAC に追加します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

確認するには、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

iDRAC6 ユーザーの削除

RACADM を使用している場合は、ユーザーを手動で個別に無効にする必要があります。設定ファイルを使用してユーザーを削除することはできません。

次の例では、RAC ユーザーの削除に使用できるコマンド構文を示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス> ""
```

二重引用符("")のヌル文字列は、指定した索引のユーザー設定を削除して、出荷時のデフォルトにリセットするように iDRAC6 に指示します。

権限のある iDRAC6 ユーザーを有効にする

ユーザーに特定の管理権限(ロールベースの権限)を与えるには、まず「作業を開始する前に」で説明する手順に従って、使用可能なユーザー索引を探します。その後、新しいユーザー名とパスワードを使用して次のコマンドラインを入力します。

メモ: 特定のユーザー権限に有効なビットマスク値については、表 B-2のリストを参照してください。デフォルトの権限値は 0 で、これはユーザーの権限が有効になっていないことを示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <インデックス> <ユーザー権限ビットマスク値>
```

目次ページに戻る

目次ページに戻る

Microsoft Active Directory での iDRAC6 の使用

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

ディレクトリサービスは、ネットワーク上のユーザー、コンピュータ、プリンタなどを制御するのに必要な全情報に共通のデータベースを管理します。会社で Microsoft® Active Directory® サービスソフトウェアを既に使用している場合は、iDRAC6 にアクセスできるように設定し、Active Directory ソフトウェアの既存のユーザーに iDRAC6 のユーザー権限を追加して制御できます。

メモ: Microsoft Windows® 2000、Windows Server® 2003、および Windows Server 2008 オペレーティングシステムでは、Active Directory を使用して DRAC 5 のユーザーを認識できます。

表 7-1 は、9 つの iDRAC6 Active Directory ユーザー権限を示しています。

表 7-1 iDRAC6 ユーザー権限

権限	説明
iDRAC へのログイン	iDRAC6 にログインできます。
iDRAC の設定	iDRAC6 を設定できます。
ユーザーの設定	特定ユーザーのシステムアクセスを許可できるようにします。
ログのクリア	iDRAC6 のログをクリアできます。
サーバーコントロールコマンドの実行	RACADM コマンドを実行できます。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告（電子メールと PET）を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

---

iDRAC6 用に Active Directory 認証を有効にするための必要条件

Active Directory で iDRAC6 を認証する機能を使用するには、Active Directory インフラストラクチャが既に展開されている必要があります。Active Directory インフラストラクチャがまだ構築されていない場合、その設定方法については、Microsoft のウェブサイト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（PIK）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で Secure Socket Layer (SSL) を有効にする必要もあります。詳細については、「ドメインコントローラの SSL を有効にする」を参照してください。

サポートされている Active Directory の認証機構

Active Directory を使用して 2 通りの方法で 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。これらソリューションについての詳細は、以降に続く該当するセクションを参照してください。

Active Directory を使用して iDRAC6 へのアクセスを設定する場合は、拡張スキーマソリューションか標準スキーマソリューションかを選択する必要があります。

拡張スキーマソリューションを使用する場合の長所は次のとおりです。

- 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。
- 異なる iDRAC6 でさまざまな権限レベルのユーザーアクセスを設定できます。

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 Dell 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、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 をディレクトリに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: 新しいスキーマを拡張しても、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、以前の製品には効果がありません。

スキーマエクステンダおよび Active Directory ユーザーとコンピュータ MMC スナップイン拡張子は、『Dell Systems Management Tools and Documentation DVD』に収録されています。詳細については、『Active Directory の拡張』および『Active Directory ユーザーとコンピュータ スナップインへの Dell 拡張子のインストール』を参照してください。iDRAC6 向けのスキーマ拡張および Active Directory ユーザーとコンピュータ MMC スナップインのインストールの詳細については、**support.dell.com¥manuals** 上の『Dell OpenManage インストールとセキュリティ ユーザーズガイド』を参照してください。

メモ: iDRAC 関連オブジェクトまたは iDRAC デバイスオブジェクトを作成する場合は、**Dell 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。

Dell の拡張子: dell

Dell ベースの OID: 1.2.840.113556.1.8000.1280

RAC LinkID の範囲: 12070 ～ 12079

iDRAC スキーマ拡張の概要

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、ユーザーが達成したい成果に応じて設定できるプロパティを用意しています。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 iDRAC デバイスにリンクするために使用します。このモデルでは、ユーザー、iDRAC 権限、およびネットワーク上の iDRAC デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

Active Directory オブジェクトの概要

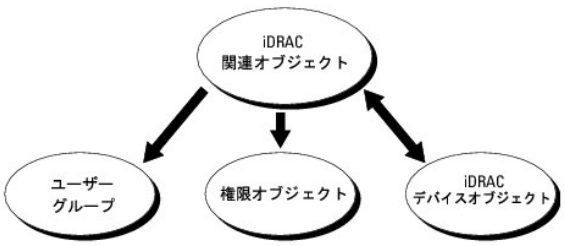
認証と許可のために Active Directory に統合するネットワーク上の物理 iDRAC のそれぞれに少なくとも 1 個、関連オブジェクトと RAC デバイスオブジェクトを作成しておきます。関連オブジェクトは必要な数だけ作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、iDRAC デバイスオブジェクトの数にも制限はありません。ユーザーと iDRAC デバイスオブジェクトは、企業内のどのドメインのメンバーでも構いません。

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

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

図 7-1 は、関連オブジェクトがすべての認証と認可に必要な関連付けを提供する仕組みを示しています。

図 7-1 Active Directory オブジェクトの典型的なセットアップ



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

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

Active Directory ユーザーとコンピュータ MMC スナップインへの Dell 拡張子は、関連オブジェクトと同じドメインの権限オブジェクトおよび iDRAC オブジェクトのみに関連付けることができます。Dell 拡張は、異なるドメインのグループまたは iDRAC オブジェクトを関連オブジェクトの製品メンバーとして追加することを許可していません。

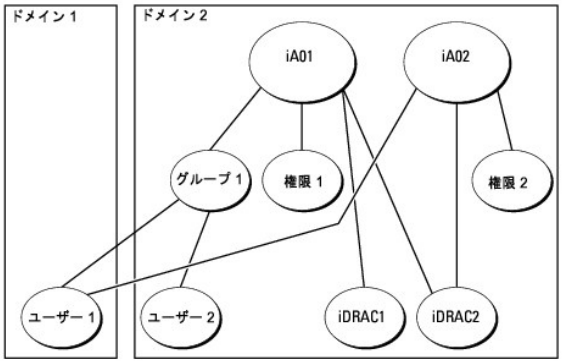
任意のドメインのユーザー、ユーザーグループ、またはネストされたユーザーグループを関連オブジェクトに追加できます。拡張スキーマソリューションは、Microsoft Active Directory によって許可されている複数のドメインにわたってネストされたユーザーグループやユーザーグループの種類をサポートしています。

拡張スキーマを使用した権限の蓄積

拡張スキーマ認証機構は、異なる関連オブジェクトを通して同じユーザーに関連付けられ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 7-2 に、拡張スキーマを使用した権限の蓄積例を示します。

図 7-2 ユーザーの権限の蓄積



この図は、2 つの関連オブジェクト iA01 と iA02 を示しています。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与えられています。

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。また、この図によると、ユーザー1 は異なるドメインに属することができ、ネストされたグループに関連付けることができます。

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

Active Directory を使用して 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 iDRAC ユーザーと権限の追加」 を参照)。
4. SSL を各ドメインコントローラで有効にします(「ドメインコントローラの SSL を有効にする」を参照)。
5. iDRAC6 ウェブインタフェースまたは RACADM を使用して、iDRAC6 Active Directory プロパティを設定します(「iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定」または「RACADM を使用した拡張スキーマの Active Directory の設定」を参照)。

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

次のいずれかの方法を使用してスキーマを拡張できます。

- Dell Schema Extender ユーティリティ
- 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。

- DVD ドライブ**:¥SYSMGMT¥ManagementStation¥support¥OMActiveDirectory_Tools¥Remote_Management_Advanced¥LDIF_Files**
- <**DVD** ドライブ**>:¥SYSMGMT¥ManagementStation¥support¥OMActiveDirectory_Tools¥Remote_Management_Advanced¥Schema Extender**

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

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

Dell Schema Extender の使用

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

1. **ようこそ** 画面で、**次へ** をクリックします。
2. 警告を読んでから、もう一度 **次へ** をクリックします。
3. **資格情報で現在のログオン使用** 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. **Finish**(終了)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。

   - クラス(表 7-2～表 7-7を参照)。
   - 属性(表 7-8)

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 7-2 Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられるオブジェクト識別番号(OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 7-3 dellRacDevice クラス

OID	**1.2.840.113556.1.8000.1280.1.7.1.1**
説明	Dell iDRAC デバイスを表します。iDRAC デバイスは、Active Directory で delliDRACDevice として設定する必要があります。この設定を使用して、iDRAC は Lightweight Directory Access Protocol(LDAP)クエリを Active Directory に送信できます。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	**dellSchemaVersion** **dellRacType**

表 7-4 delliDRACAssociationObject クラス

OID	**1.2.840.113556.1.8000.1280.1.7.1.2**
説明	Dell 関連オブジェクトを表します。この関連オブジェクトはユーザーとデバイスを連結します。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	**dellProductMembers** **dellPrivilegeMember**

表 7-5 dellRAC4Privileges クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
説明	iDRAC デバイスの権限(許可権限)を定義します。
クラスの種類	補助クラス
SuperClasses	なし

属性	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

表 7-6 dellPrivileges クラス

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

表 7-7 dellProduct クラス

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

表 7-8 Active Directory スキーマに追加された属性のリスト

属性名 / 説明	**割り当てられる OID / 構文オブジェクト識別子**	**単一値**
dellPrivilegeMember この属性に属する dellPrivilege オブジェクトのリスト	1.2.840.113556.1.8000.1280.1.1.2.1 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers この役割に属する dellRacDevice および 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
dellIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE

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。	ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsVirtualMediaUser ユーザーにデバイスの仮想メディア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser ユーザーにデバイスのテスト警告ユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion スキーマのアップデートに現在のスキーマバージョンが使用されます。	1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType この属性は delliDRACDevice オブジェクトの現在の RACタイプで dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers オブジェクトのリスト。この属性は dellProductMembers リンク属性へのバックワードリンクです。 リンク ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

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

『Dell Systems Management Tools and Documentation DVD』を使ってシステム管理ソフトウェアをインストールする場合、インストール手順中に **Active Directory ユーザーとコンピュータ スナップイン**のオプションを選択するとスナップインを拡張できます。システム管理ソフトウェアのインストールの手順については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。64 ビット Windows オペレーティングシステムでは、スナップインのインストーラは **<DVD ドライブ >:¥SYSMGMT¥ManagementStation¥support¥OMActiveDirectory_SnapIn64** にあります。

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

Administrator Pack のインストール

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

詳細については、「Active Directory ユーザーとコンピュータスナップインの開始」を参照してください。

Active Directory ユーザーとコンピュータスナップインの開始

Active Directory ユーザーとコンピュータスナップインを開くには、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** の順にクリックし、MMC と入力して **Enter** を押します。

   MMC が表示されます。

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 iDRAC ユーザーと権限の追加

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

- iDRAC デバイスオブジェクトの作成
- 権限オブジェクトの作成
- 関連オブジェクトの作成
- 関連オブジェクトの設定

iDRAC デバイスオブジェクトの作成

1. MMC **コンソールルート** ウィンドウでコンテナを右クリックします。
2. **新規→ Dell リモート管理オブジェクトの詳細設定** の順で選択します。

   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。この名前は、「iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定」のステップ A で入力する iDRAC 名と同一でなければなりません。
4. i**DRAC デバイスオブジェクト** を選択します。
5. **OK** をクリックします。

権限オブジェクトの作成

メモ: 権限オブジェクトは、関係する関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールのルート**（MMC）ウィンドウでコンテナを右クリックします。
2. **新規→ Dell リモート管理オブジェクトの詳細設定** の順に選択します。

   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **権限オブジェクト** を選択します。
5. **OK** をクリックします。
6. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。
7. **リモート管理特権** タブをクリックし、ユーザーに与える権限を選択します。

関連オブジェクトの作成

メモ: iDRAC 関連オブジェクトは、グループ から派生し、その範囲は、ドメインローカル に設定されます。

1. **コンソールのルート**（MMC）ウィンドウでコンテナを右クリックします。
2. **新規→ Dell リモート管理オブジェクトの詳細設定** の順で選択します。

   新規オブジェクト ウィンドウが開きます。
3. 新しいオブジェクトの名前を入力します。
4. **関連オブジェクト** を選択します。
5. **関連オブジェクト** のスコープを選択します。
6. **OK** をクリックします。

関連オブジェクトの設定

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーまたはユーザーグループ、権限オブジェクト、iDRAC デバイス間の関連付けができます。

ユーザーのグループを追加できます。Dell 関連グループと Dell に関連しないグループを作成する手順は同じです。

ユーザーまたはユーザーグループの追加

1. **関連オブジェクト** を右クリックし、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限オブジェクト タブをクリックして、iDRAC デバイスに認証するときにユーザーまたはユーザーグループの権限を定義する関連付けに、権限オブジェクトを追加します。関連オブジェクトに追加できる権限ブジェクトは 1 つだけです。

権限の追加

1. **権限オブジェクト** タブを選択し、**追加** をクリックします。
2. 権限オブジェクト名を入力し、**OK** をクリックします。

定義されたユーザーまたはユーザーグループが利用できるネットワークに接続している iDRAC デバイスを 1 つ追加するには、**製品** タブをクリックします。関連オブジェクトには複数の iDRAC デバイスを追加できます。

iDRAC デバイスの追加

iDRAC デバイスを追加するには、以下の手順を実行します。

1. **製品** タブを選択して **追加** をクリックします。
2. iDRAC デバイス名を入力して、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。

iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 のウェブベースのインタフェースにログインします。
3. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
4. **設定** タブをクリックして、**Active Directory**を選択します。
5. **Active Directory 設定と管理** ページの下にスクロールし、**Active Directory の設定** をクリックします。

   Active Directory の設定と管理 ページのステップ **1 / 4** が表示されます。
6. Active Directory の SSL 証明書を検証する場合は、**証明書設定** の下の **Enable Certificate Validation(証明書検証を有効にする)** を選択します。検証しない場合は、ステップ 9 へ進みます。
7. **Active Directory CA 証明書のアップロード** の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照します。

   メモ: フルパスおよび正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。
8. **アップロード** をクリックします。

   アップロードした Active Directory CA 証明書の情報が表示されます。

9. **Kerberos Keytab のアップロード** で、keytab ファイルのパスを入力するか、このファイルを参照します。**アップロード** をクリックします。Kerberos keytab が iDRAC6 にアップロードされます。

10. **次へ** をクリックして、**Active Directory 設定と管理 ステップ 2 / 4** へ進みます。

11. **Active Directory を有効にする** をクリックします。

注意: 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 ファクタ認証(TFA)とシングルサインオン(SSO)機能はサポートされません。

12. **追加** をクリックして、ユーザードメイン名を入力します。

13. 表示されるプロンプトにユーザードメイン名を入力し、**OK** をクリックします。このステップは省略できます。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で表示されます。リストから選択すると、ユーザー名を入力するだけです。

14. iDRAC6 が Active Directory の応答を待つ **タイムアウト** 時間を秒数で指定します。デフォルト値は 120 秒です。

15. ドメインコントローラサーバーのアドレス を入力します。ログイン処理に最大 3 つの Active Directory サーバーを指定できますが、少なくとも 1 台のサーバーは、IP アドレスまたは完全修飾ドメイン名(FQDN)を入力して設定する必要があります。iDRAC6 は、設定した各サーバーに接続が確立されるまで接続を試みます。

メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject(件名) または Subject Alternative Name(代替名) フィールドの値と一致する必要があります。

16. **次へ** をクリックして、**Active Directory 設定と管理 ステップ 3 / 4** へ進みます。

17. **スキーマの選択** で、**拡張スキーマ** をクリックします。

18. **次へ** をクリックして、**Active Directory 設定と管理 ステップ 4 / 4** へ進みます。

19. **拡張スキーマの設定** で、iDRAC 名およびドメイン名を入力して iDRAC のデバイスオブジェクトを設定します。iDRAC ドメイン名は、iDRAC オブジェクトが作成されるドメインです。

20. Active Directory 拡張スキーマの設定を保存するには、**完了** をクリックします。

    iDRAC6 ウェブサーバーは、自動的に **Active Directory 設定と管理** ページに戻ります。

21. Active Directory 拡張スキーマの設定を確認するには、設定のテスト をクリックします。

22. Active Directory ユーザー名とパスワードを入力します。

    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、iDRAC 上で DNS サーバーが正しく設定されている必要があります。**リモートアクセス→ 設定→ ネットワーク** ページに移動し、手動で DNS サーバーを設定するか、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の代わりに RACADM CLI ツールを使用して、拡張スキーマで iDRAC Active Directory 機能を設定するには、次のコマンドを使用します。

1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config -g cfgActiveDirectory -o
cfgADRacName <RAC コモンネーム>

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

racadm config -g cfgActiveDirectory -o cfgDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

racadm config -g cfgActiveDirectory -o cfgDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

racadm config -g cfgActiveDirectory -o cfgDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

メモ: 3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。拡張スキーマのオプションが選択されている場合、iDRAC デバイスが所在するドメインコントローラの FQDN または IP アドレスとなります。拡張スキーマモードでは、グローバルカタログサーバーは全く使用されません。

メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject(件名) または Subject Alternative Name(代替名) フィールドの値と一致する必要があります。

注意: このリリースでは、Active Directory に拡張スキーマ用に設定されている場合、スマートカードベースの 2 ファクタ認証(TFA)とシングルサインオン(SSO)機能はサポートされません。

SSL ハンドシェイク中の証明書の検証を無効にしたい場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

この場合、CA 証明書をアップロードする必要はありません。

SSL ハンドシェイク中の証明書の検証を強制したい場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

次の RACADM コマンドの使用は省略できる場合があります。詳細については、「iDRAC6 ファームウェア SSL 証明書のインポート」を参照してください。

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. iDRAC で DHCP が無効な場合や、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中にユーザー名を入力するだけで済むように、ユーザードメインのリストを設定する場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName -i <索引>
```

1 から 40 の索引番号で、最大 40 のユーザードメインを設定できます。

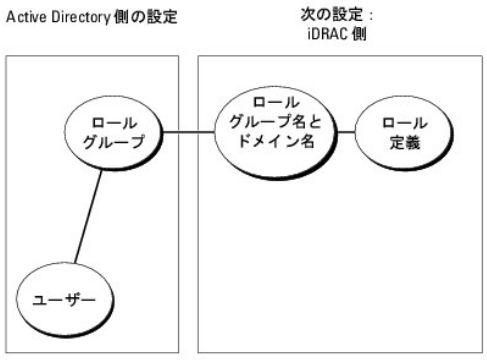
ユーザードメインの詳細については、「Active Directory を使用した iDRAC6 へのログイン」を参照してください。

5. 拡張スキーマの Active Directory 設定を完了するには、**Enter** キーを押します。

標準スキーマの Active Directory の概要

図 7-3 に示すように、Active Directory を統合するために標準スキーマを使用する場合は、Active Directory と iDRAC6 の両方で設定が必要になります。

図 7-3 Microsoft Active Directory と標準スキーマで iDRAC の設定



Active Directory 側では、標準グループオブジェクトがロール(役割)グループとして使用されます。iDRAC6 へのアクセス権を持つユーザーは役割グループのメンバーとなります。指定した iDRAC6 へのアクセスをこのユーザーに与えるには、役割グループ名とそのドメイン名を特定の iDRAC6 で設定する必要があります。拡張スキーマソリューションとは異なり、役割と権限レベルは Active Directory でなく、各 iDRAC6 で定義されます。各 iDRAC について、最大 5 つまでロール(役割)グループを設定そて定義できます。表 7-9 は、デフォルトのロールグループの権限を示し

ています。

表 7-9 デフォルトのロールグループの権限

ロール(役割)グループ	デフォルトの権限レベル	許可する権限	ビットマスク
ロールグループ 1	管理者	**iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバーコントロールコマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。**	0x000001ff
ロールグループ 2	オペレータ	iDRAC **へのログイン、iDRAC の設定、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。**	0x000000f9
ロールグループ 3	読み取り専用。	iDRAC へのログイン	0x00000001
ロールグループ 4	なし	権限の割り当てなし	0x00000000
ロールグループ 5	なし	権限の割り当てなし	0x00000000

メモ: ビットマスク値を使用するのは、RACADM で標準スキーマを設定する場合に限ります。

シングルドメインとマルチドメインのシナリオ

すべてのログインユーザー、ロールグループ、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ロールグループのすべて、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、すべてのロール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。

iDRAC にアクセスするために標準スキーマ Active Directory を設定する方法

Active Directory ユーザーが iDRAC6 にアクセスするためには、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。

1. Active Directory サーバー(ドメインコントローラ)で、**Active Directory ユーザーとコンピュータスナップイン** を開きます。
2. グループを作成するか、既存のグループを選択します。グループとドメインの名前は、ウェブインタフェースまたは RACADM を使用して iDRAC6 上で設定する必要があります(「iDRAC6 ウェブインタフェースを使用した Active Directory と標準スキーマの設定」または「RACADM を使用した標準スキーマの Active Directory の設定」を参照)。
3. iDRAC にアクセスする Active Directory グループのメンバーとして Active Directory ユーザーを追加します。

iDRAC6 ウェブインタフェースを使用した Active Directory と標準スキーマの設定

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 のウェブベースのインタフェースにログインします。
3. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
4. **設定** タブをクリックして、**Active Directory** を選択します。
5. **Active Directory 設定と管理** ページの下にスクロールし、**Active Directory の設定** をクリックします。

   Active Directory の設定と管理 ページの**ステップ 1 / 4** が表示されます。
6. Active Directory の SSL 証明書を検証する場合は、**証明書設定** の下の **Enable Certificate Validation(証明書検証を有効にする)** を選択します。検証しない場合は、ステップ 9 へ進みます**。**
7. **Active Directory CA 証明書のアップロード** の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照します。

   メモ: フルパス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。
8. **アップロード** をクリックします。

   有効な Active Directory CA 証明書の情報が表示されます。
9. **Kerberos Keytab のアップロード** で、keytab ファイルのパスを入力するか、このファイルを参照します。**アップロード** をクリックします。Kerberos keytab が iDRAC6 にアップロードされます。

10. **次へ** をクリックして、**Active Directory 設定と管理 ステップ 2 / 4** へ進みます。

11. **Active Directory を有効にする** を選択します。

12. 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** を選択します。

13. **追加** をクリックして、ユーザードメイン名を入力します。

14. 表示されるプロンプトにユーザードメイン名を入力し、**OK** をクリックします。

15. iDRAC6 が Active Directory の応答を待つ **タイムアウト** 時間を秒数で指定します。デフォルト値は 120 秒です。

16. ドメインコントローラサーバーのアドレス を入力します。ログイン処理に最大 3 つの Active Directory サーバーを指定できますが、少なくとも 1 台のサーバーは、IP アドレスまたは完全修飾ドメイン名(FQDN)を入力して設定する必要があります。iDRAC6 は、設定された各サーバーに、接続が確立されるまで接続を試みます。

    メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject(件名) または Subject Alternative Name(代替名) フィールドの値と一致する必要があります。

17. **次へ** をクリックして、**Active Directory 設定と管理 ステップ 3 / 4** へ進みます。

18. **スキーマの選択** の下の **拡張スキーマ** をクリックします。

19. **次へ** をクリックして、**Active Directory 設定と管理 ページ** の**ステップ 4a / 4** へ進みます。

20. **標準スキーマの設定** で、グローバルカタログサーバーのアドレスを入力して、Active Directory での場所を指定します。少なくとも 1 つのグローバルカタログサーバーの場所を設定する必要があります。

    メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject(件名) または Subject Alternative Name(代替名) フィールドの値と一致する必要があります。

    メモ: ユーザーアカウントとロールグループが異なるドメインにある場合、グローバルカタログサーバーは標準スキーマのみに必要です。また、このようなマルチドメインのシナリオで使用できるのは、ユニバーサルグループのみです。

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

    ステップ 4 の 4b ページが表示されます。

22. **役割グループ名** を指定します。

    役割グループ名は、Active Directory における iDRAC に関連付けられた役割グループを識別します。

23. 役割グループのドメインとなる **役割グループドメイン** を指定します。

24. **役割グループの権限レベル**を選択して、**役割グループの権限**を指定します。たとえば、**システム管理者** を選択すると、そのアクセス権レベルのすべての特権がされます。

25. **適用** をクリックして、役割グループの設定を保存します。

    iDRAC6 ウェブサーバーによって、**設定が表示されるステップ 4a / 4 Active Directory 設定と管理** ページに自動的に戻ります。

26. 手順 20 ～ 手順 25 を繰り返し、追加する役割グループを設定します。

27. **終了** をクリックし、**Active Directory の設定と管理 ページ**に戻ります。

28. Active Directory 標準スキーマの設定を確認するには、**設定のテスト** をクリックします。

29. iDRAC6 ユーザー名とパスワードを入力します。

    テスト結果およびテストログが表示されます。詳細については、「設定のテスト」を参照してください。

メモ: Active Directory ログインをサポートするには、iDRAC 上で DNS サーバーが正しく設定されている必要があります。**リモートアクセス** → **設定** → **ネットワーク** ページに移動し、手動で DNS サーバーを設定するか、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の代わりに RACADM CLI を使用して、標準スキーマの iDRAC Active Directory 機能を設定するには、次のコマンドを使用します。

1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 2
   ```

   racadm config -g cfgStandardSchema -i <索引> -o
   cfgSSADRoleGroupName <役割グループのコモンネーム>

   racadm config -g cfgStandardSchema -i <索引> -o
   cfgSSADRoleGroupDomain <完全修飾ドメイン名>

   racadm config -g cfgStandardSchema -i <索引> -o
   cfgSSADRoleGroupPrivilege <特定のユーザー権限の
   ビットマスク番号>

   メモ: ビットマスク番号については、表 B-2を参照してください。

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

   メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject(件名) または Subject Alternative Name(代替名) フィールドの値と一致する必要があります。

   メモ: ドメインの FQDN だけではなく、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: ユーザーアカウントとロールグループが異なるドメインにある場合、グローバルカタログサーバーは標準スキーマのみに必要です。また、このようなマルチドメインのシナリオでは、ユニバーサルグループのみを使用できます。

   メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の Subject(件名) または Subject Alternative Name(代替名) フィールドの値と一致する必要があります。

   SSL ハンドシェイク中の証明書の検証を無効にしたい場合は、次の RACADM コマンドを入力します。

   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0

   この場合、認証局(CA)の証明書をアップロードする必要はありません。

   SSL ハンドシェイク中の証明書の検証を強制したい場合は、次の RACADM コマンドを入力します。

   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

   この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

   ```
   racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
   ```

   次の RACADM コマンドは任意で実行できます。詳細については、「iDRAC6 ファームウェア SSL 証明書のインポート」を参照してください。

   ```
   racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
   ```

2. iDRAC6 で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```

3. iDRAC6 で DHCP が無効になっている場合や、手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
   ```

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>
   ```

   racadm config -g cfgLanNetworking -o cfgDNSServer1 <二次 DNS IP アドレス>

4. iDRAC6 ウェブインタフェースにログインする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する場合は、次のコマンドを入力します。

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName -i <索引>
   ```

   1 から 40 の索引番号で、最大 40 のユーザードメインを設定できます。

ユーザードメインの詳細については、「Active Directory を使用した iDRAC6 へのログイン」を参照してください。

設定のテスト

設定が正常に動作するか確認する場合や、Active Directory ログインが失敗する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、ユーザー名（例：ユーザー名@ドメイン.com）とパスワードを入力する必要があります。設定によっては、テストのすべてのステップを実行し、各ステップの結果が表示されるまでに時間がかかる場合があります。結果ページの下部に詳細なテストログが表示されます。

いずれかのステップにエラーが発生した場合は、テストログで詳細を確認し、問題と解決策を特定します。一般的なエラーについては、「Active Directory について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

iDRAC は Active Directory ドメインコントローラに対してユーザーを認証するとき、ドメインコントローラと SSL セッションを開始します。この時点で、ドメインコントローラは認証局（CA）によって署名された証明書を発行し、そのルート証明書も iDRAC にアップロードされます。つまり、iDRAC が（ルートまたは子ドメインコントローラにかかわらず）どの ドメインコントローラに対しても認証できるためには、ドメインコントローラがそのドメインの CA によって署名された SSL が有効な証明書を所有している必要があります。

Microsoft エンタープライズのルート CA を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。

iDRAC へのドメインコントローラのルート CA 証明書のエクスポート

メモ: システムで Windows 2000 が実行している場合は、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** のフィールドに「mmc」と入力し、**OK** をクリックします。
4. **コンソール 1**（MMC）ウィンドウで、**ファイル**（Windows 2000 システムでは **コンソール**）をクリックし、**スナップインの追加 / 削除** を選択します。
5. **スナップインの追加と削除** ウィンドウで **追加** をクリックします。
6. **スタンドアロンスナップイン** ウィンドウで **証明書** を選択して **追加** をクリックします。
7. **コンピュータ アカウント**を選択して **次へ** をクリックします。
8. **ローカルコンピュータ** を選択して **完了** をクリックします。
9. **OK** をクリックします。
10. **コンソール 1** ウィンドウで、**証明書** フォルダを展開し、**パーソナル** フォルダを展開して、**証明書** フォルダをクリックします。
11. ルート CA 証明書を見つけて右クリックし、**すべてのタスク** を選択してから **エクスポート...** を選択します。
12. **証明書のエクスポート ウィザード**で **次へ** を選択し、**いいえ、秘密キーをエクスポートしない** を選択します。
13. **次へ** をクリックし、フォーマットとして **Base-64 エンコード X.509 (.cer)** を選択します。
14. **次へ** をクリックし、システムのディレクトリに証明書を保存します。

15. 手順 14 に保存した証明書を iDRAC にアップロードします。

    RACADM を使って証明書をアップロードする場合は、「iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定」または「RACADM を使用した標準スキーマの Active Directory の設定」を参照してください。

    ウェブインタフェース を使って証明書をアップロードする場合は、「iDRAC6 ウェブベースのインタフェースを使用した Active Directory と拡張スキーマの設定」または「iDRAC6 ウェブインタフェースを使用した Active Directory と標準スキーマの設定」を参照してください。

iDRAC6 ファームウェア SSL 証明書のインポート

メモ: Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証する設定になっている場合、iDRAC サーバー証明書を Active Directory ドメインコントローラにもアップロードする必要があります。Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証しない場合、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 証明書がよく知られている CA によって署名され、その CA の証明書が既にドメインコントローラの信頼できるルート認証局のリストに含まれている場合は、この項の手順を実行する必要はありません。

iDRAC の SSL 証明書は、iDRAC のウェブサーバーで使用される証明書と同じです。iDRAC のコントローラにはすべて、デフォルトの自己署名付き証明書が付属しています。

iDRAC SSL 証明書をダウンロードするには、次の RACADM コマンドを実行します。

racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>

1. ドメインコントローラで、**MMC コンソール** ウィンドウを開き、**証明書**→**信頼できるルート認証局** の順に選択します。
2. **証明書** を右クリックし、**すべてのタスク** を選択して **インポート** をクリックします。
3. **次へ** をクリックして SSL 証明書ファイルまで参照します。
4. 各ドメインコントローラの**信頼できるルート認証局**に iDRAC SSL 証明書をインストールします。

   独自の証明書をインストールした場合は、その証明書に署名する CA が **信頼できるルート認証局** リストにあるかどうか確認してください。この認証局がリストにない場合は、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 を使用して、次のいずれかの方法で iDRAC6 にログインできます。

- ウェブインタフェース
- リモート RACADM
- シリアルまたは Telnet コンソール

ログイン構文は、3 つの方法にすべて共通です。

<ユーザー名@ドメイン>

または

<ドメイン>¥<ユーザー名> または<ドメイン>/<ユーザ名>

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、ユーザードメインが設定されている場合、ウェブインタフェースのログイン画面のプルダウンメニューにすべてのユーザードメインが表示されます。プルダウンメニューからユーザードメインを選択する場合は、ユーザー名のみを入力します。**This iDRAC(この iDRAC)**を選択した場合も、上記「Active Directory を使用した iDRAC6 へのログイン」のログイン構文を使用して、Active Directory ユーザーとしてログインできます。

スマートカードを使用して iDRAC6 にログインすることもできます。詳細については、「スマートカードを使用した iDRAC6 へのログイン」を参照してください。

メモ: Windows 2008 Active Directory サーバーは、最長 256 文字の <ユーザー名>@<ドメイン名> 文字列のみをサポートしています。

Active Directory シングルサインオンの使用

iDRAC6 を有効にしてネットワーク認証プロトコルである Kerberos を使用すると、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. **リモートアクセス** → **設定** タブ → **Active Directory** サブタブ → に移動し、**Active Directory の設定** を選択します。

2. **Active Directory 設定と管理** ページのステップ 2/4 で、**シングルサインオンを有効にする** を選択します。**シングルサインオンを有効にする** オプションは、**Active Directory を有効にする** オプションが選択されている場合にのみ有効になります。

   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ことが条件となります。また、Active Directory 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。キャッシュに格納された Active Directory 資格情報を使用して 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
   ```

シングルサインオンを使用した iDRAC6 へのログイン

1. ネットワークアカウントを使用してワークステーションにログインします。

2. iDRAC6 ウェブページにアクセスするには、次のように入力します。

   ```
   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 のシングルサインオンページが表示されます。

3. **ログイン** をクリックします。

有効な Active Directory 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を使用して iDRAC6 にログインできます。

Active Directory についてよくあるお問い合わせ（FAQ）

Active Directory ログインに失敗しました。どうすれば問題を解決できますか。

iDRAC6 は、ウェブインタフェースから診断ツールを提供しています。ウェブインタフェースから、システム管理者権限のあるローカルユーザーとしてログインします。リ**モート**アクセス→設定→**Active Directory** をクリックします。**Active Directory 設定と管理** ページの下にスクロールし、設定のテスト をクリックします。テストユーザー名とパスワードを入力し、**Start Test（テストの開始）** をクリックします。iDRAC6 は、順を追ってテストを実行し、各ステップの結果を表示します。問題の解決に役立つように、詳細なテスト結果がログに記録されます。**Active Directory 設定と管理** ページ に戻るには、**Active Directory** タブをクリックします。設定を変更し、テストユーザーが認証ステップに合格するまでテストを再実行するには、ページの下までスクロールし、**Active Directory の設定** をクリックします。

証明書の検証を有効にしましたが、Active Directory ログインに失敗しました。GUI から診断を実行しましたが、テスト結果に次のエラーメッセージが表示されています。

ERROR（エラー）: Can't contact LDAP server（LDAP サーバーと通信できません）, error（エラー）:14090086:SSL routines（SSL ルーチン）:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed（証明書の検証に失敗しました）: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC（iDRAC に正しい認証局（CA）証明書がアップロードされていることを確認してください。）Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.
（ 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。）

何が問題なのでしょうか。どうすれば修正できますか。

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。証明書の iDRAC6 の日付と有効期限を確認してください。

2. iDRAC6 で設定されたドメインコントローラのアドレスがディレクトリサーバー証明書の件名または代替名と一致しない。IP アドレスを使用している場合は、次の質問と回答をお読みください。FQDN を使用している場合は、ドメインではなく、ドメインコントローラの FQDN を使用しているかどうか確認してください（たとえば、example.com ではなく、servername.example.com）。

ドメインコントローラのアドレスに IP アドレスを使用していますが、証明書の検証に失敗します。何が問題なのでしょうか。

ドメインコントローラ証明書の 件名または代替名 フィールドを確認してください。通常、Active Directory はドメインコントローラ証明書の 件名または代替名 フィールドにドメインコントローラの IP アドレスではなく、ホスト名を使用します。この問題は複数の方法で修正できます。

1. サーバー証明書の件名または代替名と一致するように、iDRAC6 で指定するドメインコントロールアドレスにドメインコントローラのホスト名(FQDN)を設定します。
2. iDRAC6 で設定された IP アドレスと一致する IP アドレスを件名または代替名フィールドで使用するようにサーバー証明書を再発行します。
3. SSL ハンドシェイク時に証明書の検証がなくても、このドメインコントローラを信頼する場合は、証明書の検証を無効にします。

マルチドメイン環境で拡張スキーマを使用していますが、ドメインコントローラのアドレスはどのように設定すればよいのですか。

iDRAC6 オブジェクトが属するドメインのドメインコントローラのホスト名(FQDN)または IP アドレスを使用します。

いつグローバルカタログアドレスを設定する必要がありますか。

拡張スキーマを使用している場合、グローバルカタログアドレスは使用されません。

標準スキーマを使用し、ユーザーとロールグループが異なるドメインに属する場合は、グローバルカタログアドレスを設定する必要があります。この場合、使用できるのはユニバーサルグループのみです。

標準スキーマを使用し、すべてのユーザーとロールグループが同じドメインに属する場合は、グローバルカタログアドレスを設定する必要はありません。

標準スキーマクエリ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、ユーザーと役割グループがそのドメインにある場合は、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は、iDRAC6 グローバルカタログのクエリを継続します。グローバルカタログから追加の権限が取得された場合は、これらの権限が蓄積されます。

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 CONNECT を行いますが、不安定な接続では LDAP BIND を行いません。

iDRAC6 で、証明書の検証がデフォルトで有効になっているのはなぜですか。

iDRAC6 は、接続先となるドメインコントローラの身元を確認するために、強力なセキュリティ対策を実施しています。証明書を検証しないと、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。

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。

Active Directory を使用して iDRAC6 にログインできない場合は、何を確認すればいいですか。

iDRAC6 ウェブインタフェースの Active Directory 設定と管理 ページの下部にある 設定のテスト をクリックすると、**問題を診断できます。次に、テスト結果で特定された問題を修正します。**詳細については、「設定のテスト」を参照してください。

この項では、最もよくある問題について説明します。一般的に、以下の事項を確認してください。

1. ログインに NetBIOS 名でなく、正しいユーザードメイン名が使用されていることを確認します。
2. ローカル iDRAC6 ユーザーアカウントがある場合は、ローカルの資格情報を使用して iDRAC6 にログインします。

   ログインした後、以下を行います。

   a. iDRAC6 **Active Directory 設定と管理** ページにある **Active Directory を有効にする** ボックスが選択されていることを確認します。

   b. iDRAC6 ネットワーク設定 ページの DNS 設定が正しいことを確認します。

   c. 証明書の検証を有効にした場合は、iDRAC6 に正しい Active Directory ルート CA 証明書がアップロードされていることを確認します。iDRAC6 の日時が CA 証明書の有効期限内であることを確認します。

   d. 拡張スキーマを使用している場合は、**iDRAC6 名** と **iDRAC6 ドメイン名** が 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 **グループドメイン名** が Active Directory の環境設定と一致していることを確認します。

3. iDRAC6 の日時がドメインコントローラ SSL 証明書の有効期限内であることを確認します。

目次ページに戻る

目次ページに戻る

スマートカード認証の設定

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

iDRAC6 では、**スマートカードログオン** の有効化による 2 要素認証（TFA）機能がサポートされています。

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）の入力を義務づけて、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

ウェブベースのインタフェースから iDRAC6 スマートカードログオン機能を有効にするには、**リモートアクセス** → **設定** → **スマートカード** に移動し、**有効にする** を**選択**します。

以下の事項に留意してください。

- **有効にする** または **リモート RACADM で有効にする** を選択すると、ウェブベースのインターフェースを使用する以降のログイン試行でスマートカード のログオンを要求されます。

  有効にする を選択すると、telnet、SSH、シリアル、リモート RACADM、IPMI オーバー LAN などのコマンドラインインタフェース（CLI）の帯域外インタフェースのサービスは 1 要素の認証しかサポートしないため、無効になります。

  リモート RACADM で有効にする を選択すると、CLI 帯域外インタフェース（リモート racadm 以外）はすべて無効になります。

  メモ: **リモート RACADM で有効にする** は、iDRAC6 管理者がリモート RACADM コマンドを使ってスクリプトを実行するために iDRAC6 ユーザーインタフェースにアクセスする場合にのみ設定することをお勧めします。リモート RACADM を使用する必要がないときは、スマートカードログインを **有効にする** 設定を選択してください。また、iDRAC6 のローカルユーザー設定や Active Directory の設定が完了してから、**スマートカードログオン** を有効にしてください。

- スマートカードの設定を**無効にします**（デフォルト）。これを選択すると、TFA スマートカードログイン機能が無効になり、次回 iDRAC6 GUI にログインしたときに、ウェブインターフェースからのデフォルトのログインメッセージとして表示される指示に従って Microsoft® Active Directory® またはローカルのログインユーザー名とパスワードを入力します。
- **スマートカードログオンの CRL チェックを有効にする**：証明書失効リスト（CRL）配信サーバーからダウンロードしたユーザーの iDRAC 証明書と照合してチェックします。

  メモ: CRL 配信サーバーは、ユーザーのスマートカード証明書に含まれています。

ローカル iDRAC6 ユーザーに対するスマートカードログオンの設定

ローカル iDRAC6 ユーザーがスマートカードを使って iDRAC6 にログインするように設定できます。**リモートアクセス** → **設定** → **ユーザー** をクリックします。

ただし、ユーザーがスマートカードを使用して iDRAC6 にログインするには、まずユーザーのスマートカード証明書と、信頼されている認証局（CA）の証明書を iDRAC6 にアップロードする必要があります。

スマートカード証明書のエクスポート

ユーザーの証明書を取得するには、カード管理ソフトウェア（CMS）を使用して、スマートカードから Base64 符号化形式ファイルにスマートカード証明書をエクスポートします。CMS は通常、スマートカードのベンダーから入手できます。この符号化ファイルをユーザーの証明書として iDRAC6 にアップロードしてください。スマートカードのユーザー証明書の発行元である信頼された認証局も、CA 証明書を Base64 エンコード形式でファイルにエクスポートする必要があります。ユーザー用の信頼された CA 証明書としてこのファイルをアップロードします。スマートカード証明書内でユーザーのユーザープリンシプル名（UPN）を形成するユーザー名を使用してユーザーを設定します。

メモ: iDRAC6 にログインするには、iDRAC6 で設定するユーザー名が、大文字と小文字の区別を含め、スマートカード証明書の User Principal Name（UPN）と同じでなければなりません。

たとえば、スマートカード証明書が "sampleuser@domain.com" というユーザーに発行された場合、ユーザー名は "sampleuser" となります。

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 ユーザーがスマートカードを使って iDRAC6 にログインできるように設定するには、iDRAC6 管理者は DNS サーバーを設定して、Active Directory CA 証明書を iDRAC6 にアップロードし、Active Directory ログオンを有効にします。Active Directory ユーザーの設定方法については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。

メモ: スマートカードユーザーが Active Directory に存在する場合は、スマートカードの PIN と同時に Active Directory のパスワードが必要です。

リモートアクセス → **設定** → **Active Directory** の順に選択して、Active Directory を設定できます。

スマートカードの設定

メモ: これらの設定を変更するには、**iDRAC の設定** 権限が必要です。

1. **システム** ツリーを拡張し、**リモートアクセス** をクリックします。
2. **設定** タブをクリックし、**スマートカード** をクリックします。
3. スマートカードのログオン設定を指定します。

   表 8-1 に、**スマートカード** ページの設定を示します。
4. **変更の適用** をクリックします。

表 8-1 スマートカードの設定

設定	説明
スマートカードログオンの設定	• **無効** - スマートカードログオンを無効にします。以降、グラフィカルユーザーインタフェース（GUI）からログインすると、通常のログインページが表示されます。セキュアシェル（SSH）、Telnet、シリアル、リモート RACADM を含むすべての帯域外インタフェースはデフォルト状態に戻ります。 • **有効** - スマートカードログオンを有効にします。変更を適用した後、ログアウトして、スマートカードを挿入し、**ログイン** をクリックしてスマートカード PIN を入力します。スマートカードログインを有効にすると、SSH、Telnet、シリアル、リモート RACADM、IPMI オーバー LAN などの CLI 帯域外インタフェースがすべて無効になります。 • **リモート RACADM と共に有効にする** - スマートカードログオンとリモート RACADM を有効にします。その他の CLI 帯域外インタフェースはすべて無効になります。 **メモ:** スマートカードログインでは、適切な証明書を使用してローカル iDRAC6 ユーザーを設定する必要があります。スマートカードログオンを Microsoft Active Directory ユーザーのログインに使用する場合は、そのユーザーの Active Directory ユーザー証明書を設定する必要があります。ユーザー証明書は、**ユーザー**→ **ユーザーメインメニュー** ページで設定できます。
スマートカードログオンの CRL チェックを有効にする	このチェックはスマートカードのローカルユーザーにのみ使用可能です。このオプションは、ユーザーのスマートカード証明書を失効させるために iDRAC6 で証明書失効リスト（CRL）をチェックする場合に選択します。CRL が機能するには、ネットワーク構成の過程で iDRAC6 に DNS の有効な IP アドレスが設定されている必要があります。iDRAC6 の **リモートアクセス**→ **設定** → **ネットワーク** で DNS の IP アドレスを設定できます。 以下の場合には、ユーザーはログインできません。 • ユーザー証明書が CRL ファイルのリストで失効となっている。 • iDRAC6 が CRL 配信サーバーと通信できない。 • iDRAC6 が CRL をダウンロードできない。 **メモ:** このチェックに成功するには、**設定** → **ネットワーク** ページで DNS サーバーの IP アドレスを正しく設定する必要があります。

スマートカードを使用した iDRAC6 へのログイン

iDRAC6 ウェブインタフェースは、スマートカードを使用するように設定されているすべてのユーザーに、スマートカードログオンページを表示します。

メモ: ユーザー用のスマートカードログオンを有効にする前に、iDRAC6 のローカルユーザーと Active Directory の設定が完了していることを確認してください。

メモ: ブラウザの設定によっては、この機能を初めて使用するときに Smart Card reader ActiveX 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場合があります。

1. https を使用して iDRAC6 のウェブページにアクセスします。

   `https://<IP アドレス>`

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

   `https://<IP アドレス>:<ポート番号>`

   <IP address> は iDRAC6 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

   iDRAC6 ログインページが表示され、スマートカードの挿入を要求されます。

2. スマートカードをリーダーに挿入して **ログイン** をクリックします。

   スマートカードの PIN を入力するように指示が表示されます。

3. ローカルスマートカードのスマートカード PIN を入力したとき、このユーザーがローカルで作成されていない場合は、ユーザーの Active Directory アカウントのパスワードを入力するように指示が表示されます。

メモ: スマートカードログオンの CTL チェックを有効にする が選択されている Active Directory ユーザーの場合は、CRL がダウンロードされ、ユーザーの証明書の CRL がチェックされます。証明書が CRL に失効と表示されているか、何らかの理由で CRL をダウンロードできない場合は、Active Directory を通したログインに失敗します。

これで、iDRAC6 にログインできます。

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

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 address> は iDRAC6 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

   iDRAC6 ログインページが表示され、スマートカードの挿入を要求されます。

2. スマートカードを挿入して、**ログイン** をクリックします。

   PIN ポップアップダイアログボックスが表示されます。

3. パスワードを入力して、**OK** をクリックします。

4. ユーザーの Active Directory パスワードを入力し、ユーザーを認証して **OK** をクリックします。

   Active Directory に設定した資格情報で iDRAC6 にログインします。

メモ: スマートカードユーザーが Active Directory に存在する場合は、スマートカードの PIN と同時に Active Directory のパスワードが必要です。今後のリリースでは、Active Directory パスワードが不要になる可能性があります。

---

iDRAC6 へのスマートカードログインのトラブルシューティング

以下は、スマートカードにアクセスできないときのデバッグに役立つヒントです。

ActiveX プラグインがスマートカードリーダーを検出しません

スマートカードが Microsoft Windows® オペレーティングシステムでサポートされていることを確認します。Windows がサポートしているスマートカード暗号サービスプロバイダ(CSP)の数は限られています。

ヒント:スマートカード CSP が特定のクライアントに含まれているか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を入手方法について、組織のスマートカード発行者に問い合わせてください。

ローカル iDRAC6 へのログインを無効にする

ローカルの iDRAC6 ユーザーがログインできない場合は、ユーザー名とユーザー証明書が iDRAC6 にアップロードされているかどうか確認します。iDRAC6 のトレースログに、エラーに関する重要なログメッセージが含まれていることがあります。ただし、セキュリティ上の理由から、エラーメッセージは意図的に曖昧になっている場合があります。

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

Active Directory ユーザーとして iDRAC6 にログインできない場合は、スマートカードログオンを有効にしないで iDRAC6 にログインしてみてください。CRL チェックを有効にしている場合は、CRL チ

ェックを有効にしないで Active Directory にログインしてみてください。iDRAC6 追跡ログには、CRL に失敗した場合の重要なメッセージが入っています。

次のコマンドを使用してローカル racadm からスマートカードログオンを無効にすることもできます。

```
racadm config -g cfgActiveDirectory -o cfgADSmartCardLogonEnable 0
```

目次ページに戻る

目次ページに戻る

GUI コンソールリダイレクトの使用

Integrated Dell™ Remote Access Controller 6（iDRAC6）バージョン 1.1 ユーザーズガイド

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、ローカルのコンソールにリモートからグラフィックモードまたはテキストモードでアクセスできます。この機能を使用すると、1 つの場所から単一または複数の iDRAC6 システムを制御できます。

日常的なメンテナンスを各サーバーの前に座って行う必要はありません。デスクトップまたはラップトップコンピュータを使ってリモートからサーバーを管理できます。また、リモートから即座に他のユーザーと情報を共有することもできます。

コンソールリダイレクトの使用

メモ: コンソールリダイレクトセッションを開いたとき、管理下サーバーはそのコンソールがリダイレクトされていることを示しません。

メモ: 管理ステーションから iDRAC6 へのコンソールリダイレクトのセッションが既に開いている場合に、同じ管理ステーションからその iDRAC6 への新しいセッションを開こうとすると、既存のセッションがアクティブになります。新しいセッションは生成されません。

メモ: 1 つの管理ステーションから複数の iDRAC6 コントローラに対して、コンソールリダイレクトの複数のセッションを同時に開くことができます。

コンソールリダイレクト ページでは、ローカルの管理ステーションのキーボード、ビデオ、およびマウスを使ってリモートシステムを管理し、リモート管理下サーバーでそのデバイスを制御できます。この機能を仮想メディア機能と併用すると、リモートでソフトウェアのインストールを実行できます。

コンソールリダイレクトセッションには次の規則が適用されます。

- 最大 4 つのコンソールリダイレクトセッションが同時にサポートされます。すべてのセッションで、同じ管理下サーバーのコンソールが同時に表示されます。
- 同じクライアントコンソール（管理ステーション）からリモートサーバー（iDRAC6）に対して開くことができるセッションは、1 つだけです。ただし、同じクライアントから複数のリモートサーバーに対しては、複数のセッションを開くことができます。
- 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 MB/秒以上 のネットワーク帯域幅が必要です。

iDRAC への最初のコンソールリダイレクトセッションは、フルアクセスのセッションとなります。2 番目のユーザーがコンソールリダイレクトセッションを要求すると、最初のユーザーは通知を受け取り、拒否、**読み取り専用で許可**、または**許可**のオプションから選択できます。2 番目のユーザーには、別のユーザーに制御権があることが通知されます。1 番目のユーザーが 30 秒以内に応答しないと、2 番目のユーザーには自動的にフルアクセスが拒否されます。

最後のフルアクセスのセッションが終了すると、**読み取り専用で許可** のセッションはすべて自動終了します。

管理ステーションの設定

管理ステーションでコンソールリダイレクトを使用するには、次の手順を実行してください。

1. 対応ウェブブラウザをインストールして設定します。詳細については、以下の項を参照してください。
   - 「対応ウェブブラウザ」
   - 「対応ウェブブラウザの設定」

   メモ: コンソールリダイレクト機能が正常に動作するには、管理ステーション上に Java Run Time Environment（JRE）がインストールされている必要があります。

2. Internet Explorer を使用している場合、次の手順に従って、ブラウザが暗号化されたコンテンツをダウンロードできるようにします。
   - Internet Explorer で **ツール** → **インターネットオプション** → **詳細設定** の順に選択します。
   - **セキュリティ** のセクションまでスクロールし、次のオプションをオフにします。

     暗号化されたページをディスクに保存しない

3. 画面解像度は 1280x1024 ピクセル以上に設定することをお勧めします。

メモ: システムで Linux オペレーティングシステムを実行している場合は、ローカルモニターで X11 コンソールが表示されない可能性があります。iDRAC KVM で <Ctrl><Alt><F1> キーを押すと、Linux がテキストコンソールに切り替わります。

メモ: 「Expected: ; 」という Java Script コンパイルエラーが発生する場合があります。この問題を解決するには、JavaWebStart で「ダイレクト接続」を使用するようにネットワーク設定を調整します。編集 -> プリファレンス -> 全般 -> ネットワーク設定 の順に選択し、「ブラウザ設定を使用する」の代わりに「ダイレクト接続」を選択します。

iDRAC6 ウェブインタフェースでのコンソールリダイレクトの設定

iDRAC6 のウェブインタフェースでコンソールリダイレクトを設定するには、次の手順を実行してください。

1. iDRAC コンソールリダイレクトを設定するには、**システム** → **コンソール/メディア** → **設定** の順にクリックします。
2. コンソールリダイレクトのプロパティを設定します。表 10-1 は、コンソールリダイレクトの設定について説明しています。
3. 完了したら、**変更の**適用 をクリックします。
4. 適切なボタンをクリックして続行します。表 10-2を参照してください 。

表 10-1 コンソールリダイレクトの設定プロパティ

プロパティ	説明
有効	クリックして、コンソールリダイレクトを有効または無効にします。このオプションが有効の場合は、コンソールリダイレクトが有効であることを示します。デフォルト値は **有効** です。 **メモ:** 仮想 KVM の起動後に **有効** オプションをオンまたはオフにすると、既存の仮想 KVM セッションがすべて切断される可能性があります。
最大セッション数	コンソールリダイレクトの最大セッション数(1 ～ 4)が表示されます。コンソールリダイレクトで許可する最大セッション数を変更するには、ドロップダウンメニューを使用します。デフォルトは **2** です。
アクティブセッション数	アクティブなコンソールセッション数を表示します。このフィールドは読み取り専用です。
リモートプレゼンスポート	コンソールリダイレクトのキーボード/マウスオプションへの接続に使用するネットワークポート番号。トラフィックは常に暗号化されます。別のプログラムでデフォルトのポートが使用されている場合は、この番号を変更しなければならない可能性があります。デフォルトは **5900** です。 **メモ:** 仮想 KVM の起動後に **リモートプレゼンスポート** の値を変更すると、既存の仮想 KVM セッションがすべて切断される可能性があります。
ビデオ暗号化有効	**チェックボックスがオン** の場合は、ビデオ暗号化が有効です。ビデオポートを経由するすべてのトラフィックは、暗号化されます。 **チェックボックスがオフ** の場合は、ビデオ暗号化が無効です。ビデオポートを経由するトラフィックは暗号化されません。 デフォルトは、**暗号化** されます**。暗号化を無効にすると、低速なネットワークパフォーマンスを改善できる場合があります。** **メモ:** 仮想 KVM の起動後に **ビデオ暗号化の有効** オプションをオンまたはオフにすると、既存の仮想 KVM セッションがすべて切断される可能性があります。
ローカルサーバービデオ有効	チェックボックスがオンの場合は、コンソールリダイレクト中 iDRAC KVM モニターへの出力は無効になります。これにより、**コンソールリダイレクト** を使って実行したタスクは、管理下サーバーのローカルモニターに表示されなくなります。

メモ: コンソールリダイレクトで仮想メディアを使用する方法については、「仮想メディアの設定と使用法」を参照してください。

表 10-2 のボタンは **設定** ページにあります。

表 10-2 設定ページのボタン

ボタン	定義
印刷	ページを印刷します。
更新	**設定** ページを再ロードします。
変更の適用	新しいまたは変更された設定を保存します。

コンソールリダイレクトセッションの開始

コンソールリダイレクトセッションを開くと、Dell™ 仮想 KVM ビューアアプリケーションが開始し、リモートシステムのデスクトップがビューアに表示されます。この仮想 KVM ビューアアプリケーションを使用すると、ローカル管理ステーションからリモートシステムのマウスとキーボードの機能を制御できます。

ウェブインタフェースでコンソールリダイレクトセッションを開くには、次の手順を実行してください。

1. **システム** → **コンソール / メディア** → **コンソールリダイレクトと仮想メディア** をクリックします。

2. 表 10-3の情報を使用して、コンソールリダイレクトセッションが利用可能であることを確認します。

   表示されているプロパティ値の設定を変更する場合は、「iDRAC6 ウェブインタフェースでのコンソールリダイレクトの設定」を参照してください。

表 10-3 コンソールリダイレクト

プロパティ	説明
コンソールリダイレクト有効	はい / いいえ(チェックボックスがオン ¥ チェックボックスがオフ)
ビデオ暗号化有効	はい / いいえ(チェックボックスがオン ¥ チェックボックスがオフ)
最大セッション数	サポートされているコンソールリダイレクトの最大セッション数を表示します。
アクティブセッション数	現在アクティブなコンソールリダイレクトセッション数を表示します。
ローカルサーバービデオ有効	はい = 有効、いいえ = 無効。
リモートプレゼンスポート	コンソールリダイレクトのキーボード/マウスオプションへの接続に使用するネットワークポート番号。トラフィックは常に暗号化されます。別のプログラムでデフォルトのポートが使用されている場合は、この番号を変更しなければならない可能性があります。デフォルトは 5900 です。

メモ: コンソールリダイレクトで仮想メディアを使用する方法については、「仮想メディアの設定と使用法」を参照してください。

表 10-4 のボタンは、**コンソールリダイレクトおよび 仮想メディア** ページで使用できます。

表 10-4 コンソールリダイレクトおよび仮想メディアページのボタン

ボタン	定義
更新	**コンソールリダイレクト**および仮想メディア ページを再ロードします。
ビューアの起動	目的のリモートシステムのコンソールリダイレクトセッションを開きます。
印刷	**コンソールリダイレクトおよび仮想メディア** ページを印刷します。

3. コンソールリダイレクトセッションが使用可能な場合は、**ビューアの起動** をクリックします。

   メモ: アプリケーションが起動すると、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 分間内に参照する必要があります。そうしないと、アプリケーションの再起動を要求されます。

   メモ: 以下の手順の途中で **セキュリティ警告** ウィンドウが表示された場合は、その内容を読んでから、**はい** をクリックして続行します。

   管理ステーションが iDRAC6 に接続し、iDRAC KVM ビューアアプリケーションにリモートシステムのデスクトップが表示されます。

4. 2 つのマウスポインタ(1 つはリモートシステム用、もう 1 つはローカルシステム用)が ビューアウィンドウに表示されます。iDRAC KVM メニューの **ツール** で **単一カーソル**) オプションを選択すると、1 つのカーソルに変更できます。

ビデオビューアの使用

ビデオビューアは管理ステーションと管理下サーバー間のユーザーインタフェースを提供するので、管理ステーション側から管理下サーバーのデスクトップを表示して、マウスやキーボードの機能を制御できます。リモートシステムに接続すると、ビデオビューアが別のウィンドウで開始します。

メモ: リモートサーバーの電源がオフになっていると、**「信号がありません」** というメッセージが表示されます。

ビデオビューアは、マウスの同期、スナップショット、キーボードマクロ、仮想メディアへのアクセスなど、さまざまなコントロール調整機能を提供します。これらの機能の詳細については、**システム → コンソール/メディア** の順にクリックし、**コンソールリダイレクトおよび仮想メディア ページで ヘルプ** をクリックします。

コンソールリダイレクトセッションを開始し、ビデオビューアが表示されたら、マウスポインタの同期が必要になる場合があります。

ローカルサーバービデオの有効または無効

iDRAC6 ウェブインタフェースで、iDRAC KVM の接続を無効にするように iDRAC6 を設定できます。

管理下サーバーのコンソールへの排他的アクセスを確保する場合は、ローカルコンソールを無効にし、また **コンソールリダイレクトの設定 ページ** で **最大セッション数** を 1 に 再設定する必要があります。

メモ: サーバー上のローカルビデオを無効にする(オフにする)と、iDRAC KVM に接続しているモニター、キーボード、マウスが無効になります。

ローカルコンソールを無効または有効にするには、次の手順を実行してください。

1. 管理ステーション上で、対応ウェブブラウザを開いて iDRAC6 にログインします。詳細については、「ウェブインタフェースへのアクセス」を参照してください。

2. **システム** → **コンソール / メディア** → **設定** の順にクリックします。

3. サーバー上でローカルビデオを無効にする(オフにする)には、**設定** ページで **ローカルサーバービデオ有効** チェックボックスをオフにしてから **適用** をクリックします。デフォルト値は [オフ] です。

   メモ: ローカルサーバービデオをオンにした場合、オフにするには 15 秒かかります。

4. サーバー上でローカルビデオを有効にする(オンにする)には、**設定** ページで **ローカルサーバービデオ有効** チェックボックスをオンにしてから **適用** をクリックします。

コンソールリダイレクトについてよくあるお問い合わせ(FAQ)

表 10-5 は、よくあるお問い合わせとその回答です。

表 10-5 コンソールリダイレクトの使用:よくあるお問い合わせ(FAQ)

質問	回答
サーバー上のローカルビデオがオフになっている場合に、新しいリモートコンソールビデオセッションを開始できますか。	はい。
ローカルビデオをオフにするように要求してからサーバー上のローカルビデオがオフになるまで 15 秒もかかるのはなぜですか。	ビデオがオフに切り替わる前に、ローカルユーザーが必要に応じて別の操作を実行できるように配慮されています。
ローカルビデオをオンにする場合に、遅延時間は発生しますか。	いいえ。ローカルビデオを **オン** にする要求を iDRAC6 が受信すると、ビデオは瞬時にオンになります。
ローカルユーザーがビデオをオフにすることもできますか。	ローカルコンソールを無効にすると、ローカルユーザーがビデオをオフにすることはできません。
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。	ローカルコンソールを無効にすると、ローカルユーザーがビデオをオンにすることはできません。
ローカルビデオをオフに切り替えると、ローカルキーボードとマウスもオフになりますか。	いいえ
ローカルコンソールをオフにすると、リモートコンソールセッションのビデオはオフになりますか。	いいえ。ローカルビデオのオン / オフを切り替えても、リモートコンソールセッションには影響しません。
iDRAC6 ユーザーがローカルサーバービデオをオン / オフにするために必要な権限は何ですか。	iDRAC6 の設定権限を持つユーザーであれば、ローカルコンソールをオン / オフにできます。
ローカルサーバービデオの現在のステータスを取得するには、どのようにしますか。	ステータスは iDRAC6 ウェブインタフェースの **コンソールリダイレクトの設定** ページに表示されます。 RACADM CLI コマンドの **racadm getconfig -g cfgRacTuning** は、**cfgRacTuneLocalServerVideo** のオブジェクトにステータスを表示します。
コンソールリダイレクトウィンドウからシステム画面の下部が見えません。	管理ステーションのモニターの解像度が 1280x1024 に設定されていることを確認してください。また、iDRAC KVM 上のスクロールバーも使ってみてください。
コンソールウィンドウが文字化けします。	Linux のコンソールビューアには UTF-8 文字コードが必要です。ロケールを確認し、必要に応じて文字コードをリセットしてください。
Linux テキストコンソールでマウスが同期しないのはなぜでしょうか。	仮想 KVM は USB マウスドライバを必要としますが、USB マウスドライバは X-Window オペレーティングシステムでしか使用できません。。
マウスの同期の問題がまだ解決しません。	コンソールリダイレクトセッションの開始前に、オペレーティングシステム用に正しいマウスが選択されていることを確認します。 iDRAC KVM クライアント上で iDRAC6 KVM メニューの **ツール** で **単一カーソル** オプションが選択されていることを確認します。
iDRAC6 コンソールリダイレクトを使用してリモートで 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。	良好なパフォーマンスを得るためには、5 MB/秒の接続を推奨します。最低限必要なパフォーマンスを得るためには、1 MB/秒の接続が必要です。
管理ステーションでコンソールリダイレクトを実行するために最低限必要なシステム要件を教えてください。	管理ステーションには、256 MB 以上の RAM を搭載した Intel® Pentium® III 500 MHz プロセッサが必要です。
iDRAC KVM ビデオビューア内に **No Signal (シグナルなし)** のメッセージが表示されるのはなぜですか。	iDRAC Virtual KVM プラグインがリモートサーバーのデスクトップビデオを受信していない場合に、このメッセージが表示されます。一般的に、これはリモートサーバーの電源がオフになると、この現象が発生します。リモートサーバーのビデオ受信の誤動作によって、このメッセージが表示される場合もあります。
iDRAC KVM ビデオビューアに **Out of Range (範囲外)** というメッセージが表示されるのはなぜ	ビデオをキャプチャするために必要なパラメータが、iDRAC がビデオをキャプチャできる範囲を超えている場合に、このメッセージが表示されます。ディスプレイの解像度やリフレッシュレートなどのパラメータが高すぎると、範囲外の状態が発生します。通常、パラメータの最大範囲は、ビデ

ですか。	オのメモリサイズや帯域幅などの物理的な制限に基づいて設定されます。

目次ページに戻る