Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

メモと注意

メモ: メモでは、コンピュータを使いこなすために役立つ重要な情報を説明しています。

注意: **注意では、記載されている指示に従わないと、ハードウェアの損傷やデータの損失につながる可能性がある事項を示しています。**

2010 年 7 月

目次ページに戻る

iDRAC6 Enterprise 概要

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

Integrated Dell Remote Access Controller(iDRAC6)は、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する、ハードウェアとソフトウェアのシステム管理ソリューションです。

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搭載し、管理下 Dell PowerEdge サーバーとシステム基板上で共存します。サーバーのオペレーティングシステムがアプリケーションプログラムを実行し、iDRAC6 はオペレーティングシステム外のサーバーの環境と状態を監視および管理します。

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

管理下サーバーは、モジュール式電源装置、冷却ファン、Chassis Management Controller(CMC) と共に Dell M1000-e システムエンクロージャ(シャーシ)に設置されています。CMC は、シャーシに搭載されているすべてのコンポーネントの監視と管理を行います。冗長 CMC を追加すると、一次 CMC に障害が発生した場合にホットフェールオーバーを提供することもできます。シャーシは、LCD ディスプレイ、ローカルコンソール接続、およびウェブインタフェースを介して iDRAC6 へのアクセスを提供します。シャーシ内の各ブレードに iDRAC6 があります。M1000e には合計 16 台のブレードを搭載できます。

iDRAC6 へのネットワーク接続はすべて、CMC ネットワークインタフェース(「GB1」というラベルの CMC RJ45 接続ポート)を経由します。CMC は、内部の専用ネットワークを使用してトラフィックをブレードの iDRAC6 デバイスに転送します。この専用の管理ネットワークは、サーバーのデータパス外で、オペレーティングシステムの制御域外、つまり帯域外にあります。 管理下サーバーの帯域内ネットワークインタフェースへは、シャーシに搭載されている I/O モジュール(IOM)からアクセスします。

メモ: iDRAC6 と CMC によって使用されるシャーシ管理ネットワークを運用ネットワークから分離することを推奨しています。管理ネットワークと運用やアプリケーションネットワークのトラフィックを混在させると、輻輳やネットワーク飽和が発生して、CMC と iDRAC6 の通信に遅延が生じる可能性があります。また、遅延によってシャーシが予期しない動作を行うことがあります。たとえば、iDRAC6 が正常に稼動しているのに CMC にはオフラインと表示されたりします。これにより、他の予期しない動作が引き起こされることもあります。

iDRAC6 ネットワークインタフェースは、デフォルトで無効になっています。これを設定しなければ、iDRAC6 にアクセスできません。ネットワークで iDRAC6 を有効にして設定すると、iDRAC6 ウェブインタフェース、Telnet、SSH、さらに Intelligent Platform Management Interface(IPMI)などのサポートされているネットワーク管理プロトコルを使用して、割り当てられた IP アドレスを使ってアクセスできるようになります。

IPv6 対応証明ロゴ

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

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

---

iDRAC6 のセキュリティ機能

- Microsoft Active Directory、汎用 LDAP ディレクトリサービス、またはローカル管理のユーザー ID および パスワードを使用したユーザー認証。
- スマートカードログオン機能で提供される 2 要素認証。2 要素認証は、ユーザーが所有するもの(スマートカード)とユーザーが知っているもの(暗証番号)に基づきます。
- システム管理者がユーザー別に権限を設定できる役割ベースの許可
- ユーザー ID とパスワードの設定
- SM-CLP と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
- セッションタイムアウトの設定(秒数指定)
- 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回数の制限により、制限を超えた IP アドレスからのログインを阻止
- iDRAC6 に接続するクライアントの IP アドレス範囲を設定可能

---

iDRAC6 Enterprise と vFlash メディア

iDRAC6 Enterprise には vFlash SD メディア用のカードスロットがあります。iDRAC6 Enterprise と vFlash メディアの詳細については、**support.dell.com/manuals** で『ハードウェアオーナーズマニュアル』を参照してください。

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

表 1-1 iDRAC6 の機能リスト

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

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

対応プラットフォーム

最新の対応プラットフォームについては、**support.dell.com / manuals** にあるiDRAC6 Readme ファイルと『Dell システムソフトウェア サポートマトリックス』を参照してください。

対応 OS

最新の対応プラットフォームについては、**support.dell.com / manuals** にあるiDRAC6 Readme ファイルと『Dell システムソフトウェア サポートマトリックス』を参照してください。

対応ウェブブラウザ

最新の情報については、**support.dell.com / manuals** にあるiDRAC6 Readme ファイルと『Dell システムソフトウェア サポートマトリックス』を参照してください。

メモ: SSL 2.0 にはセキュリティ上の不具合があるため、サポートされなくなりました。お使いのブラウザで SSL 3.0 が有効に設定されていることを確認してください。

対応リモートアクセス接続

表 1-2 は接続機能のリストです。

表 1-2 対応リモートアクセス接続

接続	機能
iDRAC6 NIC	• 10Mbps/100Mbs/1Gbps Ethernet(CMC GB Ethernet ポート経由) • DHCP のサポート • SNMP トラップと電子メールによるイベント通知 • iDRAC6 設定、システム起動、リセット、電源投入、シャットダウンなどの操作を行うための SM-CLP シェルおよび RACADM コマンドは、SSH と Telnet を介してサポートされています。 • IPMItool や ipmish などの IPMI ユーティリティのサポート

iDRAC6 のポート

表 1-3 は、iDRAC6 が接続を待ち受けるポートのリストです。表 1-4 は、iDRAC6 がクライアントとして使用するポートです。この情報は、ファイアウォールを開いて iDRAC6 にリモートからアクセスする場合に必要です。

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

表 1-3 iDRAC6 サーバーリスニングポート

ポート番号	機能
22*	セキュアシェル(SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668、3669	仮想メディアサービス
3670、3671	仮想メディアセキュアサービス
3672	vFlash サービス
5900*	仮想コンソールのキーボード / マウス
5901*	仮想コンソールビデオ
5988*	WSMAN に使用

*設定可能なポート

表 1-4 iDRAC6 クライアントポート

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

その他の必要マニュアル

このガイドのほかに、以下のドキュメントにもシステム内の iDRAC6 の設定と操作に関する追加情報が記載されています。これらのガイドは、デルサポートサイト **support.dell.com / manuals** で入手できます。**マニュアル** ページで、**ソフトウェア→ システム管理** をクリックします。右側の製品リンクをクリックして、ドキュメントにアクセスします。

- 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説明しています。
- 『Dell システムソフトウェアサポートマトリックス』では、各種の Dell システム、各システムでサポートされているオペレーティングシステム、各システムにインストールできる Dell OpenManage コンポーネントについて説明しています。
- 『Dell OpenManage Server Administrator インストールガイド』では、Dell OpenManage Server Administrator のインストール手順が説明されています。
- 『Dell OpenManage Management Station Software インストールガイド』では、Dell OpenManage Management Station Software(ベースボード管理ユーティリティ、DRAC ツール、Active Directory スナップインを含む)のインストール手順が説明されています。
- 『Dell Chassis Management Controller ユーザーガイド』および『Dell Chassis Management Controller システム管理者リファレンス ガイド』では、Dell PowerEdge サーバーが設置されているシャーシ内のすべてのモジュールを管理するコントローラの使用法について説明しています。
- 『Dell OpenManage IT Assistant ユーザーズガイド』では、IT Assistant の使用法について説明しています。
- 『Dell Management Console ユーザーズガイド 』では、Dell 管理コンソールの使用法について説明しています。
- 『Dell OpenManage Server Administrator ユーザーズガイド』では、Server Administrator のインストールと使用法について説明しています。
- 『Dell Update Packages ユーザーズガイド』では、システムアップデート対策の一環としての Dell Update Packages の入手と使用法について説明しています。
- 『Dell Lifecycle Controller ユーザーズガイド』では、Unified Server Configurator(USC)、Unified Server Configurator - Lifecycle Controller Enabled(USC - LCE)、および Remote Services について説明しています。
- **デルエンタープライズテクノロジーセンター www.delltechcenter.com** で入手可能な『iDRAC6 CIM エレメントマッピング』と『iDRAC6 SM-CLP プリパティデータベース』では、iDRAC6 SM-CLP プロパティデータベース、WS-MAN クラスと SM-CLP ターゲット間のマッピング、および Dell 実装の詳細について説明しています。
- 『iDRAC6 管理者リファレンスガイド』では、iDRAC6 Enterprise on Blade Servers と iDRAC6 Enterprise または Express on Rack and Tower の RACADM サブコマンド、サポートされている RACADM インタフェース、および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ついて説明しています。
- 用語集 では、本書で使用されている用語について説明しています。

次のシステム文書にも、iDRAC6 をインストールするシステムに関する詳細が含まれています。

- システムに同梱の「安全にお使いいただくために」には、安全および法規制に関する重要な情報が記載されています。法規制の詳細については、**www.dell.com / regulatory_compliance** にある Regulatory Compliance(法規制情報)ホームページを参照してください。保証情報は、このマニュアルに含まれている場合と、別の文書として付属する場合があります。
- 『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、システム管理ソフトウェアの機能、動作要件、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。

- リリースノートや 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

iDRAC6 Enterprise の設定

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

本項では、iDRAC6 へのアクセスを確立し、iDRAC6 を使用する管理環境を設定する方法について説明します。

作業を開始する前に

iDRAC6 を設定する前に、下記をご用意ください。

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

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

- DVD root - サーバーセットアップおよびシステムインストール情報を提供する Dell Systems Build and Update Utility が含まれます。
- SYSMGMT - Dell OpenManage Server Administrator を含むシステム管理ソフトウェアの製品が含まれます。

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

---

iDRAC6 を設定するためのインタフェース

iDRAC6 の設定は、iDRAC6 設定ユーティリティ、iDRAC6 ウェブインタフェース、Chassis Management Controller(CMC)ウェブインタフェース、シャーシの LCD パネル、ローカルおよびリモート RACADM CLI、iVMCLI、または SM-CLP CLI を使用して実行できます。管理下サーバーにオペレーティングシステムと Dell OpenManage ソフトウェアをインストールすると、ローカル RACADM CLI が使用可能になります。表 2-1 は、これらのインタフェースについて説明しています。

セキュリティ強化のために、iDRAC6 設定ユーティリティまたはローカル RACADM CLI から iDRAC6 の設定へのアクセスを、RACADM コマンド(**support.dell.com / manuals** の『iDRAC6 管理者リファレンスガイド』参照))または GUI(「設定へのローカルアクセスの有効化と無効化」参照)から無効にすることができます。

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

表 2-1 設定インタフェース

インタフェース	説明
iDRAC6 設定ユーティリティ	起動時にアクセスできる iDRAC6 設定ユーティリティは、新しい Dell PowerEdge サーバーをインストールする場合に便利です。ネットワークや基本的なセキュリティ機能の設定や、その他の機能を有効にするときに使用してください。
iDRAC6 ウェブインタフェース	iDRAC6 ウェブインタフェースは、iDRAC6 の管理と管理下サーバーの監視をインタラクティブに実行できるブラウザベースの管理アプリケーションです。システム正常性の監視、システムイベントログの表示、ローカル iDRAC6 ユーザーの管理、CMC ウェブインタフェースや仮想コンソールセッションの開始などの日常的なタスクに使用する主要インタフェースです。
CMC ウェブインタフェース	シャーシの監視と管理に加えて、CMC ウェブインタフェースは、管理下サーバーの状態の確認、iDRAC6 ファームウェアのアップデート、iDRAC6 ネットワークの指定、iDRAC6 ウェブインタフェースへのログオン、管理下サーバーの起動、終了、リセットなどに使用できます。
シャーシ LCD パネル	iDRAC6 を搭載したシャーシの LCD パネルは、シャーシ内のサーバーの大まかな状態を表示するために使用できます。CMC の初期設定中、設定ウィザードを使用して iDRAC6 ネットワークの DHCP 設定を有効にできます。
ローカルおよびリモート RACADM	ローカル RACADM コマンドラインインタフェースは管理下サーバーで実行されます。これには、iDRAC6 ウェブインタフェースから開始する仮想コンソールのセッションからアクセスします。RACADM は、Dell OpenManage Server Administrator のインストール時に管理下サーバーにインストールされます。 リモート RACADM は、管理ステーションで実行されるクライアントユーティリティです。帯域外のネットワークインタフェースを使用して、管理下サーバーに RACADM コマンドを実行します。**-r** オプションはネットワーク経由で RACADM コマンドを実行します。 RACADM コマンドは、iDRAC6 のほぼすべての機能へのアクセスを提供します。センサーデータや、システムイベントログのレコード、iDRAC6 で管理される現在の状態や設定値を調べることができます。さらに、iDRAC6 の設定値の変更、ローカルユーザーの管理、機能の有効 / 無効化、管理下サーバーのシャットダウンや再起動などの電源機能の実行も可能です。
iVMCLI	iDRAC6 仮想メディアコマンドラインインタフェース(iVMCLI)は、管理下サーバーが管理ステーションのメディアにアクセスできるようにします。複数の管理下サーバーにオペレーティングシステムをインストールするスクリプトの作成に便利です。
SM-CLP	SM-CLP は、iDRAC6 に組み込まれたサーバー管理ワークグループサーバー管理 - コマンドラインプロトコル(SM-CLP)の実装です。SM-CLP コマンドラインには、Telnet または SSH を使用して iDRAC6 にログインし、CLI プロンプトで `smclp` と入力してアクセスします。 SM-CLP コマンドは、ローカル RACADM コマンドの便利なサブセットを実装しています。これらのコマンドは管理ステーションのコマンドラインから実行できるため、スクリプト

	の記述に便利です。コマンドの出力は、XML などの明確に定義されたフォーマットで取得でき、スクリプトの記述や、既存のレポートツールや管理ツールとの統合を円滑にします。
IPMI	IPMI は、iDRAC6 などの内蔵管理サブシステムが他の内蔵システムや管理アプリケーションと通信するための標準的な方法を定義しています。 IPMI のプラットフォームイベントフィルタ(PEF)やプラットフォームイベントトラップ(PET)を設定するには、iDRAC6 ウェブインタフェース、SM-CLP、または RACADM コマンドを使用できます。 PEF は、特定の状態を検知した際に、iDRAC6 に特定の処置(たとえば、管理下サーバーの再起動)を実施させます。PET は、特定のイベントまたは状態を検知したときに電子メールまたは IPMI 警告を送信するよう iDRAC6 に指示します。 また iDRAC6 では、IPMI オーバー LAN を有効にしている場合に **IPMItool** や **ipmish** などの標準的な IPMI ツールも使用できます。

設定タスク

本項では、管理ステーション、iDRAC6、管理下サーバーの設定タスクについて概説します。実行するタスクには、iDRAC6 をリモートからアクセスするための設定、使用する iDRAC6 機能の設定、管理下サーバーへのオペレーティングシステムのインストール、管理ステーションおよび管理下サーバーへの管理ソフトウェアのインストールなどがあります。

各タスクの下に、そのタスクの実行に使用できる設定タスクが一覧表示されています。

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

管理ステーションの設定

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

iDRAC6 ネットワークの設定

iDRAC6 ネットワークを有効にし、IP、ネットマスク、ゲートウェイ、DNS のアドレスを設定します。

メモ: セキュリティ強化のために、iDRAC6 設定ユーティリティまたはローカル RACADM CLI から iDRAC6 の設定へのアクセスを、RACADM コマンド(**support.dell.com / manuals** の『iDRAC6 管理者リファレンスガイド』参照))または GUI(「設定へのローカルアクセスの有効化と無効化」参照)から無効にすることができます。

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

メモ: LCD パネルを使用してサーバーを設定するオプションは、CMC の初期設定中のみに使用できます。シャーシを実装すると、その後で LCD パネルを使用して iDRAC6 を再設定することはできません。

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

- シャーシの LCD パネル - 『Dell Chassis Management Controller ファームウェアユーザーガイド』を参照してください。
- iDRAC6 設定ユーティリティ - 「iDRAC6 設定ユーティリティの使用」を参照
- CMC ウェブインタフェース - 「CMC ウェブインタフェースによるネットワークオプションの設定」を参照
- リモートおよびローカル RACADM - **support.dell.com / manuals** で 『iDRAC6 管理者リファレンスガイド』の「**cfgLanNetworking**」を参照

iDRAC6 ユーザーの設定

ローカル iDRAC6 のユーザーと権限を設定します。iDRAC6 では、ファームウェアに 16 のローカルユーザーを表示するテーブルがあります。これらのユーザーにユーザー名、パスワード、および役割を設定できます。

- iDRAC6 設定ユーティリティ(システム管理ユーザーのみの設定) - 「LAN ユーザー設定」を参照
- iDRAC6 ウェブインタフェース - 「iDRAC6 ユーザーの追加と設定 」を参照
- リモートおよびローカル RACADM - 「iDRAC6 ユーザーの追加」を参照

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

ディレクトリサービスの設定

ローカル iDRAC6 ユーザーだけでなく、Microsoft Active Directory または一般的な LDAP ディレクトリサービスを使用して iDRAC6 のユーザーログインを認証できます。

詳細については、「iDRAC6 ディレクトリサービスの使用」を参照してください。

IP フィルタおよび IP ブロックの設定

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

す。

- iDRAC6 ウェブインタフェース - 「IP フィルタと IP ブロックの設定」を参照
- RACADM - 「IP フィルタ(IpRange)の設定」と「IP ブロックの設定」を参照

プラットフォームイベントの設定

プラットフォームイベントは、iDRAC6 が管理下サーバーのセンサーから「警告」状態または「重要」状態を検知した場合に発生します。

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

- iDRAC6 ウェブインタフェース - 「プラットフォームイベントフィルタ(PEF) の設定」を参照
- RACADM - 「PEF の設定」を参照

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

- iDRAC6 ウェブインタフェース - 「プラットフォームイベントトラップ(PET)の設定」を参照
- RACADM - 「PET の設定」を参照

設定へのローカルアクセスの有効化と無効化

ネットワーク設定やユーザー権限などの重要な設定パラメータへのアクセスは、無効にすることができます アクセスを無効にすると、再起動を行ってもその設定が保持されます。設定への書き込みアクセスは、ローカル RACADM プログラムと iDRAC6 設定ユーティリティに対して(起動時に)ブロックされます。設定パラメータへのウェブアクセスが妨げられることはなく、いつでも設定データを表示できます。iDRAC ウェブインタフェースの詳細については、「設定へのローカルアクセスの有効化と無効化」を参照してください。RACADM コマンドの場合は、**support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』の「**cfgRacTuning**」を参照してください。

iDRAC6 サービスの設定

iDRAC6 ネットワークサービス(Telnet、SSH、ウェブサーバーインタフェースなど)を有効 / 無効にしたり、ポートや他のサービスパラメータの設定を変更したりします。

- iDRAC6 ウェブインタフェース - 「iDRAC6 サービスの設定」を参照
- RACADM - 「ローカル RACADM を使用した iDRAC6 Telnet および SSH サービスの設定」を参照

Secure Socket Layer(SSL)の設定

iDRAC6 ウェブサーバーの SSL 設定

- iDRAC6 ウェブインタフェース - 「SSL(Secure Sockets Layer)」を参照
- RACADM - デルサポートサイト **support.dell.com / manuals** にある『iDRAC6 管理者リファレンスガイド』の「cfgRacSecurity」、「sslcsrgen」、「sslcertupload」、「sslcertdownload」、「sslcertview」を参照してください。.

仮想メディアを設定する

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

- iDRAC6 ウェブインタフェース - 「仮想メディアの設定と使用」を参照
- iDRAC6 設定ユーティリティ - 「仮想メディアの設定」を参照

vFlash メディアカードの設定

iDRAC6 で使用する vFlash メディアカードをインストールして設定します。

- iDRAC6 ウェブインタフェースと RACADM の使用 - 「vFlash SD カードの設定とvFlash パーティションの管理」を参照

管理下サーバーソフトウェアのインストール

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

- 仮想コンソールリ - 「管理下サーバーへのソフトウェアのインストール」を参照
- iVMCLI - 「仮想メディアコマンドラインインタフェースユーティリティの使用」を参照

管理下サーバーへの前回クラッシュ画面機能の設定

オペレーティングシステムのクラッシュまたはフリーズ後に iDRAC6 が画面イメージをキャプチャできるように管理下サーバーを設定します。

- 管理下サーバー - 「管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定」と「Windows の自動再起動オプションを無効にする」を参照

CMC ウェブインタフェースによるネットワークオプションの設定

メモ: CMC から iDRAC6 ネットワーク設定を行うには、シャーシ設定のシステム管理者権限が必要です。

メモ: デフォルトの CMC ユーザーは **root** で、デフォルトのパスワードは **calvin** です。

メモ: CMC の IP アドレスは、**システム** → **リモートアクセス** → **CMC** の順にクリックすることで、iDRAC6 ウェブインタフェースに表示されます。この画面から CMC ウェブインタフェースを起動することもできます。

CMC からの iDRAC6 ウェブインタフェースの起動

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

CMC から iDRAC6 を起動するには、以下の手順を実行します。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで、**サーバーの概要** を選択します。使用可能なサーバーのリストが **サーバーの状態** 画面に表示されます。
3. 管理するサーバーの **iDRAC** をクリックします。新しいブラウザウィンドウで iDRAC GUI が起動します。

1 台のサーバーの iDRAC6 ウェブインタフェースを CMC から起動するには、以下の手順を実行します。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで **サーバーの概要** を展開します。展開された**サーバー** リストに、すべてのサーバーが表示されます。
3. 表示するサーバーをクリックします。選択したサーバーの **サーバー状態** 画面が表示されます。
4. **iDRAC6 GUI の起動** をクリックします。

シングルサインオン

シングルサインオン機能を利用すると、もう一度ログインしなくても CMC から iDRAC6 ウェブインタフェースを起動できます。以下に、シングルサインオンの詳細について説明します。

- **ユーザー権限** で **Server Administrator** の権限が設定されている CMC ユーザーは、シングルサインオンを使用して iDRAC6 ウェブインタフェースに自動的にログインされます。ログイン後、ユーザーには自動的に iDRAC6 Administrator 権限が与えられます。これは、iDRAC6 のアカウントを持たない同じユーザーや、アカウントに Administrator 権限がない場合でも同様です。
- **ユーザー権限** で **Server Administrator** の権限が設定されていないが、iDRAC6 上で同じアカウントを保有している場合は、シングルサインオンを利用して自動的に iDRAC6 ウェブインタフェースにログインされます。iDRAC6 ウェブインタフェースに一度ログインすると、このユーザーには iDRAC6 アカウントに作成されている権限が与えられます。

  メモ: この場合、「同じアカウント」とは、ユーザーが CMC と iDRAC6 に同じログイン名とパスワードを持っていることを指します。同じログイン名を持つが、異なるパスワードを持つユーザーは、有効なユーザーとして認識されません。

- **ユーザー権限** で **サーバー管理者** の権限が設定されていないか、iDRAC6 に同じアカウントがない場合は、シングルサインオンを利用して自動的に iDRAC6 ウェブインタフェースにログインされません。このユーザーは、**iDRAC6 GUI の起動** をクリックした後、iDRAC6 ログイン画面にリダイレクトされます。

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

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

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

iDRAC6 ネットワークの設定

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

シリアルオーバー LAN を有効または無効にするには:

a. **シリアルオーバー LAN** をクリックします。

   シリアルオーバー LAN 画面が表示されます。

b. **シリアルオーバー LAN を有効にする** チェックボックスを選択します。**ボーレート** や **チャネル権限レベルの制限** 設定を変更することも可能です。

c. **適用** をクリックします。

IPMI オーバー LAN を有効または無効にするには:

a. **ネットワーク** をクリックします。

   ネットワーク 画面が表示されます。

b. **IPMI の設定** をクリックします。

c. **IPMI オーバー LAN を有効にする** チェックボックスを選択します。**チャネル権限レベルの制限** および **暗号化キー** の設定を変更することも可能です。

d. **適用** をクリックします。

DHCP を有効または無効にするには:

a. **ネットワーク** をクリックします。

   ネットワーク 画面が表示されます。

b. **IPv4 の設定** セクションの **DHCP を有効にする** チェックボックス と **IPv6 の設定** の **自動構成を有効にする** チェックボックスをオンにして DHCP を有効にします。DNS サーバーアドレスの取得に DHCP を使用するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオンにします。

c. **適用** をクリックします。

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

FlexAddress(フレックスアドレス)メザニンカードのファブリック接続の表示

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

メモ: 管理下サーバーの電源を投入できなくするようなエラーを防ぐために、各ポートとファブリック接続には正しいタイプのメザニンカードを取り付けることが必要です。

FlexAddress 機能の設定は、CMC ウェブインタフェースを使って行います。FlexAddress 機能とその設定の詳細については、『Dell Chassis Management Controller ユーザーガイド』と『Chassis Management Controller(CMC)セキュアデジタル(SD)カード仕様』を参照してください。

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

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

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

iDRAC6 用 FlexAddress MAC

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

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

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

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

メモ: FlexAddress 機能は CMC からのみ有効または無効にできます。iDRAC6 の GUI は状態のみを報告します。CMC FlexAddress ページで FlexAddress の設定を変更すると、仮想コンソールまたは仮想メディアの既存のセッションがすべて終了します。

RACADM から FlexAddress を有効にする方法

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

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

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

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

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

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

   `racadm setflexaddr -f idrac 1`

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

リモートシスログ

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

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

リモートシスログはリモートのウェブインタフェースから有効にできます。

1. サポートされているウェブブラウザのウィンドウを開きます。

2. iDRAC6 ウェブインタフェースにログインします。

3. システムツリーで、**システム** →**設定** タブ →**リモートシスログの設定** の順に選択します。**リモートシスログの設定** 画面が表示されます。

表 2-2 はリモートシスログの設定一覧です。

表 2-2 リモートシスログの設定

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

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

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

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogEnable [1/0]、default is 0

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer1 <サーバー名1>、default is blank

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer2 <サーバー名2>、default is blank

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogServer3 <サーバー名3>、default is blank

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPort <ポート番号>、default is 514
```

最初の起動デバイス

この機能を使用すると、システムの最初の起動デバイスを選択して、ブートワンス を有効にできます。システムは次回以降の再起動時に選択したデバイスから起動し、iDRAC6 GUI または BIOS の起動順序から再度変更されるまで、BIOS の起動順序にある最初の起動デバイスのままになります。ブートワンスが有効の場合、システムは選択したデバイスから 1 回だけ起動し、そのデバイスは起動順序の最初の起動デバイスのままにはなるわけではありません。

最初の起動デバイスは、リモートウェブインタフェースから選択できます。

1. サポートされているウェブブラウザのウィンドウを開きます。

2. iDRAC6 ウェブインタフェースにログインします。

3. システムツリーで、**システム** →**セットアップ** タブ→**最初の起動デバイス** の順に選択します。**最初の起動デバイス** 画面が表示されます。

表 2-3 は、**最初の起動デバイス** の設定をリストしています。

表 2-3 最初の起動デバイス

属性	説明
最初の起動デバイス	ドロップダウンメニューから最初の起動デバイスを選択します。システムは次回以降の再起動時に選択したデバイスから起動します。
ブートワンス	選択 = 有効、選択解除 = 無効。このオプションをオンにすると、システムは次回起動時に、選択したデバイスから起動します。それ以降は、システムは BIOS の起動順序にある最初の起動デバイスから起動します。

リモートファイル共有

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

メモ: この機能は IPv4 アドレスでのみ使用できます。IPv6 アドレスは現在サポートされていません。

メモ: Linux ディストリビューションの場合、ランレベル init 3 で運用していると、この機能で手動のマウントコマンドが必要になる可能性があります。
コマンドの構文は次のとおりです。
mount /dev/OS_specific_device /<ユーザー定義のマウントポイント>
<ユーザー定義のマウントポイント> は、他のマウントコマンドの場合と同様にマウントに使用するディレクトリです。
RHEL の場合、CD デバイス(**.iso** 仮想デバイス)は **/dev/scd0** で、フロッピーデバイス(**.img** 仮想デバイス)は **/dev/sdc** です。
SLES の場合、CD デバイスは **/dev/sr0** で、フロッピーデバイスは **/dev/sdc** です。
正しいデバイス(SLES か RHEL か)が使用されるように、Linux OS で仮想デバイスを接続し次第、次のコマンドを実行する必要があります。
tail /var/log/messages | grep SCSI
これで、デバイスを識別するテキストが表示されます(たとえば、SCSI デバイス sdc)。
この手順は、Linux ディストリビューションをランレベル init 3 で使用している場合にも実行します。デフォルトでは、仮想メディアは init 3 では自動マウントされません。

CIFS 共有イメージのパスは次の形式で指定します。

```
//<IP アドレスまたはドメイン名>/<共有名>/<イメージのパス>
```

NFS 共有イメージのパスは次の形式で指定します。

```
<IP アドレス>:/<イメージファイルのパス>
```

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

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

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

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

メモ: iDRAC6 の vFlash 機能と RFS は関係がありません

iDRAC ウェブインタフェースを介してリモートファイル共有を有効にするには、次の手順に従います。

1. サポートされているウェブブラウザのウィンドウを開きます。

2. iDRAC6 ウェブインタフェースにログインします。

3. **システム** → **リモートファイル共有** タブの順に選択します。

   リモートファイル共有 画面が表示されます。

表 2-4 はリモートファイル共有の設定一覧です。

表 2-4 リモートファイルサーバーの設定

属性	説明
ユーザー名	NFS/CIFS ファイルシステムに接続するユーザー名。

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

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

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

リモートファイル共有の場合、リモート RACADM コマンドは

`racadm remoteimage` です。

`racadm remoteimage <オプション>`

以下のオプションがあります。

`-c`:イメージを接続

`-d`:イメージを切断

`-u <ユーザー名>`:ネットワーク共有にアクセスするユーザー名

`-p <パスワード>`:ネットワーク共有にアクセスするパスワード

`-l <イメージの場所>`:ネットワーク共有上のイメージの場所(場所を二重引用符で囲む)

`-s`:現在の状態を表示

注意: ユーザー名、パスワード、イメージ場所には、英数字と特殊文字を含む、'(一重引用符)、"(二重引用符)、,(コンマ)、<(より小記号)、>(より大記号)以外のすべての文字を使用できます。リモートファイル共有を使用するとき、上記の文字はユーザー名、パスワード、イメージ場所には使用できません。

内蔵デュアル SD モジュール

内蔵デュアル SD モジュール(IDSDM)は、該当するプラットフォームでのみ使用可能です。IDSDM は、最初の SD カードの内容をミラーする別の SD カードを使用して、hypervisor SD カードで冗長性を提供します。iDRAC6 の vFlash SD カードは、2 番目の SD カードを使用して IDSDM に設定できます。その場合は、システム BIOS 設定の **オンボードデバイス** 画面で、**冗長性** オプションを **ミラーモード** に設定します。IDSDM 機能を有効にすると、iDRAC6 vFlash SD カードの vFlash 機能は使用できなくなり、このカードは IDSDM で二次 SD カードとして設定されます。IDSDM の BIOS オプションの詳細については、デルサポートサイト **support.dell.com/manuals** にある『ハードウェアオーナーズ マニュアル』を参照してください。

メモ: BIOS 設定では、**オンボードデバイス** 画面の **内蔵 USB ポート** オプションを **オン** に設定する必要があります。これを **オフ** に設定した場合、システムは IDSDM を起動デバイスとして認識しません。

2 枚の SD カードのどちらかをマスターにできます。たとえば、IDSDM に新しい SD カード 2 枚を取り付けている場合、SD1 がアクティブ、つまりマスターカードになります。SD2 はバックアップカードになり、すべてのファイルシステム IDSDM の書き込みは両方のカードに行われますが、読み取りは SD1 からのみ行われます。SD1 が故障したり、取り外されたりした場合には、SD2 が自動的にアクティブ(マスター)カードになります。

表 2-5 IDSDM の状態

IDSDM - ミラーモード	SD カード	vFlash SD カード
有効	アクティブ(SD2 カード)	vFlash 非アクティブ、アクティブ SD2 カードとして切り替わる
無効	アクティブ(SD2 カード)	vFlash のみアクティブ

iDRAC を使用して、IDSDM の状態、正常性、可用性を確認できます。

SD カードの冗長性状態とエラーイベントは SEL に記録され、LCD で表示され、警告が有効になっている場合は、PET 警告が生成されます。

GUI による内蔵デュアル SD モジュールの状態

1. iDRAC 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、**リムーバブルフラッシュメディア** をクリックします。**リムーバブル vFlash メディア** ページが表示されます。このページには以下の 2 つのセクションが表示されます。

- **内蔵 SD モジュール** - IDSDM が冗長モードの場合にのみ表示されます。冗長性**状態** は **完全** と表示されます。このセクションが表示されない場合、カードは非冗長モードの状態です。有効な **冗長性状態** のインジケータは次のとおりです。
  - **完全** - SD カード 1 と 2 が正常に機能しています。
  - **喪失** - どちらか一方または両方の SD カードが正常に機能していません。

- **内蔵 SD モジュールの状態** - SD1 と SD2 の SD カードの状態を以下の情報で示します。
  - 状態
    -  - カードが正常であることを示します。
    -  - カードがオフラインまたは書き込み禁止であることを示します。
    -  - 警告が出されたことを示します。
  - 場所 - SD カードの場所。
  - オンライン状態 - SD1 と SD2 カードが以下のいずれかの状態になっている可能性があります表 2-6。

表 2-6 SD1 と SD2 カードの状態

状態	説明
起動	コントローラの電源が入って起動中です。
アクティブ	カードがすべての SD 書き込みを受け取り、SD 読み取りに使用されています。
スタンバイ	このカードは二次カードです。SD 書き込みすべてのコピーを受け取っています。
エラー	SD カードの読み取りまたは書き込み中にエラーが報告されました。
不在	SD カードが検出されません。
オフライン	起動時に、カードの CID 署名が NV ストレージの値と異なるか、カードが、進行中のコピー操作のコピー先となっています。
書き込み禁止	SD カードの物理的なラッチによって、カードが書き込み禁止されています。IDSDM で書き込み禁止のカードは使用できません。

---

iDRAC6 ファームウェアのアップデート

iDRAC6 ファームウェアをアップデートすると、フラッシュメモリに新しいファームウェアがインストールされます。次のいずれかの方法でファームウェアをアップデートできます。

- iDRAC6 ウェブインタフェース
- RACADM CLI
- Dell アップデートパッケージ(Linux または Microsoft Windows 用)
- DOS iDRAC6 ファームウェアアップデートユーティリティ
- CMC ウェブインタフェース

ファームウェアまたはアップデートパッケージのダウンロード

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

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

管理下サーバーから iDRAC6 ファームウェアをアップデートするには、アップデートする iDRAC6 のサーバーで稼動するオペレーティングシステム専用の Dell アップデートパッケージ(DUP)をダウンロードします。

DOS iDRAC6 ファームウェアアップデートユーティリティを使用して iDRAC6 ファームウェアをアップデートするには、自己解凍式のアーカイブファイルにパッケージ化されたアップデートユーティリティとバイナリイメージの両方をダウンロードします。

ファームウェアアップデートの実行

メモ: iDRAC6 ファームウェアのアップデートが開始すると、既存の iDRAC6 セッションがすべて切断され、アップデートプロセスが完了するまで新しいセッションを開始できません。

メモ: シャーシのファンは iDRAC6 ファームウェアのアップデート中 100% で稼動します。アップデートが完了すると、正常なファン速度制御が再開されます。これは正常な動作で、センサー情報を CMC に送信できないときにサーバーをオーバーヒートから保護するように設計されています。

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

iDRAC6 ウェブインタフェースまたは CMC ウェブインタフェースを使用する場合は、ウェブインタフェースを開いている管理ステーションにアクセス可能なディスク上に、ファームウェアのバイナリイメージを保存してください。iDRAC6 ファームウェアのアップデート を参照してください。

メモ: iDRAC6 ウェブインタフェースを使用すると、iDRAC6 の設定を出荷時の設定にリセットすることもできます。

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

メモ: ファームウェアアップデート中に設定を保存していない場合は、SSL 証明書の SHA1 キーと MD5 キーが新規生成されます。このキーは、開いているウェブブラウザのキーとは異なるため、ファームウェアアップデートの完了後、iDRAC6 に接続しているブラウザウィンドウをすべて閉じる必要があります。ブラウザウィンドウを閉じないと、**無効な証明書** というエラーメッセージが表示されます。

メモ: iDRAC6 ファームウェアを以前のバージョンに戻す場合は、ファームウェアが互換性のある ActiveX プラグインバージョンをインストールできるように、Window ベースの管理ステーションにインストールされている既存の Internet Explorer ActiveX ブラウザ プラグインを削除する必要があります。

Linux DUP のデジタル署名の検証

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

デジタル署名を検証する Gnu Privacy Guard(GPG)をまだシステムにインストールしていない場合は、これをインストールしてください。

標準的な検証方法を使用するには、次の手順に従います。

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

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

   ```
   gpg --import <公開キーのファイル名>
   ```

   メモ: このプロセスを完了するには秘密キーが必要です。

3. 信頼できないキーという警告を回避するには、Dell GPG 公開キーの信頼レベルを変更します。

   a. 次のコマンドを入力します。

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

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

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

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

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

      ```
      Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from
      different sources, etc.) ( (パスポートや異なるソースのフィンガープリントの確認などによって) 他のユーザーのキーを検証するうえで、このユーザーをどこまで信頼するかを決定します。)


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

      Your decision (どこまで信頼しますか)?
      ```

   d. 「5」と入力し、<Enter> キーを押します。次のプロンプトが表示されます。

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

   e. 「y」と入力し、<Enter> キーを押します。

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

   公開キーのインポートと検証は 1 回だけ実行します。

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

   メモ: 各 Linux アップデートパッケージには、個別の署名ファイルがあり、同じウェブページにアップデートパッケージとして表示されます。検証には、アップデートパッケージおよびそれに関連する署名ファイルの両方が必要です。デフォルトでは、署名ファイルの名前は DUP と同じファイル名に拡張子 **.sign** が付いたものです。たとえば、iDRAC6 ファームウェアのイメージには **.sign** ファイル(**IDRAC_FRMW_LX_2.2.BIN.sign**)が関連付けられ、ファームウェアイメージ(**IDRAC_FRMW_LX_2.2.BIN**)と共に自動解凍アーカイブに含まれています。ファイルをダウンロードするには、**ダウンロード** リンクを右クリックして、**名前を付けて保存** オプションを使用します。

5. アップデートパッケージの検証:

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

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

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

   - IDRAC_FRMW_LX_2.2.BIN.sign

- IDRAC_FRMW_LX_2.2.BIN

2. 次のコマンドラインを実行して公開キーをインポートします。

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

   次の出力メッセージが表示されます。

   ```
   gpg: key 23B66A9D: "Dell Computer Corporation (キー 23B66A9D: "Dell Computer Corporation) (Linux Systems Group (Linux システムグループ))
   <linux-security@dell.com>" not changed (変更なし)
   gpg: Total number processed (合計処理数): 1
   gpg: unchanged (変更なし): 1
   ```

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

   a. 次のコマンドを入力します。

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

   b. コマンドプロンプトで、次のコマンドを入力します。

      ```
      fpr
      trust
      ```

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

   d. 「y」と入力し、<Enter> キーを押します。

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

   これで、Dell 公開キーの検証が完了します。

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

   ```
   gpg --verify IDRAC_FRMW_LX_2.2.BIN.sign IDRAC_FRMW_LX_2.2.BIN
   ```

   次の出力メッセージが表示されます。

   ```
   gpg: Signature made Fri Jul 11 15:03:47 2008 CDT using DSA key ID 23B66A9D (Fri Jul 11 15:03:47 2008 CDT に DSA キー ID 23B66A9D で行
   われた署名)
   gpg: Good signature from "Dell, Inc. (Product Group) <linux-security@dell.com>" ("Dell, Inc. (Product Group) <linux-
   security@dell.com>" からの正しい署名)
   ```

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

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

iDRAC6 ウェブインタフェースの使用

メモ: 完了前に iDRAC6 ファームウェアアップレートの進行を中断すると、iDRAC6 ファームウェアの破損を招く恐れがあります。そのような場合は、CMC ウェブインタフェースを使用して iDRAC6 を回復できます。

メモ: ファームウェアアップデートは、デフォルトで現在の iDRAC6 設定を保持します。アップデート中に、iDRAC6 設定を工場出荷時のデフォルト設定にリセットするオプションが提供されます。設定を出荷時のデフォルト設定にすると、アップデート完了時に外部ネットワークアクセスが無効になります。iDRAC6 設定ユーティリティを使用して、ネットワークを有効にして設定する必要があります。

1. iDRAC6 ウェブインタフェースを開始します。

2. システムツリーで、**システム**→ **リモートアクセス**→ **iDRAC6** の順に選択します。

3. **アップデート** タブをクリックします。

   ファームウェアアップデート 画面が表示されます。

   メモ: ファームウェアをアップデートするには、iDRAC6 がアップデートモードになっている必要があります。このモードでは、アップデートプロセスをキャンセルした場合でも iDRAC6 は自動的にリセットされます。

4. **アップロード** セクションで、**参照** をクリックし、ダウンロードしたファームウェアイメージを**探します**。テキストフィールドにパスを入力することも可能です。たとえば、次のとおりです。

   ```
   C:\Updates\V2.2\<イメージ名>
   ```

   デフォルトのファームウェアイメージ名は **firmimg.imc** です。

5. **アップロード** をクリックします。

ファイルが iDRAC6 にアップロードされます。この処理には数分かかる場合があります。

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

アップロードが完了すると、**アップロード(手順 2 / 3)** 画面が表示されます。

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

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

6. デフォルトでは、アップグレード後も iDRAC6 で現在の設定を保存するための **設定の保存** チェックボックスが選択されています。設定を保存しない場合は、**設定の保存** チェックボックスを選択解除します。
7. **アップデートの開始** をクリックして、アップグレードプロセスを開始します。アップグレードプロセスには割り込まないでください。
8. **アップロード(手順 3 / 3)** ウィンドウで、アップデートの状況が表示されます。ファームウェアアップグレード操作の進行状況は、**進行状況** 列にパーセントで表示されます。
9. ファームウェアのアップデートが完了すると、**アップロード(手順 3 / 3)** ウィンドウが結果を反映して更新され、iDRAC6 が自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC6 に再接続する必要があります。

RACADM を使用した iDRAC6 ファームウェアのアップデート

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

1. デルサポートサイト **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。

   たとえば、次のとおりです。

   ```
   C:\downloads\firmimg.imc
   ```

2. 次の RACADM コマンドを実行します。

   たとえば、次のとおりです。

   ```
   racadm -r <iDRAC6 IP アドレス> -u <ユーザー名> -p <パスワード> fwupdate -g -u -a <パス>
   ```

   ここでパスは、**firmimg.imc** が保存されている TFTP サーバー上の場所です。

DOS アップデートユーティリティの使用

DOS アップデートユーティリティを使用して iDRAC6 ファームウェアをアップデートするには、管理下サーバーを DOS で起動し、**idrac16d** コマンドを実行してください。コマンドの構文は次のとおりです。

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

オプションなしで実行すると、**idrac16d** コマンドは現在のディレクトリにあるファームウェアイメージファイル **firmimg.imc** を使って iDRAC6 ファームウェアをアップデートします。

オプションは次のとおりです。

- `-f` - アップデートを強制します。`-f` オプションは、ファームウェアを以前のイメージにダウングレードする場合に使用できます。
- `-i=<ファイル名>` - ファームウェアイメージの名前を指定します。この オプションは、ファームウェアのファイル名をデフォルト名 **firmimg.imc** から変更した場合に必要です。
- `-l=<ログファイル>` - アップデートアクティブティからの出力を記録します。このオプションはデバッグに使用します。

メモ: **idrac16d** コマンドに誤ったパラメータを入力、
または、`-h` オプションを追加した場合、追加オプションの `-nopresconfig` が利用可能になります。このオプションは、設定情報を保存せずにファームウェアをアップデートする場合に使用します。IP アドレス、ユーザー、およびパスワードなどの既存の iDRAC6 設定情報がすべてが削除されてしまうため、このオプションを**使用しない**ことをお勧めします。

USC 修復パッケージのアップデート

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

IT Assistant で使用するために iDRAC6 を設定する

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

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

---

iDRAC6 設定ユーティリティを使用して検出と監視を有効にする方法

iDRAC6 が IPMI を検出して iDRAC6 設定ユーティリティレベルで警告トラップを送信するように設定するには、管理下サーバー(ブレード)を再起動し、仮想コンソールと、リモートモニタとコンソールキーボードかシリアルオーバー LAN(SOL)接続を使用して起動状態を監視します。 Press <Ctrl-E> for Remote Access Setup (リモートアクセスセットアップに アクセスするには <Ctrl-E> キーを押しますが)、表示されたら、<Ctrl><E> キーを押します。

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

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

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

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

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

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

---

iDRAC6 ウェブインタフェースを使用して検出と監視を有効にする方法

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

1. サポートされているウェブブラウザのウィンドウを開きます。
2. システム管理者権限のあるユーザー名とパスワードで、iDRAC6 ウェブインターフェースにログインします。
3. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** の順に選択します。
4. **ネットワーク / セキュリティ** タブをクリックします。

   ネットワーク 画面が表示されます。
5. **IPMI の設定** をクリックします。
6. **IPMI オーバー LAN を有効にする** チェックボックスがオンになっていることを確認します。
7. **チャネル権限レベルの制限** ドロップダウンメニューから **システム管理者** を選択します。
8. サイトの **RMCP+ 暗号化キー**を入力します(使用されている場合)。
9. この画面で変更を加えた場合は、**適用** をクリックします。
10. システムツリーで **システム** を選択します。
11. **警告管理** タブをクリックして、**プラットフォームイベント** をクリックします。

    プラットフォームイベント 画面が表示され、電子メール警告を生成するために、iDRAC6 に設定できるイベントの一覧が現れます。

12. **警告の生成** 列でチェックボックスを選択して、1 つまたは複数のイベントの電子メール警告を有効にします。
13. この画面で変更を加えた場合は、**適用** をクリックします。
14. **トラップの設定** をクリックします。

    トラップの設定 画面が表示されます。
15. **IPv4 送信先リスト** セクションの最初の **送信先 IP アドレス** フィールドで、**有効** チェックボックスを選択し、管理ステーションの IP アドレスを入力します。
16. この画面で変更を加えた場合は、**適用** をクリックします。

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

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

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

   ユーザー 画面が表示され、(定義済みまたは未定義の)すべてのユーザーが一覧になります。
3. 未定義のユーザーの **ユーザー ID** をクリックします。

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

IT Assistant を使用して iDRAC6 状態およびイベントを表示する

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

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

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

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

目次ページに戻る

目次ページに戻る

管理ステーションの設定

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

管理ステーションは、Dell PowerEdge サーバーや、シャーシ内のその他のモジュールの監視と管理に使用されるコンピュータです。本項では、iDRAC6 Enterprise と連動する管理ステーションを設定するソフトウェアのインストールと設定タスクについて説明します。iDRAC6 の設定を開始する前に、本項の手順に従って必要なツールのインストールと設定を行ってください。

管理ステーションの設定手順

管理ステーションを設定するには、次の手順を実行してください。

1. 管理ステーションネットワークを設定します。
2. 対応ウェブブラウザをインストールして設定します。
3. Java ランタイム環境(JRE)をインストールします(Firefox を使用している場合に必要)。
4. 必要に応じて Telnet または SSH クライアントをインストールします。
5. 必要に応じて TFTP サーバーをインストールします。
6. Dell OpenManage IT Assistant をインストールします(省略可)。
7. Dell 管理コンソールをインストールします(省略可)。

管理ステーションのネットワーク要件

iDRAC6 にアクセスするには、管理ステーションが「GB1」のラベルが付いた CMC RJ45 接続ポートと同じネットワーク上に存在する必要があります。管理ステーションが LAN 経由で iDRAC6 に アクセスできても管理下サーバーにはアクセスできないようにするために、管理下サーバーのネットワークから CMC ネットワークを切り離すことも可能です。

iDRAC6 仮想コンソール機能(「シリアルオーバー LAN の設定と使用」を参照)を使用すると、サーバーのポートにネットワークアクセスがない場合でも、管理下サーバーのコンソールにアクセスできます。また、コンピュータの再起動や iDRAC6 の機能の使用など、複数の管理機能を管理下サーバー上で実行できます。ただし、管理下サーバーでホストされるネットワークやアプリケーションサービスにアクセスするには、管理下サーバーに追加の NIC が必要な場合があります。

対応ウェブブラウザの設定

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

ウェブブラウザを開く

iDRAC6 ウェブインタフェースは、幅 800 ピクセル × 高さ 600 ピクセル以上の画面解像度で、サポートされているウェブブラウザから表示できるように設計されています。インタフェースを表示してすべての機能にアクセスするには、必要に応じて解像度を 800 × 600 ピクセル以上に設定したり、ブラウザのサイズを変更してください。

メモ: 状況によっては(特に、ファームウェアのアップデート後の最初のセッション時に)、Internet Explorer で、メインブラウザウィンドウのページの一部しか描画されず、「**完了、エラーあり**」というメッセージが状態バーに表示されることがあります。このエラーは、接続上の問題がある場合にも発生します。これは Internet Explorer で確認されている不具合です。この場合は、ブラウザを閉じてから、再スタートしてください。

ウェブインタフェースに接続するウェブブラウザの設定

プロキシサーバー経由でインターネットに接続している管理ステーションから iDRAC6 ウェブインタフェースに接続する場合は、このサーバーからインターネットにアクセスするようにウェブブラウザを設定する必要があります。

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

1. ウェブブラウザのウィンドウを開きます。

2. **ツール** をクリックして、**インターネットオプション** をクリックします。

   インターネットオプション ウィンドウが表示されます。

3. **ツール** →**インターネットオプション** →**セキュリティ** →**ローカルネットワーク** の順に選択します。

4. **レベルのカスタマイズ** をクリックします。

5. ドロップダウンメニューから **中 低** を選択し、**リセット** をクリックします。**OK** をクリックして確定します。**レベルのカスタマイズ** ダイアログに戻るには、もう一度このボタンをクリックする必要があります。

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

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

   ダウンロードのセクション:

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

   その他 のセクション:

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

   スクリプト セクション:

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

- **ツール** →**インターネットオプション** →**詳 細** の順に選択します。

- 以下の項目にチェックが付いているか、いないかを確認します。

  ブラウズ のセクション:

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

  HTTP 1.1 設 定 セクション:

  - HTTP 1.1 を使用する:チェック付き

- プロキシ接続で HTTP 1.1 を使用する:チェック付き

Java(Sun) セクション:

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

マルチメディア セクション:

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

セキュリティ セクション:

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

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

9. **適用** をクリックし、**OK** をクリックします。
10. **接続** タブをクリックします。
11. **ローカルエリアネットワーク(LAN)設定** で **LAN 設定** をクリックします。
12. **プロキシサーバーを使用** チェックボックスがオンになっている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** チェックボックスをオンにします。
13. **OK** を 2 度クリックします。
14. ブラウザを閉じてから再起動し、すべての変更が適用されることを確認します。

信用できるドメインリストへの iDRAC6 の追加

ウェブブラウザから iDRAC6 ウェブインタフェースにアクセスし、iDRAC6 の IP アドレスが信頼済みドメインのリストにない場合は、IP アドレスをリストに加えるように要求される可能性があります。完了したら、**更新** をクリックするか、ウェブブラウザを再起動して、iDRAC6 ウェブインタフェースへの接続を確立します。

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

メモ: ブラウザに信頼されていない証明書を使用して iDRAC ウェブインタフェースに接続すると、ブラウザの最初の証明書エラー警告を受け入れた後、再表示される場合があります。これはセキュリティを確保するための想定内の動作です。

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

1. **ツール** → **インターネットオプション** → **セキュリティ** →**信頼済みサイト** →**サイト** の順に選択します。
2. **この Web サイトをゾーンに追加する** に、iDRAC6 IP アドレスを入力します。
3. **追加** をクリックします。
4. **OK** をクリックします。
5. **閉じる** をクリックします。
6. **OK** をクリックし、ブラウザを更新します。

Active-X プラグインを使用して IE8 から初めて仮想コンソールを起動したとき、Certificate Error: Navigation Blocked(証明書エラー:ナビゲーションはブロックされました)というメッセージが表示される場合があります。

1. **このサイトの閲覧を続行する** をクリックします。
2. **セキュリティ警告** ウィンドウで Active-X コントロールをインストールするには、**インストール** をクリックします。

仮想コンソールセッションが開始します。

他言語のウェブインタフェースの表示

iDRAC6 ウェブインタフェースは、次のオペレーティングシステム言語に対応しています。

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

かっこ内の ISO 識別子は、サポートされている特定の言語タイプを表します。その他の方言や言語でのインタフェースの使用はサポートされておらず、意図したように機能しない可能性があります。一部の対応言語ですべての機能を表示するには、ブラウザウィンドウを 1024 ピクセル幅にサイズ変更することが必要です。

iDRAC6 ウェブインタフェースは、上記の言語専用にローカライズされたキーボードと連携するように設計されています。仮想コンソールなど、iDRAC6 ウェブインタフェースの一部の機能を使用するには、特定の機能キーや文字にアクセスするための追加手順が必要になる場合があります。このような状況で、ローカライズされたキーボードを使う方法については、「ビデオビューアの使用」を参照してください。他のキーボードの使用はサポートされておらず、使用すると予期せぬ問題が発生する可能性があります。

メモ: さまざまな言語の設定方法と、iDRAC6 ウェブインタフェースのローカライズバージョンを表示する方法については、ブラウザのマニュアルを参照してください。

Linux のロケール設定

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

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

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

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

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

   現在のエントリ:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_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。

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

Firefox のホワイトリスト機能を無効にする

Firefox には、プラグインをホストする各サイトにプラグインをインストールするときにユーザーの許可を求める「ホワイトリスト」と呼ばれるセキュリティ機能があります。ホワイトリスト機能が有効になっている場合、ビューアのバージョンが同じでも iDRAC6 にアクセスするたびに仮想コンソールビューアのインストールが要求されます。

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

1. Firefox ウェブブラウザのウィンドウを開きます。
2. アドレスフィールドに `about:config` と入力し、<Enter> キーを押します。
3. **プリファレンス名** 列で、**xpinstall.whitelist.required** を見つけてダブルクリックします。

   プリファレンス名、**状態**、**タイプ**、**値** の値は太字に変わります。**状態** の値は **ユーザー設定** に変わり、**値** の値は **false** に変わります。
4. **プリフ→ス名** 列で、**xpinstall.enabled** を見つけます。

   値 が **true** になっていることを確認します。なっていない場合は、**xpinstall.enabled** をダブルクリックして **値** を **true** に設定します。

管理ステーションへの iDRAC6 ソフトウェアのインストール

システムには、『Dell Systems Management Tools and Documentation DVD』が同梱されています。この DVD には、以下のコンポーネントが入っています。

- 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。

管理ステーションへの RACADM のインストールおよびアンインストール

リモート RACADM 機能を使用するには、管理ステーションに RACADM をインストールします。Microsoft Windows オペレーティングシステムが稼動する管理ステーションへの DRAC ツールのインストール方法については、**support.dell.com / manuals** にある『Dell OpenManage Management Station Software インストールガイド』を参照してください。

Linux への RACADM のインストールおよびアンインストール

1. 管理ステーションコンポーネントをインストールするシステムに、ルート権限でログオンします。
2. 必要に応じて、次のコマンドまたは同等のコマンド を使って、『Dell Systems Management Tools and Documentation DVD』をマウントします。

   ```
   mount /media/cdrom
   ```
3. **/linux/rac** ディレクトリに移動して、次のコマンドを実行します。

   ```
   rpm -ivh *.rpm
   ```

RACADM コマンドに関するヘルプは、コマンドを入力した後「**racadm help**」と入力してください。

RACADM をアンインストールするには、コマンドプロンプトを開いて次のように入力します。

```
rpm -e <racadm パッケージ名>
```

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

たとえば、RPM パッケージ名が **srvadmin-racadm5** であれば、次のように入力します。

```
rpm -e srvadmin-racadm5
```

Java Runtime Environment（JRE）のインストール

メモ: Internet Explorer を使用している場合、仮想コンソールビューア用に ActiveX コントロールが提供されます。JRE をインストールし、iDRAC6 ウェブインタフェースで仮想コンソールビューアを起動前に設定すると、Firefox でも Java 仮想コンソールビューアを使用できます。詳細については、iDRAC6 ウェブインタフェースでの仮想コンソール と仮想メディアの設定を参照してください。

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

Firefox ブラウザを使用している場合、仮想コンソール機能を使用するには JRE(または Java Development Kit [JDK])をインストールする必要があります。仮想コンソールビューアは Java アプリケーションで、iDRAC6 ウェブインタフェースから管理ステーションにダウンロードした後 Java Web Start を使用して起動します。

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

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

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

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

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

メモ: ファイルには既に PATH 修正行が含まれている可能性があります。入力したパス情報によって競合が発生しないように注意してください。

Telnet または SSH クライアントのインストール

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

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

iDRAC6 のあるTelnet

Telnet は、Windows および Linux オペレーティングシステムに含まれており、コマンドシェルから実行できます。オペレーティングシステムに組み込まれている標準バージョンのほかに、便利な機能が追加された市販またはフリーウェアの Telnet クライアントをインストールすることもできます。

Telnet セッションのための Backspace キーの設定

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

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

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

   ```
   telnet
   ```

   Telnet セッションを実行している場合は、<Ctrl><]> を押します。
3. コマンドプロンプトで、次のコマンドを入力します。

   ```
   set bsasdel
   ```

   次のメッセージが表示されます。

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

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

1. シェルを開いて次のように入力します。

   ```
   stty erase ^h
   ```
2. コマンドプロンプトで、次のコマンドを入力します。

   ```
   telnet
   ```

iDRAC6 のあるSSH

セキュアシェル(SSH)は、Telnet セッションと同じ機能を持つコマンドライン接続ですが、セキュリティを強化するセッションネゴシエーションと暗号化の機能を備えています。iDRAC6 は、パスワード認証付きの SSH バージョン 2 をサポートしています。SSH は iDRAC6 上のデフォールトで有効になっています。

管理下サーバーの iDRAC6 に接続するには、管理ステーションで PuTTY や OpenSSH などのフリーウェアを使用できます。ログイン時にエラーが発生した場合は、**SSH** クライアントからエラーメッセージが発行されます。メッセージのテキストはクライアントによって異なり、iDRAC6 で制御することはできません。

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

iDRAC6 は最大 4 つの Telnet セッションと 4 つの SSH セッションを同時にサポートします。ただし、それら 8 つのセッション中 1 つだけが SM-CLP を使用できます。つまり、iDRAC6 がサポートしているのは一度に 1 つの SM-CLP セッションのみです。セッションのタイムアウトは `cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。これについては、デルのサポートウェブサイト **support.dell.com / manuals** に掲載している『iDRAC6 管理者リファレンスガイド』で説明しています。

iDRAC6 SSH の実装では、「表 3-1」に示すように複数の暗号化スキームがサポートされています。

メモ: SSHv1 はサポートされていません。

表 3-1 暗号化スキーマ

スキーマの種類	スキーム
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

TFTP サーバーのインストール

メモ: SSL 証明書の転送と新しい iDRAC6 ファームウェアのアップロードに iDRAC6 ウェブインタフェースのみを使用する場合、TFTP サーバーは不要です。

簡易ファイル転送プロトコル(TFTP)は、ファイル転送プロトコル(FTP)を簡単にしたものです。iDRAC6 とのファイル転送には、SM-CLP および RACADM コマンドラインインタフェースが併用されます。

iDRAC6 とのファイル複写が必要になるのは、iDRAC6 ファームウェアをアップデートしたとき、あるいは iDRAC6 の証明をインストールするときだけです。これらのタスクを実行するときに RACADM を使用する場合は、iDRAC6 が IP アドレスまたは DNS 名でアクセスできるコンピュータで TFTP サーバーを実行している必要があります。

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

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

Dell OpenManage IT Assistant のインストール

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

- Dell Systems Management Tools and Documentation DVD
- デルサポートサイトと Readme ファイル:デル製品に関する最新情報については、Readme ファイルまたはデルサポートサイト **support.dell.com / manuals** を参照してください。

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

Dell 管理コンソールのインストール

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

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

このソフトウェアのインストール手順については、**support.dell.com / manuals** で『Dell 管理コンソールユーザーズガイド』を参照してください。

目次ページに戻る

目次ページに戻る

管理下サーバーの設定

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

本項では、リモート管理機能を強化するように管理下サーバーを設定する作業について説明します。これらの作業には、Dell Open Manage Server Administrator ソフトウェアのインストールや管理下サーバーの前回クラッシュ画面のキャプチャ設定が含まれます。

管理下サーバーへのソフトウェアのインストール

デル管理ソフトウェアには、次の機能が含まれています。

- RACADM CLI - iDRAC6 の設定と管理ができます。設定タスクおよび管理タスクのスクリプトをサポートする強力なツールです。
- Server Administrator - iDRAC6 の前回クラッシュ画面機能を使用する場合に必要になります。
- Server Administrator Instrumentation Service - 業界標準のシステム管理エージェントによって収集される詳細なエラー情報およびパフォーマンス情報へのアクセスを提供し、シャットダウン、起動、セキュリティを含む監視下システムのリモート管理を可能にします。
- Server Administration Storage Management Service - 内蔵グラフィカル表示でストレージ管理情報を表示します。
- Server Administrator ログ - システムに対してまたはシステムによって発行されたコマンド、監視されたハードウェアイベント、POST イベント、システム警告のログを表示します。ログはホームページで表示したり、レポートとして印刷または保存したり、指定のサービス担当者に電子メールで送信したりできます。

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

管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定

iDRAC6 は、管理下システムのクラッシュ原因についてトラブルシューティングを支援するために前回クラッシュ画面をキャプチャし、ウェブインタフェースに表示できます。前回クラッシュ画面機能を有効にするには、次の手順を実行します。

1. 管理下サーバーソフトウェアをインストールします。詳細については、『Dell OpenManage Server Administrator インストールガイド』および『Dell OpenManage 管理ステーションソフトウェアインストールガイド』を参照してください。これらの文書は、デルサポートサイト **support.dell.com / manuals** から入手できます。

2. Windows を実行している場合は、**Windows 起動と回復** 画面の **自動的に再起動する** のチェックがオフになっていることを確認してください。Windows の自動再起動オプションを無効にする を参照してください。

3. iDRAC6 ウェブインタフェースの **前回クラッシュ画面**（デフォルトでは無効）を有効にします。

   iDRAC6 ウェブインタフェースで **前回クラッシュ画面** 機能を有効にするには、**システム** → **リモートアクセス** → **iDRAC6**→ **ネットワーク / セキュリティ** タブ → **サービス** の順でクリックし、**自動システムリカバリエージェント** 設定の見出しの下にある **有効** チェックボックスをオンにします。

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

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

4. Server Administrator ウェブインタフェースで、**自動リカバリ** タイマーを有効にし、**自動リカバリ** 処置を **リセット**、**電源オフ**、または **電源の入れ直し** に設定します。

   自動リカバリ タイマーの設定の詳細については、『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。前回クラッシュ画面が確実にキャプチャされるようにするには、**自動リカバリ** タイマーを 60 秒以上に設定する必要があります。デフォルト値は 480 秒です。

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

Windows の自動再起動オプションを無効にする

iDRAC6 が前回クラッシュ画面をキャプチャできるようにするには、Windows Server または Windows Vista が稼動する管理下サーバー上の **自動再起動** オプションを無効にします。

1. Windows **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。

2. **詳細** タブをクリックします。

3. **起動と回復** で **設定** をクリックします。

4. **自動再起動** チェックボックスを選択解除します。

5. **OK** を 2 回クリックします。

目次ページに戻る

目次ページに戻る

ウェブインタフェースを使用した iDRAC6 Enterprise の設定

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

iDRAC6 は、iDRAC6 プロパティとユーザーの設定、リモート管理タスクの実行、問題が起きた時のリモート(管理下)システムのトラブルシューティングが可能なウェブインタフェースを提供します。通常は、ウェブインタフェースを使用して日常のシステム管理タスクを実行します。本章では、iDRAC6 のウェブインタフェースから一般的なシステム管理タスクを実行する方法について説明し、関連情報へのリンクも掲載しています。

ウェブインタフェースを使用する設定タスクのほとんどは、ローカルおよびリモートの RACADM コマンドまたは SM-CLP コマンドでも実行できます。

ローカル RACADM コマンドは、管理下サーバーから実行します。リモート RACADM は、管理ステーションで実行するクライアントユーティリティで、帯域外のインタフェースを利用して管理下サーバーと通信します。ネットワーク経由でコマンドを実行するには、このユーティリティを **-r** オプションを指定して使用します。RACADM の詳細については、「RACADM コマンドラインインタフェースの使用」を参照してください。

SM-CLP コマンドは、Telnet または SSH 接続でリモートからアクセスできるシェルで実行されます。SM-CLP の詳細については、「iDRAC6 Enterprise の使用 SM-CLP コマンドラインインタフェース」を参照してください。

ウェブインタフェースへのアクセス

iDRAC6 ウェブインタフェースにアクセスするには、次の手順を実行してください。

1. サポートされているウェブブラウザのウィンドウを開きます。
2. **アドレス** フィールドに、`https://<iDRAC6 の IP アドレス>` を入力し、<Enter> キーを押します。

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

   `https://<iDRAC6 の IP アドレス>:<ポート番号>`

   iDRAC6 IP アドレス は iDRAC6 の IP アドレスで、ポート番号 は HTTPS のポート番号です。

   iDRAC6 **ログイン** ウィンドウが表示されます。

ログイン

iDRAC6 ユーザー、Microsoft Active Directory ユーザー、または LDAP ユーザーとしてログインできます。デフォルトのユーザー名とパスワードはそれぞれ **root** と **calvin** です。

iDRAC6 にログインするには、システム管理者から **iDRAC へのログイン** 権限が与えられている必要があります。

ログインするには、次の手順に従ってください。

1. **ユーザー名** フィールドで、以下のいずれかを入力します。
   - iDRAC6 ユーザー名。

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

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

     Active Directory の名前には、<ドメイン>\<ユーザー名>、<ドメイン>/<ユーザー名> または <ユーザー>@<ドメイン> の形式を利用できます。大文字と小文字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。あるいは、**ドメイン** フィールドにドメイン名を入力することも可能です。

   - LDAP ユーザー名(ドメイン名の入力なし)。
2. **パスワード** フィールドに、iDRAC6 ユーザーパスワード、Active Directory ユーザーパスワード、または LDAP パスワードのいずれかを入力します。パスワードでは大文字と小文字が区別されます。
3. **OK** をクリックするか、<Enter> を押します。

ログアウト

1. セッションを閉じるには、メインウィンドウの右上隅にある **ログアウト** をクリックします。

2. ブラウザウィンドウを閉じます。

メモ: **ログアウト** ボタンは、ログインするまで表示されません。

メモ: 正常なログアウトをしないでブラウザを閉じると、タイムアウトになるまでセッションがアクティブなままになる可能性があります。**ログアウト** ボタンをクリックしてセッションを終了することをお勧めします。

メモ: Internet Explorer 内で、ウィンドウ右上隅の閉じるボタン(x)を使用して iDRAC6 ウェブインタフェースを閉じると、アプリケーションエラーが発生する可能性があります。この不具合を修正するには、Microsoft サポートウェブサイト **support.microsoft.com** から、最新の Internet Explorer 用累積セキュリティアップデートをダウンロードしてください。

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

複数のブラウザタブとウィンドウの使用

新しいタブやウィンドウを開くときのウェブブラウザの動作は、バージョンによって異なります。Internet Explorer(IE)7 および IE 8 では、ウィンドウだけでなくタブを開くオプションもあります。各タブは、最後に開いたタブの特性を継承します。新しいタブを開くには Ctrl+T を押し、アクティブなセッションから新しいブラウザウィンドウを開くには Ctrl+N を押します。すでに認証済みの資格情報でログインします。いずれか 1 つのタブを閉じると、すべての iDRAC6 ウェブインタフェースタブが終了します。たとえば、あるユーザーがパワーユーザー権限で 1 つのタブにログインした後、システム管理者権限で別のタブにログインすると、開いている両方のタブがシステム管理者権限を持つことになります。

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

表 5-1 対応ブラウザでのユーザー権限動作

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

---

iDRAC6 NIC の設定

ここでは、iDRAC6 がすでに設定され、ネットワーク上でアクセス可能である状態を想定しています。iDRAC6 のネットワーク初期設定については、「iDRAC6 ネットワークの設定」を参照してください。

ネットワーク、IPMI、VLAN の設定

メモ: 次の手順を実行するには、**iDRAC6 の設定** 権限が必要です。

メモ: ほとんどの DHCP サーバーは、予約テーブルにクライアントの ID トークンを保存するためのサーバーを必要とします。このトークンは、クライアント(たとえば iDRAC6)が DHCP ネゴシエーション中に提供する必要があります。iDRAC6 は、1 バイトのインタフェース番号(0)に続く 6 バイトの MAC アドレスを使用して、クライアント ID オプションを提供します。

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

   ネットワーク 画面が表示されます。
3. 必要に応じて、ネットワーク、IPMI、および VLAN を設定します。**ネットワーク、IPMI**、および **VLAN の設定** オプションの説明は、「表 5-2」、「表 5-3」、および「表 5-4」を参照してください。
4. **適用** をクリックします。
5. 適切なボタンをクリックして続行します。

表 5-2 ネットワークの設定

設定	説明
ネットワークインタフェースカードの設定	
MAC アドレス	ネットワークの各ノードを一意に識別するメディアアクセスコントロール(MAC)アドレスを表示します。MAC アドレスは変更できません。
NIC を有効にする	このチェックボックスをオンにすると、NIC が有効になり、このグループの残りのコントロールがアクティブになることを示します。NIC が無効になっていると、ネットワーク経由の iDRAC6 とのすべての通信がブロックされます。 デフォルトでは **チェックボックスがオフ** になっています。
共通設定	
iDRAC6 を DNS に登録す	DNS サーバーに iDRAC6 の名前を登録します。

る	デフォルトでは **チェックボックスがオフ** になっています。
DNS iDRAC6 Name（名前）	iDRAC6 の名前を表示します。デフォルト名は idrac-service_tag で、service_tag はデルサーバーのサービスタグ番号です。例：iDRAC-HM8912S
DNS ドメイン名に DHCP を使用	**チェックボックスがオン**：DHCP からの DNS 取得を有効にします。 **チェックボックスがオフ**：DHCP からの DNS 取得を無効にします。
DNS ドメイン名	デフォルトの **DNS ドメイン名** は空白です。**DNS ドメイン名に DHCP を使用** チェックボックスがオンの場合、この オプションはグレー表示になっており、フィールドの内容を変更できません。
IPv4 の設定	
有効	IPv4 プロトコルのサポートを有効（**チェックボックスがオン**）または無効（**チェックボックスがオフ**）にします。この設定をアクティブにするには、**NIC を有効にする** オプションをオンにする必要があります。
DHCP 有効	**チェックボックスがオン** の場合、Server Administrator は iDRAC6 NIC の IP アドレスを DHCP サーバーから取得します。また、**IP アドレス**、**サブネットマスク**、および **ゲートウェイ** のフィールドを無効にします。
IP アドレス	iDRAC6 NIC の静的 IP アドレスを入力または編集できます。この設定を変更するには、**DHCP 有効** オプションを選択解除します。
Subnet Mask（サブネットマスク）	iDRAC6 NIC のサブネットマスクを入力または編集できます。この設定を変更するには、**DHCP 有効** オプションを選択解除します。
ゲートウェイ	iDRAC6 NIC の静的 IPv4 アドレスを入力または編集できます。この設定を変更するには、**DHCP 有効** オプションを選択解除します。
DHCP を使用して DNS サーバーアドレスを取得する	**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオンにして DNS サーバーのアドレスを取得するには、**DHCP 有効** オプションを選択します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、**優先 DNS サーバー** フィールドと **代替 DNS サーバー** フィールドに IP アドレスを入力します。
優先 DNS サーバー	優先 DNS サーバーの静的 IP アドレスを入力または編集できます。この設定を変更するには、最初に **DHCP を使用して DNS サーバーアドレスを取得する** オプションを選択解除します。
代替 DNS サーバー	二次 DNS サーバー IP アドレスは、**DHCP を使用して DNS サーバーアドレスを取得する** が **選択されていない** 場合に使用します。代替 DNS サーバーが存在しない場合は、IP アドレスとして「0.0.0.0」を入力します。
IPv6 の設定	
有効	**チェックボックスがオン** の場合は、IPv6 が有効になります。**チェックボックスがオフ** の場合は、IPv6 が無効になります。デフォルトでは **チェックボックスがオフ** になっています。
自動構成有効	このチェックボックスをオンにすると、iDRAC6 は動的ホスト設定プロトコル（DHCPv6）サーバーから iDRAC6 NIC の IPv6 アドレスを取得できます。**自動設定有効** を有効にすると、**IPv6 アドレス**、**プレフィックス長**、および **ゲートウェイ** の静的な値を無効にして消去します。
IPv6 アドレス	iDRAC6 NIC の IPv6 アドレスを設定します。この設定を変更するには、まず関連付けられたチェックボックスをオフにして **自動構成有効** を無効にする必要があります。 **メモ：** ネットワーク設定で IPv6 DHCP が設定されている場合、表示されるのは 2 つの IPv6 アドレス（リンクローカルアドレスとグローバルアドレス）だけで、ネットワークルータがルータアドバタイズメントメッセージを送信するように設定されている場合は 16 の IPv6 アドレスすべてが表示されます。 **メモ：** 8 を超えるグループから成る IPv6 アドレスを入力した場合は、設定を保存できません。
プレフィックス長	IPv6 アドレスのプレフィックス長を設定します。この値は 1 ～ 128 です。この設定を変更するには、まず **自動構成有効** チェックボックスをオフにして、自動構成を無効にする必要があります。
ゲートウェイ	iDRAC6 NIC の静的な IPv6 ゲートウェイを設定します。この設定を変更するには、まず **自動構成有効** チェックボックスをオフにして、自動構成を無効にする必要があります。
DHCPv6 を使用して DNS サーバーアドレスを取得する	**DHCPv6 を使用して DNS サーバーアドレスを取得する** チェックボックスをオンにして DHCP を有効にし、IPv6 DNS サーバーのアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、**優先 DNS サーバー** フィールドと **代替 DNS サーバー** フィールドに IP アドレスを入力します。デフォルトでは **チェックボックスがオフ** になっています。 **メモ：** **DHCPv6 を使用して DNS サーバーアドレスを取得する** チェックボックスがオンの場合は、**優先 DNS サーバー** フィールドと **代替 DNS サーバー** フィールドに IP アドレスを入力できません。
優先 DNS サーバー	優先 DNS サーバーの静的 IPv6 アドレスを設定します。この設定を変更するには、**DHCPv6 を使用して DNS サーバーアドレスを取得する** を選択解除します。
代替 DNS サーバー	代替 DNS サーバーの静的 IPv6 アドレスを設定します。この設定を変更するには、**DHCPv6 を使用して DNS サーバーアドレスを取得する** を選択解除します。

表 5-3 IPMI 設定

設定	**説明**
IPMI オーバー LAN を有効にする	選択されていると、IPMI LAN チャネルが有効であることを示します。デフォルトでは **チェックボックスがオフ** になっています。
チャネル権限レベルの制限	LAN チャネルで受け入れられるユーザーの最大権限レベルを設定します。**システム管理者**、**オペレータ**、**ユーザー** のオプションから 1 つを選択します。デフォルトは **システム管理者** です。
暗号化キー	暗号化キーを設定します。暗号化キーは、40 文字までの偶数の 16 進数で指定します。デフォルトの IPMI 暗号化キーはすべてゼロです。

表 5-4 VLAN の設定

ボタン	**説明**
VLAN ID を有効にする	**はい**：有効になります。**いいえ**：無効になります。有効の場合は、一致する仮想 LAN（VLAN）ID トラフィックのみが受け入れられます。

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

表 5-5 ネットワーク設定ボタン

ボタン	説明
詳細設定	**ネットワークセキュリティ** 画面を表示します。ここで IP 範囲と IP ブロックの属性を入力できます。
印刷	画面に表示される **ネットワーク** 設定の値を印刷します。
更新	**ネットワーク** 画面を再ロードします。
適用	ネットワーク設定画面に追加された新規設定を保存します。 **メモ:** NIC の IP アドレス設定を変更すると、すべてのユーザーセッションが終了します。ユーザーは、更新後の IP アドレス設定を使用して iDRAC6 ウェブインタフェースに再接続する必要があります。その他の変更でも、NIC をリセットする必要があり、このため接続が一時的に途絶える場合があります。

IP フィルタと IP ブロックの設定

メモ: 次の手順を実行するには、**iDRAC6 の設定** 権限が必要です。

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

   ネットワーク 画面が表示されます。
3. **詳細設定** をクリックします。

   ネットワークセキュリティ 画面が表示されます。
4. 必要に応じて、IP フィルタおよびブロック設定を行います。**IP フィルタおよびブロック** 設定の説明については、「表 5-6」を参照してください。
5. **適用** をクリックします。
6. 適切な**ボタン**をクリックして続行します。表 5-7 を参照してください。

表 5-6 IP フィルタとブロックの設定

設定	説明
IP 範囲を有効にする	IP 範囲のチェック機能を有効にします。これにより、iDRAC6 にアクセスできる IP アドレスの範囲を定義できます。デフォルトは **無効** です。
IP 範囲のアドレス	受け入れる IP サブネットアドレスを指定します。デフォルトは **192.168.1.0** です。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。デフォルトは **255.255.255.0** です。
IP ブロックを有効にする	事前に選択した時間枠で、1 つの IP アドレスからログインに失敗できる回数を制限する IP アドレスブロック機能を有効にします。デフォルトは **無効** です。
IP ブロックするログイン失敗回数	1 つの IP アドレスからのログインの失敗を許可する回数を設定し、それを超えたら、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 ブロックするログイン失敗回数の時間枠	ここで指定した時間枠（秒）内に IP ブロックするログイン失敗回数が制限値を超えると、IP ブロックペナルティ時間がトリガされます。デフォルトは **3600** です。
IP ブロック持続時間	ログイン失敗回数が制限値を超えた IP アドレスからのログインを拒否する時間を秒で指定します。デフォルトは **3600** です。

表 5-7 ネットワークセキュリティのボタン

ボタン	説明
印刷	画面に表示されている **ネットワークセキュリティ** 値を印刷します。
更新	**ネットワークセキュリティ** 画面を再ロードします。
適用	**ネットワークセキュリティ** 画面に追加された新規設定を保存します。
ネットワーク設定ページに戻る	**ネットワーク** 画面に戻ります。

プラットフォームイベントの設定

プラットフォームイベントの設定では、特定のイベントメッセージが返されたときに iDRAC6 が選択した処置を実行するように設定できます。処置には、処置の必要なし、システムの再起動、システムの電源を入れ直す、システムの電源を切る、警告の生成（プラットフォームイベントトラップ [PET] 、電子メール）があります。

表 5-8 に、フィルタ可能なプラットフォームイベントを示します。

表 5-8 フィルタ可能なプラットフォームイベント

インデックス	プラットフォームイベント
1	バッテリプローブ警告
2	バッテリプローブエラー
3	離散的電圧プローブエラー
4	温度プローブ警告
5	温度プローブエラー
6	プロセッサエラー
7	プロセッサ不在
8	ハードウェアログエラー
9	自動システム回復
10	SD カードの不具合
11	冗長性喪失

プラットフォームイベント（たとえば、バッテリープローブ警告）が発生すると、システムイベントが生成され、システムイベントログ（SEL）に記録されます。このイベントが、有効になっているプラットフォームイベントフィルタ（PEF）と一致し、警告（PET または電子メール）を生成するようにフィルタを設定している場合は、設定されている 1 つまたは複数の送信先に 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が別の処置（システムの再起動など）も実行するように設定されていると、その処置も実行されます。

プラットフォームイベントフィルタ（PEF）の設定

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

1. iDRAC6 ウェブインタフェースにログインします。
2. **システム** をクリックし **警告管理** タブをクリックします。

   プラットフォームイベント 画面が表示されます。
3. **プラットフォームイベントのフィルタ警告** チェックボックスをオンにします。プラットフォームの警告を有効な宛先に送信する場合は、このオプションを選択する必要があります。
4. 各イベントが発生したときに有効にする処置を以下から 1 つ選択します。
   - システムの再起動 - イベントが発生すると、システムを再起動します（ウォームブート）。
   - システムの電源を入れ直す - イベントが発生すると、システムを停止して電源を切ってから、再起動します（コールドブート）。
   - システムの電源オフ - イベントが発生すると、システムを停止して電源を切ります。
   - 処置の必要なし - イベントが発生すると、処置が実行されません。これはイベントのデフォルト設定です。
5. 警告を生成するイベントごとに、その横にある **警告の生成** オプションを選択します。

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

6. **適用** をクリックします。

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. iDRAC6 ウェブインタフェースにログインします。

2. 「プラットフォームイベントフィルタ(PEF) の設定」の手順に必ず従ってください。

3. **システム** をクリックし **警告管理** タブをクリックします。

   プラットフォームイベント 画面が表示されます。

4. **トラップの設定** をクリックします。

   トラップの設定 画面が表示されます。

5. PET の送信先 IP アドレスを設定します。

   a. アクティブにする **送信先番号** の **有効** チェックボックスをオンにします。

   b. 該当する IPv4 または IPv6 の **送信先 IP アドレス** ボックスに IP アドレスを入力します。

   c. **適用** をクリックします。

   メモ: トラップを正しく送信するには、**コミュニティ文字列** の値を設定します。**コミュニティ文字列** の値は、iDRAC6 から送信される簡易ネットワーク管理プロトコル(SNMP)の警告トラップで使用するコミュニティ文字列を示します。SNMP 警告トラップは、プラットフォームイベントの発生時に iDRAC6 によって送信されます。**コミュニティ文字列** のデフォルト設定は、**Public** です。

   d. 設定した警告をテストするには、**送信** をクリックします。

   e. 宛先 IP アドレスを追加するには、「手順 a」から「手順 d」の手順を繰り返します。最大 4 個の IPv4 アドレスと最大 4個の IPv6 送信先アドレスを指定できます。

電子メール警告の設定

1. iDRAC6 ウェブインタフェースにログインします。

2. 「プラットフォームイベントフィルタ(PEF) の設定」の手順に必ず従ってください。

3. **システム** をクリックし **警告管理** タブをクリックします。

   プラットフォームイベント 画面が表示されます。

4. **電子メール警告の設定** をクリックします。

   電子メール警告の設定 画面が表示されます。

5. 電子メール警告の宛先を指定します。

   a. 最初の未定義の電子メール警告の **有効** チェックボックスを選択します。

   b. **送信先の電子メールアドレス** フィールドに有効な電子メールアドレスを入力します。

   c. **適用** をクリックします。

   メモ: テストメールを正しく送信するには、**電子メール警告設定** 画面で **SMTP(電子メール)サーバーアドレス設定** セクションの SMTP(電子メール)サーバーを設定する必要があります。提供されるフィールドに、ドット区切り形式(例:192.168.1.1)または DNS 名で SMTP サーバーを指定します。プラットフォームイベントが発生すると、設定した IP アドレスにある SMTP サーバー は iDRAC6 と通信して電子メール警告を送信します。

   d. **電子メールの差出人名を変更する** フィールドに、電子メール警告の差出人を入力します。デフォルトの差出人を使用する場合は、空白のままにします。デフォルトは、blade_slot@iDRAC6 IP アドレスです。

      - **電子メールの差出人名を変更する** フィールドが空白で、iDRAC6 ホスト名が設定されており、かつ DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<iDRAC6 ホスト名>@<DNS ドメイン名> となります。
      - このフィールドと iDRAC6 ホスト名が空白で、DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<iDRAC6 Slotx>@<DNS ドメイン名> となります。
      - このフィールド、iDRAC6 ホスト名、および DNS ドメイン名が空白の場合、差出人の電子メールアドレスは、<iDRAC6 Slotx>@<iDRAC6 IP アドレス> となります。
      - このフィールドに @ マークがない文字列が入力され、DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<@ が含まれない文字列>@<DNS ドメイン名> となります。
      - このフィールドに @ マークがない文字列が入力され、DNS ドメイン名が空白の場合、差出人の電子メールアドレスは、<@ が含まれない文字列>@<iDRAC6 IP アドレス> となります。
      - このフィールドに @ マークがない文字列が入力され、DNS ドメイン名がアクティブな場合、差出人の電子メールアドレスは、<@ が含まれない文字列>@<DNS ドメイン名> となります。
      - このフィールドに @ マークを含んだ文字列が入力され、DNS ドメイン名が空白の場合、差出人の電子メールアドレスは、<@ を含んだ文字列>@<iDRAC6 IP アドレス> となります。

   e. 必要に応じて **送信** をクリックし、設定した電子メール警告をテストします。

   f. 電子メール警告の送信先を追加するには、「手順 a」から「手順 e」の手順を繰り返します。電子メール警告の送信先は、最大 4 つまで指定できます。

IPMI オーバー LAN の設定

1. iDRAC6 ウェブインタフェースにログインします。

2. IPMI オーバー LAN を設定します。

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

      ネットワーク 画面が表示されます。

   b. **IPMI の設定** をクリックします。

   c. **IPMI オーバー LAN を有効にする** チェックボックスを選択します。

   d. 必要に応じて、**チャネル権限レベルの制限** を更新します。

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

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

   e. 必要に応じて、IPMI LAN チャネルの暗号化キーを設定します。

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

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

   f. **適用** をクリックします。

3. IPMI シリアルオーバー LAN (SOL)を設定します。

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

      ネットワーク 画面が表示されます。

   b. **シリアルオーバー LAN** タブをクリックします。

   c. **シリアルオーバー LAN を有効にする** を選択します。

   d. 必要に応じて、**ボーレート**ドロップダウンメニューからデータ速度を選択して、IPMI SOL の **ボーレート** を更新します。

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

   e. **適用** をクリックします。

   f. 必要に応じて、**詳細設定** ページで IP フィルタとブロックの設定を指定します。

---

iDRAC6 ユーザーの追加と設定

iDRAC6 を使用してシステムを管理し、システムのセキュリティを確保するには、個々のユーザーを、それぞれ特定の管理者権限(または役割ベースの権限)を持たせて作成します。

iDRAC6 のユーザーを追加して設定するには、次の手順に従ってください。

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

1. **システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ**→ **ユーザー** をクリックします。

   ユーザー 画面に、各ユーザーの **ユーザー ID**、**状態**、**ユーザー名**、**IPMI LAN 権限**、iDRAC6 権限、および **シリアルオーバー LAN 機能** が表示されます。

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

2. **ユーザー ID** 列で、ユーザー ID をクリックします。

3. **ユーザーメインメニュー** ページ(「表 5-9」、「表 5-10」、および「表 5-11」を参照)では、ユーザーの設定、SSH 公開キーファイルのアップロード、指定した SSH キーまたはすべての SSH キーを表示あるいは削除することができます。

SSH 経由の公開キー認証

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

作業を開始する前に

SSH インタフェース経由で各ユーザーに設定できる公開キーは最大 4 つまでです。公開キーを追加または削除する前に、表示コマンドを使って設定済みのキーを確認し、キーを誤って上書きしたり削除したりしないようにしてください。SSH 経由の PKA を正しく設定し、使用すると、iDRAC6 へのログイン時にパスワードを入力する必要はありません。これは、自動化されたスクリプトを設定してさまざまな機能を実行する場合に便利です。

この機能の設定準備をする際は、以下の点に留意してください。

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

Windows 用の公開キーの生成

アカウントを追加する前に、SSH 経由で iDRAC6 にアクセスするシステムで公開キーが必要になります。公開 / 秘密キーペアを生成する方法には、Windows を実行しているクライアントの PuTTY キー生成アプリケーションを使用する方法と Linux を実行しているクライアントの ssh-keygen を使用する方法の 2 通りあります。ssh-keygen CLI ユーティリティは、デフォルトですべての標準インストールパッケージに同梱されています。

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

Windows クライアント用の PuTTY キー生成アプリケーションを使用して基本キーを作成するには、次の手順に従います。

1. アプリケーションを起動し、生成するキータイプとして SSH-2 RSA または SSH-2 DSA を選択します SSH-1 はサポートされていません。
2. キーのビット数を入力します。サポートされているキー生成アルゴリズムは RSA と DSA のみです。RSA の場合は、768 ～ 4096 ビット、DSA の場合は 1024 ビットにする必要があります。
3. **生成** をクリックし、指示に従ってマウスポインタをウィンドウ内で移動します。キーを作成したら、キーコメントフィールドを変更できます。パスフレーズを入力すると、キーをセキュリティ保護することもできます。秘密キーを保存したことを確認します。
4. 公開キーファイルを後でアップロードできるように、**公開キーを保存する** オプションを使用して公開キーをファイルに保存できます。アップロードするキーはすべて、RFC4716 または openSSH 形式でなければなりません。これら形式でない場合は、変換する必要があります。

Linux 用の公開キーの生成

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

ターミナルウィンドウを開き、シェルプロンプトで次を入力します。

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

メモ: オプションでは大文字小文字が区別されます。

ここで、

-t は dsa または rsa です。

-b は 768～4096 で、ビット暗号化サイズを指定します。

-C を使用すると、公開キーコメントを変更できます。これは任意選択です。

コマンドを実行した後、公開ファイルをアップロードします。

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

メモ: iDRAC6 では、キーの ssh-agent フォワード機能はサポートされていません。

公開キー認証を使用したログイン

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

たとえば、次のとおりです。

ログイン

```
ssh username@<ドメイン>
```

または

```
ssh username@<IP アドレス>
```

<IP アドレス> には、iDRAC6 の IP アドレスを指定します。

RACADM コマンドの送信:

```
ssh username@<ドメイン> racadm getversion

ssh username@<ドメイン> racadm getsel
```

RACADM を使用して SSH キーをアップロード、表示、削除する方法については、「RACADM を使った SSH キーのアップロード、表示、削除」を参照してください。

表 5-9 SSH キーの設定

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

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

注意: SSH キーのアップロード、表示、削除の機能は、ユーザー設定 権限に基づきます。この権限のあるユーザーは、他のユーザーの SSH キーを設定できます。この権限を与えるときには、注意が必要です。詳細については、「表 5-14」を参照してください。

表 5-10 SSH キーのアップロード

オプション	説明
ファイル / テキスト	**ファイル** オプションを選択し、キーのあるパスを入力します。または、**テキスト** オプションを選択し、ボックス内にキーの内容を貼り付けることもできます。新しいキーをアップロードしたり、既存のキーを上書きしたりできます。キーファイルをアップロードするには、**参照** をクリックしファイルを選択してから、**適用** ボタンをクリックします。 **メモ:** キーテキストを貼り付けるオプションは、openSSH 形式の公開キーでサポートされています。RFC4716 形式のキーでは、テキストを貼り付けるオプションはサポートされていません。
参照	キーの完全パスとファイル名を見つけるには、このボタンをクリックします。

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

表 5-11 SSH キーの表示 / 削除

オプション	説明
削除	アップロードしたキーはボックス内に表示されます。既存のキーを削除するには、**削除** オプションを選択して、**適用** をクリックします。

1. **ユーザーの設定** を選択して **次へ** をクリックすると、**ユーザー設定** ページが表示されます。
2. **ユーザーの設定** 画面で、ユーザーのプロパティと権限を設定します。

   表 5-12は、iDRAC6 ユーザー名とパスワードを設定するための **一般** 設定について説明しています。

   表 5-13 に、ユーザーの LAN 権限を設定するための **IPMI ユーザー権限**について説明します。

   表 5-14 では、**IPMI LAN 権限** と iDRAC6 **ユーザー権限** を設定するための **ユーザーグループ** 権限 について説明しています。

   表 5-15では、**iDRAC6 グループ**権限について説明しています。**iDRAC6 ユーザー権限** を **システム管理者**、**パワーユーザー**、または **ゲストユーザー** に追加すると、iDRAC6 **グループ** が **カスタム** グループに変わります。
3. 設定が完了したら、**適用** をクリックします。
4. 適切なボタンをクリックして続行します。表 5-16 を参照してください。

表 5-12 一般プロパティ

プロパティ	説明
ユーザー ID	16 個ある設定済みユーザー ID 番号の 1 つが入っています。このフィールドは編集できません。
ユーザーを有効にする	**チェックボックスをオン** にすると、iDRAC6 へのユーザーのアクセスが有効になります。**チェックボックスをオフ** にすると、ユーザーアクセスが無効になります。
ユーザー名	iDRAC6 ユーザー名は、16 文字以内で指定できます。各ユーザーは一意のユーザー名を持つ必要があります。 - 0 ～ 9 - A ～ Z

	• A ～ Z • 特殊文字: + % = , - {] § ! (? ; _ } I #) * : $ [| **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。
パスワードの変更	**新しいパスワード** と **新しいパスワードの確認** フィールドを有効にします。選択解除すると、ユーザーの パスワード を変更できません。
新しいパスワード	iDRAC6 ユーザーのパスワードの編集を有効にします。20 文字以内で **パスワード** を入力します。入力lt文字は表示されません。 • 0 ～ 9 • A ～ Z • a ～ z • 特殊文字: + % = , - {] . ! (? ; _ } I | #) * : $ [/ @
新しいパスワードの確認	確認のために、iDRAC6 ユーザーのパスワードを再入力します。

表 5-13 IPMI LAN 権限

プロパティ	説明
LAN ユーザーに許可する最大権限	IPMI LAN チャネルでのユーザーの最大権限を、**なし**、**システム管理者**、**オペレータ**、**ユーザー** の中から指定します。
シリアルオーバー LAN を有効にする	ユーザーに IPMI シリアルオーバー LAN の使用を許可します。**このチェックボックスをオン** にすると、この権限が有効になります。

表 5-14 その他の権限

プロパティ	説明
iDRAC6 グループ	ユーザーの最大 iDRAC6 ユーザー権限を **システム管理者**、**パワーユーザー**、**ゲストユーザー**、**カスタム**、**なし** の中から指定します。 **iDRAC6 グループ** 権限については、「表 5-15」を参照してください。
iDRAC6 へのログイン	ユーザーに iDRAC6 へのログインを許可します。
iDRAC6 の設定	ユーザーに iDRAC6 の設定を許可します。
ユーザーの設定	ユーザが指定したユーザーのシステムアクセスを許可できるようにします。 **注意:この権限は通常、iDRAC の管理者ユーザーグループのメンバーに予約されていまが、「カスタム」ユーザーグループのユーザーにこの権限を割り当てることもできます。この権限のあるユーザーは、他のユーザーの設定を変更できます。これには、ユーザーの作成や削除、ユーザーの SSH キーの管理なども含まれます。そのため、この権限を割り当てるときには注意が必要です。**
ログのクリア	ユーザーに iDRAC6 のログのクリアを許可します。
サーバーコントロールコマンドの実行	ユーザーに RACADM コマンドの実行を許可します。
仮想コンソールへのアクセス	ユーザーに仮想コンソールの実行を許可します。 **注意:この権限は通常、iDRAC の管理者ユーザーグループかパワーユーザーグループのメンバーに予約されています。仮想コンソールへのアクセス権限があるユーザーは、仮想コンソールを使用できるほか、仮想コンソールを使用している人の操作を iDRAC6 ウェブインタフェースで見ることができます。そのため、この権限を割り当てるときには注意が必要です。**
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	現在設定されている警告受信者にユーザーがテスト警告(電子メールと PET)を送信できます。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

表 5-15 iDRAC6 グループ権限

ユーザーグループ	許可する権限
管理者	**iDRAC6 へのログイン、iDRAC6 の設定、ユーザーの設定、ログのクリア、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行**
パワーユーザー	**iDRAC6 へのログイン、ログのクリア、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、テスト警告**

ゲストユーザー	**iDRAC6 へのログイン**
カスタム	次のアクセス権を組み合わせて選択してください。**iDRAC6 へのログイン**、**iDRAC6 の設定**、**ユーザーの設定**、**ログのクリア**、**サーバー制御コマンドの実行**、**仮想コンソールへのアクセス**、**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**
None(なし)	権限の割り当てなし

表 5-16 ユーザー設定のボタン

ボタン	**操作**
印刷	画面に表示されている **ユーザー設定** 値を印刷します。
更新	**ユーザー設定** 画面を再ロードします。
適用	ユーザー設定に追加された新規設定を保存します。
ユーザー メインメニューに戻る	**ユーザーメインメニュー画面**に戻ります。

SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保

ここでは、iDRAC6 に組み込まれているデータセキュリティ機能について説明します。

- 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
- 新しい 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 ウェブサーバーには、デフォルトでデルの署名付き SSL デジタル証明書(サーバー ID)があります。インターネット上で高いセキュリティを確保するには、ウェブサーバーの SSL 証明書を、大手認証局(CA)によって署名された証明書に置き換えてください。認証局(CA)は、信頼できる高水準の審査、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るとして、IT 業界で認められたビジネス団体です。CA には、Thawte や VeriSign などがあります。署名された証明書を取得するには、まず、iDRAC6 ウェブインタフェースを使用して企業情報を掲載した証明書署名要求(CSR)を生成します。生成した CSR を VeriSign や Thawte などの CA に送信します。

証明書署名要求 (CSR)

CSR は、認証局(CA)に対してセキュアサーバー証明書の発行を求めるデジタル要求です。セキュアサーバー証明書を使用すると、サーバーのクライアントは接続しているサーバーの身元を信用できるほか、サーバーとの暗号化されたセッションを交渉できます。

CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ基準を満たしていれば、ネットワークおよびインターネットを介したトランザクションを行う申請者を一意に識別するデジタル署名済みの証明書を発行します。

CA が CSR を承認して証明書を送信したら、それを iDRAC6 ファームウェアにアップロードします。iDRAC6 ファームウェアに保存されている CSR 情報が、証明書に含まれている情報と一致する必要があります。つまり、証明書は iDRAC6 で作成された CSR に則して生成されている必要があります。

SSL メインメニューへのアクセス

1. **システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブをクリックします。
2. **SSL** をクリックして **SSL** 画面を開きます。

表 5-17 では、CSR の生成時に使用可能なオプションについて説明します。

表 5-18 では、**SSL メインメニュー** 画面上のボタンについて説明します。

表 5-17 SSL メインメニューオプション

フィールド	説明
新しい証明書署名要求(CSR)の生成	オプションを選択し、**次へ** をクリックして **証明書署名要求(CSR)の生成** 画面を開きます。 **メモ:** 新しい CSR はそれぞれ、ファームウェア上の古い CSR を上書きします。CA が CSR を受け入れるためには、ファームウェアにある CSR が CA から返された証明書に一致する必要があります。
サーバー証明書のアップロード	オプションを選択し、**次へ** をクリックして **証明書のアップロード** 画面を開き、CA から送信された証明書をアップロードします。 **メモ:** iDRAC6 で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER でエンコードされた証明書は受け入れられません。
サーバー証明書の表示	オプションを選択し、**次へ** をクリックして **サーバー証明書の表示** 画面を開き、既存のサーバー証明書を表示します。

表 5-18 SSL メインメニューボタン

ボタン	説明
印刷	画面に表示されている **SSL** の値を印刷します。
更新	**SSL** 画面を再ロードします。
次へ	**SSL** 画面の情報を処理し、次のステップに進みます。

新しい証明書署名要求の生成

メモ: 新しい CSR はファームウェアに保存されている古い CSR データを上書きします。ファームウェアの CSR は、CAから返された証明書と一致している必要があります。一致しない場合、iDRAC6 は証明書を受け入れません。

1. **SSL** 画面で、**新しい証明書署名要求(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** 画面で、各 CSR 属性の値を入力します。

   表 5-19 に、**証明書署名要求(CSR)の生成** 画面のオプションを示します。
3. CSR を作成するには、**生成** をクリックします。
4. **ダウンロード** をクリックして CSR ファイルをリモート管理ステーションに保存します。
5. 適切なボタンをクリックして続行します。表 5-20 を参照してください。

表 5-19 証明書署名要求(CSR)の生成のオプション

フィールド	説明
共通名	証明する名前(通常は、**www.xyzcompany.com** のようなウェブサーバーのドメイン名)。英数字、スペース、ハイフン、アンダースコア、ピリオドのみが有効です。
組織名	この組織に関連付けられた名前(たとえば「XYZ Corporation」)。英数字、ハイフン、アンダースコア、ピリオド、スペースのみが有効です。
組織単位	部門など組織単位に関連付ける名前(例、Information Technology)。英数字、ハイフン、アンダースコア、ピリオド、スペースのみが有効です。
地域	証明する会社が所在する市または地域(たとえば Kobe)。英数字とスペースのみが有効です。アンダースコアや他の文字で単語を区切らないでください。
都道府県名	証明書を申請している組織が所在する都道府県(たとえば 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。会社の電子メールアドレスまたは CSR に関連付ける電子メールアドレスを入力します。このフィールドは省略可能です。
キーサイズ	生成する証明書署名要求(CSR)キーのサイズ。サイズの選択肢は 1024 KB または 2048 KB です。

表 5-20 証明書署名要求(CSR)生成 ボタン

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

生成	CSR を生成し、指定のディレクトリに保存するようユーザーに指示します。
ダウンロード	証明書をローカルコンピュータにダウンロードします。
SSL メインメニューに戻る	**SSL** 画面に戻ります。

サーバー証明書のアップロード

1. **SSL** 画面で **サーバー証明書のアップロード** を選択して、**次へ** をクリックします。

   証明書のアップロード 画面が表示されます。

2. **ファイルパス** フィールドに証明書のパスを入力するか、**参照** をクリックして、管理ステーションの証明書ファイルに移動します。

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

3. **適用** をクリックします。

4. 適切なボタンをクリックして続行します。表 5-21 を参照してください。

表 5-21 証明書のアップロードのボタン

ボタン	説明
印刷	**証明書のアップロード** 画面に表示されている値を印刷します。
更新	**証明書のアップロード** 画面を再ロードします。
適用	証明書を iDRAC6 ファームウェアに適用します。
SSL メインメニューに戻る	**SSL メインメニュー** 画面に戻ります。

サーバー証明書の表示

1. **SSL** 画面で **サーバー証明書の表示** を選択して **次へ** をクリックします。

   表 5-22 に、**サーバー証明書の表示** ウィンドウに表示されるフィールドとその説明を示します。

2. 適切なボタンをクリックして続行します。表 5-23 を参照してください。

表 5-22 サーバー証明書情報の表示

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

表 5-23 サーバー証明書の表示のボタン

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

Microsoft Active Directory 証明書の設定と管理

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

メモ: Active Directory の設定と、Active Directory に標準スキーマまたは拡張スキーマを設定する方法の詳細については、「iDRAC6 ディレクトリサービスの使用」を参照してください。

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

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

表 5-24 Active Directory のオプション

フィールド	説明
共通設定	共通して設定される Active Directory の設定を表示します。
Active Directory CA 証明書	すべてのドメインコントローラの SSL サーバー証明書に署名をする CA の証明書を表示します。
標準スキーマの設定 / 拡張スキーマの設定	Active Directory の設定によって、拡張スキーマの設定または標準スキーマの設定が表示されます。
Active Directory の設定	Active Directory の設定で手順 1/4 を設定するには、このオプションをクリックします。**Active Directory 手順 1 / 4** ページでは、Active Directory の CA 証明書を iDRAC6 にアップロードしたり、iDRAC6 にアップロードされた現在の Active Directory CA 証明書を表示したり、証明書の検証を有効にしたりできます。
設定のテスト	指定した設定を使用して Active Directory の設定をテストするには、このオプションをクリックします。
Kerberos Keytab のアップロード	iDRAC6 に Kerberos Keytab をアップロードするには、このオプションをクリックします。keytab ファイルの作成方法については、「iDRAC6 へのシングルサインオンとスマートカードログインの設定」を参照してください。

表 5-25 Active Directory のボタン

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

Active Directory の設定(標準スキーマと拡張スキーマ)

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

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

表 5-26 Active Directory 設定の設定

設定	説明
Active Directory の設定と管理 手順 1 / 4	
証明書検証を有効にする	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。**このチェックボックスをオン** にすると、証明書の検証が有効になります。iDRAC6 は Active Directory への接続中、SSL(Secure Socket Layer)で LDAP を使用します。デフォルトでは、iDRAC6 は、iDRAC6 にロードされた CA 証明書を使用してドメインコントローラの SSL サーバー証明書を SSL ハンドシェーク中に検証する強力なセキュリティを提供します。証明書の検証はテスト目的で無効にできます。
Active Directory CA 証明書のアップロード	Active Directory CA 証明書をアップロードするには、**参照** をクリックし、ファイルを選択して **アップロード** をクリックします。ドメインコントローラの SSL 証明書が同じ認証局によって署名され、iDRAC6 にアクセスする管理ステーションにこの証明書があることを確認してください。アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。証明書を参照しない場合は、完全パスと正式ファイル名とファイル拡張子を含めてファイルのパスを入力してください。
現在の Active Directory CA 証明書	iDRAC6 にアップロードされた Active Directory CA 証明書を表示します。
Active Directory の設定と管理 手順 2 / 4	
Active Directory を有効にする	Active Directory を有効にする場合は、このオプションを選択します。
スマートカードログインを有効にする	スマートカードログインを有効にするには、このオプションを選択します。以降 GUI を使用してログイン試行すると、スマートカードログオンのプロンプトが表示されます。 **メモ:** スマートカードベースの 2 要素認証(TFA)とシングルサインオンは、Internet Explorer を搭載した Microsoft Windows オペレーティングシステムでのみサポートされています。なお、Windows XP 下のターミナルサービス(リモートデスクトップ)はスマートカードの操作をサポートしていませんが、Windows Vista はこの用途をサポートしています。
シングルサインオンを有効にする	ユーザー名やパスワードなどのドメインユーザー認証情報を入力せずに iDRAC6 にログインする場合は、このオプションを選択します。シングルサインオン(SSO)を有効にしてからログアウトした場合は、SSO を使用して再ログインできます。既に SSO を使用してログインしてからログアウトした場合や、SSO に失敗した場合は、通常のログインウェブページが表示されます。 **メモ:** スマートカードログオン**または**シングルサインオンを有効にしても、SSH、Telnet、リモート RACADM、IPMI オーバー LAN などのコマンドラインの帯域外インタフェースは無効になりません。

	メモ: 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、スマートカードを使用する 2 要素認証(TFA)機能はサポートされていません。シングルサインオン(SSO)機能は、標準スキーマでも拡張スキーマまでもサポートされています。
ユーザードメイン名	ユーザードメイン名のエントリを入力します。設定されている場合は、ログインページにユーザードメイン名のリストがドロップダウンメニューとして表示されます。設定されていない場合でも、Active Directory ユーザーはユーザー名を user_name@domain_name または domain_name\user_name の形式で入力するとログインできます。**追加**:新しいユーザードメイン名をリストに加えます。**編集**:既存のユーザードメイン名を編集します。**削除**:ユーザードメイン名をリストから削除します。
タイムアウト	Active Directory のクエリが完了するまで待つ最大時間を秒で指定します。
DNS を使用したドメインコントローラのルックアップ	**DNS ルックアップドメインコントローラ** オプションを選択し、DNS ルックアップから Active Directory ドメインコントローラを取得します。このオプションを選択すると、ドメインコントローラサーバーのアドレス 1～3 は無視されます。**ログインのユーザードメイン** を選択し、ログインユーザーのドメイン名を使って DNS ルックアップを実行します。そうでない場合は、**ドメインを指定する** を選択し、DNS ルックアップに使用するドメイン名を入力します。iDRAC6 は接続が確立されるまで、各アドレス(DNS ルックアップによって返される最初の 4 つのアドレス)に対して、1 つずつ接続を試みます。 **拡張スキーマ** を選択した場合、ドメインコントローラは、iDRAC6 デバイスオブジェクトと関連オブジェクトが存在する場所になります。**標準スキーマ** を選択した場合、これらはユーザーアカウントと役割グループが存在するドメインコントローラを表します。
ドメインコントローラのアドレスの指定	iDRAC6 に指定した Active Directory ドメインコントローラのサーバーアドレスを使用させるには、**ドメインコントローラアドレスを指定する** オプションを選択します。このオプションを選択すると、DNS ルックアップは実行されません。ドメインコントローラの IP アドレスまたは完全修飾ドメイン名(FQDN)を指定します。**ドメインコントローラアドレスを指定する** オプションが選択されている場合、3 つのアドレスのうち、少なくとも 1 つのアドレスが設定されている必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、1 つずつ接続を試みます。 **標準スキーマ** を選択した場合、これらはユーザーアカウントと役割グループが存在するドメインコントローラのアドレスです。**拡張スキーマ** を選択した場合、これらは iDRAC6 デバイスオブジェクトと関連オブジェクトが存在するドメインコントローラのアドレスです。
Active Directory の設定と管理 手順 3 / 4	
拡張スキーマの選択	Active Directory で拡張スキーマを使用する場合は、このオプションを選択します。 **次へ** をクリックして、Active Directory 設定と管理 **手順 4 / 4** ページを表示します。 **iDRAC6 名**: Active Directory で iDRAC6 を一意に識別する名前を指定します。この値はデフォルトでは NULL になっています。 **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 iDRAC6 を使用するように設定されている場合にのみ表示されます。
標準スキーマの選択	Active Directory で標準スキーマを使用する場合は、このオプションを選択します。 **次へ** をクリックして、Active Directory **手順 4a / 4** ページを表示します。 **DNS のルックアップグローバルカタログ** オプションを選択し、Active Directory グローバルカタログサーバーを取得するのに DNS ルックアップで使用する **ルートドメイン名** を入力します。このオプションを選択すると、**グローバルカタログサーバー**のアドレス 1～3 は無視されます。iDRAC6 は接続が確立されるまで、各アドレス(DNS ルックアップによって返される最初の 4 つのアドレス)に対して、1 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。 **グローバルカタログサーバーアドレスを指定する** オプションを選択し、グローバルカタログサーバーの IP アドレスまたは FQDN を入力します。このオプションを選択すると、DNS ルックアップは実行されません。これらの 3 つのアドレスの少なくとも 1 つは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、1 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**:役割グループが存在するグループドメインを指定します。 **役割グループの権限**: グループの権限レベルを指定します。(「表 5-27」を参照) これらの設定は、標準 Active Directory スキーマで iDRAC6 を使用するように設定されている場合にのみ表示されます。

表 5-27 役割グループの権限

設定	**説明**
役割グループの権限レベル	ユーザーの最大 iDRAC6 ユーザー権限を **システム管理者**、**パワーユーザー**、**ゲストユーザー**、**なし**、**カスタム** から指定します。 **役割グループ** 権限については、「表 5-28」を参照してください。
iDRAC6 へのログイン	グループに iDRAC6 へのログインアクセスを許可します。
iDRAC6 の設定	iDRAC6 を設定するグループ権限を許可します。
ユーザーの設定	ユーザーを設定するグループ権限を許可します。
ログのクリア	ログをクリアするグループ権限を許可します。
サーバーコント役割コマンドの実行	サーバーコントロールコマンドを実行するグループ権限を許可します。
仮想コンソールへのアクセス	仮想コンソールへのグループアクセスを許可します。
仮想メディアへのアクセス	仮想メディアへのグループアクセスを許可します。
テスト警告	グループがテスト警告(電子メールおよび PET)を特定のユーザーに送信できます。
診断コマンドの実行	診断コマンドを実行するグループ権限を許可します。

表 5-28 役割グループの権限

プロパティ	**説明**

管理者	iDRAC6 へのログイン、iDRAC6 の設定、ユーザーの設定、、ログのクリア、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
パワーユーザー	iDRAC6 へのログイン、ログのクリア、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、テスト警告。
ゲストユーザー	iDRAC6 へのログイン
Custom（カスタム）	次の権限を組み合わせて選択します。iDRAC6 へのログイン、iDRAC6 の設定、ユーザーの設定、ログのクリア、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。
なし	権限の割り当てなし

Active Directory CA 証明書の表示

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

表 5-29 Active Directory CA 証明書の情報

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

設定へのローカルアクセスの有効化と無効化

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

設定へのローカルアクセスを有効にする

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

設定へのローカルアクセスを無効にする

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

---

iDRAC6 サービスの設定

メモ: これらの設定を変更するには、**iDRAC6 の設定** 権限が必要です。

メモ: サービスに変更を適用すると、変更はすぐに反映されます。既存の接続は、警告なしで終了されることがあります。

メモ: Microsoft Windows 提供の Telnet クライアントには、既知の問題があります。ハイパーターミナルや PuTTY といった他の Telnet クライアントを使用してください。

1. **システム** → **リモートアクセス** → **iDRAC6** の順にクリックして、**ネットワーク / セキュリティ** タブをクリックします。
2. **サービス** をクリックして **サービス**設定 画面を開きます。
3. 必要に応じて、次のサービスを設定します。
   - ウェブサーバー - ウェブサーバーの設定については「表 5-30」を参照
   - SSH - SSH 設定については「表 5-31」を参照

- Telnet - Telnet の設定については「表 5-32」を参照
- SNMP エージェント - SNMP エージェントの設定については、「表 5-33」を参照してください。
- 自動システムリカバリエージェント - 自動システムリカバリエージェントの設定については「表 5-34」を参照

4. **適用** をクリックします。

表 5-30 ウェブサーバーの設定

設定	説明
有効	iDRAC6 ウェブサーバーを有効または無効にします。**この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。デフォルトで**このチェックボックスがオン になっています**。
最大セッション数	このシステムで同時に許可されるウェブサーバー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 4 つのウェブサーバーセッションが同時に存在できます。
アクティブセッション数	システムの現在のセッション数(**最大セッション数** 以下)。このフィールドは編集できません。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更はすぐに有効になり、ウェブサーバーはリセットされます。タイムアウトの範囲は 60〜10800 秒です。デフォルトは **1800** 秒です。
HTTP ポート番号	ブラウザ接続で iDRAC6 が通信するポート。デフォルトは **80** です。
HTTPS ポート番号	セキュアなブラウザ接続で iDRAC6 が通信するポート。デフォルトは **443** です。

表 5-31 SSH の設定

設定	説明
有効	SSH を有効または無効にします。**このチェックボックスがオン** の場合は、SSH が有効であることを示します。
最大セッション数	システムで同時に許可される最大 SSH セッション数。最大 4 つの SSH セッションが同時にサポートされます。このフィールドは編集できません。
アクティブセッション数	システムの現在のセッション数。このフィールドは編集できません。
タイムアウト	セキュアシェルのアイドルタイムアウト(秒)。タイムアウトの範囲は 60〜10800 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **1800** です。
ポート番号	SSH 接続で iDRAC6 が通信するポート。デフォルトは **22** です。

表 5-32 Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。**このチェックボックスがオン** の場合は、Telnet が有効になります。デフォルトではこの**チェックボックスがオフ** です。
最大セッション数	システムで同時に許可される最大 Telnet セッション数。最大 4 つの Telnet セッションが同時にサポートされます。このフィールドは編集できません。
アクティブセッション数	システムの現在の Telnet セッション数。このフィールドは編集できません。
タイムアウト	Telnet のアイドルタイムアウト(秒)。タイムアウトの範囲は 60〜10800 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **1800** です。
ポート番号	iDRAC6 が Telnet 接続を待ち受けるポート。デフォルトは **23** です。

表 5-33 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 5-34 自動システム回復エージェント

設定	説明
有効	自動システムリカバリエージェントを有効にします。

---

iDRAC6 ファームウェアのアップデート

メモ: iDRAC6 ファームウェアのアップデートが完了前に中断されるなどで、iDRAC6 ファームウェアが破損した場合は、CMC を使用して iDRAC6 を修復できます。手順については、『CMC ファームウェアユーザーガイド』を参照してください。

メモ: ファームウェアアップデートは、デフォルトで現在の iDRAC6 設定を保持します。アップデート中に、iDRAC6 設定を工場出荷時のデフォルト設定にリセットするオプションが提供されます。設定を出荷時のデフォルト設定にすると、アップデート完了時に外部ネットワークアクセスが無効になります。iDRAC6 設定ユーティリティまたは CMC ウェブインタフェースを使ってネットワークを有効にし、設定する必要があります。

1. iDRAC6 ウェブインタフェースを開始します。
2. **システム** → **リモートアクセス** → **iDRAC6** の順にクリックして、**アップデート** タブをクリックします。

   ファームウェアアップデート 画面が表示されます。

   メモ: ファームウェアをアップデートするには、iDRAC6 がアップデートモードになっている必要があります。このモードでは、アップデートプロセスをキャンセルした場合でも iDRAC6 は自動的にリセットされます。
3. **アップロード** セクションで **参照** をクリックしてファームウェアイメージを選択します。

   例:

   `C:\Updates\V2.2\<イメージ名>`

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

メモ: **設定の保存** チェックボックスをオフにすると、iDRAC6 がデフォルト設定にリセットされます。デフォルト設定では LAN は無効になっています。iDRAC6 ウェブインタフェースにログインできません。BIOS POST 中に、CMC ウェブインタフェースを使用して LAN を再設定し、iDRAC6 設定ユーティリティを使用して仮想コンソール再設定する必要があります。

6. デフォルトでは、アップグレード後も iDRAC6 の現在の設定を維持するための **設定の保存 チェックボックスがオン**になっています。設定を維持しない場合は、**設定の保存** チェックボックスをオフにします。
7. **アップデートの開始** をクリックして、アップグレードプロセスを開始します。アップグレードプロセスには割り込まないでください。
8. **アップロード(手順 3 / 4)** ウィンドウに、アップグレードの状態が表示されます。ファームウェアアップグレード操作の進行状況は、**進行状況** 列にパーセントで表示されます。
9. ファームウェアのアップデートが完了すると、**アップロード(手順 3 / 3)** ウィンドウが結果を反映して更新され、iDRAC6 が自動的にリセットされます。引き続きウェブインタフェースから iDRAC6 にアクセスするには、現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使用して iDRAC6 に再接続します。

CMC を使用した iDRAC6 ファームウェアのアップデート

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

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

メモ: CMC ウェブインタフェースの使用方法については、『Chassis Management Controller ファームウェアユーザーガイド』を参照してください。

iDRAC6 ファームウェアをアップデートするには、次の手順を実行してください。

1. **support.dell.com** から管理コンピュータに最新の iDRAC6 ファームウェアをダウンロードします。
2. CMC ウェブインタフェースにログインします。
3. **システムツリーで シャーシ** をクリックします。
4. **アップデート** タブをクリックします。**ファームウェアアップデート** 画面が表示されます。
5. **ターゲットのアップデート** チェックボックスをオンにして、同じモデルの iDRAC6 を選択します(複数可)。
6. iDRAC6 コンポーネントのリストの下にある **iDRAC6 Enterprise アップデートの適用** ボタンをクリックします。
7. **参照** をクリックして、ダウンロードした iDRAC6 ファームウェアイメージに移動し、**開く** をクリックします。
8. **ファームウェアアップデートを開始する** をクリックします。

ファームウェアイメージファイルを CMC にアップロードすると、iDRAC6 はそのイメージを使用して自動的にアップデートされます。

iDRAC6 ファームウェアのロールバック

iDRAC6 は、2 つの同時ファームウェアイメージを保持できます。任意のファームウェアイメージから起動（またはその時点までロールバック）できます。

1. iDRAC6 ウェブインタフェースを開いてリモートシステムにログインします。

   システム → **リモートアクセス** → **iDRAC6** の順にクリックして、**アップデート** タブをクリックします。

2. **ロールバック** をクリックします。現在およびロールバックのファームウェアバージョンは **ロールバック（手順 2 / 3）** ページに表示されます。

3. **次へ** をクリックしてファームウェアのロールバックプロセスを開始します。

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

   ファームウェアのロールバックに成功すると、iDRAC6 は自動的にリセットされます。引き続きウェブインタフェースから iDRAC6 を操作するには、現在のブラウザを閉じ、新しいブラウザウィンドウを使用して iDRAC6 に再接続します。エラーが発生した場合、該当するエラーメッセージが表示されます。

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

目次ページに戻る

目次ページに戻る

iDRAC6 ディレクトリサービスの使用

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

ディレクトリサービスは、ユーザー、コンピュータ、プリンタなどの情報を保存するための共通のデータベースを保持します。会社で Microsoft Active Directory または LDAP ディレクトリサービスソフトウェアを使用している場合は、iDRAC6 にアクセスできるように設定し、ディレクトリサービスの既存のユーザーに iDRAC6 のユーザー権限を追加して制御できます。

Microsoft Active Directory での iDRAC6 の使用

メモ: Active Directory を使用した iDRAC6 ユーザーの認識は、Microsoft Windows 2000、Windows Server 2003、Windows Server 2008 オペレーティングシステムでサポートされています。

ユーザー権限は、Microsoft Active Directory から iDRAC6 にログインして設定できます。また、管理者が各ユーザーに特定の権限を設定できる役割ベースの権限を提供することもできます。詳細については、以下の項を参照してください。

表 6-1 に、iDRAC6 Active Directory ユーザー権限を示します。

表 6-1 iDRAC6 ユーザー権限

権限	説明
iDRAC6 へのログイン	ユーザーに iDRAC へのログインを許可します。
iDRAC6 の設定	ユーザーに iDRAC6 の設定を許可します。
ユーザーの設定	ユーザが指定した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	ユーザーに iDRAC6 のログのクリアを許可します。
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。
仮想コンソールへのアクセス	ユーザーに仮想コンソール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)を指定した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。

Active Directory と次のいずれかの方法を利用して、iDRAC6 にログインできます。

- ウェブインタフェース
- ローカル RACADM
- SM-CLP CLI 用の SSH または Telnet コンソール

ログイン構文は、3 つの方法にすべて共通です。

<ユーザー名@ドメイン>

または

<ドメイン>\<ユーザー名> または<ドメイン>/<ユーザ名>

ユーザー名 は 1 ~ 256 バイトの ASCII 文字列です。

ユーザー名やドメイン名には、空白スペースと特殊文字(\, /, @ など)は使用できません。

メモ: Americas などの NetBIOS ドメイン名は名前解決できないため、指定できません。

ウェブインタフェースからログインし、ユーザードメインを設定している場合は、ウェブインタフェースのログイン画面のプルダウンメニューにすべてのユーザードメインが表示されます。プルダウンメニューからユーザードメインを選択する場合は、ユーザー名のみを入力します。**この iDRAC** を選択した場合も、上記「Microsoft Active Directory での iDRAC6 の使用」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。

---

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場合は、Active Directory インフラストラクチャがすで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 は標準の公開キー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場合は、iDRAC6 に接続するすべてのドメインコントローラ上で Secure Socket Layer(SSL)を有効にする必要もあります。詳細については、「ドメインコントローラの SSL を有効にする」を参照してください。

ドメインコントローラの SSL を有効にする

iDRAC6 は Active Directory ドメインコントローラに対してユーザーを認証するとき、ドメインコントローラと SSL セッションを開始します。このとき、ドメインコントローラは認証局(CA)によって署名された証明書を発行し、そのルート証明書も iDRAC6 にアップロードされます。つまり、iDRAC6 が(ルートか子ドメインコントローラかにかかわらず) どの ドメインコントローラに対しても認証できるためには、そのドメインコントローラはそのドメインの CA によって署名された SSL 対応証明書を持っている必要があります。

Microsoft Enterprise のルート CA を使用して自動的にすべてのドメインコントローラ SSL に証明書を割り当てる場合は、次の手順で各ドメインコントローラの SSL を有効にする必要があります。

1. 各コントローラの SSL 証明書をインストールして、各ドメインコントローラで SSL を有効にします。
    a. **スタート**→ **管理ツール**→ **ドメインセキュリティポリシー** をクリックします。
    b. **公開キーのポリシー** フォルダを展開し、**自動証明書要求の設定** を右クリックして**自動証明書要求** をクリックします。
    c. **自動証明書要求の設定ウィザード** で **次へ** をクリックし、**ドメインコントローラ** を選択します。
    d. **次へ** をクリックして、**完了** をクリックします。

iDRAC6 へのドメインコントローラのルート CA 証明書のエクスポート

メモ: システムで Windows 2000 が実行されている場合は、以下の手順が異なる可能性があります。

メモ: スタンドアロンの CA を利用している場合は、以下の手順が異なる可能性があります。

1. Microsoft Enterprise CA サービスを実行しているドメインコントローラを見つけます。
2. **スタート**→**ファイル名を指定して実行** の順にクリックします。
3. **ファイル名を指定して実行** フィールドに mmc と入力し、**OK** をクリックします。
4. **コンソール 1**(MMC)ウィンドウで、**ファイル**(Windows 2000 システムでは **コンソール**)をクリックし、**スナップインの追加 / 削除** を選択します。
5. **スナップインの追加と削除** ウィンドウで **追加** をクリックします。
6. **スタンドアロンスナップイン** ウィンドウで **証明書** を選択して **追加** をクリックします。
7. **コンピュータ** アカウントを選択して **次へ** をクリックします。
8. **ローカルコンピュータ** を選択して **完了** をクリックします。
9. **OK** をクリックします。
10. **コンソール 1** ウィンドウで、**証明書** フォルダを展開し、**パーソナル** フォルダを展開して、**証明書** フォルダをクリックします。
11. ルート CA 証明書を見つけて右クリックし、**すべてのタスク** を選択して **エクスポート** をクリックします。
12. **証明書のエクスポート ウィザード**で **次へ** を選択し、**いいえ、秘密キーをエクスポートしません** を選択します。
13. **次へ** をクリックし、フォーマットとして **Base-64 エンコード X.509 (.cer)** を選択します。
14. **次へ** をクリックし、システムのディレクトリに証明書を保存します。
15. 手順 14 に保存した証明書を iDRAC6 にアップロードします。

    RACADM を使って証明書をアップロードする場合は、「RACADM を使用した標準スキーマの Active Directory の設定」を参照してください。

    ウェブインタフェース を使用して証明書をアップロードする場合は、「iDRAC6 ウェブインタフェースを使用して Active Directory を標準スキーマで設定する方法」を参照してください。

iDRAC6 ファームウェア SSL 証明書のインポート

メモ: Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証する設定になっている場合は、iDRAC6 サーバー証明書を Active Directory ドメインコントローラにもアップロードする必要があります。Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証しない場合、この手順は不要です。

次の手順に従って、すべてのドメインコントローラの信頼された証明書のリストに iDRAC6 ファームウェア SSL 証明書をインポートします。

メモ: システムで Windows 2000 が実行されている場合は、以下の手順が異なる可能性があります。

メモ: iDRAC6 ファームウェア SSL 証明書が知名度の高い CA によって署名され、その CA の証明書が既にドメインコントローラの信頼できるルート認証局のリストに含まれている場合は、この項の手順を実行する必要はありません。

iDRAC6 の SSL 証明書は、iDRAC6 のウェブサーバーで使用される証明書と同じです。iDRAC6 のコントローラにはすべて、デフォルトの自己署名付き証明書が付随しています。

iDRAC6 SSL 証明書をダウンロードする場合は、次の RACADM コマンドを実行します。

racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>

1. ドメインコントローラで、**MMC コンソール** ウィンドウを開き、**証明書** →**信頼できるルート認証局** の順に選択します。
2. **証明書** を右クリックし、**すべてのタスク** を選択して **インポート** をクリックします。
3. **次へ** をクリックして SSL 証明書ファイルまで参照します。
4. 各ドメインコントローラの **信頼できるルート認証局** に iDRAC6 SSL 証明書をインストールします。

   独自の証明書をインストールした場合は、その証明書に署名する CA が **信頼できるルート認証局** リストにあるかどうか確認してください。この 認証局 がリストにない場合は、それをすべてのドメインコントローラにインストールする必要があります。
5. **次へ** をクリックし、証明書の種類に基づいて証明書の保存場所を Windows に自動的に選択させるか、保存する場所を参照します。
6. **完了** をクリックして **OK** をクリックします。

サポートされている Active Directory の認証機構

Active Directory を使用して iDRAC6 へのユーザーアクセスを定義する方法には 2 通りあります。その 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 1 つは、Active Directory グループオブジェクトのみを使用する標準スキーマソリューションを使用する方法です。これらのソリューションの詳細については、以下の各項を参照してください。

Active Directory を使用して iDRAC6 へのアクセスを設定する場合は、拡張スキーマソリューションまたは標準スキーマソリューションを選択する必要があります。

拡張スキーマソリューションを使用する場合の利点は次のとおりです。

- 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。
- さまざまな権限レベルで異なる iDRAC6 カードへのユーザーアクセスを設定するために、最大限の柔軟性が提供されています。

標準スキーマソリューションを使用する利点は、スキーマ拡張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、それぞれ一意の ID で定義する必要があります。業界内で一意の ID の保持するために、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。

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

iDRAC6 スキーマ拡張の概要

デルでは、さまざまな顧客環境に柔軟に対応できるように、ユーザーが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 iDRAC6 デバイスにリンクするために使用します。このモデルでは、ユーザー、iDRAC6 権限、およびネットワーク上の iDRAC6 デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

Active Directory オブジェクトの概要

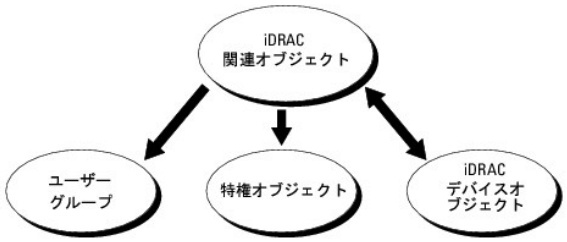
認証と許可のために Active Directory に統合するネットワーク上の物理 iDRAC6 の 1 台につき、少なくとも 1 個ずつ関連オブジェクトと iDRAC6 デバイスオブジェクトを作成しておきます。関連オブジェクトは必要な数だけ作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、iDRAC6 デバイスオブジェクトの数にも制限はありません。ユーザーと iDRAC6 デバイスオブジェクトは、企業内のどのドメインのメンバーでもかまいません。

ただし、各関連オブジェクトは 1 つの権限オブジェクトにしかリンクできません。つまり、ユーザー、ユーザーグループ、または iDRAC6 デバイスオブジェクトをそれぞれ 1 つの権限オブジェクトにしかリンクできません。この例では、システム管理者は個々の iDRAC6 での各ユーザーの権限を制御できます。

iDRAC6 デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための iDRAC6 ファームウェアへのリンクです。iDRAC6 をネットワークに追加した場合、システム管理者は iDRAC6 とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と許可を実行できるようにする必要があります。さらに、システム管理者はユーザーが認証できるように、iDRAC6 を少なくとも 1 つの関連オブジェクトに追加する必要があります。

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

図 6-1 Active Directory オブジェクトの標準的なセットアップ



作成する関連オブジェクトの数に制限はありません。ただし、iDRAC6 で認証と許可を実行する場合は、関連オブジェクトを少なくとも 1 つ作成する必要があり、Active Directory と統合するネットワーク上の iDRAC6 デバイスごとに iDRAC6 デバイスオブジェクトが 1 つ必要となります。

関連オブジェクトに含むことができるユーザー、グループ、iDRAC6 デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる権限オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは、iDRAC6 デバイスに権限のあるユーザーを接続します。

Active Directory ユーザーとコンピュータ MMC スナップインへの Dell 拡張子は、関連オブジェクトと同じドメインの権限オブジェクトおよび iDRAC6 オブジェクトのみに関連付けることができます。Dell 拡張子は、異なるドメインのグループまたは iDRAC6 オブジェクトを関連オブジェクトの製品メンバーとして追加することを許可していません。

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

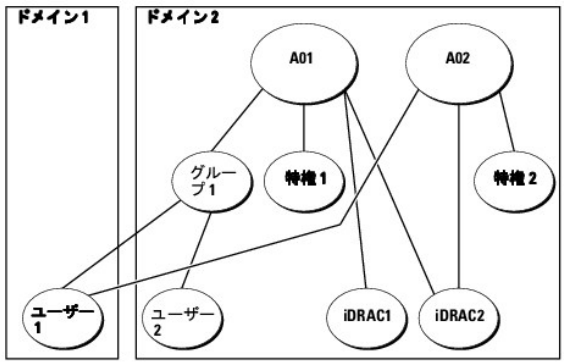
任意のドメインのユーザー、ユーザーグループ、またはネストされたユーザーグループを関連オブジェクトに追加できます。拡張スキーマソリューションは、Microsoft Active Directory によって許可されている複数のドメインにわたってネストされたユーザーグループやユーザーグループの種類をサポートしています。

拡張スキーマを使用した権限の蓄積

拡張スキーマ認証機構は、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 6-2 に、拡張スキーマを使用した権限の蓄積例を示します。

図 6-2 ユーザーの権限の蓄積



この図には、A01 と A02 の 2 つの関連オブジェクトが示されています。ユーザー 1 は、両方の関連オブジェクトを通して、iDRAC2 に関連付けられています。したがって、ユーザー 1 には iDRAC2 で オブジェクト Priv1 と Priv2 に設定された権限を組み合わせて蓄積された権限が与えられます。

たとえば、Priv1 には、ログイン、仮想メディア、およびログのクリアの権限が割り当てられ、Priv2 には、iDRAC へのログイン、テスト、およびテスト警告の権限が割り当てられているとします。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ます。

拡張スキーマ認証は、同じユーザーに関連付けられている異なる権限オブジェクトに割り当てられた権限を考慮し、このように権限を蓄積して、ユーザーに最大限の権限を与えます。

この設定では、ユーザー 1 は iDRAC2 では Priv1 と Priv2 を持っています。ユーザー1 は、iDRAC1 では Priv1 だけ持っています。ユーザー2 は、iDRAC1 と iDRAC2 の両方で Priv1 を持っています。さらに、この図では、ユーザー1 は異なるドメインに属し、グループのメンバーであることも許可されていることを示しています。

---

iDRAC6 にアクセスするための拡張スキーマ Active Directory の設定

Active Directory を使って iDRAC6 にアクセスする前に、次の手順を実行して、Active Directory ソフトウェアと iDRAC6 を設定する必要があります。

1. Active Directory スキーマを拡張します(「Active Directory スキーマの拡張」を参照)。
2. Active Directory ユーザーおよびコンピュータのスナップイン を拡張します(「Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール」を参照)。
3. iDRAC6 ユーザーとその権限を Active Directory に追加します(「Active Directory への iDRAC6 ユーザーと権限の追加」 を参照してください)。
4. iDRAC6 ウェブインタフェースまたは RACADM を使用して、iDRAC6 Active Directory のプロパティを設定します(「iDRAC6 ウェブインタフェースを使用して Active Directory と拡張スキーマを設定する方法」または「RACADM を使用した拡張スキーマの Active Directory の設定」を参照してください)。

Active Directory スキーマの拡張

重要: この製品のスキーマ拡張は、前の世代の 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、ディレクトリ上に新しい **Active Directory ユーザーとコンピュータ Microsoft 管理コンソール(MMC)スナップイン** をインストールする必要があります。古いスキーマはこの製品には対応していません。

メモ: 新しいスキーマの拡張または Active Directory ユーザーとコンピュータ スナップインに新しい拡張子をインストールしても、製品の古いバージョンには何の影響もありません。

スキーマエクステンダおよび Active Directory ユーザーとコンピュータ MMC スナップイン拡張子は、『Dell Systems Management Tools and Documentation DVD』にあります。 インストールの詳細については、「Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール」を参照してください。iDRAC6 のスキーマ拡張と、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については、**support.dell.com / manuals** 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: iDRAC6 関連オブジェクトまたは iDRAC6 デバイスオブジェクトを作成する場合は、**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 スキーマを拡張すると、デルの組織単位、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場合は、ドメインフォレストのスキーママスター FSMO(Flexible Single Master Operation)役割所有者のスキーマ 管理 権限が必要です。

次のいずれかの方法でスキーマを拡張できます。

- 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場合は、**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場合は、「Dell Schema Extender の使用」を参照してください。

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

Dell Schema Extender の使用

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

1. **ようこそ** 画面で、**次へ** をクリックします。
2. 警告を読んでから、もう一度 **次へ** をクリックします。
3. **資格情報で現在のログオン使用** 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 を実行する場合は、**次へ** をクリックします。

5. **完了** をクリックします。

スキーマが拡張されます。スキーマ拡張を確認する場合は、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 6-2」～「表 6-7」を参照)。
- 属性(「表 6-8」)

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

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

クラス名	割り当てられたオブジェクト識別番号(OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
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 6-3 dellRacDevice クラス

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

表 6-4 delliDRACAssociationObject クラス

OID	**1.2.840.113556.1.8000.1280.1.7.1.2**
説明	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の間の接続を提供します。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	**dellProductMembers** **dellPrivilegeMember**

表 6-5 dellRAC4Privileges クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
説明	iDRAC6 の権限(認証権限)を定義します。
クラスの種類	補助クラス
SuperClasses	なし
属性	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

表 6-6 dellPrivileges クラス

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

表 6-7 dellProduct クラス

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

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

属性名 / 説明	割り当てられた OID / 構文オブジェクト識別子	単一値
dellPrivilegeMember この属性に属する dellPrivilege オブジェクトのリスト。	1.2.840.113556.1.8000.1280.1.1.2.1 識別名(LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers この役割に属する dellRacDevice および DelliDRACDevice オブジェクトのリスト。この属性は dellAssociationMembers バックワードリンクへのフォワードリンクです。 リンク ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名(LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser ユーザーにデバイスへのログイン権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin ユーザーにデバイスのカード設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin ユーザーにデバイスのユーザー設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser ユーザーにデバイスの仮想コンソール権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser ユーザーにデバイスの仮想メディア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser ユーザーにデバイスのテスト警告ユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion スキーマのアップデートに現在のスキーマバージョンが使用されます。	1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE

dellRacType この属性は 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、iDRAC6 デバイス、ユーザーとユーザーグループ、iDRAC6 関連付け、iDRAC6 権限などを管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『Dell Systems Management Tools and Documentation DVD』を使ってシステム管理ソフトウェアをインストールする場合、インストール手順中に **Active Directory ユーザーとコンピュータ スナップイン** のオプションを選択するとスナップインを拡張できます。システム管理ソフトウェアのインストールの手順については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。64 ビットの Windows オペレーティングシステムでは、スナップインのインストーラは、次の場所にあります。

<DVD ドライブ>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

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

Administrator Pack のインストール

Active Directory iDRAC6 オブジェクトを管理している各システムに、Administrator Pack をインストールする必要があります。Administrator Pack をインストールしないと、コンテナ内の Dell iDRAC6 オブジェクトを表示できません。

詳細については、Active Directory ユーザーとコンピュータスナップインの開始を参照してください。

Active Directory ユーザーとコンピュータスナップインの開始

Active Directory ユーザーとコンピュータスナップインを開くには、以下の手順を実行します。

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

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

   MMC が表示されます。

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

Active Directory への iDRAC6 ユーザーと権限の追加

デルの拡張 Active Directory ユーザーとコンピュータスナップインを使用して、iDRAC6、関連、および権限オブジェクトを作成すると、iDRAC6 のユーザーと権限を追加できます。各オブジェクトタイプを追加するには、次の手順に従います。

- iDRAC6 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
- 関連オブジェクトへのオブジェクトの追加

iDRAC6 デバイスオブジェクトの作成

1. MMC **コンソールルート** ウィンドウでコンテナを右クリックします。

2. **新規**→ **Dell リモート管理オブジェクトの詳細設定** の順に選択します。

   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。この名前は、「iDRAC6 ウェブインタフェースを使用して Active Directory と拡張スキーマを設定する方法」の手順 A で入力する iDRAC6 の名前と同じにする必要があります。

4. **iDRAC デバイスオブジェクト** を選択します。

5. **OK** をクリックします。

権限オブジェクトの作成

メモ: 権限オブジェクトは、その関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。

2. **新規**→ **Dell リモート管理オブジェクトの詳細設定** の順で選択します。

   新規オブジェクト ウィンドウが表示されます。

3. 新しいオブジェクトの名前を入力します。

4. **権限オブジェクト** を選択します。

5. **OK** をクリックします。

6. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。

7. **リモート管理権限** タブをクリックし、ユーザーまたはグループに与える権限を選択します(「表 5-14」を参照)。

関連オブジェクトの作成

メモ: iDRAC6 の関連オブジェクトは、グループ から派生し、その範囲は、ドメインローカル に設定されています。

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。

2. **新規**→ **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。

7. 認証されたユーザーに、作成された関連オブジェクトのアクセス権限を与えます。これには、次の操作を行います。

   a. **管理ツール** → **ADSI の編集** に移動します。**ADSI の編集** ウィンドウが表示されます。

   b. 右ペインで、作成された関連オブジェクトに移動して右クリックし、**プロパティ** を選択します。

   c. **セキュリティ** タブで **追加** をクリックします。

   d. `Authenticated Users` (認証されたユー)ザー を入力し、**名前の確認** をクリックして **OK** をクリックします。**認証されたユーザー** が **グループとユーザー名** のリストに追加されます。

   e. **OK** をクリックします。

関連オブジェクトへのオブジェクトの追加

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーまたはユーザーグループ、権限オブジェクト、iDRAC6 デバイスまたは iDRAC6 デバイスグループ間の関連付けができます。

ユーザーおよび iDRAC6 デバイスのグループを追加できます。デル関連グループとデルに関連しないグループを作成する手順は同じです。

ユーザーまたはユーザーグループの追加

1. **関連オブジェクト** を右クリックし、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限の追加

1. **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。

権限オブジェクト タブをクリックして、iDRAC6 デバイスに認証するときにユーザーまたはユーザーグループの権限を定義する関連付けに、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは 1 つだけです。

iDRAC6 デバイスまたは iDRAC6 デバイスグループの追加

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

1. **製品** タブを選択して **追加** をクリックします。
2. iDRAC6 デバイスまたは iDRAC6 デバイスグループの名前を入力し、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。

定義済みのユーザーまたはユーザーグループが利用できるネットワークに接続している iDRAC6 デバイスを 1 台追加するには、**製品** タブをクリックします。1 つの関連オブジェクトに対して複数の iDRAC6 デバイスを追加できます。

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

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 ウェブインタフェースにログインします。
3. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ→ **ディレクトリサービス** → **Microsoft Active Directory** の順にクリックします。

   Active Directory 概要の画面が表示されます。
4. 画面の下までスクロールし、**Active Directory の設定** をクリックします。

   Active Directory 手順 1 / 4 画面が表示されます。
5. Active Directory サーバーの SSL 証明書を検証するには、**証明書の設定** で **証明書の検証有効** チェックボックスをオンにします。

   Active Directory サーバーの SSL 証明書を検証しない場合は、手順 7 に進んでください。
6. **Active Directory CA 証明書のアップロード** の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照して、**アップロード** をクリックします。

   メモ: フルパス、完全なファイル名、ファイル拡張子を含む絶対ファイルパスを入力する必要があります。

   アップロードした Active Directory CA 証明書の証明書情報は、**現在の Active Directory CA 証明書** セクションに表示されます。
7. **次へ** をクリックします。

   Active Directory の設定と管理 手順 2 / 4 画面が表示されます。
8. **Active Directory 有効** チェックボックスをオンにします。

メモ: このリリースでは、Active directory に拡張スキーマが設定されている場合、スマートカードを使用する 2 要素認証(TFA)はサポートされていません。シングルサインオン(SSO)機能は、標準スキーマと拡張スキーマの両方でサポートされています。

9. **追加** をクリックして、**ユーザードメイン名** を入力します。テキストフィールドにドメイン名を入力して **OK** をクリックします。この手順は省略できます。ユーザードメインのリストを設定した場合は、ウェブインタフェースのログイン画面に表示されます。リストから選択する場合、ユーザー名のみを入力する必要があります。

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

11. **DNS ルックアップドメインコントローラ** オプションを選択し、DNS ルックアップから Active Directory ドメインコントローラを取得します。すでに設定されている場合は、**ドメインコントローラのサーバーアドレス 1～3** は無視されます。**ログインのユーザードメイン** を選択し、ログインユーザーのドメイン名を使って DNS ルックアップを実行します。そうでない場合は、**ドメインを指定する** を選択し、DNS ルックアップに使用するドメイン名を入力します。iDRAC6 は接続が確立されるまで、各アドレス(DNS ルックアップによって返される最初の 4 つのアドレス)に対して、1 つずつ接続を試みます。**拡張スキーマ** を選択した場合、これらは iDRAC6 デバイスオブジェクトと関連オブジェクトが存在するドメインコントローラのアドレスです。**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。

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

12. 指定した Active Directory ドメインコントローラのサーバーアドレスをiDRAC6 に使用させるには、**ドメインコントローラアドレスを指定する** オプションを選択します。DNS ルックアップは実行されません。ドメインコントローラの IP アドレスまたは FQDN を指定します。**ドメインコントローラアドレスを指定する** オプションが選択されている場合、3 つのアドレスのうち、少なくとも 1 つのアドレスが設定されている必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、1 つずつ接続を試みます。**拡張スキーマ** を選択した場合、これらは iDRAC6 デバイスオブジェクトと関連オブジェクトが存在するドメインコントローラのアドレスです。

    メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の **件名** または **代替名** フィールドの値と一致する必要があります。

13. **次へ** をクリックします。

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

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

15. **次へ** をクリックします。

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

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

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

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

18. 画面の下までスクロールし、**テストの設定** をクリックします。

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

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

    テスト結果とテストログが表示されます。詳細については、「設定のテスト」を参照してください。

    メモ: Active Directory ログインをサポートするには、iDRAC6 上で DNS サーバーが正しく設定されている必要があります。**ネットワーク** 画面に移動して(**システム** → **リモートアクセス** → **iDRAC6**→をクリックし、**ネットワーク / セキュリティ** → **ネットワーク** タブの順にクリック)、DNS サーバーを手動で設定するか、DHCP を使用して DNS サーバーを取得します。

これで、拡張スキーマの Active Directory の設定が完了しました。

RACADM を使用した拡張スキーマの Active Directory の設定

ウェブインタフェースではなく、RACADM コマンドラインインタフェース(CLI)を使用して拡張スキーマを備えた iDRAC6 Active Directory 機能を設定する場合は、次のコマンドを使用します。

1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config -g cfgActiveDirectory -o
cfgADRacName <RAC 共通名>

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

racadm config -g cfgActiveDirectory -o cfgADDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

racadm config -g cfgActiveDirectory -o cfgADDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

メモ: 3 つのアドレスのうち、少なくとも 1 つを設定する必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、1 つずつ接続を試みます。拡張スキーマでは、iDRAC6 デバイスが置かれてい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。

SSL ハンドシェイク中に証明書の検証を実行する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

この場合、CA 証明書をアップロードする必要はありません。

SSL ハンドシェイク中に証明書の検証を実行する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

```
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

次の RACADM コマンドの使用は任意選択です。詳細については、「iDRAC6 ファームウェア SSL 証明書のインポート」を参照してください。

```
racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

2. iDRAC6 で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```

3. iDRAC6 で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

   racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <二次 DNS IP アドレス>
   ```

4. iDRAC6 ウェブインタフェースにログインするときにユーザー名の入力だけで済むように、ユーザードメインのリストを設定しておく場合は、次のコマンドを入力します。

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName <ドメインコントローラの完全修飾ドメイン名または IP アドレス> -i <インデックス>
   ```

   1 ～ 40 のインデックス番号で、最大 40 のユーザードメインを設定できます。

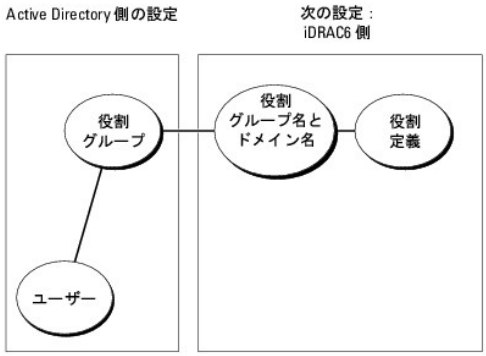
   ユーザードメインの詳細については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。

5. 拡張スキーマの Active Directory 設定を完了するには、**Enter** キーを押します。

標準スキーマの Active Directory の概要

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

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



Active Directory 側では、標準グループオブジェクトが役割グループとして使用されます。iDRAC6 へのアクセス権を持つユーザーは役割グループのメンバーとなります。このユーザーに特定の iDRAC6 カードへのアクセスを与えるには、その iDRAC6 カードで役割グループ名とドメイン名を設定する必要があります。拡張スキーマソリューションとは異なり、役割と権限レベルは Active Directory ではなく各 iDRAC6 カード上で定義されます。各 iDRAC6 につき最大 5 つの役割グループを設定および定義できます。表 6-9 は、デフォルトの役割グループの権限を示しています。

表 6-9 デフォルトのロールグループの権限

役割グループ	デフォルトの権限レベル	許可する権限	ビットマスク
役割グループ 1	なし	**iDRAC へのログイン、iDRAC の設定、ユーザーの設定、ログのクリア、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行**	0x000001ff
役割グループ 2	なし	**iDRAC へのログイン、iDRAC の設定、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行**	0x000000f9
役割グループ 3	なし	iDRAC へのログイン	0x00000001
役割グループ 4	なし	権限の割り当てなし	0x00000000
役割グループ 5	なし	権限の割り当てなし	0x00000000

メモ: ビットマスク値を使用するのは、RACADM で標準スキーマを設定する場合に限ります。

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、役割グループ、およびネストされたグループが同じドメインに属する場合、iDRAC6 で設定する必要が有るのはドメインコントローラのアドレスのみです。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、役割グループ、またはネストされたグループのいずれかが複数ドメインに属する場合は、iDRAC6 でグローバルカタログサーバーのアドレスを設定する必要があります。このようなマルチドメインのシナリオでは、すべての役割グループとネストされたグループ（あれば）がユニバーサルグループタイプであることが必要です。

---

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

Active Directory ユーザーが iDRAC6 にアクセスするためには、まず以下の手順に従って Active Directory を設定する必要があります。

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。Active Directory ユーザーを、iDRAC6 にアクセスする Active Directory グループのメンバーとして追加します。
3. ウェブインタフェースまたは RACADM を使用して、iDRAC6 でグループとドメイン名を設定します（「iDRAC6 ウェブインタフェースを使用して Active Directory を標準スキーマで設定する方法」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）。

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

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 ウェブインタフェースにログインします。
3. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ→ **ディレクトリサービス** → **Microsoft Active Directory** の順にクリックします。

   Active Directory 概要ページが表示されます。
4. 画面の下までスクロールし、**Active Directory の設定** をクリックします。

   Active Directory 手順 1 / 4 画面が表示されます。
5. **証明書の設定** で、**証明書の検証有効** を選択します。
6. **Active Directory CA 証明書のアップロード** の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照して、**アップロード** をクリックします。

   メモ: フルパスおよび完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

   アップロードした Active Directory CA 証明書の証明書情報は、**現在の Active Directory CA 証明書** セクションに表示されます。
7. **次へ** をクリックします。

   Active Directory の設定と管理 手順 2 / 4 画面が表示されます。
8. **Active Directory** を有効にする チェックボックスをオンにします。

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

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

11. **追加** をクリックして、**ユーザードメイン名** を入力します。テキストフィールドにドメイン名を入力して **OK** をクリックします。この手順は省略できます。ユーザードメインのリストを設定した場合は、ウェブインタフェースのログイン画面に表示されます。リストから選択できます。この場合に入力する必要があるのは、ユーザー名のみです。

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

13. **DNS ルックアップドメインコントローラ** オプションを選択し、DNS ルックアップから Active Directory ドメインコントローラを取得します。すでに設定されている場合は、**ドメインコントローラのサーバーアドレス 1～3** は無視されます。**ログインのユーザードメイン** を選択し、ログインユーザーのドメイン名を使って DNS ルックアップを実行します。そうでない場合は、**ドメインを指定する** を選択し、DNS ルックアップに使用するドメイン名を入力します。iDRAC6 は接続が確立されるまで、各アドレス（DNS ルックアップによって返される最初の 4 つのアドレス）に対して、1 つずつ接続を試みます。**標準スキーマ** を選択した場合、これらはユーザーアカウントと役割グループが存在するドメインコントローラのアドレスです。

14. iDRAC6 に指定した Active Directory ドメインコントローラのサーバーアドレスを使用させるには、**ドメインコントローラアドレスを指定する** オプションを選択します。DNS ルックアップは実行されません。ドメインコントローラの IP アドレスまたは FQDN を指定します。**ドメインコントローラアドレスを指定する** オプションが選択されている場合、3 つのアドレスのうち、少なくとも 1 つのアドレスが設定されている必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、1 つずつ接続を試みます。**標準スキーマ** を選択した場合、これらはユーザーアカウントと役割グループが存在するドメインコントローラのアドレスです。

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

15. **次へ** をクリックします。

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

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

17. **次へ** をクリックします。

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

18. Active Directory グローバルカタログサーバーを取得するには、**標準スキーマ設定** で、**DNS でグローバルカタログサーバーをルックアップする** オプションを選択し、DNS ルックアップで使用する **ルートドメイン名** を入力します。すでに設定されている場合は、ドメインコントローラのサーバーアドレス 1～3 は無視されます。iDRAC6 は接続が確立されるまで、各アドレス（DNS ルックアップによって返される最初の 4 つのアドレス）に対して、1 つずつ接続を試みます。ユーザーアカウントと役割グループが異なるドメインにある場合に限り、標準スキーマにグローバルカタログサーバーが必要です。

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

19. **グローバルカタログサーバーのアドレスの指定** オプションを選択し、グローバルカタログサーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。DNS ルックアップは実行されません。3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、1 つずつ接続を試みます。

    メモ: グローバルカタログサーバーは、ユーザーアカウントと役割グループがそれぞれ異なるドメインに属する標準スキーマの場合においてのみ、必要となります。また、このようなマルチドメインのシナリオでは、ユニバーサルグループのみを使用できます。iDRAC6 ウェブ GUI を使用して Active Directory を設定する場合は、ユーザーとグループが同じドメインでもグローバルアドレスを入力する必要があります。

20. 役割グループを追加する場合は、**役割グループ** ボタンをクリックします。

    役割グループの設定 手順 4b / 4 画面が表示されます。

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

22. **グループドメイン** を入力します。**グループドメイン** はフォレストのルートドメインの完全修飾名です。

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

    メモ: 権限を変更すると、既存の役割グループの権限（システム管理者、パワーユーザー、ゲストユーザー）は、変更した権限に基づいてカスタムグループまたは適切な役割グループの権限に変更されます。

24. **OK** をクリックして、役割グループの設定を保存します。

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

25. ロールグループを追加するには、手順 20 から 手順 24 の手順を繰り返します。

26. **完了** をクリックしてから、**終了** をクリックします。

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

27. 画面の下までスクロールし、**テストの設定** をクリックします。

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

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

    テスト結果とテストログが表示されます。詳細については、「設定のテスト」を参照してください。

    メモ: Active Directory ログインをサポートするには、iDRAC6 上で DNS サーバーが正しく設定されている必要があります。**ネットワーク** 画面に移動して(**システム** → **リモートアクセス** → **iDRAC6** をクリックし、**ネットワーク / セキュリティ** → **ネットワーク** タブの順にクリック)、DNS サーバーを手動で設定するか、DHCP を使用して DNS サーバーを取得します。

これで、標準スキーマの Active Directory の設定が完了しました。

RACADM を使用した標準スキーマの Active Directory の設定

ウェブインタフェースではなく、RACADM CLI を使用して iDRAC6 Active Directory 機能を標準スキーマで設定するには、次のコマンドを使用します。

1. コマンドプロンプトを開き、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1

   racadm config -g cfgActiveDirectory -o cfgADType 2

   racadm config -g cfgStandardSchema -i <インデックス> -o
   cfgSSADRoleGroupName <役割グループの共通名>

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

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

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

   ```
   racadm config -g cfgActiveDirectory -o cfgADDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

   racadm config -g cfgActiveDirectory -o cfgADDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

   racadm config -g cfgActiveDirectory -o cfgADDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
   ```

   メモ: ドメインの FQDN ではなく、ドメインコントローラの FQDN を入力します。たとえば、dell.com ではなく、servername.dell.com と入力します。

   メモ: 3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、1 つずつ接続を試みます。標準スキーマでは、ユーザーアカウントと役割グループが存在するドメインコントローラのアドレスとなります。

   ```
   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
   ```

   メモ: グローバルカタログサーバーは、ユーザーアカウントと役割グループがそれぞれ異なるドメインに属する標準スキーマの場合においてのみ、必要となります。また、このようなマルチドメインのシナリオでは、ユニバーサルグループのみを使用できます。

   メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書の **件名** または **代替名** フィールドの値と一致する必要があります。

   SSL 中に証明書の検証を実行する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
   ```

   この場合、認証局(CA)の証明書をアップロードする必要はありません。

   SSL ハンドシェイク中に証明書の検証を実行する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
   ```

   この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

   ```
   racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
   ```

   次の RACADM コマンドは任意で実行できます。詳細については、「iDRAC6 ファームウェア SSL 証明書のインポート」を参照してください。

   ```
   racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
   ```

2. iDRAC6 上で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. iDRAC6 上で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>

racadm config -g cfgLanNetworking -o cfgDNSServer1 <二次 DNS IP アドレス>
```

4. ウェブインタフェースにログインするときにユーザー名だけの入力で済むように、ユーザードメインのリストを設定しておく場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName <ドメインコントローラの完全修飾ドメイン名または IP アドレス> -i <インデックス>
```

1 から 40 のインデックス番号で、最大 40 のユーザードメインを設定できます。

ユーザードメインの詳細については、「Microsoft Active Directory での iDRAC6 の使用」を参照してください。

設定のテスト

設定が正常に機能するかを確認する場合や、Active Directory へのログイン失敗の問題を診断する必要がある場合は、iDRAC6 ウェブインタフェースから設定をテストできます。

iDRAC6 ウェブインタフェースで設定を完了したら、画面下部の **設定のテスト** をクリックします。テストを実行する場合は、テストユーザーの名前（例：**username@domain.com**）とパスワードを入力する必要があります。設定によっては、テストのすべての手順を実行し、各手順の結果が表示されるまでに時間がかかる場合があります。結果画面の下部に詳細なテストログが表示されます。

いずれかの手順にエラーが発生した場合は、テストログで詳細を確認し、問題と解決策を特定します。一般的なエラーについては、「よくあるお問い合わせ（FAQ）」を参照してください。

設定を変更する場合は、**Active Directory** タブをクリックし、手順に従って設定に変更を加えます。

---

iDRAC6 の LDAP ディレクトリサービスとの使用

iDRAC6 は、ライトウェイトディレクトリアクセスプロトコル（LDAP）ベースの認証をサポートする汎用ソリューションを提供します。この機能を使用する場合は、ディレクトリサービスのスキーマ拡張は必要ありません。

iDRAC6 LDAP の実装を汎用的なものにするには、異なるディレクトリサービスの共通点によってユーザーをグループ化した後、ユーザーとグループの関係をマッピングします。ディレクトリサービス固有の処置がスキーマとなります。たとえば、グループ、ユーザー、およびユーザーとグループの間のリンクの属性名が異なる場合があります。これらの処置は iDRAC6 で設定できます。

ログイン構文（ディレクトリユーザーとローカルユーザーの比較）

Active Directory とは異なり、LDAP ユーザーをローカルユーザーと区別するのに特殊文字（"@"、"\"、"/"）は使用しません。ログインユーザーには、ドメイン名を除いたユーザー名を入力する必要があります。iDRAC6 はユーザー名を入力したとおりに受け入れ、ユーザー名とユーザードメインを分割しません。汎用 LDAP が有効である場合、iDRAC6 は最初にユーザーをディレクトリユーザーとしてログインしようと試みます。これに失敗すると、ローカルユーザーのルックアップが有効になります。

メモ: Active Directory のログイン構文には動作上の変更はありません。汎用 LDAP が有効な場合、GUI ログインページは、ドロップ_ウンメニューに **この iDRAC** のみを表示します。

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

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

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 ウェブインタフェースにログインします。
3. **システム** ツリーを展開し、**リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ→ **ディレクトリサービス** → **汎用 LDAP ディレクトリサービス** の順にクリックします。
4. **汎用 LDAP の設定と管理** ページには、現在の iDRAC6 の汎用 LDAP 設定が表示されます。**汎用 LDAP 設定と管理** ページにスクロールし、**汎用 LDAP の設定** をクリックします。

   メモ: このリリースでは、標準スキーマの Active Directory（SSAD）（拡張なし）のみがサポートされています。

   汎用 LDAP の設定と管理 手順 1 / 3 ページが表示されます。このページを使用して、汎用 LDAP サーバーと通信するときに SSL 接続の起動中に使用するデジタル証明書を設定します。これらの通信には LDAP オーバー SSL（LDAPS）を使用します。証明書の検証機能を有効にするには、SSL 接続の起動中に LDAP サーバーが使用する証明書を発行した認証局（CA）の証明書をアップロードします。CA の証明書は、SSL の起動中に LDAP サーバーによって提供された証明書の信頼性を検証するのに使用します。

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

5. 証明書の検証を有効にするには、**証明書の設定** の下の **証明書の検証を有効にする** を選択します。有効である場合、iDRAC6 は CA 証明書を使ってセキュアソケットレイヤ(SSL)ハンドシェイク中に LDAP サーバーの証明書を検証します。無効である場合は、SSL ハンドシェイクの証明書の検証手順をスキップします。テスト中またはシステム管理者が SSL 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を信頼する場合は、証明書の検証機能を無効にできます。

   注意: 証明書の生成中に LDAP サーバー証明書の件名フィールドで、CN = open LDAP FQDN が設定されている(CN= openldap.lab など)ことを確認します。証明書の検証に行うには、サーバー証明書の CN フィールドの値が iDRAC6 の LDAP サーバーアドレス フィールドの値と一致する必要があります。

6. **ディレクトリサービスの CA 証明書のアップロード** の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照します。

   メモ: フルパスと正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

7. **アップロード** をNリックします。

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

8. **次へ** をクリックして、**汎用 LDAP の設定と管理 手順 2 / 3** ページへ移動します。このページを使用して、汎用 LDAP サーバーとユーザーアカウントに関する位置情報を設定します。

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

9. **汎用 LDAP を有効にする** を選択します。

   メモ: このリリースでは、ネストされたグループはサポートされていません。ファームウェアはユーザー DN に一致するグループの直接メンバーを検索します。また、シングルドメインのみがサポートされています。クロスドメインはサポートされていません。

10. グループメンバーとして識別名(DN)を使用する場合は、**グループメンバーシップの検索に識別名を使用する** オプションを選択します。iDRAC6 はディレクトリから取得しいたユーザー DN をグループのメンバーと比較します。このチェックボックスがオフになっている場合は、ログインユーザーが指定したユーザー名がグループのメンバーと比較されます。

11. **LDAP サーバーアドレス** フィールドに、LDAP サーバーの FQDN または IP アドレスを入力します。同じドメインに使用する複数の冗長 LDAP サーバーを指定する場合は、すべてのサーバーのリストをカンマ区切りで入力します。iDRAC6 は接続を確立できるまで、各サーバーへの接続を順番に試みます。

12. **LDAP サーバーポート** フィールドに LDAP オーバー SSL に使用するポートを入力します。デフォルト値は 636 です。

13. **バインド DN** フィールドに、ログインユーザーの DN を検索するときにサーバーにバインドするユーザーの DN を入力します。指定しないと、匿名のバインドが使用されます。

14. 使用する **バインドパスワード** を **バインド ID** と一緒に入力します。これは、匿名のバインドを使用できない場合に必要です。

15. **検索するベース DN** フィールドに、すべての検索を開始するディレクトリのブランチの DN を入力します。

16. **ユーザーログインの属性** フィールドに、検索するユーザー属性を入力します。デフォルトは UID です。この値を選択したベース DN 内で一意になるように設定することをお勧めします。そうしない場合は、ログインユーザーが一意になるように検索フィルタを設定する必要があります。属性と検索フィルタを組み合わせて検索を行った後でユーザー DN を一意に識別できない場合は、ログインに失敗します。

17. **グループメンバーシップの属性** フィールドに、グループメンバーシップの確認に使用する LDAP 属性を指定します。これは、グループクラスの属性です。指定されていない場合は、member 属性と uniquemember 属性が使用されます。

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

19. **次へ** をクリックして、**汎用 LDAP の設定と管理 手順 3a / 3** ページへ移動します。このページを使用して、ユーザーを認証する権限グループを設定します。汎用 LDAP が有効である場合は、役割グループを使って iDRAC6 ユーザーの認証ポリシーを指定します。

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

    汎用 LDAP の設定と管理 手順 3b / 3 ページが表示されます。このページを使用して、ユーザーの認証ポリシーを制御する各役割グループを設定します。

21. iDRAC6 に関連付けられた汎用 LDAP ディレクトリサービスの役割グループを識別する **グループ識別名(DN)** 入力します。

22. **役割グループの権限** セクションで、**役割グループの権限レベル** を選択して、グループに関連付けられた権限を指定します。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権限が選択されます。

23. **適用** をクリックして、役割グループの設定を保存します。

    役割グループの設定が表示されている **汎用 LDAP の設定と管理 手順 3a / 3** ページに自動的に戻ります。

24. 必要に応じて、追加の役割グループを設定します。

25. **汎用 LDAP の設定と管理** 概要**ページ**に戻るには、**完了** をクリックします。

26. 汎用 LDAP 設定を確認するには、**設定のテスト** をクリックします。

27. LDAP 設定をテストするのに選択したディレクトリユーザーのユーザー名とパスワードを入力します。フォーマットは使用する ユーザーログインの属性 によって異なり、入力したユーザー名は選択した属性に一致する必要があります。

    メモ: 証明書の検証を有効にする を選択して LDAP の設定をテストする場合、LDAP サーバーは IP アドレスではなく、FQDN で識別される必要があります。IP アドレスで LDAP サーバーが識別される場合、iDRAC6 が LDAP サーバーと通信できないため、証明書の検証は失敗します。

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

よくあるお問い合わせ（FAQ）

Active Directory ログインの問題

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

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

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

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

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

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

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

iDRAC6 のウェブインタフェースで診断ツールが提供されています。

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

   Active Directory 概要の画面が表示されます。
3. 画面の下までスクロールし、**テストの設定** をクリックします。

   Active Directory 設定のテスト 画面が表示されます。
4. テストユーザー名とパスワードを入力し、**テストの開始** をクリックします。

   iDRAC6 は、順を追ってテストを実行し、各手順の結果を表示します。また、iDRAC6 は問題解決に役立つ詳細なテスト結果もログに記録します。

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

証明書の検証を有効にしましたが、Active Directory のログインに失敗しました。GUI から診断を実行しましたが、テスト結果に次のエラーメッセージが表示されました。何が問題で、どうすれば修復できるでしょうか。

```
ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. 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. (エラー: LDAP サーバーと通信できません、エラー:14090086:SSL ルーチン:SSL3_GET_SERVER_CERTIFICATE:証明書の検証に失敗しました: iDRAC に正しい認証局（CA）証明書がアップロードされていることを確認してください。iDRAC の日付が証明書の有効期限内かどうか、また iDRAC で設定されたドメインコントローラのアドレスがディレクトリサーバーの証明書の件名と一致するかどうか確認してください。)
```

証明書の検証が有効になっていると、iDRAC6 がディレクトリサーバーとの SSL 接続を確立したときに、iDRAC6 はアップロードされた CA 証明書を使用してディレクトリサーバーの証明書を検証します。認証の検証が失敗する最も一般的な理由として、次が挙げられます。

- 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ない。iDRAC6 の日付と証明書の有効期限を確認してください。
- 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、「ドメインコントローラのアドレスに IP アドレスを使用していますが、証明書の検証に失敗しました。何が問題なのでしょうか。」を参照してください。
  - FQDN を使用している場合は、ドメインの FQDN ではなく、ドメインコントローラの FQDN を使用していることを確認してください。たとえば、example.com ではなく、servername.example.com を使用します。

Active Directory を使用して iDRAC6 にログインできない場合は、何を確認すればいいですか。

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

次に、テスト結果で特定される問題を修正します。詳細については、「設定のテスト」を参照してください。

ほとんどの一般的な問題については、本項で説明します。なお、一般的には、次の事項を確認してください。

1. ログインに NetBIOS 名でなく、正しいユーザードメイン名が使用されていることを確認します。
2. ローカル iDRAC6 ユーザーアカウントがある場合は、ローカルの資格情報を使用して iDRAC6 にログインします。
   a. **Active Directory の設定と管理 手順 2 / 4** ページで **Active Directory 有効** チェックボックスがオンであることを確認します。
   b. 証明書の検証を有効にしている場合は、iDRAC6 に正しい Active Directory ルート CA 証明書をアップロードしたことを確認します。証明書は**現在の Active Directory CA 証明書** 領域に表示されます。iDRAC6 の日時が CA 証明書の有効期限内であることを確認します。
   c. 拡張スキーマを使用している場合は、**iDRAC6 名** と **iDRAC6 ドメイン名** が Active Directory の環境設定と一致していることを確認します。

      標準スキーマを使用している場合は、**グループ名** と **グループドメイン** が Active Directory の設定と一致することを確認します。
   d. **ネットワーク** 画面に移動します。**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ**→**ネットワーク** の順に選択します。DNS の設定が正しいことを確認します。
   e. ドメインコントローラの SSL 証明書を調べて、iDRAC6 の日時が 証明書の有効期限内であることを確認します。

Active Directory 証明書の検証

ドメインコントローラのアドレスに IP アドレスを使用していますが、証明書の検証に失敗しました。何が問題なのでしょうか。

ドメインコントローラ証明書の 件名または代替名 フィールドを確認してください。通常、Active Directory はドメインコントローラ証明書の 件名または代替名 フィールドにドメインコントローラの IP アドレスではなく、ホスト名を利用します。次のいずれかの処置を実施することで、問題を解決できます。

- サーバー証明書の件名または件名の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ラ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。
- iDRAC6 で設定された IP アドレスと一致するように、件名または代替名に IP アドレスを使用するようサーバー証明書を再発行します。
- SSL ハンドシェイク時に証明書の検証がなくても、このドメインコントローラを信頼する場合は、証明書の検証を無効にします。

iDRAC6 で、証明書の検証がデフォルトで有効になっているのはなぜですか。

iDRAC6 は、接続先となるドメインコントローラの身元を確認するために、強力なセキュリティ対策を実施しています。証明書を検証しないと、ハッカーはドメインコントローラになりすまし、SSL 接続を乗っ取る危険があります。証明書の検証なしに、自分のセキュリティ境界内のドメインコントローラをすべて信頼する場合は、GUI または CLI を使用して無効にすることもできます。

拡張および標準スキーマ

マルチドメイン環境において拡張スキーマを使用しています。ドメインコントローラのアドレスは、どのように設定すればいいですか。

iDRAC6 オブジェクトが存在するドメインにサービスを提供しているドメインコントローラのホスト名（FQDN）または IP アドレスを使用します。

グローバルカタログアドレスを設定する必要はありますか。

拡張スキーマを使用している場合、拡張スキーマで使用されないグローバルカタログアドレスを設定できません。

標準スキーマを使用し、ユーザーと役割グループが異なるドメインに属する場合は、グローバルカタログアドレスを設定する必要があります。この場合は、ユニバーサルグループしか使用できません。

標準スキーマを使用し、すべてのユーザーと役割グループが同じドメインに属する場合は、グローバルカタログアドレスを設定する必要はありません。

標準スキーマクエリの仕組みを教えてください。

iDRAC6 はまず、設定されたドメインコントローラアドレスに接続します。ユーザーおよび役割グループがそのドメインに属する場合は、権限が保存されます。

グローバルコントローラアドレスが設定されている場合、iDRAC6 は継続してグローバルカタログをクエリします。グローバルカタログから追加の権限が取得された場合、これらの権限は上乗せされます。

その他

iDRAC6 は、常に LDAP オーバー SSL を使用しますか。

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

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

iDRAC6 は NetBIOS 名をサポートしていますか。

このリリースでは、サポートされていません。

目次ページに戻る

目次ページに戻る

iDRAC6 へのシングルサインオンとスマートカードログインの設定

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

本項では、ローカルユーザーおよび Active Directory ユーザーのためのスマートログインと、Active Directory ユーザーのためのシングルサインオン(SSO)ログインを iDRAC6 に設定する方法を説明します。

iDRAC6 は Kerberos ベースの Active Directory 認証を使用して、Active Directory スマートカードログインとシングルサインオン(SSO)ログインをサポートしています。

Kerberos 認証について

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ようにするネットワーク認証プロトコルです。これは、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することで、達成されます。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、スマートカードベースの 2 要素認証(TFA)がActive Directory ログインを有効にするための資格情報として使用されます。

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

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>
```

Active Directory SSO とスマートカード認証の必要条件

Active Directory SSO 認証とスマートカード認証に必要な条件は、以下のとおりです。

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

  詳細については、iDRAC6 オンラインヘルプ を参照してください。
- これら 2 種類の新しい認証方式をサポートするために、iDRAC6 は Windows Kerberos ネットワークで Kerberos サービスとして 自動的に有効になる設定をサポートしています。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、サービスプリンシパル名(SPN)のユーザーアカウントへのバインドを作成し、信頼情報を MIT 形式の Kerberos keytab ファイルにエクスポートするのに使用します。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、サーバーと KDC の間の情報を暗号化するための暗号キーが含まれています。ktpass ツールを使用すると、Kerberos 認証をサポートする UNIX ベースのサービスで、Windows Server の Kerberos KDC サービスによって提供される相互運用性機能を使用できます。

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

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

  たとえば、次の **ktpass** コマンドを使用すると、Kerberos keytab ファイルを作成できます。

  ```
  C:\> ktpass.exe -princ HTTP/idracname.domainname.com@DOMAINNAME.COM -mapuser DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5 -ptype
  ```

KRB5_NT_PRINCIPAL -pass <パスワード> +DesOnly -out c:\krbkeytab

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

上記のコマンドが正しく実行されたら、次のコマンドを実行します。

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

iDRAC6 が Kerberos 認証に使用する暗号タイプは DES-CBC-MD5 です。プリンシパルタイプは KRB5_NT_PRINCIPAL です。サービスプリンシパル名のマップ先となるユーザーアカウントのプロパティで、このアカウントプロパティの「DES 使用」暗号化タイプが有効になっている必要があります。

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

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

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

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

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

- iDRAC6 の時刻が Active Directory ドメインコントローラと同期していることが必要です。

Active Directory SSO を有効にするためのブラウザ設定

Internet Explorer のブラウザ設定を指定するには、以下の手順を実行します。

1. Internet Explorer ブラウザを開きます。
2. **ツール**→ **インターネットオプション**→ **セキュリティ**→**ローカルイトラネット** の順に選択します。
3. **サイト** をクリックします。
4. 以下のオプションのみを選択します。
   - ほかのゾーンにないローカル（イントラネット）のサイトをすべて含める
   - プロキシサーバーを使用しないサイトをすべて含める
5. **詳細設定** をクリックします。
6. SSO 設定の一部である iDRAC インスタンスに使用される関連ドメイン名をすべて追加します（たとえば、myhost.example.com）。
7. **Close**（閉じる）をクリックして **OK** をクリックします。
8. **OK** をクリックします。

Firefox のブラウザ設定を指定するには、以下の手順を実行します。

1. Firefox Web ブラウザを開きます。
2. アドレスバーに about:config と入力します。
3. **Filter** で network.negotiate と入力します。
4. network.negotiate-auth.trusted-uris に iDRAC の名前を追加します（コンマ区切りのリスト）。
5. network.negotiate-auth.trusted-uris に iDRAC の名前を追加します（コンマ区切りのリスト）。

Active Directory SSO の使用

iDRAC6 が Kerberos（ネットワーク認証プロトコルの 1 つ）を使用できるようにして、シングルサインオンを有効にできます。iDRAC6 に Active Directory シングルサインオン機能の使用を設定する方法については、「Active Directory SSO とスマートカード認証の必要条件」を参照してください。

iDRAC6 への SSO 使用の設定

1. サポートされているウェブブラウザのウィンドウを開きます。

2. iDRAC6 ウェブインタフェースにログインします。

3. システムツリーで、**システム** → **リモートアクセス**→ **iDRAC6** → **ネットワーク / セキュリティ** タブ→ **ネットワーク** の順に選択します。**ネットワーク** ページで、**DNS iDRAC6 名** が正しく、iDRAC6 の完全修飾ドメイン名に使用されている名前と同じかどうか確認します。

4. システムツリーで、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ→ **ディレクトリサービス** → **Microsoft Active Directory** の順でクリックします。

   Active Directory 概要の画面が表示されます。

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

   Active Directory の設定と管理のステップ 1 / 4 画面が表示されます。

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

   Active Directory サーバーの SSL 証明書を検証しない場合は、このステップを実行せずに「手順 8」に進んでください。

7. **Active Directory CA 証明書のアップロード** の下に、証明書のファイルパスを入力するか、証明書ファイルの場所を参照して、**アップロード** をクリックします。

   メモ: フルパスおよび完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

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

8. **次へ** をクリックします。

   Active Directory の設定と管理のステップ 2 / 4 画面が表示されます。

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

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

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

    iDRAC6 にシングルサインオン(SSO)の使用を設定する前に、必ず以下の操作を実行してください。

    a. Active Directory サーバーで、デバイスオブジェクト、特権オブジェクト、および関連オブジェクトを作成しておく。

    b. 作成した特権オブジェクトにアクセス権を設定する。管理者権限はセキュリティチェックを通過するので、提供しないことをお勧めします。

    c. 関連オブジェクトを使用して、デバイスオブジェクトと特権オブジェクトを関連付ける。

    d. デバイスオブジェクトに先行 SSO ユーザー(ログインユーザー)を追加する。

    e. 作成した関連オブジェクトにアクセスするためのアクセス権を 認証済みユーザー にアクセス権を与える。

       以上の手順を実行する方法については、「Active Directory への iDRAC6 ユーザーと権限の追加」を参照してください。

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

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

11. **ユーザードメイン名** を追加し、ドメインコントローラサーバーアドレスの IP アドレスを入力します。**DNS でドメインコントローラをルックアップする** または **ドメインコントローラアドレスを指定する** のいずれかを選択します。**次へ** を選択します。**Active Directory の設定と管理のステップ 3 / 4** 画面が表示されます。

12. **標準スキーマ** または **拡張スキーマ** のオプションを選択して、**次へ** をクリックします。

    標準スキーマ を選択した場合は、ステップ 13 に進んでください。**拡張スキーマ** を選択した場合は、ステップ 14 に進んでください。

13. 標準スキーマの場合は、以下の手順を実行します。

    a. **Active Directory ステップ 4a / 4** 画面で、**グローバルカタログサーバー** の IP アドレスを入力するか、**DNS でグローバルカタログサーバーをルックアップする** オプションを選択し、Active Directory グローバルカタログサーバーを取得するために DNS ルックアップで使用する **ルートドメイン名** を入力します。

    b. 役割グループのいずれかをクリックし、有効な Active Directory ユーザーが属している役割グループの情報を追加します。**Active Directory ステップ 4b / 4** 画面が表示されます。

    c. 役割グループ名、グループのドメイン、役割グループの権限レベル、および必要な権限を入力して、完了をクリックします。Configuration set successfully(設定が完了しました)というメッセージが表示されます。**OK** をクリックします。ステップ **4a / 4** 画面に、作成したグループ名、グループのドメイン、およびグループの権限レベルが表示されます。

d. **完了** をクリックします。完了メッセージが表示されます。

14. 拡張スキーマの場合は、**Active Directory ステップ 4 / 4** 画面で、**iDRAC6 名** と **iDRAC6 ドメイン名** を入力して **完了** をクリックします。完了メッセージが表示されます。

SSO による iDRAC6 へのログイン

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

   http: / / idracname.domain.com

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

スマートカード認証の設定

iDRAC6 では、**スマートカードログオン** を有効にすると、2 要素認証（TFA）機能がサポートされます。

従来の認証方式では、ユーザーの認証にユーザー名とパスワードを使用しますが、これは最小レベルのセキュリティを提供します。

一方 TFA は、ユーザーに 2 つの認証要素、つまり使用している装置（スマートカード、物理デバイス）と知っている情報（パスワードや PIN などのシークレットコード）の入力を義務付けて、より高いレベルのセキュリティを実現します。

2 要素認証では、ユーザーが両方の要素を提供して身元を証明する必要があります。

---

iDRAC6 へのスマートカードログインの設定

ウェブインタフェースから iDRAC6 スマートカードログオン機能を有効にするには、以下の手順を実行してください。

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

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

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

メモ: ブラウザの設定によっては、この機能を初めて使うときに、スマートカードリーダー ActiveX プラグインをダウンロードしてインストールするように要求される場合があります。

1. https を使用して iDRAC6 にログインします。

   https://<IP アドレス>

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

   https://<IP アドレス>:<ポート番号>

   <IP アドレス> は iDRAC6 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

   iDRAC6 ログインページが表示され、スマートカードの挿入を要求されます。

2. スマートカードを挿入します。

3. PIN を入力して、**ログイン** をクリックします。

   Active Directory に設定した資格情報で iDRAC6 にログインします。

   メモ: スマートカードをリーダーに入れたままにしなくても、ログイン状態を継続できます。

よくあるお問い合わせ - シングルサインオン

Windows 7 と Windows Server 2008 R2 でシングルサインのログインに失敗します。

Windows 7 と Windows Server 2008 R2 で暗号化タイプ DES_CBC_CRC と DES_CBC_MD5 を有効にする必要があります。これらの暗号化タイプを有効にするには、以下の手順を実行します。

1. 管理者または管理者権限のあるユーザーとしてログインします。
2. **スタート** から、**gpedit** を実行します。**ローカルグループポリーエディタ** ウィンドウが表示されます。
3. **ローカルコンピュータ設定→Windows 設定→セキュリティ設定→ ローカルポリシー→セキュリティオプション** の順に選択します。
4. **ネットワークセキュリティ: kerberos に許可される暗号化方式の設定** を右クリックして、**プロパティ** を選択します。
5. 全てのオプションを有効にします。
6. **OK** をクリックします。

---

iDRAC6 へのスマートカードログインのトラブルシューティング

以下は、スマートカードにアクセスできないときのデバッグに役立つヒントです。

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

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

ActiveX プラグインがスマートカードリーダーを検出しません

スマートカードが Microsoft Windows オペレーティングシステムでサポートされていることを確認します。Windows がサポートしているスマートカード暗号サービスプロバイダ(CSP)の数は限られています。

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

間違ったスマートカード PIN

間違った PIN でログインを試みた回数が多すぎるためにスマートカードがロックアウトされたかどうかをチェックします。このような場合は、新しいスマートカードの入手方法について、組織のスマートカ

ード発行者に問い合わせてください。

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

- Active Directory ユーザーとして iDRAC6 にログインできない場合は、スマートカードログオンを有効にしないで iDRAC6 にログインしてみてください。スマートカードログオンを無効にするには、RACADM で次のコマンドを使用します。

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

- 64 ビット Windows プラットフォームの場合、64 ビットバージョンの「Microsoft Visual C++ 2005 再頒布可能パッケージ」がインストールされていると、iDRAC6 認証プラグインが正しくインストールされません。プラグインが正常にインストールされて実行されるように、32 ビットバージョンの「Microsoft Visual C++ 2005 再配布可能パッケージ」をインストールする必要があります。

- エラーメッセージ "Not able to load the Smart Card Plug-in. Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in" (「スマートカードプラグインをロードできません。IE の設定を確認するか、スマートカードプラグインを使用する権限がない可能性があります」)と表示された場合は、Microsoft Visual C++ 2005 再配布可能パッケージをインストールしてください。このファイルは Microsoft のウェブサイト **www.microsoft.com** にあります。C++ 再配布可能パッケージの 2 種類の配布バージョンがテストされ、Dell スマートカードプラグインをロードできます。

表 7-1 C++ 再配布可能パッケージの配布バージョン

再配布パッケージのファイル名	Version(バージョン)	リリース日	Size(サイズ)	説明
vcredist_x86.exe	6.0.2900.2180	2006 年 3 月 21 日	2.56 MB	MS Redistributable 2005
vcredist_x86.exe	9.0.21022.8	2007 年 11 月 7 日	1.73 MB	MS Redistributable 2008

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

目次ページに戻る

目次ページに戻る

管理下サーバーの設定と正常性の表示

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

システム概要

システム概要 ページでは、システムの正常性やその他の基本的な iDRAC6 情報を一目で把握できるうえ、システムの正常性やその他の情報ページにアクセスするためのリンクもあります。また、このページから共通のタスクをすばやく起動したり、システムイベントログ(SEL)にログされている最近のイベントを表示したりすることもできます。

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

システム詳細

システム詳細 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。

- メインシステムエンクロージャ
- Integrated Dell Remote Access Controller 6(iDRAC6) - Enterprise

メインシステムエンクロージャ

システム情報

iDRAC6 のウェブインタフェースのこのセクションは、管理下サーバーについて以下の基本情報を提供します。

- 説明 - 管理下サーバーのモデル番号または名前
- BIOS バージョン - 管理下サーバーの BIOS のバージョン番号
- サービスタグ - サーバーのサービスタグ番号
- ホスト名 - 管理下サーバーに関連付けられている DNS ホスト名
- OS 名 - 管理下サーバーにインストールされているオペレーティングシステムの名前

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

- システムリビジョン - シャーシのリビジョン番号。

I/O メザニンカード

iDRAC6 ウェブインタフェースのこのセクションでは、管理下サーバーにインストールされている I/O メザニンカードについて、以下の情報を提供します。

- 接続 - 管理下サーバーにインストールされている I/O メザニンカードのリスト。このリストには、拡張カードをサポートする I/O メザニン カードも表示されます。
- 存在状態 - メザニンカードがあるかないか、または別のファブリックのメザニンカードスロットの拡張かどうかを示します。
- カードタイプ - インストールされているメザニンカード / 接続の物理タイプ
- モデル名 - インストールされているメザニンカードのモデル番号、タイプ、または説明

内蔵ストレージカード

iDRAC6 ウェブインタフェースのこのセクションでは、管理下サーバーにインストールされている内蔵ストレージコントローラカードについて、以下の情報を提供します。

- カードタイプ - 搭載されているストレージカードのモデル名を表示します(例:SAS6/iR)。

内蔵ネットワークカード

iDRAC6 ウェブインタフェースのこのセクションでは、管理下サーバーにインストールされている内蔵ストレージコントローラカードについて、以下の情報を提供します。これは、該当するプラットフォームについてのみ表示されます。

- カードタイプ - ボードに内蔵されているネットワークカードの種類(ギガビット イーサネットなど)を表示します。
- モデル名 - 内蔵ネットワークカードのモデル名を表示します。

内蔵ネットワークカードの詳細については、デルサポートサイト **support.dell.com / manuals** にある『ハードウェアオーナーズマニュアル』を参照してください。

自動リカバリ

iDRAC6 ウェブインタフェースのこのセクションでは、Open Manage Server Administrator で設定された管理下サーバーの自動リカバリ機能の現在の処理モードについて、以下の情報を提供します。

- リカバリ処置 - システム障害やハングが検出されたときに実行する処置。使用できる処置は、**処置なし**、**ハードリセット**、**パワーダウン**、または**パワーサイクル** です。
- 初期カウントダウン - システムハング検出後、iDRAC6 がリカバリ処置を実行するまでの時間(秒単位)。
- 現在のカウントダウン - カウントダウンタイマーの現在値(秒単位)。

Integrated Dell Remote Access Controller 6(iDRAC6) - Enterprise

iDRAC6 情報

iDRAC6 ウェブインタフェースのこのセクションでは、iDRAC6 自体について、以下の情報を提供します。

- 日付 / 時刻 - iDRAC6 の現在の日付と時刻(前回のページ更新時点)を表示します。
- ファームウェアのバージョン - 管理下サーバーにインストールされている iDRAC6 ファームウェアの現在のバージョンを表示します。
- CPLD バージョン - Complex Programmable Logic Device(CPLD)ボードのバージョンを表示します。
- 拡張 CPLD バージョン - 拡張ボード CPLD のバージョンを表示します。
- ファームウェアのアップデート - iDRAC6 ファームウェアが最後に正しくアップデートされた日時を表示します。
- MAC アドレス - iDRAC6 の LOM(LAN on Motherboard)ネットワークインタフェースコントローラに関連付けられている MAC アドレスを表示します。

IPv4 の設定

- 有効 - IPv4 プロトコルのサポートが有効か無効かを表示します。

  メモ: IPv4 プロトコルオプションはデフォルトで有効になっています。

- DHCP 有効 - iDRAC6 が DHCP サーバーからその IP アドレスと関連情報をフェッチするように設定されている場合に有効になります。
- IP アドレス - iDRAC6 (管理下サーバーではない)に関連付けられている IP アドレスを表示します。
- サブネットマスク - iDRAC6 用に設定されたTCP/IP サブネットマスクを表示します。
- ゲートウェイ - iDRAC6 用に設定されたネットワークゲートウェイの IP アドレスを表示します。
- DHCP を使用して DNS サーバーアドレスを取得する - DNS サーバーアドレスの取得に DHCP を使用するかどうかを表示します。
- 優先 DNS サーバー - 現在アクティブなプライマリ DNS サーバーを表示します。
- 代替 DNS サーバー - 代替 DNS サーバーアドレスを表示します。

IPv6 の設定

- 有効 - IPv6 プロトコルのサポートが有効か無効かを表示します。
- 自動設定有効 - 自動設定が有効か無効かを表示します。
- リンクのローカルアドレス - iDRAC6 NIC の IPv6 アドレスを表示します。
- IPv6 アドレス 1〜16 - iDRAC6 NIC の IPv6 アドレスを最大 16 個(IPv6 アドレス 1 〜 IPv6 アドレス 16)表示します。
- ゲートウェイ - iDRAC6 用に設定されたネットワークゲートウェイの IP アドレスを表示します。
- DHCPv6 を使用して DNS サーバーアドレスを取得する - DNS サーバーアドレスの取得に DHCP を使用するかどうかを表示します。
- 優先 DNS サーバー - 現在アクティブなプライマリ DNS サーバーを表示します。
- 代替 DNS サーバー - 代替の DNS サーバーアドレスを表示します。

メモ: この情報は **iDRAC6** →**プロパティ**→**リモートアクセス情報** の順にクリックしても表示できます。

内蔵 NIC MAC アドレス

- NIC 1 - 内蔵ネットワークインタフェースコントローラ(NIC)1 の MAC アドレスを表示します。

  MAC アドレスは、メディアアクセス制御層でネットワーク内の各ノードを一意に識別します。

  Internet Small Computer System Interface(iSCSI)NIC は、ホストコンピュータで実行している iSCSI スタックを搭載したネットワークインタフェースコントローラです。

  Ethernet NIC は有線 Ethernet 標準をサポートし、サーバーのシステムバスにプラグインします。
- NIC 2 - ネットワーク内で内蔵 NIC 2 を一意に識別する MAC アドレスを表示します。
- NIC 3 - ネットワーク内で内蔵 NIC 3 を一意に識別する MAC アドレスを表示します。内蔵 NIC 3 の MAC アドレスは、一部のシステムで表示されない場合があります。
- NIC 4 - ネットワーク内で内蔵 NIC 4 を一意に識別する MAC アドレスを表示します。内蔵 NIC 4 の MAC アドレスは、一部のシステムで表示されない場合があります。

WWN / MAC

インストールされている I/O メザニンカードおよびそれに関連付けられているネットワークファブリックの現在の設定を表示するには、**システム** → **プロパティ** タブ → **WWN / MAC** の順にクリックします。CMC で FlexAddress(フレックスアドレス) 機能が有効になっている場合は、グローバルに割り当てられた(シャーシ割り当ての)持続的 MAC アドレスが 各 LOM のハードウェア割り当てアドレスに優先されます。

サーバーの正常性

iDRAC6 および iDRAC6 が監視するコンポーネントの正常性に関する重要な情報を表示するには、**システム** → **プロパティ** タブ → **システム概要** → **サーバーの正常性** の順にクリックします。**状態** 列に、各コンポーネントの状態が表示されます。状態 アイコンのリストとその意味は、「表 19-3」を参照してください。**コンポーネント** 列のコンポーネント名をクリックすると、コンポーネントに関する詳細が表示されます。

メモ: コンポーネントの情報は、ウィンドウの左側のペインでコンポーネント名をクリックしても表示できます。コンポーネントは、選択されているタブや画面とは関係なく、左側のペインに表示されたままです。

iDRAC6

リモートアクセス情報 画面には、iDRAC6 の名前、ファームウェアリビジョン、ファームウェアアップデート、iDRAC6 の時間、IPMI バージョン、CPLD バージョン、サーバーの種類、ネットワークパラメータなど、iDRAC6 に関する重要な詳細情報が表示されます。画面上部の適切なタブをクリックすると、追加情報が表示されます。

CMC

CMC 画面には、Chassis Management Controller の正常性の状態、ファームウェアリビジョン、IP アドレスが表示されます。また、**CMC ウェブインタフェースの起動** ボタンをクリックして、CMC ウェブインタフェースを起動することもできます。詳細については、『Chassis Management Controller ファームウェアユーザーガイド』を参照してください。

メモ: iDRAC6 から CMC ウェブ GUI を起動すると、それと同じ IP アドレス形式で検索が行われます。たとえば、IPv6 アドレス形式で iDRAC6 ウェブ GUI を開いた場合は、CMC ウェブページも有効な IPv6 アドレスで開きます。

バッテリー

バッテリー 画面には、管理下システムのリアルタイムクロック(RTC)と CMOS 設定データストレージを管理するシステム基板コインセルバッテリーの状態が表示されます。

温度

温度 画面には、オンボードの周囲温度プローブの状態と測定値が表示されます。警告 と 失敗 状態の温度の上限と下限のしきい値、およびプローブの現在の正常性状態が表示されます。

メモ: サーバーのモデルによっては、警告 と 失敗 状態の温度しきい値やプローブの正常性状態が表示されない場合があります。

電圧

電圧プローブ 画面には、電圧プローブの状態と測定値が表示され、オンボード電圧レールや CPU コアセンサーなどの状態情報が提供されます。

電源監視

電源モニタ 画面には、以下のような監視情報と電力統計情報を表示できます。

- 電源モニタ - システムボード電流モニタによって測定された、サーバーの使用電力量(AC ワット数で測定した 1 分間の平均電力値)を表示します。
- アンペア数 - アクティブな電源装置の現在の消費量(AC アンペア数)を表示します。
- 電力追跡統計値 - 読み取り値が最後にリセットされてからシステムが使用した電力量についての情報を表示します。
- ピーク統計値 - 読み取り値が最後にリセットされてからシステムが使用したピーク電力量についての情報を表示します。
- 電力消費量 - 過去 1 分間、過去 1 時間、過去 1 日間、過去 1 週間のシステムの電力消費量の平均、最小、最大と、電力時間の最大と最小を表示します。
- グラフの表示 - 1 時間、24 時間、3 日間、1 週間の電力消費量をグラフで表示します。

メモ: 電力とアンペア数は AC で測定されます。

CPU

CPU 画面は、管理下サーバーの各 CPU の正常性について表示します。この正常性状態は、熱、電力、機能などの多数の個別テストをまとめたものです。

POST

POST コード 画面には、管理下サーバーのオペレーティングシステム起動前の最後のシステム POST コード(16 進数)が表示されます。

その他の正常性

その他の正常性 画面からは、以下のシステムログにアクセスできます。

- システムイベントログ - 管理下システムで発生したシステムの重要イベントを表示します。
- POST コード 画面には、管理下サーバーのオペレーティングシステム起動前の最後のシステム POST コード(16 進数)が表示されます。
- 前回クラッシュ画面 - 一番新しいクラッシュ画面と時間を表示します。
- 起動キャプチャ - 最後の 3 つの起動画面を再生します。

メモ: この情報は、**システム**→**ログ** タブ →**システムイベントログ** でも表示できます。

目次ページに戻る

目次ページに戻る

電源モニタおよび電源管理

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

Dell PowerEdge システムには、電源管理の新機能と拡張機能が多数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まで、プラットフォーム全体が電源効率、電源監視、電源管理に焦点を当てた設計となっています。

メモ: iDRAC6 の電力管理ロジックでは、ブレード サーバーに搭載されている Complex Programmable Logic Device(CPLD)が使用されています。一部のプラットフォームでは拡張 CPLD もサポートされています。CPLD デバイスのアップデートは、デルサポートサイト **support.dell.com** の **システムファームウェア** セクションまたは **システムボード** セクションから入手できます。CPLD ファームウェアの最新バージョンでブレードサーバーをアップデートすることをお勧めします。CPLD と拡張 CPLD ファームウェアの現在のバージョン(該当するプラットフォーム用)が iDRAC6 ウェブインタフェースに表示されます。

Dell PowerEdge システムは、電源モニタおよび管理機能を多数提供しています。

- **電源モニタ**: **iD**RAC6 は、電力測定の履歴を収集し、移動平均やピーク値などを計算します。 iDRAC6 ウェブインタフェースを使用すると、**電源モニタ** 画面でこれらの情報を確認できます。**電源モニタ** 画面下部の **グラフの表示** をクリックすることで、グラフ形式で情報を表示させることも可能です。 詳細については、電源監視を参照してください。
- **電力バジェット:** 起動時に、システムインベントリにより、現在の設定のシステム電力バジェットが算出されます。詳細については、電力バジェットを参照してください。
- **電源制御:** iDRAC6 を使用することで、管理下システム上でさまざまな電源管理操作をリモートから実行できます。詳細については、電源制御を参照してください。

電源の設定と管理

iDRAC6 ウェブインタフェースと RACADM コマンドラインインタフェース(CLI)を使用して、Dell PowerEdge システムの電源制御の管理と設定ができます。具体的には、以下のことが可能です。

- サーバーの電源状態を表示する。電源モニタの表示 を参照してください。
- 最小および最大電力消費量など、サーバーの電力バジェット情報を表示する。電力バジェットの表示 を参照してください。
- サーバーの電力バジェットのしきい値を表示する。電力バジェットのしきい値 を参照してください。
- サーバーの PCIe 拡張カードに割り当てられた電力を表示する。PCIe 電力割り当ての表示と変更 を参照してください。
- サーバーに電源制御操作(例:電源オン、電源オフ、システムリセット、電源の入れ直し、正常なシャットダウンなど)を実行します。サーバーに対する電源制御操作の実行 を参照してください。

電源監視

iDRAC6 は、継続的に Dell PowerEdge サーバーの消費電力を監視します。iDRAC6 は以下の電力値を計算し、ウェブインタフェースまたは RACADM CLI を使って表示します。

- 累積システム電力
- システムピーク電力とシステムピークアンペア数
- 平均、最小、最大の電力消費量
- 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)
- 最大と最小の電力時間

電源モニタの表示

ウェブインタフェースの使用

電源モニタデータを表示するには

1. iDRAC6 ウェブインタフェースにログインします。
2. システムツリーで、**電源モニタ** を選択します。

   電源モニタ 画面に以下の情報が表示されます。

電源モニタ

- **状態**:**緑色のチェックマーク** は、電源の正常状態、**警告** は警告状態、**重大** はエラー状態を示します。
- **プローブ名**:センサーの名前を表示します。
- **読み取り値**:プローブが報告するワット数を示します。
- **警告しきい値**:システム動作に推奨される消費電力の許容量(ワットおよび BTU/時単位)。消費電力量がこの値を超えると、警告イベントが発生します。
- **エラーしきい値**:システム動作に必要とされる消費電力の最大許容量(ワットおよび BTU/時単位)。消費電力量がこの値を超えると、重要 / エラーイベントが発生します。

アンペア数

- **場所**:システム基板センサーの名前を表示します。
- **読み取り値**:現在の消費電力量(ACアンペア)。

電力追跡統計値とピーク統計値

- **統計:**
  - **累積システム電力** には、サーバーの現在の累積エネルギー消費量(キロワット / 時)が表示されます。この値は、システムによって消費される総エネルギー量を表します。表の最終行の **リセット** をクリックすることで、この値を 0 にリセットできます。
  - **システムピーク電力** は、システムのピーク値を AC ワットで示します。
  - **システムピークアンペア数** はシステムのピークアンペア数を示します。ピーク値は、**測定開始時刻** から現在までに記録された最高値です。ピーク時刻は、ピーク値が発生した時点です。テーブルの行の終わりで **リセット** をクリックすると、現在の瞬時値に戻ります(サーバーが実行中の場合、0 にはなりません)。リセットをクリックすると、測定開始時刻も現在の時刻に戻ります。
  - **測定開始時刻** は、システムエネルギー消費量の値が最後にクリアされ、新しい測定サイクルが開始された日時を表示します。**累積システム電力** 、**システムピークアンペア数**、および **システムピーク電力** 統計の場合、リセットするとピーク値に直ちに現在の瞬時値が反映されます。
  - **累積システム電力** の **現在の測定時刻** は、システムエネルギー消費量が算出された現在の日付と時刻を表示します。**システムピークアンペア数** と **システムピーク電力** の場合、**ピーク時間** フィールドは、これらのピークが発生した時刻を表示します。
  - **読み取り値**:カウンタが開始してからの該当する統計値:**累積システム電力**、**システムピーク電力**、および**システムピークアンペア数**。

メモ: 電力追跡統計は、システムのリセットしても保持されるため、指定した測定開始から現時点までのすべてのアクティビティを反映します。電力消費量表に表示された電力値は、それぞれの期間(過去 1 分間、1 時間、1 日間、1 週間)の累積平均です。開始から終了までの間隔が電源追跡統計値と異なる場合もあるため、ピーク電力値(最大ピークワット数と最大電力消費量)も異なる可能性があります。

電力消費量

- **平均電力消費量**:過去 1 分間、過去 1 時間、過去 1 日、および過去 1 週間の平均値。
- **最大電力消費量** と **最小電力消費量**: 指定された時間間隔において測定された最大と最小電力消費量。
- **最大電力時間** と **最小電力時間**: 最大と最小電力消費量が記録された時間(分、時間、日、週)。

グラフの表示

過去 1 時間、24 時間、3 日、1 週間の iDRAC6 の電力消費量をワット単位でグラフ表示するには、**グラフの表示** をクリックします。対象期間を選択するには、グラフの上のドロップダウンメニューを使用します。

メモ: グラフに描かれた各データポイントは、読み取り値の 5 分間の平均値を表します。このため、電力消費量や電流消費量の短時間の変動はグラフに反映されない場合もあります。

電力バジェット

電力バジェット 画面には、高負荷環境のシステムがデータセンターに提供する AC 電力消費量の範囲をカバーする電力しきい値制限が表示されます。

サーバーに電源が入る前に、iDRAC6 は CMC にその電力エンベロープの要件を示します。実際にサーバーが消費する電力に応じて、電源投入後にこれより小さい電力エンベロープを要求する場合もあります。時間の経過に伴い電力消費量が増えて、サーバーが最大割り当てに近い電力を消費している場合、iDRAC6 は最大潜在電力消費量の増大を要求し、電力エンベロープを上げることがあります。iDRAC6 が CMC に要求するのは最大潜在電力消費量の増大分だけです。電力消費量が減った場合に、最小潜在電力の減少は要求しません。

CMC は優先順位の低いサーバーの未使用電力を取り戻し、その電力を優先順位の高いインフラストラクチャモジュールやサーバーに割り当てます。

十分な電力が割り当てられていない場合は、ブレードサーバーに電源が入りません。ブレードに十分な電力が割り当てられている場合は、システムに電源が入ります。

iDRAC6 は、該当するプラットフォームの PCIe 拡張カードの電力割り当てもサポートしています。サーバーの拡張スロットに挿入されている PCIe 拡張カードに割り当てられている電力を変更できます。該当するプラットフォームに PCIe カードを 2 枚搭載できます。iDRAC は、ブレードの実際のシステム要件に近づくように電力エンベロープを動的に調整し、拡張カードのスロットに割り当てられた電力を追加して、CMC に電力の結合を要求します。拡張カードの詳細については、デルサポートサイト **support.dell.com / manuals** にある『ハードウェアオーナーズマニュアル』を参照してください。PCIe 電力割り当ての変更については、「PCIe 電力割り当ての表示と変更」を参照してください。

ブレードの電源が入った後、BIOS が起動して、搭載されている PCIe 拡張カードの実際の電力消費量を検出します。これは POST 中に行われます。両方のカードが検出された場合、iDRAC は、初期化前処理の段階でこれらの拡張カードに使用された値を維持します。現在搭載されている PCIe カードを基に更新された値を取得した後、iDRAC はその値を拡張カードの推定電力消費量と併せて、ブレード全体の新しい電力値として報告します。CMC が十分な電力を割り当てなかった場合は、iDRAC はブレードの電源を切ります。CMC が十分な電力を割り当てた場合は、BIOS の起動が継続し、サーバーを開始できます。

たとえば、iDRAC が初期化前に想定した値が 500W の場合、PCIe 拡張カードの割り当てに別の値を設定しない限り、この値が使用されます。別の値を設定した場合は、初期化前処理中に常にこの

値が使用されます。この値は AC 電源の入れ直し中、維持されます。その後、システムの POST が行われるときに、搭載されているカード数と入力値が比較されます。

電力バジェットの表示

サーバーは、電源サブシステムの電力バジェット状態の概要を **電力バジェット** 画面に提供します。

ウェブインタフェースの使用

メモ: 電源管理操作を行うには、**システム管理者** 権限が必要です。

1. iDRAC6 ウェブインタフェースにログインします。
2. システム ツリーで **システム** をクリックします。
3. **電源管理** タブをクリックして、**電力バジェット** をクリックします。

   電力バジェット 画面が表示されます。

電力バジェット情報 の表には、現在のシステム設定における電力しきい値の上限と下限値が表示されます。これらの値は、しきい値が設定されたシステムから高負荷時にデータセンターに報告される AC 電力消費量の範囲をカバーします。

- **最小潜在電力消費量** は、電力バジェットの下限しきい値を表します。
- **最大潜在電力消費量** は、電力バジェットの上限しきい値を表します。この値は、現在のシステム構成での絶対最大電力消費量でもあります。

RACADM の使用

管理下サーバーで、コマンドラインインタフェースを開き、次のコマンドを入力します。

```
racadm getconfig -g cfgServerPower
```

メモ: 出力の詳細を含め cfgServerPower の詳細については、デルサポートサイト **support.dell.com / manuals** にある『iDRAC6 管理者リファレンスガイド』の「cfgServerPower」を参照してください。

電力バジェットのしきい値

電力バジェットしきい値を有効にすると、システム電力が制限されます。指定したしきい値内に消費電力を維持するために、システムパフォーマンスが動的に調整されます。

低負荷環境では実際の電力消費量の方が少ない場合もあり、パフォーマンスの調整が完了するまでは、一時的にしきい値を下回る可能性があります。

メモ: 電力バジェットしきい値の情報は、読み取り専用であるため、iDRAC6 で有効にしたり、設定を変更することはできません。

ウェブインタフェースの使用

1. iDRAC6 ウェブインタフェースにログインします。
2. システム ツリーで **システム** をクリックします。
3. **電源管理** タブをクリックして、**電力バジェット** をクリックします。

   電力バジェット 画面が表示されます。電力**バジェットしきい値** 表にはシステムの電力制限に関する以下の情報が表示されます。

   - **有効** は、システムが電力バジェットしきい値を守るかどうかを示します。
   - **ワット単位のしきい値** と **BTU / 時単位のしきい値** は、制限値をそれぞれ AC ワットと BTU/ 時単位で表示します。
   - **パーセント表示のしきい値（最大）** には、電力制限範囲のパーセントが表示されます。

RACADM の使用

ローカル RACADM から電力バジェットのしきい値を表示するには、管理下サーバーで、コマンドラインインタフェースを開いて次のように入力します。

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts
```

<電力制限値 AC ワット> を返します

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr
```

<電力制限値 BTU/ 時> を返します

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent
```

<電力制限値 %> を返します

メモ: 出力の詳細を含め cfgServerPower, の詳細については、デルサポートサイト **support.dell.com / manuals** にある『iDRAC6 管理者リファレンスガイド』の「cfgServerPower」を参照してください。

PCIe 電力割り当ての表示と変更

PCIe 電力割り当てでは、PCIe 拡張カードに割り当てられた最大電力を表示したり変更したりできます。割り当てる電力は 100W ～ 500W とします。割り当て電力が大きすぎると、ブレードに電源が入らなかったり、シャーシ内の他のブレードに電源が入らなかったりする場合があります。PCIe 拡張カードが割り当てた以上の電力を消費すると、ブレードの電源が切れます。PCIe の電力割り当てを変更すると、システムの起動時に新しい電力割り当てが使用されます。

メモ: PCIe の電力割り当てが該当しないプラットフォームもあり、その場合は、この情報は表示されません。

メモ: PCIe の電力割り当て値を編集するには、システム管理者権限（ iDRAC の設定とサーバー制御コマンドの実行）が必要です。

ウェブインタフェースの使用

1. iDRAC6 ウェブインタフェースにログインします。
2. システム ツリーで **システム** をクリックします。
3. **電源管理** タブをクリックして、**電力バジェット** をクリックします。**PCIe の電力割り当て** テーブルの **電力しきい値（W）** フィールドに、現在の電力割り当て値が表示されます。
4. 必要な値を入力するか、**デフォルト値** をクリックしてデフォルト値を指定します。有効な値は 100W ～ 500W です。デフォルト値は 500W です。
5. **適用**をクリックして新しい値を保存します。新しい値はシステムの起動時に使用されます。

RACADM の使用

PCIe 拡張カードに割り当てられている現在の電力を、リモートシステムでリモート RACADM を使用して表示するには、コマンドプロンプトを開き、次のコマンドを入力します。

```
racadm -r <idracip> -u <ユーザー> -p <パスワード> config -g cfgServerPower -o cfgServerPowerPCIeAllocation
```

<AC ワット単位の電力制限値または BTU/時間> を返します。デフォルト値は 500W です。

電力割り当て値を変更するには（たとえば、250W）、次のコマンドを入力します。

```
racadm -r <idracip> -u <ユーザー> -p <パスワード> config -g cfgServerPower -o cfgServerPowerPCIeAllocation 250
```

値を 250W に設定します

メモ: cfgServerPowerPCIeAllocation オブジェクトはリモート RACADM でのみサポートされ、ローカル RACADM ではサポートされていません。

メモ: 詳細については、デルサポートサイト **support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』の「owerPCIeAllocation」を参照してください。

電源制御

iDRAC6 では、電源オン、リセット、正常なシャットダウン、マスク不可割り込み（NMI）、電源の入れ直し などをリモートから実行できます。再起動時と電源のオン / オフ時に、オペレーティングシステムを通した正常なシャットダウンを実行するには、**電源制御** 画面を使用します。

サーバーに対する電源制御操作の実行

メモ: 電源管理操作を実行するには、**システム管理者** 権限が必要です。

iDRAC6 では、電源オン、リセット、正常なシャットダウン、NMI または電源の入れ直しをリモートから実行できます。

ウェブインタフェースの使用

1. iDRAC6 ウェブインタフェースにログインします。
2. システムツリーで **システム** を選択します。

3. **電源管理** タブをクリックします。

   電源制御 画面が表示されます。

4. ラジオボタンをクリックして、以下の **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** を選択すると、サーバーの電源がオンになります（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には、このオプションは無効になっています。
   - **システムの電源を切る** を選択すると、サーバーの電源がオフになります。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）:** NMI を生成し、システム動作を一時停止させます。NMI は、オペレーティングシステムに高レベルの割り込みを送信し、重要な診断またはトラブルシューティングを可能にするためにシステム動作を一時停止させます。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
   - **正常なシャットダウン** を選択すると、オペレーティングシステムが停止してからシステムの電源が切れます。これには、システムによる電源管理を可能にする ACPI（Advanced Configuration and Power Interface）対応のオペレーティングシステムが必要です。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
   - **システムのリセット（ウォームブート）** は、電源を切らずにシステムを再起動します。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
   - **システムの電源の入れ直し（コールドブート）** を選択すると、電源が切られてからシステムが再起動します。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。

5. **適用** をクリックします。

   確認を求めるダイアログボックスが表示されます。

6. 選択した電源管理操作を実行するには、**OK** をクリックします。

RACADM の使用

ローカル RACADM から電源処置を実行するには、コマンドプロンプトで次のコマンドを入力します。

```
racadm serveraction <操作>
```

ここで、<操作> は、電源投入、電源切断、電源の入れ直し、ハードリセットまたは電源状態 です。

メモ: serveraction の詳細については、デルサポートサイト **support.dell.com / manuals** にある『iDRAC6 管理者リファレンスガイド』の「serveraction」を参照してください。

目次ページに戻る

目次ページに戻る

シリアルオーバー LAN の設定と使用

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

シリアルオーバー LAN(SOL)は、従来シリアル I/O ポートに送信される管理下サーバーのテキストベースのコンソールデータを、iDRAC6 の専用帯域外 Ethernet 管理ネットワーク経由でリダイレクトできるようにする IPMI 機能です。SOL 帯域外コンソールを使うと、システム管理者はブレードサーバーのテキストベースのコンソールをネットワークアクセスのある任意の場所からリモート管理できます。SOL のメリットは次のとおりです。

- タイムアウトなしにオペレーティングシステムにリモートアクセスできる。
- Windows の Emergency Management Services(EMS)または Special Administrator Console(SAC)、Linux シェルでホストシステムを診断できる。
- POST 中のブレードサーバーの進行状況を表示し、BIOS セットアッププログラムを再構成できる(シリアルポートへのリダイレクト中)。

BIOS でシリアルオーバー LAN を有効にできる

サーバーにシリアルオーバー LAN を設定するには、以下に説明する設定手順が必要になります。

1. BIOS でシリアルオーバー LAN を設定する(デフォルトは無効)
2. シリアルオーバー LAN 用に iDRAC6 を設定する
3. シリアルオーバー LAN の初期化方法を選択する(SSH、telnet、SOL プロキシ、IPMI ツール)
4. SOL 用のオペレーティングシステムを設定する

BIOS ではシリアル通信はデフォルトで **オフ** になっています。ホストのテキストコンソールデータをシリアルオーバー LAN にリダイレクトするには、COM1 で仮想コンソールを有効にする必要があります。BIOS 設定を変更するには、次の手順を実行してください。

1. 管理下サーバーを起動します。
2. POST 中に <F2> キーを押して BIOS セットアップユーティリティを起動します。
3. シリアル通信にスクロールダウンして <Enter> キーを押します。

   ポップアップウィンドウにシリアル通信リストと以下のオプションが表示されます。

   - オフ
   - 仮想コンソールなしでオン
   - 仮想コンソール使用でオン

   方向キーを使用して、オプション間を移動します。
4. **仮想コンソールリダイレクト使用でオン** が有効になっていることを確認します。**シリアルポートアドレス** が COM1 であることを確認します。
5. **フェイルセーフボーレート** が、iDRAC6 で設定されている SOL ボーレートと同一であることを確認します。フェイルセーフボーレートと iDRAC6 の SOL ボーレートのデフォルト値は 115.2 kbps です。
6. **起動後のリダイレクト** が有効になっていることを確認します。このオプションは、その後の再起動での BIOS SOL リダイレクトを有効にします。BIOS には **リモートターミナルタイプ** の値 VT100/VT220 と ANSI があります。
7. 変更を保存して終了します。

   管理下サーバーが再起動します。

---

iDRAC6 ウェブ GUI でのシリアルオーバー LAN の設定

1. **システム→リモートアクセス→iDRAC→ネットワーク / セキュリティ→シリアルオーバー LAN** の順に選択して、**シリアルオーバー LAN 設定** 画面を開きます。
2. **シリアルオーバー LAN** を有効にする オプションが選択されている(有効になっている)ことを確認します。デフォルトで有効になっています。

3. **ボーレート**ドロップダウンメニューからデータ速度を選択して、IPMI SOL ボーレートを更新します。オプションは 9600 bps、19.2 kbps、57.6 kbps、115.2 kbps です。デフォルト値は 115.2 kbps です。

4. シリアルオーバー LAN の権限レベルの制限を選択します。

   メモ: SOL ボーレート が、BIOS で設定されているフェイルセーフボーレートと同一であることを確認します。

5. 変更した場合は **適用** をクリックします。

表 9-1 シリアルオーバー LAN 設定画面の設定

設定	説明
シリアルオーバー LAN を有効にする	チェックボックスが選択されている場合は、シリアルオーバー LAN が有効であることを示します。
ボーレート	データ速度を示します。データ速度を **9600 bps**、**19.2 kbps**、**57.6 kbps**、**115.2 kbps** の中から選択します。
チャネル権限レベルの制限	シリアルオーバー LAN の権限レベルの制限を選択します。

表 9-2 シリアルオーバー LAN 設定画面のボタン

ボタン	説明
印刷	画面に表示される **シリアルオーバー LAN** の値を印刷します。
更新	**シリアルオーバー LAN** 画面を再ロードします。
詳細設定	**シリアルオーバー LAN の詳細設定** 画面を開きます。
適用	**シリアルオーバー LAN** 画面の表示中に行った新しい設定を適用します。

6. 必要に応じて、**シリアルオーバー LAN 詳細設定** 画面で設定を変更します。デフォルト値を使用することをお勧めします。**詳細設定** では、**文字累積間隔** と **文字送信しきい値** を変更することで SOL のパフォーマンスを調整できます。最適なパフォーマンスを得るためには、デフォルト設定の 10 ミリ秒と 255 文字を使用してください。

表 9-3 シリアルオーバー LAN の詳細設定

設定	説明
文字累積間隔	SOL データパケットの一部を送信するまでの iDRAC6 の標準的な待ち時間。このパラメータはミリ秒で指定します。
文字送信しきい値	SOL データパケットあたりの文字数を指定します。iDRAC6 が受け入れた文字数が文字送信しきい値以上になると、iDRAC6 は文字送信しきい値以下の文字数を含む SOL データパケットの送信を開始します。含まれている文字数がこの値より少ないパケットは、部分 SOL データパケットとして定義されます。

メモ: これらの値を下げると、SOL の仮想コンソール機能のパフォーマンスが低下する可能性があります。また、SOL セッションは次のパケットを送信する前に各パケットの確認メッセージを受信するまで待つ必要があります。このため、パフォーマンス が著しく低下します。

表 9-4 シリアルオーバー LAN 設定の詳細 設定画面のボタン

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

7. **システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** タブ→ **サービス** でシリアルオーバー LAN に SSH と Telnet を設定します。

   メモ: 各ブレードサーバーはアクティブな SOL セッションを 1 つだけサポートします。

   メモ: SSH プロトコルはデフォルトでは有効になっています。Telnet プロトコルはデフォルトでは無効になっています。

8. **サービス** をクリックして **サービス** 画面を開きます。

   メモ: SSH および Telnet プログラムは共にリモートマシンでのアクセスを提供します。

9. 必要に応じて、**SSH** または **Telnet** で **有効** をクリックします。

10. **適用** をクリックします。

メモ: セキュリティと暗号化のメカニズムが優れている SSH を推奨します。

メモ: タイムアウト値を 0 に設定すると、SSH/Telnet セッション期間が無限になります。デフォルトのタイムアウト値は 1800 秒です。

11. **システム→リモートアクセス→iDRAC6→ネットワーク / セキュリティ→ネットワーク** の順に選択して、iDRAC6 帯域外インタフェース(IPMI オーバー LAN)を有効にします。
12. **IPMI 設定** で **IPMI オーバー LAN を有効にする** オプションを選択します。
13. **適用** をクリックします。

シリアルオーバー LAN(SOL)の使用

本項では、Telnet プログラム、SSH クライアント、IPMItool、SOL プロキシなど、シリアルオーバー LAN セッションの開始方法について説明します。シリアルオーバー LAN 機能の目的は、管理下サーバーのシリアルポートを iDRAC6 を介して管理ステーションのコンソールにリダイレクトすることです。

Telnet または SSH を通して SOL をリダイレクトするモデル

Telnet(ポート 23)/SSH(ポート 22)クライアント ↔ WAN 接続 ↔ iDRAC6 サーバー

SSH/Telnet 経由の IPMI ベース SOL を実装すると、シリアルとネットワーク間の変換が iDRAC6 内で行われるため、追加のユーティリティは不要になります。使用する SSH または Telnet コンソールは、管理下サーバーのシリアルポートから届くデータを解釈して応答できることが必要です。通常、シリアルポートは ANSI または VT100/VT220 ターミナルをエミレートするシェルに連結しています。シリアルコンソールは自動的に SSH または Telnet コンソールにリダイレクトされます。

SOL セッションを開始するには、SSH/Telnet で iDRAC6 に連結して、iDRAC6 コマンドラインコンソールを開きます。次に、ドル記号のプロンプトで 「connect」と入力します。

iDRAC で Telnet および SSH クライントを使用する方法の詳細については、「Telnet または SSH クライアントのインストール」を参照してください。

SOL プロキシのモデル

Telnet クライアント(ポート 623) ↔ WAN 接続 ↔ SOL プロキシ ↔ iDRAC6 サーバー

SOL プロキシは、管理ステーションの Telnet クライアントと通信するとき TCP/IP プロトコルを使用します。一方、SOL プロキシは管理下サーバーの iDRAC6 とは、UDP ベースの RMCP/IPMI/SOL プロトコルを使用して通信します。このため、管理下システムの iDRAC6 に SOL プロキシから WAN 接続経由で通信する場合は、ネットワークパフォーマンスに問題がある可能性があります。推奨される使用モデルは、SOL プロキシと iDRAC6 サーバーを同じ LAN に接続したものです。これによって、Telnet クライアントと管理ステーションを WAN 接続で SOL プロキシに接続できるようになります。この使用モデルでは、SOL プロキシは期待通りに機能します。

IMPItool を通して SOL をリダイレクトするモデル

IPMItool ↔ WAN 接続 ↔ iDRAC6 サーバー

IPMI ベースの SOL ユーティリティである IPMItool は、UDP データグラムを使ってポート 623 に配信された RMCP+ プロトコルを使用します。iDRAC6 では、この RMCP+ 接続が暗号化されている必要があります。暗号化キー(KG キー)には、iDRAC6 ウェブ GUI または iDRAC6 設定ユーティリティで設定できるゼロまたは NULL 文字が含まれている必要があります。また、Backspace キーを押して、暗号化キーを消し、iDRAC6 にデフォルト暗号化キーの NULL 文字を提供させることもできます。RMCP+ を使用する利点としては、認証の強化、データ整合性チェック、暗号化、および複数タイプのペイロードのサポートがあります。詳細については、「IPMItool 経由で SOL を使用」または IPMItool のウェブサイト **http://ipmitool.sourceforge.net/manpage.html** を参照してください。

iDRAC6 コマンドラインコンソールでの SOL セッションの切断

SOL セッションを切断するには、ユーティリティのコマンドを使用します。SOL セッションを完全に終えなければ、ユーティリティを終了できません。SOL セッションを切断するには、iDRAC6 コマンドラインコンソールから SOL セッションを終了します。

SOL リダイレクトを終了する準備ができたら、<Enter>、<Esc>、<t> の順に続けてキーを押します。それに応答して、SOL セッションが終了します。このエスケープシーケンスは、SOL セッションが接続した直後に、画面にも出力されます。管理下サーバーが オフ の場合は、SOL の確立に若干時間がかかります。

メモ: ユーティリティで SOL セッションを正常に閉じないと、それ以上の SOL セッションは使用できなくなる可能性があります。この状況を解決するには、ウェブ GUI の **システム→リモートアクセス→iDRAC6→ネットワーク / セキュリティ→セッション** でコマンドラインコンソールを終了します。

PuTTY 経由で SOL を使用

Windows 管理ステーションで PuTTY から SOL を起動するには、次の手順を実行してください。

メモ: 必要に応じて、**システム → リモートアクセス→ iDRAC6 → ネットワーク / セキュリティ → サービス** でデフォルトの SSH/Telnet を変更できます。

1. コマンドプロンプトで次のコマンドを使用して iDRAC6 に接続します。

```
putty.exe [-ssh | -telnet] <ログイン名>@<iDRAC の ip アドレス> <ポート番号>
```

メモ: ポート番号はオプションです。ポート番号の再割り当てを行った場合のみ必要です。

2. SOL を開始するには、コマンドプロンプトで次のコマンドを入力します。

```
connect
```

メモ: これで、管理下サーバーのシリアルポートに接続します。SOL セッションが正常に確立すると、iDRAC6 コマンドラインコンソールは使用できなくなります。エスケープシーケンスの手順に従って、iDRAC6 コマンドラインコンソールにアクセスします。「iDRAC6 コマンドラインコンソールでの SOL セッションの切断」で説明したコマンドシーケンスを使用して、SOL セッションを終了し、新しいセッションを開始します。

メモ: Windows では、Emergency Management System(EMS)コンソールをホストの再起動直後に開いた場合、Special Admin Console(SAC)ターミナルが破損する可能性があります。「iDRAC6 コマンドラインコンソールでの SOL セッションの切断」の説明に従ってシリアルオーバー LAN を終了し、別のターミナルを開いて、上記と同じコマンドを使用してシリアルオーバー LAN セッションを開始してください。

Linux での SOL オーバー Telnet の使用

Linux 管理ステーションで Telnet から SOL を起動するには、次の手順を実行してください。

メモ: 必要に応じて、**システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **サービス** でデフォルトの Telnet タイムアウトを変更できます。

1. シェルを起動します。
2. 次のコマンドで iDRAC6 に接続します。

```
telnet <iDRAC6 の IP アドレス>
```

メモ: Telnet サービスのポート番号をデフォルトポート 23 から変更した場合は、Telnet コマンドの末尾にポート番号を追加します。

3. SOL を開始するには、コマンドプロンプトで次のコマンドを入力します。

```
connect
```

4. Linux 上で Telnet から SOL セッションを終了するには、<Ctrl> +] を押します(<Ctrl> キーを押しながら右角カッコキーを押し、その後手を離します)。Telnet のプロンプトが表示されます。quit と入力して Telnet を終了します。

Linux で OpenSSH 経由で SOL を使用

OpenSSH は、SSH プロトコルを使用するためのオープンソースユーティリティです。Linux 管理ステーションで OpenSSH から SOL を起動するには、次の手順を実行してください。

メモ: 必要に応じて、**システム** → **リモートアクセス**→ **iDRAC6** → **ネットワーク / セキュリティ** → **サービス** で SSH のデフォルトのセッションタイムアウトを変更できます。

1. シェルを起動します。
2. 次のコマンドで iDRAC6 に接続します。

```
ssh <iDRAC の ip アドレス> -l <ログイン名>
```

3. SOL を開始するには、コマンドプロンプトで次のコマンドを入力します。

```
connect
```

メモ: これで、管理下サーバーのシリアルポートに接続します。SOL セッションが確立すると、iDRAC6 コマンドラインコンソールは使用できなくなります。エスケープシーケンスの手順に従って、iDRAC6 コマンドラインコンソールにアクセスします。シリアルオーバー LAN セッションを終了します(「iDRAC6 コマンドラインコンソールでの SOL セッションの切断」を参照してアクティブなシリアルオーバー LAN セッションを閉じます)。

IPMItool 経由で SOL を使用

IPMItool は『Dell Systems Management Tools and Documentation DVD 』からさまざまなオペレーティングシステムにインストールできます。インストールの詳細については、『ソフトウェアクイックインストールガイド』を参照してください。管理ステーションで IPMItool から SOL を起動するには、次の手順を実行してください。

メモ: 必要に応じて、**システム** → **リモートアクセス**→ **iDRAC6** → **ネットワーク / セキュリティ** →**サービス** でシリアルオーバー LAN のデフォルトのタイムアウトを変更できます。

1. 正しいディレクトリから **IPMItool.exe** を見つけます。

Windows 32 ビットオペレーティングシステムのデフォルトのパスは **C:\Program Files\Dell\SysMgt\bmc** で、Windows 64 ビットオペレーティングシステムのデフォルトのパスは **C:\Program Files (x86)\Dell\SysMgt\bmc** です。

2. **システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **ネットワーク** → **IPMI 設定** で **暗号化キー** がすべて 0 であることを確認します。

3. Windows コマンドプロンプトまたは Linux シェルプロンプトで次のコマンドを入力して、iDRAC 経由で SOL を起動します。

   ```
   ipmitool -H <iDRAC の ip アドレス> -I lanplus -U <ログイン名> -P <ログインパスワード> sol activate
   ```

   これで、管理下サーバーのシリアルポートに接続します。

4. IPMItool から SOL セッションを終了するには、<~> と <.> を押します(ティルデとピリオドを続けて押す)。iDRAC6 がキーの受け入れでビジー状態になっている可能性があるので、何度か実行してください。SOL セッションが閉じます。

   メモ: SOL セッションが正しく終了しなかった場合は、次のコマンドを入力して iDRAC を再起動します。iDRAC6 が起動を完了するまでに最大 2 分かかります。詳細については、デルサポートサイト **support.dell.com/manuals** で『iDRAC6 管理者リファレンスガイド』を参照してください。

   ```
   racadm racreset
   ```

SOL プロキシで SOL を開く

シリアルオーバー LAN プロキシ(SOL プロキシ)は、シリアルオーバー LAN(SOL)と IPMI プロトコルを使用してリモートシステムを LAN ベースで管理できる Telnet のデーモンです。デーモンの機能にアクセスするには、Microsoft Windows の HyperTerminal や Linux の Telnet など、標準的な Telnet クライアントアプリケーションを使用できます。SOL はメニューモードでもコマンドモードでも使用可能です。SOL プロトコルとリモートシステムの BIOS 仮想コンソールを組み合わせることで、システム管理者は管理下システムの BIOS 設定を LAN を介してリモート表示して変更できます。Linux シリアルコンソールと Microsoft の EMS/SAC インタフェースも SOL を使用して LAN でアクセスできます。

メモ: Windows オペレーティングシステムのすべてのバージョンに HyperTerminal ターミナルエミュレーションソフトウェアが含まれています。ただし、同梱のバージョンでは仮想コンソール中に必要な機能の多くは提供されていません。代わりに、VT100 / VT220 または ANSI エミュレーションモードをサポートしているターミナルエミュレーションソフトウェアを使用できます。システムで仮想コンソールをサポートしている完全な VT100/VT220 または ANSI ターミナルエミュレータの一例は、Hilgraeve の HyperTerminal Private Edition 6.1 以降です。また、コマンドラインウィンドウを使用して Telnet シリアル仮想コンソールを実行すると、文字化けする場合があります。

メモ: ハードウェアとソフトウェアの必要条件や、ホストとクライアントシステムで仮想コンソールを使用する手順など、仮想コンソールの詳細については、システムの『ユーザーズガイド』を参照してください。

メモ: ハイパーターミナルと Telnet の設定は、管理下システムの設定と同じである必要があります。たとえば、ボーレートとターミナルモードが一致する必要があります。

メモ: MS-DOS プロンプトから実行する Windows telnet コマンドは ANSI ターミナルエミュレーションをサポートしており、すべての画面を正しく表示するには、BIOS に ANSI ターミナルエミュレーションを設定する必要があります。

SOL プロキシを使用する前に

SOL プロキシを使用する前に、『ベースボード管理コントローラユーティリティユーザーズガイド』で管理ステーションの設定方法を確認してください。BMC 管理ユーティリティは、デフォルトでは Windows オペレーティングシステムの次のディレクトリにインストールされます。

C:\Program Files\Dell\SysMgt\bmc - (32 ビットのオペレーティングシステム)

C:\Program Files (x86)\Dell\SysMgt\bmc - (64 ビットのオペレーティングシステム)

Linux Enterprise オペレーティングシステムではインストールプログラムはファイルを次の場所にコピーします。

/etc/init.d/SOLPROXY.cfg

/etc/SOLPROXY.cfg

/usr/sbin/dsm_bmu_solproxy32d

/usr/sbin/solconfig

/usr/sbin/ipmish

SOL プロキシセッションの開始

Windows 2003 の場合

Windows システムで、インストール後に SOL プロキシサービスを開始するには、システムを再起動してください(再起動すると SOL プロキシが自動的に開始します)。または、次の手順で SOL プロキシサービスを手動で開始することもできます。

1. **マイコンピュータ** を右クリックして、**管理** をクリックします。

   コンピュータの管理 ウィンドウが表示されます。

2. **サービスとアプリケーション** をクリックしてから **サービス** をクリックします。

右側に使用可能なサービスが表示されます。

3. サービス一覧から **DSM_BMU_SOLProxy** を右クリックして、このサービスを開始します。

使用しているコンソールによっては、SOL プロキシへのアクセス手順が異なる場合があります。本項では、SOL プロキシを実行している管理ステーションを「SOL プロキシサーバー」と呼びます。

Linux の場合

SOL プロキシはシステム起動中に自動的に開始します。または、**etc/init.d** ディレクトリに移動し、次のコマンドを使用して SOL プロキシサービスを管理することもできます。

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

SOL プロキシ経由で Telnet を使用

ここでは、管理ステーションで SOL プロキシサービスが既に実行されていることを前提とします。

Windows 2003 の場合

1. 管理ステーションで、コマンドプロンプトウィンドウを開きます。

2. コマンドラインに `telnet` コマンドを入力し、SOL プロキシサーバーが同じマシンで実行している場合は IP アドレスとして `localhost` を入力し、SOL プロキシインストール時に指定したポート番号（デフォルトは 623）を入力します。たとえば、次のとおりです。

   ```
   telnet localhost 623
   ```

Linux の場合

1. 管理ステーションで Linux シェルを開きます。

2. `telnet` コマンドを入力して、IP アドレスとして `localhost` を入力し、SOL プロキシインストール時に指定したポート番号（デフォルトは 623）を入力します。たとえば、次のとおりです。

   ```
   telnet localhost 623
   ```

   メモ: ホストオペレーティングシステムが Windows であるか Linux であるかにかかわらず、SOL プロキシサーバーが管理ステーション以外のマシンで実行されている場合は、localhost ではなく SOL プロキシサーバー IP アドレスを入力します。

   ```
   telnet <SOL プロキシサーバー IP アドレス> 623
   ```

SOL プロキシ経由の HyperTerminal の使用

1. リモートステーションから **HyperTerminal.exe** を開きます。

2. **TCP/IP（Winsock）** を選択します。

3. ホストアドレス `localhost` とポート番号 623 を入力します。

リモート管理下システムの BMC への接続

SOL プロキシセッションが確立された後、次の選択肢が表示されます。

```
1. Connect to the Remote Server's BMC (リモートサーバーの BMC への接続)

2. Configure the Serial-Over-LAN for the Remote Server (リモートサーバーへのシリアルオーバー LAN の設定)

3. Activate Virtual Console (仮想コンソールのアクティブ化)

4. Reboot and Activate Virtual Console (仮想コンソールの再起動とアクティブ化)
```

5. Help (ヘルプ)

6. Exit (終了)

メモ: 管理下システムでは、複数の SOL セッションを同時にアクティブにできますが、仮想コンソールセッションは一度に 1 つしかアクティブにできません。

メモ: アクティブな SOL セッションを終了するには、<~><.> 文字シーケンスを使用します。このシーケンスによって SOL が終了し、トップレベルメニューに戻ります。

1. メインメニューでオプション 1 を選択します。
2. リモート管理下システムの iDRAC6 **IP アドレス** を入力します。
3. 管理下システムの iDRAC6 に使用する iDRAC6 **ユーザー名** と **パスワード** を入力します。iDRAC6 のユーザー名とパスワードを割り当て、これらを iDRAC6 の不揮発性ストレージに保存する必要があります。

   メモ: iDRAC6 では一度に 1 つの SOL 仮想コンソールセッションのみ許可されます。

   メモ: 必要に応じて、iDRAC6 ウェブ GUI で **システム** → **リモートアクセス** → **iDRAC6** → **ネットワーク / セキュリティ** → **サービス** で Telnet **タイムアウト** の値をゼロに変更すると、SOL セッション時間を無制限に延長できます。

4. IPMI 暗号化キーを iDRAC6 で設定した場合は、それを入力します。

   メモ: iDRAC6 GUI の **システム**→**リモートアクセス**→**iDRAC6**→**ネットワーク / セキュリティ**→**ネットワーク**→**IPMI 設定**→ **暗号化キー** で IPMI 暗号化キーを見つけることができます。

   メモ: デフォルトの IPMI 暗号化キーはすべてゼロです。暗号化オプションで <Enter> キーを押すと、iDRAC6 はこのデフォルト暗号化キーを使用します。

5. メインメニューの **リモートサーバー用シリアルオーバー LAN の設定** (オプション 2)を選択します。

   SOL 設定メニューが表示されます。現在の SOL 状態によって SOL 設定メニューの内容は次のように変わります。

   - SOL が既に有効になっている場合、現在の設定が表示され 3 つの選択肢が提示されます。

     1. Disable Serial-Over-LAN (シリアルオーバー LAN を無効にする)
     2. Change Serial-Over-LAN settings (シリアルオーバー LAN の設定を変更する)
     3. Cancel (キャンセル)

   - SOL が有効になっている場合は、SOL ボーレートが iDRAC6 のボーレートと同じで、ユーザーにシステム管理者権限が付与されていることを確認してください。
   - 現在 SOL が無効になっている場合は、Y と入力して SOL を有効にするか、N を入力して SOL を 無効のままにします。

- メインメニューで **仮想コンソールの起動** (オプション 3)を選択します。

  リモート管理下システムのテキストコンソールが管理ステーションにリダイレクトされます。

7. メインメニューで **仮想コンソールの再起動とアクティブ化** (オプション 4)を選択します(オプション)。

   リモート管理下システムの電源状態が確認されます。電源がオンの場合は、正常なシャットダウンか強制シャットダウンかを選択します。

   次に、電源状態が **オン** に変わるまで、状態が監視されます。仮想コンソールが開始し、リモート管理下システムのテキストコンソールが管理ステーションにリダイレクトされます。

   管理下システムの再起動中に BIOS システム設定プログラムに切り替えて BIOS の設定や表示ができます。

8. メインメニューで **ヘルプ** (オプション 5)を選択すると、各オプションの詳しい説明が表示されます。
9. メインメニューで **終了** (オプション 6)を選択すると、Telnet セッションが終了して SOL プロキシから切断されます。

   メモ: ユーザーが SOL セッションを正しく終了しなかった場合は、次のコマンドを入力して iDRAC を再起動します。iDRAC6 の起動が完了するのに 1〜2 分かかります。詳細については、デルのサポートウェブサイト **support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』を参照してください。

   ```
   racadm racreset
   ```

オペレーティングシステムの設定

汎用 UNIX 系 オペレーティングシステムを設定するには、次の手順を実行します。この設定は、Red Hat Enterprise Linux 5.0、SUSE Linux Enterprise Server 10 SP1、Windows 2003 Enterprise のデフォルトインストールに基づくものです。

Linux Enterprise オペレーティングシステムの場合

1. **/etc/inittab** ファイルを編集して、ハードウェアフロー制御を有効にし、ユーザーが SOL コンソールからログインできるようにします。次の行を #Run gettys in standard runlevels セクションの末尾に追加します。

   ```
   7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
   ```

元の /etc/inittab の例:

```
_____________________________________________________________________

#

# inittab     This file describes how the INIT process should set
              up the system in a certain run-level (このファイルは
              INIT プロセスで特定ランレベルのシステムを セットアップする方
              法を記述します。)

#

SKIP this part of file (ファイルのこの部分をスキップします。)

# Run gettys in standard runlevels (gettys を標準ランレベルで実行します。)

1:2345:respawn:/sbin/mingetty tty1

2:2345:respawn:/sbin/mingetty tty1

3:2345:respawn:/sbin/mingetty tty1

4:2345:respawn:/sbin/mingetty tty1

5:2345:respawn:/sbin/mingetty tty1

6:2345:respawn:/sbin/mingetty tty1

# Run xdm in runlevel 5 (xdm をランレベル 5 で実行します。)

x:5:respawn:/etc/X11/prefdm -nodaemon

_____________________________________________________________________
```

変更後の /etc/inittab の例

```
_____________________________________________________________________

#

# inittab     This file describes how the INIT process should set
              up the system in a certain run-level (このファイルは
              INIT プロセスで特定ランレベルのシステムを セットアップする方
              法を記述します。)

#

SKIP this part of file (ファイルのこの部分をスキップします。)

# Run gettys in standard runlevels (gettys を標準ランレベルで実行します。)

1:2345:respawn:/sbin/mingetty tty1

2:2345:respawn:/sbin/mingetty tty1

3:2345:respawn:/sbin/mingetty tty1

4:2345:respawn:/sbin/mingetty tty1

5:2345:respawn:/sbin/mingetty tty1

6:2345:respawn:/sbin/mingetty tty1

7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220

# Run xdm in runlevel 5 (xdm をランレベル 5 で実行します。)

x:5:respawn:/etc/X11/prefdm -nodaemon

_____________________________________________________________________
```

2. **/etc/securetty** ファイルを編集して、ユーザーが SOL コンソールからルートユーザーとしてログインできるようにします。console の後に次の行を追加します。

   ```
   ttyS0
   ```

元の /etc/securetty の例:

```
_____________________________________________________________

      コンソール

      vc/1

      vc/2

      vc/3

      vc/4

      SKIP the rest of file (ファイルの残りの部分をスキップします。)

_____________________________________________________________
```

元の /etc/securetty の例:

```
_____________________________________________________________

      コンソール

      ttyS0

      vc/1

      vc/2

      vc/3

      vc/4

      SKIP the rest of file (ファイルの残りの部分をスキップします。)

_____________________________________________________________
```

3. **/boot/grub/grub.conf** または **/boot/grub/menu.list** ファイルを編集して、SOL の起動オプションを追加します。
   e. 各種の UNIX 系オペレーティングシステムで、グラフィカル表示行をコメントアウトします。
      - splashimage=(had0,0)/grub/splash.xpm.gz(RHEL 5 の場合)
      - gfxmenu (hda0,5)/boot/message(SLES 10 の場合)

   f. 最初の title= ... 行の前に次の行を追加します。

      # SOL 経由での OS 起動のリダイレクト

   g. 最初の title= ... 行の後に次のエントリを追加します。

      SOL リダイレクト

   h. 最初の title= ...:の kernel/_ 行の後に次のテキストを追加します。

      console=tty1 console=ttyS0,115200

   メモ: Red Hat Enterprise Linux 5 での **/boot/grub/grub.conf** は **/boot/grub/menu.list** へのシンボリックリンクです。どちらの設定も変更できます。

RHEL 5 の元の /boot/grub/grub.conf の例:

```
_____________________________________________________________

      # grub.conf generated by anaconda (grub.conf(作成者: anaconda))

      #

      # Note that you do not have to return grub after making changes to this file. (このファイルに変更を加えた後、grub を再実行する必要はありませんファイル。

      # NOTICE: You have a /boot partition. This means that all
        kernel and initrd paths are relative to /boot/, eg.
        (通知:/boot パーティションがあります。これは すべてのカーネルと
        initrd パスは /boot/ 相対的であることを意味します。たとえば、)

      #          root (hd0,0)

      # kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00

      #          initrd /boot/initrd-version.img

      #boot=/dev/sda

      default=0
```

```
timeout=5

splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu

Red Hat Enterprise Linux 5

root (hd0,0)

kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet

initrd /initrd-2.6.18-8.el5.img
```

変更後の **/boot/grub/grub.conf** の例:

```
# grub.conf generated by anaconda (grub.conf（作成者： anaconda）)

#

# Note that you do not have to return grub after making changes to this file. (このファイルに変更を加えた後、grub を再実行する必要はありませんファイル。

# NOTICE: You have a /boot partition. This means that all
  kernel and initrd paths are relative to /boot/, eg.
  (通知：/boot パーティションがあります。これは すべてのカーネルと
  initrd パスは /boot/ 相対的であることを意味します。たとえば、)

#          root (hd0,0)

# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00

#          initrd /boot/initrd-version.img

#boot=/dev/sda

default=0

timeout=5

#splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu

# Redirect the OS boot via SOL (SOL 経由での OS 起動のリダイレクト)

Red Hat Enterprise Linux 5 SOL リダイレクト

root (hd0,0)

kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet console=tty1 console=ttyS0,115200

initrd /initrd-2.6.18-8.el5.img
```

SLES 10 の元の **/boot/grub/menu.list** の例:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09 UTC 2008 (変更者：YaST2 最終変更日時：Sat Oct 11 21:52:09 UTC 2008)

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message

###Don't change this comment - YaST2 identifier: Original name: linux (このコメントは変更できません - YaST2 識別子: 元の名前: linux)###

SUSE Linux Enterprise Server 10 SP1

root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

SLES 10 の変更後の **/boot/grub/menu.list** の例:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09 (変更者 : YaST2 最終変更日時 : Sat Oct 11 21:52:09 UTC 2008)

デフォルト 0

タイムアウト 8

gfxmenu (hd0.5)/boot/message

###Don't change this comment - YaST2 identifier: Original name: linux (このコメントは変更できません - YaST2 識別子: 元の名前: linux)###

SUSE Linux Enterprise Server 10 SP1 SOL リダイレクト

root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts console=tty1
console=ttyS0,115200

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Windows 2003 Enterprise

1. Windows コマンドプロンプトで bootcfg と入力して、起動エントリ ID を確認します。OS フレンドリ名である **Windows Server 2003 Enterprise** でセクション用の起動エントリ ID を探します。<Enter> キーを押して、管理ステーションの起動オプションを表示します。

2. 次を入力して Windows コマンドプロンプトで EMS を有効にします。

   ```
   bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <起動 ID>
   ```

メモ: <起動 ID> はステップ 1 の起動エントリ ID です。

3. <Enter> キーを押して、EMS コンソール設定が有効になることを確認します。

オリジナルの bootcfg 設定の例:

```
Boot Loader Settings

--------------------

timeout :30

default :multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Boot Entries

--------------------

Boot entry ID:     1

Os Friendly Name: Windows Server 2003、Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

元の bootcfg 設定の例:

```
Boot Loader Settings

--------------------

timeout: 30

default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

redirect: COM1
```

```
redirectbaudrate:115200

Boot Entries

------------

Boot entry ID: 1

Os Friendly Name: Windows Server 2003, Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

目次ページに戻る

目次ページに戻る

GUI 仮想コンソールの使用法

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

本項では、iDRAC6 仮想コンソール機能の使用法について説明します。

概要

iDRAC6 仮想コンソール機能を使用すると、グラフィックまたはテキストモードでローカルコンソールにリモートアクセスでき、1 台または複数台の iDRAC6 対応システムを 1 か所から制御できます。

仮想コンソールの使用法

仮想コンソール 画面では、ローカルの管理ステーションのキーボード、ビデオ、およびマウスを使ってリモートシステムを管理し、リモート管理下サーバー上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、ソフトウェアのリモートインストールを実行できます。

仮想コンソールセッションには次の規則が適用されます。

- 各ブレードでサポートされる仮想コンソールは、最大 2 セッションです。両セッションで、同じ管理下サーバーコンソールを同時に表示します。
- 管理下システムのウェブブラウザから仮想コンソール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。

2 番目のユーザーが仮想コンソールセッションを要求すると、最初のユーザーは通知を受け取り、アクセス拒否、ビデオのみ許可、またはフル共有アクセスを許可するオプションから選択できます。2 番目のユーザーには、別のユーザーに制御権があることが通知されます。最初のユーザーが 30 秒以内に応答しないと、2 番目のユーザーへのアクセスは許可されません。2 つのセッションが同時にアクティブな間には、2 番目のユーザーがアクティブセッションを持つことを示すメッセージが、最初のユーザーの画面の右上隅に表示されます。

1 番目と 2 番目のどちらのユーザーもシステム管理者権限を持っていない場合は、1 番目のユーザーのアクティブセッションが終了すると、2 番目のユーザーのセッションも自動的に終了します。

ブラウザのキャッシュをクリアします。

仮想コンソールの操作中に問題（範囲外エラー、同期問題など）が発生した場合は、ブラウザのキャッシュをクリアして、システムに保存されている可能性のある古いバージョンのビューアを削除してから、再試行してください。

IE7 の古いバージョンの Active-X ビューアをクリアするには、次の手順を行います。

1. ビデオビューアと Internet Explorer ブラウザを閉じます。
2. Internet Explorer ブラウザを再び開き、**Internet Explorer** → **ツール** → **アドオンの管理** に移動し、**アドオンの有効化または無効化** をクリックします。**アドオンの管理** ウィンドウが表示されます。
3. **表示** ドロップダウンメニューから **Internet Explorer で使用されたアドオン** を選択します。
4. ビデオビューア アドオンを削除します。

IE8 の古いバージョンの Active-X ビューアをクリアするには、次の手順を行います。

1. ビデオビューアと Internet Explorer ブラウザを閉じます。
2. Internet Explorer ブラウザを再び開き、**Internet Explorer** → **ツール** → **アドオンの管理** に移動し、**アドオンの有効化または無効化** をクリックします。**アドオンの管理** ウィンドウが表示されます。
3. **表示** ドロップダウンメニューから **すべてのアドオン** を選択します。
4. ビデオビューア アドオンを選択し、**詳細情報** リンクをクリックします。
5. **詳細情報** ウィンドウから **削除** を選択します。
6. **詳細情報** と **アドオンの管理** ウィンドウを閉じます。

Windows または Linux で古いバージョンの Java ビューアをクリアするには、次の手順に従います。

1. コマンドプロンプトで javaws -viewer を実行します。
2. **Java Cache Viewe**r が表示されます。
3. iDRAC6 仮想コンソールクライアント と JViewer を削除します。

コマンドプロンプトと javaws -uninstall を実行して、キャッシュからすべてのアプリケーションを削除することもできます。

サポートされている画面解像度とリフレッシュレート

表 10-1 は、管理下サーバーで実行している仮想コンソールセッションでサポートされている 画面解像度と、そのリフレッシュレートを示しています。

表 10-1 サポートされている画面解像度とリフレッシュレート

画面解像度	リフレッシュレート (Hz)
720x400	70
640x480	60、72、75、85
800x600	60、70、72、75、85
1024x768	60、70、72、75、85
1280x1024	60

管理ステーションの設定

管理ステーションで仮想コンソールを使用するには、以下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。対応ウェブブラウザおよび 対応ウェブブラウザの設定を参照してください。
2. Firefox を使用している場合、または Internet Explorer で Java ビューアを使用する場合は、Java Runtime Environment(JRE)をインストールします。Java Runtime Environment(JRE)のインストール を参照してください。
3. モニターの解像度は 1280x1024 ピクセルに設定することをお勧めします。

   メモ: アクティブな仮想コンソールセッションがあり、仮想コンソールに低解像度のモニターが接続している場合は、ローカルコンソールでサーバーを選択すると、サーバーのコンソール解像度がリセットされることがあります。サーバーで Linux オペレーティングシステムを実行している場合は、ローカルモニタで X11 コンソールが表示されない可能性があります。仮想コンソールで <Ctrl><Alt><F1> を押すと、Linux がテキストコンソールに切り替わります。

4. Java プラグインを使用している仮想コンソールセッションの起動に Internet Explorer を使用する場合は、以下の手順を実行してください。
   a. Internet Explorer で、**Tools**（ツール）→**Internet Options**（インターネットオプション）→**Security**（セキュリティ）→**Trusted sites**（信頼済みサイト）→**Custom level**（カスタムレベル）の順にクリックします。

   メモ: 64 ビットの Windows 7 では、**Tools**（ツール）→**Internet Options**（インターネットオプション）→**Security**（セキュリティ）→**Internet**（インターネット）→**Custom level**（カスタムレベル）の順にクリックします。

   b. **Security Settings**（セキュリティ設定）ウィンドウで、**Automatic prompting for file download**（ファイルダウンロードの自動プロンプト）に **Disable**（無効にする）オプションを選択します。
   c. **OK** をクリックし、もう一度 **OK** をクリックします。

iDRAC6 ウェブインタフェースでの仮想コンソール と仮想メディアの設定

iDRAC6 ウェブインタフェースで仮想コンソールを設定するには、以下の手順を実行してください。

1. **システム** をクリックし、**仮想コンソール / メディア** タブをクリックしします。
2. **設定** をクリックして **設定** 画面を開きます。
3. 仮想コンソールのプロパティを設定します。「 表 10-2」で、仮想コンソールの設定について説明します。
4. 設定が完了したら、**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 10-3 を参照してください。

表 10-2 仮想コンソールの設定プロパティ

プロパティ	説明
有効	選択して、仮想コンソール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、仮想コンソールは有効です。 **チェックボックスがオフ** の場合は、仮想コンソールは無効です。 デフォルトは **有効** です。
最大セッション数	仮想コンソールに可能な最大セッション数（**1** または **2**）を表示します。仮想コンソールで許可する最大セッション数を変更するには、ドロップダウンメニューを使用します。デフォルトは **2** です。
アクティブセッション数	アクティブなコンソールセッション数を表示します。このフィールドは読み取り専用です。
キーボードとマウスのポート番号	仮想コンソールのキーボード / マウスオプションへの接続に使用するネットワークポート番号。トラフィックは常に暗号化されます。別のプログラムでデフォルトのポートが使用されている場合は、この番号を変更しなければならない可能性があります。デフォルトは **5900** です。
ビデオポート番号	仮想コンソール画面サービスへの接続に使用されるネットワークポート番号。別のプログラムでデフォルトのポートが使用されている場合は、この設定を変更しなければならない可能性があります。デフォルトは **5901** です。
ビデオ暗号化有効	**チェックボックスがオン** の場合は、ビデオの暗号化が有効です。ビデオポートを経由するすべての トラフィックは、暗号化されます。 **チェックボックスがオフ** の場合は、暗号化が無効です。ビデオポートを経由するトラフィックは暗号化されません。 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。**
マウスモード	管理下サーバーが Windows オペレーティングシステム環境で実行されている場合は、**Windows** を選択します。 管理下サーバーが Linux 環境で実行している場合は、**Linux** を選択します。 サーバーが Windows または Linux オペレーティングシステム環境で実行していない場合は、**USC/Diags** を選択します。 **メモ:** HyperV、Dell Diagnostics、または USC（システムサービス）で **USC/Diags** を選択する必要があります。 デフォルトは **Windows** です。
IE 用コンソールプラグインタイプ	Windows オペレーティングシステム上で Internet Explorer を使用している場合は、次のビューアから選択できます。 **ActiveX** - ActiveX 仮想コンソールビューア **Java** - Java 仮想コンソールビューア **メモ:** Internet Explorer のバージョンによっては、追加のセキュリティ制限をオフにする必要があります（「仮想メディアの設定と使用」を参照）。 **メモ:** Java ビューアを使用するには、クライアントシステムに Java Runtime Environment がインストールされている必要があります。
ローカルサーバービデオを有効にする	**このチェックボックスがオン** の場合は、仮想コンソール中、仮想コンソールモニターへの出力が有効になっています。**チェックボックスがオフ** は、**仮想コンソール** を使用して実行するタスクが管理下サーバーのローカルモニターに表示されません。

メモ: 仮想コンソール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」を参照してください。

表 10-5 のボタンは **仮想コンソールの設定** 画面にあります。

表 10-3 仮想コンソールの設定ボタン

ボタン	定義
印刷	**設定** 画面を印刷します。
更新	**設定** 画面を再ロードします。
適用	仮想コンソールに追加した新しい設定を保存します。

仮想コンソールセッションを開く

仮想コンソールセッションを開くと、Dell 仮想コンソールビューアアプリケーション（**iDRACView**）が開始し、リモートシステムのデスクトップがビューアに表示されます。**iDRACView** を使用すると、ローカル管理ステーションからリモートシステムのマウスとキーボードの機能を制御できます。

メモ: Windows Vista 管利ステーションから仮想コンソールを起動すると、仮想コンソールの再起動メッセージが表示される可能性があります。これを回避するには、**コントロールパネル→電源オプション→省電力→詳細設定→ハードディスク→次の時間が経過後ハードディスクの電源を切る** と **コントロールパネル→電源オプション→高パフォーマンス→詳細設定→ハードディスク→ 次の時間が経過後ハードディスクの電源を切る** の 2 か所で適切なタイムアウト値を設定します。

ウェブインタフェースで仮想コンソールセッションを開くには、以下の手順を実行してください。

1. **システム** → **仮想コンソール / メディア** タブ → **仮想コンソールと仮想メディア** の順にクリックします。

2. **仮想コンソールと仮想メディア** 画面で、「表 10-4」の情報を使用して、仮想コンソールのセッションが使用可能であることを確認します。

   表示されているプロパティ値の設定を変更する場合は、「iDRAC6 ウェブインタフェースでの仮想コンソール と仮想メディアの設定」を参照してください。

表 10-4 仮想コンソールの情報

プロパティ	説明
仮想コンソールを有効にする	**はい** / **いいえ**
ビデオ暗号化を有効にする	**はい** / **いいえ**
最大セッション数	サポートされている仮想コンソールセッションの最大数を表示します。
アクティブなセッション数	現在アクティブな仮想コンソールセッション数を表示します。
マウスモード	現在有効なマウスアクセラレータが表示されます。**マウスモード** は、管理下サーバーにインストールされているオペレーティングシステムの種類に応じて選択する必要があります。
コンソールのプラグインタイプ	現在設定されているプラグインタイプが表示されます。 **ActiveX** - Active-X ビューアが起動します。Active-X ビューアは、Windows オペレーティングシステム上で実行する場合、Internet Explorer でのみ使用できます。 **Java** - Java ビューアが起動します。Java ビューアは、Internet Explorer を含め、どのブラウザでも使用できます。クライアントが Windows 以外のオペレーティングシステムで実行されている場合は、Java ビューアを使用する必要があります。Windows オペレーティングシステム環境で、Internet Explorer を使用して iDRAC6 にアクセスする場合は、プラグインの種類として **Active-X** または **Java** を選択できます。 **メモ:** プラグインの種類として **Java** を選択している場合、Internet Explorer 8 で初回仮想コンソールが起動しない場合があります。
ローカルサーバービデオ有効	**はい** の場合は、仮想コンソール中、仮想コンソールモニタへの出力が有効になっています。**いいえ** の場合は、**仮想コンソール**を使用して実行したタスクが管理下サーバーのローカルモニタに表示されません

メモ: 仮想コンソール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」を参照してください。

表 10-5 のボタンは **仮想コンソールの設定** 画面にあります。

表 10-5 仮想コンソールのボタン

ボタン	定義
更新	**仮想コンソールの設定** 画面を再ロードします。
仮想コンソールの起動	目的のリモートシステムで仮想コンソールセッションを開きます。
印刷	**仮想コンソールの設定** 画面を印刷します。

3. 仮想コンソールが使用可能な場合は、**仮想コンソールの起動** 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、リモートシステムのデスクトップが **iDRACView** に表示されます。

4. 2 つのマウスポインタ(1 つはリモートシステム用、もう 1 つはローカルシステム用)がビューアウィンドウに表示されます。リモートのマウスポインタがローカルのマウスポインタに従うように 2 つのマウスポインタを同期する必要があります。マウスポインタの同期 を参照してください。

仮想コンソールのプレビュー

仮想コンソールを起動する前に、**システム** →**プロパティ**→**システム概要** ページで仮想コンソールの状態をプレビューできます。**仮想コンソールのプレビュー** セクションに、仮想コンソールの状態を示すイメージが表示されます。このイメージは 30 秒ごとに自動更新されます。

メモ: 仮想コンソールイメージは、仮想コンソールを有効にしている場合にのみ表示できます。

表 10-6 で、使用可能なオプションについて説明します。

表 10-6 仮想コンソールのプレビューオプション

オプション	説明
起動	仮想コンソールを起動するには、このボタンをクリックします。 仮想メディアのみが有効になっている場合に、このリンクをクリックすると、仮想メディアが直接起動されます。 このボタンは、仮想コンソール権限がない場合や、仮想コンソールと仮想メディアの両方が無効になっている場合は、使用不可になります。
設定	仮想コンソールの設定を表示または編集するには、**仮想コンソール / 仮想メディアの設定** ページでこのリンクをクリックします。
更新	表示されたコンソールイメージを更新するには、このボタンをクリックします。

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きます。

メモ: 仮想コンソールのタイトルバーには、管理ステーションから接続している iDRAC の DNS 名または IP アドレスが表示されます。iDRAC に DNS 名がない場合は、IP アドレスが表示されます。フォーマットは次のとおりです。
`<DNS 名 / IPv6 アドレス / IPv4 アドレス>, <モデル>, <スロット番号>, User: <ユーザー名>, <fps>`

ビデオビューアは、カラーモード、マウスの同期、スナップショット、キーボードマクロ、電力操作、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の調整機能を提供しています。これらの機能の詳細については、**ヘルプ** をクリックしてください。

仮想コンソールのセッションを開始し、ビデオビューアが表示されたら、カラーモードの調整や、マウスポインタの同期が必要になる場合があります。

表 10-7 は、ビューアで使用可能なメニューオプションについて説明しています。

表 10-7 ビューアメニューバーの選択項目

メニュー項目	項目	説明
ビデオ	一時停止	仮想コンソールを一時停止します。
	再開	仮想コンソールを再開します。
	更新	ビューアの画面イメージを再描画します。
	現在の画面のキャプチャ	リモートシステムの現在の画面をキャプチャし、**.bmp** ファイルとして保存します。ダイアログボックスが表示され、指定した場所にファイルを保存できます。
	全画面	Video Viewer を全画面表示にするには、ビューアの右上隅をクリックします。
	終了	コンソールの使用を終了し、(リモートシステムのログアウト手順に従って)ログアウトしたら、**ビデオ** メニューから **終了** を選択して **Video Viewer** ウィンドウを閉じます。
キーボード	右 <Alt> キーを押し続ける	右 <Alt> キーと組み合わせるキーを入力する前にこのアイテムを選択します。
	左 <Alt> キーを押し続ける	左 <Alt> キーと組み合わせるキーを入力する前にこのアイテムを選択します。
	左 <Windows> キー	左 <Windows> キーと組み合わせる文字を入力する前に **押し続ける** を選択します。左 <Windows> キーのキーストロークを送信するには、**押して離す** を選択します。
	右 <Windows> キー	右 <Windows> キーと組み合わせる文字を入力する前に **押し続ける** を選択します。右 <Windows> キーのキーストロークを送信するには、**押して離す** を選択します。
	マクロ	マクロを選択するか、マクロに指定されたホットキーを入力すると、リモートシステムでその操作が実行されます。ビデオビューアでは、次のマクロを使用できます。 - Alt+Ctrl+Del - Alt+Tab - Alt+Esc - Ctrl+Esc - Alt+Space - Alt+Enter - Alt+ -(ハイフン) - Alt+F4 - PrtScrn - Alt+PrtScrn - F1 - 一時停止 - Alt+M - Alt+D - Alt+PrtScrn+M - Alt+PrtScrn+P
	キーボードのパススルー	キーボードのパススルーモードでは、クライアント上のすべてのキーボード機能をサーバーにリダイレクトできます。
マウス	カーソルの同期	クライアント上のマウスがサーバー上のマウスへリダイレクトされるように同期します。
	ローカルカーソルを非表示にする	仮想コンソールからのカーソルのみが表示されます。仮想コンソールで USC を実行する場合は、この設定を使用することをお勧めします。
オプション	カラーモード	ネットワークパフォーマンスを向上させるための色深度を選択できます。たとえば、仮想メディアからソフトウェアをインストールする場合は、最小の色深度を選択すると、コンソールビューアが使用するネットワーク帯域幅を減らして、より多くの帯域幅をメディアからのデータ転送用に残しておくことができます。 色モードは 15 ビットカラーと 7 ビットカラーに設定できます。
電源	システムの電源オン	システムの電源を入れます。
	システムの電源オフ	システムの電源を切ります。
	正常なシャットダウン	システムをシャットダウンします。

	システムをリセットする(ウォームブート)	電源を切らずにシステムを再起動します。
	システムの電源を入れ直す(コールドブート)	システムの電源を切ってから再起動します。
メディア	**仮想メディアウィザード**	**メディア** メニューから仮想メディアウィザードにアクセスでき、以下のようなデバイスまたはイメージにリダイレクトできます。 - フロッピードライブ - CD - DVD - ISO フォーマットのイメージ - USB フラッシュドライブ 仮想メディアの機能については、「仮想メディアの設定と使用」を参照してください。 仮想メディアを使用するときは、コンソールビューアウィンドウをアクティブにしておく必要があります。
ヘルプ	**iDRACView バージョン情報**	iDRACView のバージョンを表示します。

マウスポインタの同期

仮想コンソールを使用してリモート Dell PowerEdge システムに接続すると、リモートシステムのマウスアクセラレータ速度が管理ステーションのマウスポインタと同期せず、ビデオビューアウィンドウにマウスポインタが 2 つ表示される場合があります。

マウスポインタを同期するには、**マウス** → **カーソルの同期** の順にクリックするか、<Alt> <M> キーを押します。

カーソルの同期 メニューアイテムは切り替え式です。メニューのアイテムの横にチェックマークがあり、マウスの同期がアクティブであることを確認してください。

Red Hat Enterprise Linux または Novell SUSE Linux を使用している場合は、ビューアを起動する前に必ず Linux 用のマウスモードに設定してください。設定の詳細については、「iDRAC6 ウェブインタフェースでの仮想コンソール と仮想メディアの設定」を参照してください。iDRAC 6 **仮想コンソール** 画面でマウス矢印を制御するには、オペレーティングシステムのデフォルトのマウス設定が使用されます。

ローカルコンソールを無効 / 有効にする

iDRAC6 ウェブインタフェースを使用して、仮想コンソールの接続を許可しないように iDRAC6 を設定できます。ローカルコンソールが無効になると、黄色の状態表示ドットがサーバーリスト(OSCAR)に表示され、コンソールが iDRAC6 でロックされていることを示します。ローカルコンソールが有効なときは、状態表示ドットが緑色で表示されます。

管理下サーバーのコンソールへの排他的アクセスを確保するには、ローカルコンソールを無効にし、また **仮想コンソール 画面** で **最大セッション数** を 1 に再設定する必要があります。

メモ: サーバー上のローカルビデオを無効にする(オフにする)と、仮想コンソールに接続しているモニター、キーボード、および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、次の手順に従ってください。

1. 管理ステーションで、対応ウェブブラウザを開いて iDRAC6 にログインします。詳細については、ウェブインタフェースへのアクセス を参照してください。
2. **システム** をクリックし、**仮想コンソール / メディア** タブをクリックして、**設定** をクリックします。
3. サーバーでローカルビデオを無効にする(オフにする)には、**設定** 画面で **ローカルサーバービデオを有効にする** を選択解除してから **適用** をクリックします。デフォルト値は **有効(オン)** です。
4. サーバーでローカルビデオを有効にする(オンにする)には、**設定** 画面で **ローカルサーバービデオを有効にする** を選択してから **適用** をクリックします。

仮想コンソール 画面にローカルサーバービデオのステータスが表示されます。

仮想コンソールと仮想メディアのリモート起動

仮想コンソールまたは仮想メディアは、iDRAC6 ウェブインタフェースから起動する代わりに、サポートされているブラウザで URL を 1 つ入力して起動できます。使用しているシステム構成によっては、手動の認証手順(ログインページ)を踏むか、仮想コンソールまたは仮想メディアビューア(iDRACView)に自動転送されます。

メモ: Internet Explorer はローカル、Active Directory(AD)、スマートカード(SC)、およびシングルサインオン(SSO)ログインをサポートします。Firefox は、SSO、ローカル、および AD ログインをサポートしています。

URL フォーマット

ブラウザに **https://<idrac6_ip>/console** のリンクを入力する場合、ログイン設定によっては、通常の手動ログイン手順に従わなければならない場合があります。SSO が有効でなく、ローカル、AD、または SC ログインが有効である場合は、対応するログインページが表示されます。ログインに成功すると、仮想コンソールまたは仮想メディアのビューは起動しません。代わりに、iDRAC6 GUI ホームページに転送されます。

メモ: **iDRACView** を起動するために使用する URL は、大文字と小文字が区別され、小文字のみで入力する必要があります。

一般的なエラーシナリオ

表 10-8 は、一般的なエラーのシナリオ、それらエラーの原因、そして iDRAC6 の動作を記載しています。

表 10-8 エラーシナリオ

エラーシナリオ	原因	動作
ログインに失敗しました	無効なユーザー名または不正なパスワードが入力されました。	https://<ip> を入力してログインに失敗した場合と同じ動作が見られます。
権限が不十分です	仮想コンソールと仮想メディアの権限がありません。	iDRACView は起動せずに、仮想コンソール / メディアの設定 GUI ページにリダイレクトされます。
仮想コンソールが無効になっています。	仮想コンソールがシステムで無効になっています。	iDRACView は起動せずに、仮想コンソール / メディアの設定 GUI ページにリダイレクトされます。
不明な URL パラメータが検出されました	入力した URL に未定義のパラメータが含まれています。	「ページが見つかりません(404)」というメッセージが表示されます。

よくあるお問い合わせ(FAQ)

表 10-9 は、よくあるお問い合わせとその回答です。

表 10-9 仮想コンソールの使用法:よくあるお問い合わせ(FAQ)

質問	回答
帯域外のウェブ GUI をログアウトすると、仮想コンソールがログアウトに失敗します。	ウェブセッションをログオフしても、仮想コンソールと仮想メディアのセッションはアクティブなままになります。仮想メディアと仮想コンソールのビューアアプリケーションを終了して、それらのセッションからログアウトします。
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、ビデオはすぐにオンになります。
ローカルユーザーがビデオをオフにすることもできますか。	はい。ローカルユーザーは ローカル RACADM CLI を使ってビデオをオフにできます。
ローカルユーザーがビデオをオンにすることもできますか。	いいえ ローカルコンソールを無効にすると、ローカルユーザーのキーボードとマウスは無効になるため、設定を変更することはできません。
ローカルビデオをオフに切り替えると、ローカルキーボードとマウスもオフになりますか。	はい。
ローカルコンソールをオフにすると、リモートコンソールセッションのビデオはオフになりますか。	いいえ。ローカルビデオのオン / オフを切り替えても、リモートコンソールセッションには影響しません。
iDRAC6 ユーザーがローカルサーバービデオをオン / オフにするために必要な権限は何ですか。	iDRAC6 の設定権限を持つユーザーであれば、ローカルコンソールをオン / オフにできます。
ローカルサーバービデオの現在の状態を取得するには、どのようにしますか。	状態は iDRAC6 ウェブインタフェースの **仮想コンソールと仮想メディア** 画面に表示されます。 RACADM CLI コマンドの `racadm getconfig -g cfgRacTuning` は、**cfgRacTuneLocalServerVideo** のオブジェクトに状態を表示します。この `racadm` コマンドは、Telnet/SSH または iDRAC6 のリモートセッションから実行できます。 リモートの RACADM コマンド: `racadm -r <iDRAC の IP アドレス> -u <ユーザー> -p <パスワード> getconfig -g cfgRacTuning` ステータスは、仮想コンソールの OSCAR ディスプレイにも表示されます。ローカルコンソールが有効な場合、サーバー名の横に緑色の状態表示ドットが表示されます。無効な場合は、ローカルコンソールが iDRAC6 によってロックされていることを示す黄色の状態表示ドットが表示されます。
仮想コンソール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の解像度が `1280x1024` に設定されていることを確認してください。
コンソールウィンドウが文字化けします。	Linux の仮想コンソールビューアには UTF-8 文字セットが必要です。ロケールを確認し、必要に応じて文字コードをリセットしてください。詳細については、Linux のロケール設定を参照してください。
Windows 2000 オペレーティングシステムをロードすると、管理下サーバーの画面に何も表示されないのはなぜですか。	管理下サーバーに正しい ATI ビデオドライバがありません。ビデオドライバをアップデートしてください。
仮想コンソールを実行しているときに DOS でマウスが同期しないのはなぜですか。	Dell BIOS はマウスドライバを PS/2 マウスとしてエミュレートしています。設計上、PS/2 マウスはマウスポインタの相対位置を使用するため、同期のずれが生じます。iDRAC6 には USB マウスドライバが搭載されているので、マウスポインタの絶対位置と正確な追跡が可能です。iDRAC6 が USB の絶対的なマウスの位置を Dell BIOS に通知しても、BIOS エミュレーションによって相対的な位置に戻されるため、動作は変わりません。この問題を修正するには、**設定** 画面の **USC/Diags** でマウスモードを設定します。
Linux テキストコンソール(Dell Unified Server Configurator(USC)、Dell Lifecycle Controller(LC)、または Dell Unified Server Configurator Lifecycle Controller Enabled(USC-LCE)のいずれか)で、マウスが同期しないのはなぜですか。	仮想コンソールには USB マウスドライバが必要ですが、USB マウスドライバは X-Window オペレーティングシステムでのみ使用可能です。
マウスの同期の問題がまだ解決しません。	仮想コンソールのセッションを開始する前に、オペレーティングシステムに適したマウスが選択されていることを確認してください。 **マウス** メニューで、**マウスの同期** が選択されていることを確認します。マウスの同期を切り替えるには、<Alt><M> キーを押すか、**マウス** → **マウスの同期** の順に選択します。同期が有効になっている場合、**マウス** メニューで選択項目の横にチェックマー

	クが表示されます。
iDRAC6 仮想コンソール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している間、キーボードやマウスを使用できないのはなぜですか。	BIOS で仮想コンソールが有効になっているシステムで、サポートされている Microsoft 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、BIOS で仮想コンソールを再インストールしてから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、仮想コンソールが有効である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、必ず仮想コンソールを 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 の状態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仮想コンソールの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。	仮想コンソール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。
仮想コンソールの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。
仮想コンソールのセッションを実行するために必要な帯域幅はどれくらいですか。	良いパフォーマンスを得るには、5 MB/ 秒での接続をお勧めします。最低限必要な性能を得るためには、1 MB/秒での接続が必要です。
管理ステーションで仮想コンソールを実行するの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。
仮想コンソールを起動した後、マウスを仮想コンソールでしか使用できず、ローカルシステムで使用できません。なぜこうなるのですか。仮想コンソールとローカルシステムでマウスを使うには、どうすればよいでしょうか。	これは、**マウスモード** が **USC / Diags** に設定されている場合に起こります。ローカルシステムでマウスを使用するには、<Alt><M> ホットキーを押してください。仮想コンソールでマウスを使用するには、もう一度 <Alt><M> を押してください。

目次ページに戻る

目次ページに戻る

vFlash SD カードの設定とvFlash パーティションの管理

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

vFlash メディアカードは、セキュアデジタル(SD) カードで、システムの奥の隅にあるオプションの iDRAC6 Enterprise カードスロットに挿入します。ストレージ容量を提供し、通常の USB フラッシュキーのように動作します。これは、システムが USB デバイスとして認識するように設定できるユーザー定義パーティションの保存場所で、ブータブル USB デバイスの作成にも使用されます。選択したエミュレーションモードによって、パーティションはフロッピードライブ、ハードドライブ、または CD/DVD としてシステムに認識されます。これらはどれもブータブルデバイスとして設定できます。

vFlash SD カードと標準 SD カードがサポートされています。vFlash SD カードとは、vFlash の新機能をサポートしているカードを指します。標準 SD カードとは、vFlash の一部の機能だけをサポートしている市販の普通の SD カードを指します。

vFlash SD カードを使用すると、最大 16 個のパーティションを作成できます。パーティションの作成時にラベル名を指定したり、パーティションの管理や使用のためのさまざまな操作を実行したりできます。vFlash SD カードは 8GB までの任意のサイズにでき、各パーティションは最大 4GB までに設定できます。

標準 SD カードのサイズには制限はありませんが、サポートできるパーティションは 1 つだけです。パーティションのサイズは 256MB に制限されています。パーティションのラベル名は、デフォルトで VFLASH です。

メモ: iDRAC6 Enterprise カードスロットには、vFlash または標準 SD カード以外のカードを挿入しないでください。他のフォーマットのカード(たとえば、マルティメディアカード(MMC))を挿入すると、カードを初期化するときに、An error has occurred while initializing SD card (「SD カードの初期化中にエラーが発生しました」というメッセージが表示されます)。

システム管理者は、vFlash のパーティションのすべての操作を実行できます。それ以外のユーザーがパーティションのコンテンツを作成、削除、フォーマット、連結、コピーするには、仮想メディアへのアクセス権限が必要になります。

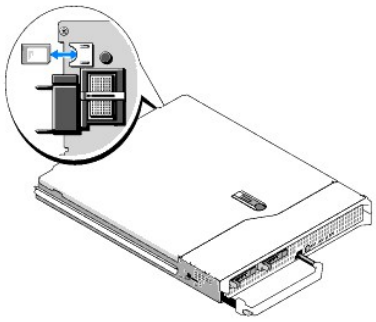
メモ: 実行できる vFlash 操作は一度に 1 つだけです。別の vflash 操作を実行する前に、最初の操作が完了する必要があります。たとえば、RACADM を使用して イメージから作成 操作を開始した場合、RACADM または GUI を使用して作成、ダウンロード、フォーマットなどの操作を実行することはできません。この操作の完了を待ってから、次の vFlash 操作を実行する必要があります。

---

vFlash または標準 SD カードの取り付け

1. シャーシからブレードを取り外します。
2. システムの奥の隅に vFlash メディアスロットがあります。

   メモ: カードの取り付けや取り出し時に、ブレードカバーを外す必要はありません。



3. ラベル側を上に向けて、SD カードの接続ピン側をモジュールのカードスロットに挿入します。

   メモ: スロットは正しい方向にしかカードを挿入できないように設計されています。

4. カードを押し込んでスロットにロックします。
5. シャーシにブレード取り付けます。

vFlash または標準 SD カードの取り外し

VFlash メディアカードを取り外すには、カードを押してロックを解除し、カードスロットから引き出します。

iDRAC6 ウェブインタフェースを使用した vFlash または標準 SD カードの設定

vFlash または標準 SD カードをインストールした後、そのプロパティを表示したり、vFlash を有効または無効にしたり、カードを初期化したりできます。パーティション管理を実行するには、カードを有効にする必要があります。カードが無効になっていると、プロパティの表示しかできません。初期化操作によって既存のパーティションが削除され、カードがリセットされます。

メモ: vFlash を有効または無効にしたり、カードを初期化したりするには、iDRAC の設定権限が必要です。

システムの iDRAC6 Enterprise カードスロットにカードがない場合は、次のエラーメッセージが表示されます。

`SD card not detected. Please insert an SD card of size 256MB or greater.` (SD カードが検出されませんでした。256MB 以上の容量の SD カードを挿入してください。)

vFlash または標準 SD カードを表示して設定するには、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、iDRAC6 ウェブインタフェースにログインします。
2. システムツリーで **システム** を選択します。
3. **vFlash** タブをクリックします。**SD カードのプロパティ** ページが表示されます。

   表 11-1 は、SD カードに表示されるプロパティのリストです。

表 11-1 SD カードのプロパティ

属性	説明
名前	サーバーの iDRAC6 Enterprise カードスロットに入っているカードの名前が表示されます。カードが vFlash の新しい拡張機能をサポートしている場合は、vFlash SD カード と表示されます。vFlash の一部の機能しかサポートしていない場合は、SD カード と表示されます。
サイズ	カードのサイズをギガバイト(GB)で表示します。
空き容量	SD カードの空き容量を MB で表示します。この容量を使用して vFlash SD カードにさらにパーティションを作成できます。 挿入されている SD カードが初期化されていない場合は、空き容量 としてカードが初期化されていないことが表示されます。
書き込み禁止	カードが書き込み禁止かどうかを表示します。
正常性	SD カードの全体的な状態を表示します。以下の状態があります。 • 正常 • 警告 • 重要 警告 の場合は、カードを再初期化してください。 重要 の場合は、カードを再インストールして再初期化してください。
vFlash 有効	カードで vFlash のパーティション管理を実行するには、このチェックボックスをオンにします。vFlash のパーティション管理を無効にするには、このチェックボックスをオフにします。

4. **適用** をクリックして、カードの vFlash パーティションの管理を有効または無効にします。

   vFlash のパーティションが連結されている場合は、vFlash を無効にできず、エラーメッセージが表示されます。

   メモ: vFlash が無効になっている場合は、SD カードのプロパティを表示できるだけで、パーティションの作成(空のパーティションの作成、およびイメージファイルを使用したパーティションの作成)、パーティションの管理、パーティションのフォーマット、パーティションのコンテンツのダウンロードなど、vFlash のその他の操作は実行できません。

5. **初期化** をクリックします。既存のパーティションがすべて削除され、カードがリセットされます。確認メッセージが表示されます。
6. **OK** をクリックします。初期化操作が完了すると、初期化が成功したことを知らせるメッセージが表示されます。

   メモ: **初期化** は、**vFlash 有効** オプションを選択した場合にのみ使用可能になります。

   vFlash のパーティションが連結されている場合は、初期化操作に失敗し、エラーメッセージが表示されます。

WSMAN プロバイダ、iDRAC6 設定ユーティリティ、RACADM などのアプリケーションが vFlash を使用している場合や、GUI の別ページに移動すると、iDRAC6 に次のメッセージが表示される可能性があります。

`SD card is temporarily unavailable. To retry, click Refresh.` (SD カードは一時的に使用不可になっています。再試行するには、更新 をクリックしてください。)

RACADM を使用した vFlash または標準 SD カードの設定

vFlash または標準 SD カードは、ローカル、リモート、Telnet/SSH コンソールから RACADM コマンドを使用して表示し、設定できます。

メモ: vFlash を有効または無効にしたり、カードを初期化したりするには、iDRAC の設定権限が必要です。

vFlash または標準 SD カードのプロパティの表示

サーバーへの Telnet/SSH/ シリアルコンソールを開いてログインし、次のコマンドを実行します。

```
racadm getconfig -g cfgvFlashSD
```

次の読み取り専用プロパティが表示されます。

- `cfgvFlashSDSize`
- `cfgvFlashSDLicense`
- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`

vFlash または標準 SD カードを有効または無効にする

サーバーへの Telnet/SSH/ シリアルコンソールを開いてログインし、次のコマンドを実行します。

- vFlash または標準 SD カードを有効にするには、次のコマンドを実行します。

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
  ```

- vFlash または標準 SD カードを有効にするには、次のコマンドを実行します。

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
  ```

メモ: RACADM コマンドは、vFlash または標準 SD 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、ERROR: SD Card not present. (エラー:SD カードがありません というメッセージが表示されます。)

vFlash または標準 SD カードの初期化

サーバーへの Telnet/SSH/ シリアルコンソールを開いてログインし、次のコマンドを実行します。

```
racadm vflashsd initialize
```

既存のパーティションがすべて削除され、カードがリセットされます。

vFlash または標準 SD カードの最後の状態の取得

サーバーへの Telnet/SSH シリアルコンソールを開いてログインし、次のコマンドを入力して、最後に vFlash または標準 SD カードに送られたコマンドの状態を取得します。

```
racadm vFlashsd status
```

vFlash または標準 SD カードのリセット

サーバーへの Telnet/SSH/ シリアルコンソールを開いてログインし、次のコマンドを実行します。

```
racadm vflashsd initialize
```

`vflashsd` の詳細については、デルサポートサイト **support.dell.com / manuals** で『iDRAC 管理者リファレンスガイド』を参照してください。

メモ: `racadm vmkey reset` コマンドは 1.5 のリリース以降は使用されなくなりました。このコマンドの機能は、現在は `vflashsd initialize` が行っています。 `vmkey reset` コマンドはまだ実行できますが、`vflashsd initialize` コマンドの使用をお勧めします。詳細については、「vFlash または標準 SD カードの初期化」を参照してください。

---

iDRAC6 ウェブインタフェースを使った vFlash パーティションの管理

以下の操作を実行できます。

- 空のパーティションの作成
- イメージファイルを使用したパーティションの作成
- パーティションのフォーマット
- 使用可能なパーティションの表示

- パーティションの変更
- パーティションの連結 / 分離
- 既存のパーティションの削除
- パーティションの内容のダウンロード
- パーティションの起動

空のパーティションの作成

空のパーティションは空の USB キーのようなものです。空のパーティションは vFlash と標準 SD カード上のどちらでも作成できます。パーティションタイプとして フロッピー または ハードディスク を選択できます。CD のパーティションタイプは、空のパーティションの作成ではサポートされていません。

メモ: 空のパーティションを作成するには、仮想メディアへのアクセス権限が必要です。

空のパーティションを作成する前に、以下の点を確認してください。

- カードが初期化されている。
- カードが書き込み禁止でない。
- カードの初期化操作がまだ実行されていない。

空の vFlash パーティションを作成するには、次の手順を実行します。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash** タブ →**空のパーティションの作成** サブタブの順に選択します。**空のパーティションの作成** ページが表示されます。
2. 「表 11-2」で説明されている情報を入力します。
3. **適用** をクリックします。新しいパーティションが作成されます。

   メモ: パーティションの作成中、進行状況や状態は表示されません。

   以下の場合には、エラーメッセージが表示されます。

   - カードが書き込み禁止である。
   - ラベル名が既存のパーティションのラベルと同じである。
   - パーティションサイズとして整数以外の値を入力したか、値がカードの空き容量を越えたか、要求したパーティションサイズが 4GB を超えている。
   - すでにカードの初期化操作が実行中である。

   メモ: 新しいパーティションがフォーマットされていない（生）。

表 11-2 空のパーティションページの作成オプション

フィールド	説明
インデックス	パーティションのインデックスを選択します。未使用のインデックスのみがドロップダウンリストに表示されます。使用可能な一番小さいインデックスがデフォルトで選択されています。ドロップダウンリスト内の別のインデックス値に変更できます。 **メモ:** 標準 SD カードでは、インデックス 1 しか使用できません。
ラベル	新しいパーティションに一意なラベルを入力します。ラベル名には最大 6 文字までの英数字を使用できます。ラベル名に空白文字を含めないでください。文字は大文字で表示されます。 **メモ:** 標準 SD カードの場合、ラベル名は VFLASH でなければなりません。それ以外のラベル名を入力すると、エラーメッセージが表示されます。
エミュレーションタイプ	パーティションのエミュレーションタイプをドロップダウンリストから選択します。使用可能なオプションは **フロッピー** と **HDD** です。
サイズ	パーティションのサイズをメガバイト（MB）で入力します。最大パーティションサイズは 4 GB、または vFlash SD カードの空き容量以下です。 **メモ:** 標準 SD カードの場合、パーティションサイズは 256MB までです。

イメージファイルを使ったパーティションの作成

イメージファイル（**.img** または **.iso** 形式）を使用して vFlash または標準 SD カードに新しいパーティションを作成できます。作成できるパーティションタイプは、フロッピー、ハードディスク、または CD です。作成されたパーティションは読み取り専用です。

メモ: パーティションを作成するには、仮想メディアへのアクセス権限が必要です。

新しく作成されたパーティションのサイズは、イメージファイルのサイズと同じです。イメージファイルサイズの要件は以下のとおりです。

- カードの空き容量以下。
- 4GB 以下。最大パーティションサイズは 4GB です。

ウェブインタフェースを使用する場合、vFlash SD カードにアップロードできるイメージのサイズは、32ビットのブラウザでも64ビットのブラウザ（Internet Explorer と FireFox）でも最大 2GB に制限されています。.

RACADM や WSMAN インタフェースを使用する場合に vFlash SD カードにアップロードできるイメージサイズは最大 4GB です。

標準 SD カードの場合、イメージサイズは 256MB 以下でなければなりません。

イメージファイルからパーティションを作成する前に、以下の点を確認してください。

- カードが初期化されている。
- カードが書き込み禁止でない。
- まだカードの初期化操作が実行されていない。

メモ: イメージファイルからパーティションを作成する場合は、イメージタイプとエミュレーションタイプが一致するようにしてください。iDRAC は、指定したイメージタイプに基づいてデバイスをエミュレートします。アップロードされたイメージとエミュレーションのタイプが一致しないと、問題が発生する可能性があります。たとえば、ISOイメージを使用してパーティションが作成され、エミュレーションタイプがハードディスクと指定されていると、BIOSはこのイメージから起動できません。

イメージファイルを使用して vFlash のパーティションを作成するには、以下の手順を実行します。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash** タブ →**イメージから作成** サブタブの順に選択します。**イメージファイルからのパーティションの作成** ページが表示されます。
2. 「表 11-3」で説明されている情報を入力します。
3. **適用** をクリックします。イメージファイルを使用して、新しいパーティションが作成されます。

   メモ: パーティションの作成中、進行状況や状態は表示されません。

   以下の場合は、エラーメッセージが表示されます。

   - カードが書き込み禁止である。
   - ラベル名が既存のパーティションのラベルと同じである。
   - イメージファイルのサイズが 4GB を超えているか、カードの空き容量を超えている。
   - イメージファイルが存在しないか、イメージファイルの拡張子が **.img** でも **.iso** でもない。
   - すでにカードの初期化操作が実行中である。

表 11-3 イメージファイルからパーティションを作成するオプション

フィールド	説明
インデックス	パーティションのインデックスを選択します。未使用のインデックスのみがドロップダウンリストに表示されます。使用可能な一番小さいインデックスがデフォルトで選択されています。ドロップダウンリスト内の別のインデックス値に変更できます。 **メモ:** 標準 SD カードでは、インデックス 1 しか使用できません。
ラベル	新しいパーティションに一意なラベルを入力します。これには最大 6 文字の英数字を使用できます。ラベル名には空白文字を含めないでください。文字は大文字で表示されます。 **メモ:** 標準 SD カードの場合、ラベル名は VFLASH でなければなりません。それ以外のラベル名を入力すると、エラーメッセージが表示されます。
エミュレーションタイプ	パーティションのエミュレーションタイプをドロップダウンリストから選択します。使用可能なオプションは、**フロッピー**、**HDD**、**CDROM** です。
イメージの場所	**参照**をクリックして、イメージファイルの場所を指定します。 **.img** ファイルまたは **.iso** ファイルのみがサポートされています。

パーティションのフォーマット

vFlash SD 上の既存のパーティションをファイルシステムに基づいてフォーマットできます。サポートされているファイルシステムの種類は、EXT2、EXT3、FAT16、FAT32 です。vFlash の機能に制限がある標準 SD カードは、FAT32 形式だけをサポートしています。

フォーマットできるのは、ハードディスクとフロッピーのパーティションだけです。CD のパーティションのフォーマットはサポートされていません。読み取り専用のパーティションはフォーマットできません。

メモ: パーティションをフォーマットするには、仮想メディアへのアクセス権限が必要です。

パーティションをフォーマットする前に、以下の点を確認してください。

- カードが有効になっている。
- パーティションが連結されていない。
- カードが書き込み禁止でない。
- まだカードの初期化操作が実行されていない。

vFlash パーティションをフォーマットするには、以下の手順を実行します。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash** タブ →**フォーマット** サブタブの順に選択します。**フォーマット** ページが表示されます。
2. 「表 11-4」で説明されている情報を入力します。
3. **適用** をクリックします。パーティション上のデータがすべて消去されるという警告メッセージが表示されます。**OK** をクリックします。選択したパーティションが、指定したファイルシステムタイプでフォーマットされます。

   以下の場合は、エラーメッセージが表示されます。

   - カードが書き込み禁止である。
   - すでにカードの初期化操作が実行中である。

表 11-4 パーティションのフォーマットページのオプション

フィールド	説明
ラベル	フォーマットするパーティションのラベルを選択します。デフォルトでは、最初に使用可能なパーティションが選択されています。 フロッピーまたはハードディスクの既存のパーティションタイプがドロップダウンリストに表示されます。連結されているパーティションや読み取り専用のパーティションはドロップダウンリストに表示されません。
フォーマットするタイプ	フォーマット後のパーティションのファイルシステムタイプを選択します。使用可能なオプションは、EXT2、EXT3、FAT16、FAT32 です。標準 SD カードでは、FAT32 しか使用できません。

使用可能なパーティションの表示

vFlash または標準 SD カードで、使用可能なパーティションリストの表示が有効になっていることを確認します。

カードに使用可能なパーティションを表示するには、以下の手順を実行します。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash**→**管理** サブタブの順に選択します。**パーティションの管理** ページに、使用可能なパーティションが表示されます。
2. 各パーティションについて、「表 11-5 」で説明されている情報を見ることができます。

表 11-5 使用可能なパーティションの表示

フィールド	説明
インデックス	パーティションには 1 ～ 16 のインデックスが付いています。パーティションのインデックスは、個々のパーティションに固有のもので、パーティションの作成時に指定します。
ラベル	パーティションの識別に使用され、パーティションの作成時に指定されます。
サイズ	パーティションのサイズをメガバイト(MB)で表した値。
読み取り専用。	パーティションの読み取り書き込みアクセス状態。 - オン = 読み取り専用パーティション。 - オフ = 読み取り書き込みパーティション。 **メモ:** 標準 SD カードでは、パーティションはすべて読み取り書き込みであるため、この列は表示されません。
連結	パーティションがオペレーティングシステムに USB デバイスとして認識されるかどうかを示します。パーティションを連結または分離するには、「パーティションの連結と分離」の項を参照してください。
エミュレーションタイプ	パーティションタイプがフロッピーか、ハードディスクか、CD かを表示します。
タイプ	パーティションタイプがフロッピーか、ハードディスクか、CD かを表示します。

パーティションの変更

カードでパーティションの変更が有効になっていることを確認します。

メモ: vFlash のパーティションを変更するには、仮想メディアへのアクセス権限が必要です。

読み取り専用と読み取り書き込み間で切り替えできます。これには、次の操作を行います。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash** タブ →**管理** サブタブの順に選択します。**パーティションの管理** ページが表示されます。
2. **読み取り専用** 列で、読み取り専用に変更するパーティションのチェックボックスをオンにし、読み取り書き込みに変更するパーティションのチェックボックスをオフにします。

   メモ: パーティションタイプが CD の場合は、状態は読み取り専用で、チェックボックスがオンになっています。この状態を読み取り書き込みに変更することはできません。
   パーティションが連結されている場合は、このチェックボックスは灰色表示になっています。
   標準 SD カードでは、パーティションはすべて読み取り書き込みであるため、**読み取り専用** 列は表示されません。
3. **適用** をクリックします。選択に従って、パーティションが読み取り専用または読み取り書き込みに変更されます。

パーティションの連結と分離

1 つまたは複数のパーティションを仮想 USB マスストレージデバイスとして連結し、オペレーティングシステムと BIOS からマスストレージデバイスとして認識されるようにできます。複数のパーティションを同時に連結すると、ホストのオペレーティングシステムには、インデックスの昇順に表示されます。対応するドライブ文字の割り当ては、オペレーティングシステムによって制御されます。

パーティションを分離すると、ホストのオペレーティングシステムで仮想 USB マスストレージデバイスとして表示されなくなり、BIOS 起動順序のメニューから削除されます。

パーティションを連結または分離した場合、システムの USB バスがリセットされます。これは、vFlash を使用しているアプリケーション(オペレーティングシステムなど)に影響することがあるので、iDRAC の仮想メディアセッションが切断されます。

メモ: パーティションを連結または分離するには、仮想メディアへのアクセス権限が必要です。

パーティションを連結または分離する前に、以下の点を確認してください。

- カードが有効になっている。
- まだカードの初期化操作が実行されていない。

パーティションを連結または分離するには、以下の手順を実行します。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash** タブ →**管理** サブタブの順に選択します。**パーティションの管理** ページが表示されます。
2. **連結** 列で、連結するパーティションのチェックボックスをオンにし、分離するパーティションのチェックボックスをオフにします。

   メモ: 分離したパーティションは起動順序に表示されません。
3. **適用** をクリックします。選択に従って、パーティションが連結または分離されます。

連結されているパーティションに対するオペレーティングシステムの動作

パーティションが連結されており、ホストオペレーティングシステムが Windows の場合は、連結されたパーティションに割り当てられるドライブ文字がオペレーティングシステムによって制御されます。

パーティションが読み取り専用の場合は、ホストオペレーティングシステムで読み取り専用と表示されます。

連結されているパーティションのファイルシステムをホストオペレーティングシステムがサポートしていない場合は、パーティションの内容をホストオペレーティングシステムから読み取ったり変更したりできません。たとえば、パーティションタイプ EXT2 は Windows オペレーティングシステムから読み取れません。

連結されているパーティションのラベル名をホストオペレーティングシステムから変更しても、iDRAC に保存されているそのパーティションのラベル名には影響しません。

既存のパーティションの削除

メモ: vFlash や標準 SD カードの既存のパーティションを削除できます。

既存のパーティションを削除する前に、以下の点を確認してください。

- カードが書き込み禁止でない。
- パーティションが連結されていない。
- まだカードの初期化操作が実行されていない。

  メモ: パーティションを変更するには、仮想メディアへのアクセス権限が必要です。

既存のパーティションを削除するには、次の手順を実行します。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash** タブ →**管理** サブタブの順に選択します。**パーティションの管理** ページが表示されます。
2. **削除** 列で、削除するパーティションの削除アイコンをクリックし、**適用** をクリックします。そのパーティションが削除されます。

パーティションの内容のダウンロード

vFlash パーティションの内容をローカルまたはリモートの場所に、**.img** または **.iso** 形式のイメージファイルとしてダウンロードできます。ローカル場所は、iDRAC6 ウェブインタフェースを操作している管理システムです。リモート場所は管理化システムです。

メモ: パーティションをダウンロードするには、仮想メディアへのアクセス権限が必要です。

ローカルまたはリモート場所に内容をダウンロードする前に、以下の点を確認してください。

- カードが有効になっている。
- まだカードの初期化操作が実行されていない。
- 読み取り書き込みパーティションは、連結しないでください。

vFlash パーティションの内容をシステム上の場所にダウンロードするには、以下の手順を実行します。

1. iDRAC6 ウェブインタフェースで、**システム**→**vFlash** タブ →**ダウンロード** サブタブの順に選択します。**パーティションのダウンロード** ページが表示されます。
2. **ラベル** ドロップダウンメニューから、ダウンロードするパーティションを選択します。連結されているパーティションを除いて、既存のパーティションがすべてリストに表示されます。デフォルトでは、最初のパーティションが選択されています。
3. **ダウンロード** をクリックします。
4. ファイルを保存する場所を指定します。

   フォルダの場所だけを指定した場合は、パーティションのラベルがファイル名として使用され、CD タイプのパーティションには **.iso**、フロッピータイプとハードディスクタイプのパーティションには **.img** の拡張子が付きます。
5. **保存** をクリックします。選択したパーティションの内容が、指定した場所にダウンロードされます。

パーティションからの起動

連結 vFlash パーティションを次回の起動時の起動デバイスとして設定できます。起動デバイスとして設定するには、vFlash パーティションに起動イメージが(**.img** または **.iso** 形式で)が含まれている必要があります。パーティションを起動デバイスとして設定する機能と、起動動作を実行する機能がカードで有効になっていることを確認します。

メモ: パーティションを起動デバイスとして設定するには、仮想メディアへのアクセス権限が必要です。

vFlash または標準 SD カードの起動操作を行うことができます。手順については、「最初の起動デバイス」の項を参照してください。

メモ: システム BIOS が起動デバイスとして vFlash をサポートしていない場合は、連結 vFlash パーティションが **最初の起動デバイス** ドロップダウンメニューに表示されない可能性があります。このため、vFlash パーティションを最初の起動デバイスとして設定する機能をサポートしている最新バージョンに BIOS をアップデートしてください。BIOS が最新バージョンであれば、サーバーを再起動すると、BIOS が iDRAC に vFlash を最初の起動デバイスとしてサポートすることを通知し、iDRAC は vFlash パーティションを **最初の起動デバイス** ドロップダウンメニューに表示します。

RACADM を使った vFlash パーティションの管理

`vFlashPartition` サブコマンド を使って、すでに初期化されている vFlash や標準 SD カード上のパーティションの作成、削除、一覧表示、または状態表示できます。形式は次のとおりです。

```
racadm vflashpartition <作成 | 削除 | 状態 | 一覧表示> <オプション>
```

メモ: vFlash のパーティション管理を実行するには、仮想メディアへのアクセス権限が必要です。

有効なオプション:

-i <インデックス>	このコマンドが適用されるパーティションのインデックス。 <インデックス> は 1 ～ 16 の整数です。 **メモ:** 標準 SD カードの場合、1 つのパーティションサイズ 256MB しかサポートされていないため、インデックス値は 1 に限られています。

作成操作でのみ有効なオプション:

-o <ラベル>	パーティションがオペレーティングシステムにマウントされるときに表示されるラベル。 <ラベル> は英数字 6 文字までの文字列で、空白文字を含むことはできません。
-e <タイプ>	パーティションのエミュレーションタイプ。<タイプ> はフロッピー、cdrom、または HDD です。
-t <タイプ>	<タイプ> の種類のパーティションを作成します。以下の <タイプ> から指定します。 • empty - 空のパーティションを作成します。 ○ -s <サイズ> - パーティションサイズ(MB)。 ○ -f <タイプ>- ファイルシステムの種類に基づくパーティションのフォーマットタイプ。有効なオプションは、RAW、FAT16、FAT32、EXT2、EXT3 です。 • image - イメージファイルを使用してパーティションを作成します。イメージファイルタイプでは以下のオプションが有効です。 ○ -l <パス> - iDRAC の相対リモートパスを指定します。このパスは、次のように、マウントされたドライブまたは共有を指定できます。 SMB path: //<ip またはドメイン>/<共有名> /<イメージのパス> NFS path: <ip アドレス>:/<イメージのパス> ○ -u <ユーザー> - リモートイメージへのアクセスに使用するユーザー名。 -p <パスワード> - リモートイメージへのアクセスに使用するパスワード。

作成操作でのみ有効なオプション:

-i	パーティションのインデックスの状態を表示します。

パーティションの作成

- 20 MB の空のパーティションを作成するには、次のコマンドを実行します。

  ```
  racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20
  ```

- リモートシステムのイメージファイルを使用してパーティションを作成するには、次のコマンドを実行します。

  ```
  racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/foo.iso -u root -p mypassword
  ```

  メモ: イメージファイルを使用したパーティションの作成は、ローカル RACADM ではサポートされていません。.

パーティションの削除

- パーティションを削除するには、次のコマンドを実行します。

  ```
  racadm vflashpartition delete -i 1
  ```

- すべてのパーティションを削除するには、vFlash SD カードを再初期化します。詳細については、「vFlash または標準 SD カードの初期化」を参照してください。

パーティションの状態の取得

- パーティション 1 の操作の状態を表示するには、次のコマンドを実行します。

  ```
  racadm vflashpartition delete -i 1
  ```

- 既存のパーティションすべての状態を取得するには、次のコマンドを実行します。

  ```
  racadm vflashpartition status -a
  ```

パーティション情報の表示

既存のパーティションとそのプロパティを一覧表示には、次のコマンドを実行します。

```
racadm vflashpartition list
```

パーティションからの起動

- 使用可能なデバイスを起動リストに表示するには、次のコマンドを実行します。

  ```
  racadm getconfig -g cfgServerInfo -o cfgServerFirstBootDevice
  ```

  vFlash SD カードでは、連結パーティションのラベル名が起動リストに表示されます。標準 SD カードで、連結パーティションの場合は、VFLASH が起動リストに表示されます。

- vFlash のパーティションを起動デバイスとして設定するには、次のコマンドを実行します。

  ```
  racadm config -g cfgServerInfo -o cfgServerFirstBootDevice "<vFlash パーティション名>"
  ```

  <vFlash パーティション名> は、vFlash SD カードのラベル名か、標準 SD カードの VFLASH です。

このコマンドを実行すると、vFlash パーティションラベルが自動的に「ブートワンス」に設定されます。つまり、**cfgserverBootOnce** が 1 に設定されます。「ブートワンス」では、デバイスがパーティションから 1 回起動するだけで、永続的に起動順序の最初に指定されるわけではありません。

パーティションの連結と分離

- パーティションを連結するには、次のコマンドを実行します。

  ```
  racadm config -g cfgvflashpartition -i 1 -o cfgvflashPartitionAttachState 1
  ```

- パーティションを分離するには、次のコマンドを実行します。

  ```
  racadm config -g cfgvflashpartition -i 0 -o cfgvflashPartitionAttachState 1
  ```

パーティションの変更

- 読み取り専用のパーティションを読み取り書き込みに変更するには、次のコマンドを実行します。

  ```
  racadm config -g cfgvflashpartition -i 1 -o cfgvflashPartitionAccessType 1
  ```

- 読み取り書き込みパーティションを読み取り専用に変更するには、次のコマンドを実行します。

  ```
  racadm config -g cfgvflashpartition -i 1 -o cfgvflashPartitionAccessType 0
  ```

RACADM サブコマンドと iDRAC6 プロパティのデータベースグループとオブジェクト定義の詳細については、デルサポートサイト **support.dell.com / manuals** にある『iDRAC 管理者リファレンスガイド』を参照してください。

よくあるお問い合わせ（FAQ）

vFlash SD カードや標準 SD カードはいつロックされますか?

仮想フラッシュメディアは、実行している処理がメディアへの排他的なアクセスを必要とする場合に、iDRAC によってロックされます。たとえば、初期化の処理中にロックされます。

目次ページに戻る

目次ページに戻る

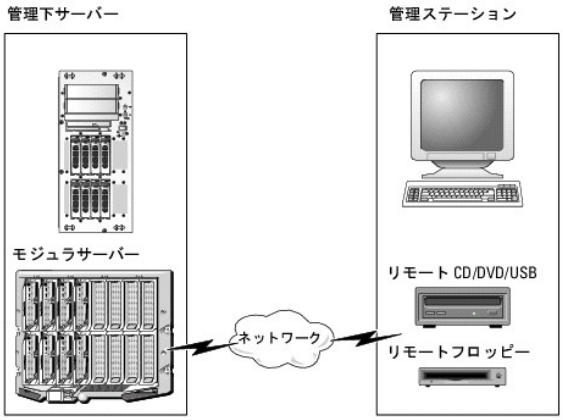
仮想メディアの設定と使用

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

概要

コンソールリダイレクトビューアを通して仮想メディア機能を使うことで、ネットワーク上のリモートシステムに接続されているメディアに管理下サーバーからアクセスできます。図 12-1に、仮想メディアの全体的なアーキテクチャを示します。

図 12-1 仮想メディアの全体的なアーキテクチャ



仮想メディアを使うと、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 やディスケットドライブからリモート実行できます。

メモ: 仮想メディアは 128 Kbps 以上のネットワーク帯域幅を必要とします。

仮想メディアは、管理下サーバーのオペレーティングシステムと BIOS に 2 つのデバイス(フロッピーディスクデバイスと光ディスクデバイス)を定義します。

管理ステーションは、物理メディアまたはイメージファイルをネットワーク経由で提供します。仮想メディアが接続していると、管理下サーバーからのすべての仮想 CD/ フロッピードライブのアクセス要求は、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、管理下システムでメディアを物理デバイスに挿入する操作と同じように見えます。仮想メディアが連結状態にある場合、管理下システム上の仮想デバイスはドライブ内にメディアが挿入されていない 2 つのドライブとして表示されます。

表 12-1 に、仮想フロッピーと仮想光ドライブでサポートされているドライブ接続を示します。

メモ: 接続中に仮想メディアを変更すると、システムの起動順序が停止する可能性があります。

表 12-1 サポートされているドライブ接続

サポートされている仮想フロッピードライブ接続	サポートされている仮想光ドライブ接続
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(最小サイズ 128 MB)	

Windows ベースの管理ステーション

Windows オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Internet Explorer の対応バージョンと ActiveX Control プラグインをインストールします。ブラウザのセキュリティを **中** 以下に設定し、Internet Explorer が署名付き ActiveX コントロールをダウンロードしてインストールできるようにします。

Internet Explorer のバージョンによっては、ActiveX のカスタムセキュリティ設定が必要な場合があります。

1. Internet Explorer を起動します。
2. **ツール**→ **インターネットオプション** をクリックし、**セキュリティ** タブをクリックします。
3. **Web コンテンツのゾーンを選択してセキュリティのレベルを設定する** で、希望するゾーンをクリックして選択します。
4. **このゾーンのセキュリティのレベル** で、**レベルのカスタマイズ** をクリックします。

   セキュリティ設定 ウィンドウが表示されます。
5. **ActiveX コントロールとプラグイン** で、次の設定が **有効にする** になっていることを確認します。
   - スクリプトレットの許可
   - ActiveX コントロールに対して自動的にダイアログを表示
   - 署名された ActiveX コントロールのダウンロード
   - 未署名の ActiveX コントロールのダウンロード
6. **OK** をクリックして変更を保存し、**セキュリティ設定** ウィンドウを閉じます。
7. **OK** をクリックして、**インターネットオプション** ウィンドウを閉じます。
8. Internet Explorer を再起動します。

ActiveX をインストールするには、Administrator 権限が必要です。ActiveX コントロールをインストールする前に、Internet Explorer でセキュリティ警告が表示される場合があります。ActiveX コントロールのインストールを完了するには、表示されるセキュリティ警告に答えて ActiveX コントロールを許可します。

Linux ベースの管理ステーション

Linux オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Firefox の対応バージョンをインストールします。

仮想コンソールプラグインを実行するには、Java ランタイム環境（JRE）が必要です。JRE は、**java.sun.com** からダウンロードできます。

仮想メディアの設定

1. iDRAC6 ウェブインタフェースにログインします。
2. **システム**→**仮想コンソール / メディア**→**設定** の順にクリックします。
3. 仮想メディア セクションで、設定値を選択します。仮想メディアの設定値の詳細については、「表 12-2」を参照してください。
4. **適用** をクリックして設定を保存します。

   警告ダイアログが開いて、`You are about to change device configuration. All existing redirection sessions will be closed. Do you want to continue` (デバイスの設定を変更しようとしています。既存のリダイレクトセッションすべてが終了します。続行します)か? というメッセージが表示されます。
5. **OK** をクリックして続行します。

   警告ダイアログが開いて、`Virtual Media Configuration successfully set.` (仮想メディアの設定は正常に設定されました) というメッセージが表示されます。

表 12-2 仮想メディアの設定値

属性	値
仮想メディアの連結	**連結** - すぐに仮想メディアをサーバーに連結します。 **分離** -すぐ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たときにのみ、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	許可されている仮想メディアの最大セッション数を表示します。この値は常に **1** です。 **メモ:** 仮想メディアユーザーセッションは、1 回のみ認められています。ただし、複数のデバイスを 1 回のセッションで取り付けることが可能です。仮想メディアの実行 を参照してください。
アクティブセッション数	現在アクティブな仮想メディアセッション数を表示します。

仮想メディアの暗号化を有効にする	仮想メディア接続の暗号化を有効(チェックボックスをオン)または無効(チェックボックスをオフ)にします。
フロッピーのエミュレーション	仮想メディア**が**サーバーにフロッピードライブとして表示されるか USB キーとして表示されるかを示します。**フロッピーのエミュレーション** チェックボックスがオンの場合、仮想メディアデバイスはサーバー上でフロッピーデバイスとして表示されます。オフの場合は、USB キードライブとして表示されます。 **メモ:** 一部の Windows Vista**?** と Red Hat? Enterprise Linux? 環境では、フロッピーのエミュレーション を有効にしている場合に、USB を仮想化できない場合があります。
ブートワンスを有効にする	ブートワンスオプションを有効(チェックボックスをオン)または無効(チェックボックスをオフ)にします。このオプションは、サーバーが 1 度起動した後で 仮想メディア セッションを自動的に終了します。仮想メディアから起動するには、この属性を使用します。次回の起動でのシステムの起動順序は、次のデバイスからになります。このオプションは、自動展開の際に便利です。

仮想メディアの実行

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

メモ: 仮想メディアにアクセスしている間は、コンソールビューア ウィンドウアプリケーションがアクティブな状態でなければなりません。

1. 管理ステーションで対応ウェブブラウザを開きます。
2. iDRAC6 ウェブインタフェースにログインします。
3. **仮想コンソール / メディア** タブをクリックします。

   仮想コンソールと仮想メディア 画面が表示されます。

   表示されている属性の値を変更するには、「仮想メディアの設定」を参照してください。

   メモ: フロップーイメージファイルは仮想フロッピーとして仮想化できるので、**フロッピードライブ** の下の**フロッピーイメージファイル** が表示されることがあります(該当する場合)。1 台の光ドライブと 1 台のフロッピーを同時に選択するか、1 台のドライブだけを選択することができます。

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

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

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

   iDRACView アプリケーションが別のウィンドウで起動します。
5. **メディア** → **仮想メディアウィザード** の順に選択します。

   メディアリダイレクト ウィンドウが開きます。
6. **メディアリダイレクト** ウィンドウの下部で **状 態** セクションを確認します。メディアが接続している場合は、別のメディアソースに接続する前に切断してください。メディアを切断するには、**状 態** ウィンドウのメディアの横にある **接続解 除** をクリックします。
7. 接続するメディアタイプの横にあるラジオボタンを選択します。
8. **フロッピーイメージ** ボタンと、**CD / DVD ドライブ** セクションのラジオボタンを 1 つ選択できます。

   メモ: 管理ステーションの CD/DVD メディアが iDRAC6 ブレードによってすでに使用中の場合は、同じメディアをリダイレクトすると、別の iDRAC6 ブレードでも使用できます。つまり、iDRAC6 は同じメディア(読み取り専用)を 2 台の iDRAC6 ブレードにリダイレクトする機能をサポートしています。一方、USB メディアは 2 台の iDRAC6 ブレードに連結できません。iDRAC6 にこれを指摘する警告メッセージが表示されます。

   フロッピーイメージまたは ISO イメージを接続する場合は、ローカルコンピュータ上のイメージのパスを入力するか、**参照** ボタンでイメージの場所に移動します。

   メモ: Java ベースの仮想メディアプラグインを使用している場合は、リモート ISO イメージをマウントできない可能性があります。たとえば、Linux のクライアントでは Java ベースのプラグインが使用されているため、イメージをマウントできません。これを回避するには、ISO イメージをローカルシステムにコピーして、ローカルでイメージファイルを使用できるようにしてください。Java ベースの仮想メディアプラグインでは、 **\\computer\share** の形式で共有名を指定することはできません。
9. **選択した各メディアタイプの横にある 接続** ボタンをクリックします**。**

   メディアが接続され、**状 態** ウィンドウが更新されます。
10. **閉じる** をクリックします**。**

メモ: 仮想メディアのセッションを開始したり、VFlash を接続したりすると、uLCDRIVEv というドライブがホストオペレーティングシステムと BIOS に表示されます。この余分のドライブは、VFlash または仮想メディアのセッションが切断されると表示されなくなります。

仮想メディアの切断

1. **メディア** → **仮想メディアウィザード** の順に選択します。

   メディアリダイレクト ウィザードが開きます。

2. 切断するメディアの横にある **接続解除** をクリックします。

   メディアが接続され、**状態** ウィンドウが更新されます。

3. **閉じる** をクリックします。

メモ: **iDRACview** を起動してから、ウェブ GUI からログオフすると、**iDRACView** は終了せず、アクティブなままになります。

仮想メディアからの起動

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

BIOS 設定を変更するには、次の手順を実行してください。

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

   ポップアップウィンドウに、仮想光デバイス 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、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、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されており起動メディアがある場合、システムはこの仮想デバイスから起動します。起動メディアがない場合は、起動メディアのない物理デバイスの場合と同様にこのデバイスは無視されます。

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

ここでは、管理ステーションに手動でインタラクティブにオペレーティングシステムをインストールする方法について説明します。完了までに数時間かかる場合があります。仮想メディア を使用してスクリプトでオペレーティングシステムをインストールする手順は 15 分以内で完了します。詳細については、オペレーティングシステムの導入を参照してください。

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

サーバーのオペレーティングシステムが実行しているときの仮想メディアの使用

Windows ベースシステム

Windows システムでは、仮想メディアドライブが連結されて、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 で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 ベースシステム

システム上でのソフトウェア設定によっては、仮想メディアドライブが自動的にマウントされない場合があります。ドライブが自動的にマウントされない場合は、Linux の **mount** コマンドを使ってドライブを手動でマウントします。

よくあるお問い合わせ（FAQ）

表 12-3 は、よくあるお問い合わせとその回答です。

表 12-3 仮想メディアの使い方 :よくあるお問い合わせ（FAQ）

質問	回答
仮想メディアのクライアントの接続が時々切断されます。どうしてでしょうか。	ネットワークのタイムアウトが発生すると、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断して接続を中断します。 仮想メディアの設定を iDRAC6 ウェブインタフェースまたはローカル RACADM コマンドで変更した場合、設定変更を適用すると、接続しているメディアがすべて切断されます。 仮想ドライブに再接続するには、仮想メディアウィザードを使用します。
どのオペレーティングシステムが iDRAC6 をサポートしていますか。	対応オペレーティングシステムについては、「対応 OS」のリストを参照してください。.
どのウェブブラウザが iDRAC6 をサポートしていますか。	対応ウェブブラウザについては、「対応ウェブブラウザ」のリストを参照してください。
時々クライアントの接続が切れるのはなぜですか。	• 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 ドライブ内の 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 ドライブ内の CD を交換した場合、新しい CD に自動起動機能が備わっていることがあります。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、中断された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すると、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断して接続を中断します。また、他の人がウェブインタフェースまたは RADACM コマンドの入力によって、仮想メディアの設定を変更した可能性があります。仮想ドライブに再接続するには、仮想メディア 機能を使用します。
Windows オペレーティングシステムのインストールに時間がかかりすぎるようです。どうしてでしょうか。	Windows オペレーティングシステムをインストールしている場合、ネットワーク接続が低速であれば、ネットワーク遅延により、インストール手順で iDRAC6 にアクセスするのに時間がかかることがあります。インストールウィンドウにはインストールが進行しているように表示されませんが、インストールプロセスは進行しています。
フロッピードライブまたは USB メモリキーの内容を見ているのですが、同じドライブを使って仮想メディア接続を確立しようとすると、接続エラーメッセージが表示されて再試行を求められます。どうしてでしょうか。	仮想フロッピードライブへの同時アクセスはできません。ドライブの仮想化を試みる前にドライブの内容を表示するアプリケーションを閉じてください。
仮想デバイスを起動デバイスとして設定するにはどうしますか。	管理下サーバーの BIOS セットアップ にアクセスして起動メニューに進みます。仮想 CD、仮想フロッピー、または vFlash を見つけ、必要に応じてデバイスの起動順序を変更します。たとえば、CD ドライブから起動するには、その CD ドライブを起動順序の最初のドライブとして設定してください。
どのタイプのメディアから起動できますか。	iDRAC6 では、以下のブータブルメディアから起動できます。 • 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（最小サイズ 128 MB） • 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 キーを起動デバイスにするための Windows プログラムである 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、起動デバイスにする USB キーです。
仮想フロッピードライブでサポートされているファイルシステムの種類を教えてください。	仮想フロッピードライブは、FAT16 または FAT32 ファイルシステムをサポートしています。
iDRAC6 ウェブインタフェースを使用してリモートでファームウェアのアップデートを実行すると、サーバーの仮想ドライブが削除されてしまいました。どうしてでしょうか。	ファームウェアのアップデートによって iDRAC6 がリセットされ、リモート接続が切れて、仮想ドライブのマウントが解除されます。 iDRAC6 のリセットが完了すると、ドライブは再表示されます。

Red Hat Enterprise Linux または SUSE Linux オペレーティングシステムを実行しているシステムで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実行します。
	
	`grep "hh:mm:ss" /var/log/messages`
	ここで、

	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されて接続され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実行します。 mount /dev/sdx /mnt/floppy ここで、 /dev/sdxは手順 4 で見つけたデバイス名です。 /mnt/floppy はマウントポイントです。

目次ページに戻る

目次ページに戻る

RACADM コマンドラインインタフェースの使用

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

RACADM コマンドラインインタフェース(CLI)を使用することで、管理下サーバーの iDRAC6 管理機能にアクセスできます。RACADM を使用すると、iDRAC6 ウェブインタフェースにあるほとんどの機能にアクセスできます。インタラクティブな管理に適しているウェブインタフェースの代わりに、RACADM をスクリプトで使用することで、複数のサーバーを簡単に設定できるようになります。

RACADM には次のインタフェースが用意されています。

- ローカル RACADM
- リモート RACADM
- Telnet/SSH RACADM

ローカル RACADM コマンドは、管理下サーバーから iDRAC6 へのアクセスにネットワーク接続を使用しません。つまり、最初の iDRAC6 ネットワークの設定にローカル RACADM コマンドを使用できます。リモート RACADM はクライアント側のユーティリティで、管理ステーションから帯域外ネットワークインタフェースを使用して実行できます。SSH/Telnet RACADM とは、SSH または Telnet プロンプトから RACADM コマンドを使用することを指します。

本項では、以下について説明します。

- RACADM コマンドとサポートされている RACADM インタフェース
- コマンドプロンプトからのローカル RACADM の使用
- リモート RACADM
- SSH/Telnet RACADM
- **racadm** コマンドを使用した iDRAC6 の設定
- RACADM 設定ファイルを使用した複数の iDRAC6 の設定

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

RACADM サブコマンド

表 13-1 は、RACADM で実行できる各 RACADM サブコマンドについて説明しています。構文や有効なエントリを含め、RACADM サブコマンドの詳しいリストについては、デルサポートサイト **support.dell.com/manuals** で『iDRAC6 管理者リファレンスガイド』を参照してください。

表 13-1 RACADM サブコマンド

コマンド	説明
arp	ARP テーブルの内容を表示します。ARP テーブルエントリの追加や削除はできません。
clearasrscreen	前回のクラッシュ(ASR)画面をクリアします
closessn	デバイスの通信セッションを終了します。
coredump	前回の iDRAC6 コアダンプを表示します。
coredumpdelete	iDRAC6 に保存されているコアダンプを削除します。
clrraclog	iDRAC6 のログをクリアします。クリアすると、ログがクリアされたときのユーザーと時刻を示すエントリが 1 つ作成されます。
clrsel	管理下サーバーのシステムイベントログのエントリをクリアします。
config	iDRAC6 を設定します。
fwupdate	iDRAC6 ファームウェアをアップデートします。
getconfig	現在の iDRAC6 設定のプロパティを表示します。
getniccfg	コントローラの現在の IP 設定を表示します。
getraclog	iDRAC6 のログを表示します。
getractime	iDRAC6 の時刻を表示します。
getsel	SEL エントリを表示します。
getssninfo[1]	アクティブセッションに関する情報を表示します。
getsvctag	サービスタグを表示します。

getsysinfo	IP 設定、ハードウェアモデル、ファームウェアバージョン、オペレーティングシステム情報を含む iDRAC6 および管理下サーバーに関する情報を表示します。
gettracelog	iDRAC6 トレースログを表示します。-i を指定して使用した場合は、iDRAC6 のトレースログのエントリ数を表示します。
help	iDRAC6 サブコマンドを一覧にします。
help <サブコマンド>	指定したサブコマンドの使用ステートメントを一覧にします。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
krbkeytabupload	Kerberos keytab ファイルをアップロードします。
localConRedirDisable	ローカルシステムから、ローカル仮想コンソールを無効にします。
netstat	ルーティングテーブルと現在の接続を表示します。
ping	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。宛先 IP アドレスが必要です。ICMP エコーパケットが現在のルーティングテーブルの内容に基づいて、目的の IP アドレスに送信されます。
ping6	現在のルーティングテーブルの内容を使用して iDRAC6 から送信先の IPv6 アドレスに到達可能かどうかを確認します。送信先の IPv6 アドレスが必要です。ICMP エコーパケットが現在のルーティングテーブルの内容に基づいて、目的の IPv6 アドレスに送信されます。
racdump	状態および iDRAC6 の一般的な情報を表示します。
racreset	iDRAC6 をリセットします。
racresetcfg	iDRAC6 をデフォルト設定にリセットします。
remoteimage	リモートファイル共有
serveraction	管理下サーバーの電源管理操作を実行します。
setniccfg	コントローラの IP 設定を指定します。
sshpkauth	最大 4 つの SSH 公開キーをアップロードしたり、既存のキーを削除したり、iDRAC6 にすでにあるキーを表示したりできます。
sslcertdownload	CA 証明書をダウンロードします。
sslcertupload	CA 証明書またはサーバー証明書を iDRAC6 にアップロードします。
sslcertview	iDRAC6 にある CA 証明書またはサーバー証明書を表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
testemail	iDRAC6 に iDRAC6 NIC 経由で電子メールを送信させます。
testtrap	iDRAC6 に iDRAC6 NIC 経由で SNMP 警告を送信させます。
traceroute	パケットがシステムから目的の IPv4 アドレスに転送されるときに通ったルーターのネットワーク経路をトレースします。
traceroute6	パケットがシステムから目的の IPv6 アドレスに転送されるときに通ったルーターのネットワーク経路をトレースします。
version	iDRAC6 のバージョン情報を表示します。
vflashsd	vflash SD カードを初期化するか、カードの状態を取得します。
vflashpartition	初期化された vFlash SD カードの作成、削除、リスト表示、パーティションの状態表示などを行います。
vmdisconnect	リモートクライアントから開いていた iDRAC 仮想メディア接続をすべて閉じます。
vmkey	VFlash パーティションをデフォルトサイズの 256MB にリセットし、パーティションからすべてのデータを削除します。
[1] SOL セッションの情報は、getssninfo コマンドの応答に含まれていません。	

ローカル RACADM コマンドの使用

コマンドプロンプトまたはシェルプロンプトからローカル（管理下サーバー上）で RACADM コマンドを実行します。

管理下サーバーにログインし、コマンドシェルを起動して、ローカル RACADM コマンドを次の形式で入力します。

- `racadm <サブコマンド> [パラメータ]`
- `racadm <getconfig|config> [-g <グループ>] [-o <オブジェクト> <値>]`

オプションを使用しなければ、RACADM コマンドによって一般的な使用情報が表示されます。RACADM サブコマンド一覧を表示するには、次のように入力します。

```
racadm help
```

または

```
racadm getconfig -h
```

サブコマンドのリストには、iDRAC6 でサポートされる RACADM コマンドがすべて含まれています。

サブコマンドのヘルプを取得するには、次のように入力します。

```
racadm help <サブコマンド>
```

このコマンドによって、サブコマンドの構文とコマンドラインオプションが表示されます。

RACADM ユーティリティを使用した iDRAC6 の設定

本項では、RACADM を使用して、さまざまな iDRAC6 設定タスクを実行する方法を説明します。

現在の iDRAC6 設定の表示

RACADM **getconfig** サブコマンドは、iDRAC6 から現在の設定を取得します。設定値は、1 つまたは複数の オブジェクト を含む グループ に整理され、オブジェクトには 値 があります。

グループとオブジェクトの詳細については、デルサポートサイト **support.dell.com / manuals** で『 iDRAC6 管理者リファレンスガイド』を参照してください。

すべての iDRAC6 グループのリストを表示するには、次のコマンドを入力します。

```
racadm getconfig -h
```

特定のグループのオブジェクトと値を表示するには、次のコマンドを入力します。

```
racadm getconfig -g <グループ>
```

たとえば、**cfgLanNetworking** グループのオブジェクト設定をすべて表示するには、次のコマンドを入力します。

```
racadm getconfig -g cfgLanNetworking
```

RACADM を使用した iDRAC6 ユーザーの管理

メモ: **racresetcfg** コマンドを使用すると、すべての 設定パラメータが元のデフォルトに戻されるため、注意してください。それまでに行った変更がすべて失われます。

メモ: 新しい iDRAC6 を設定している場合や、**racadm racresetcfg** コマンドを実行した場合、現在のユーザーは **root** のみで、パスワードは **calvin** になります。

メモ: ユーザーは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 に異なるインデックス番号を持つ場合があります。

メモ: Active Directory 環境用に作成されたユーザーとグループは、Active Directory 命名規則に準拠する必要があります。

iDRAC6 プロパティデータベースには、最大 15 のユーザーを設定できます。(16 番目のユーザーは、IPMI LAN ユーザー用に予約されています。)手動で iDRAC6 ユーザーを有効にする前に、現在のユーザーが存在しているかどうか確認してください。

コマンドプロンプトで次のコマンドを入力すると、ユーザーが存在するかどうかがわかります。

```
racadm getconfig -u <ユーザー名>
```

または

1 ～ 16 の各インデックスに 1 回ずつ次のコマンドを入力します。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```

メモ: また、racadm getconfig -f <ファイル名> と入力し、生成した <ファイル名> のファイルを表示することもできます。このファイルにはすべてのユーザーと、その他の iDRAC6 設定パラメータが含まれます。

複数のパラメータとオブジェクト ID が現在値と一緒に表示されます。対象オブジェクトは次の 2 つです。

```
# cfgUserAdminIndex=nn

cfgUserAdminUserName=
```

cfgUserAdminUserName オブジェクトに値がない場合は、**cfgUserAdminIndex** オブジェクトで示されるそのインデックス番号を使用できます。「= 」の後に名前が表示された場合は、インデックスがそのユーザー名に割り当てられています。

メモ: Active Directory 環境用に作成されたユーザーとグループは、Active Directory 命名規則に準拠する必要があります。

iDRAC6 ユーザーの追加

新しいユーザーを iDRAC6 に追加するには、次の手順を実行してください。

1. ユーザー名を設定します。
2. パスワードを設定します。
3. ログインを iDRAC6 ユーザー権限に設定します。
4. ユーザーを有効にします。

例

次の例は、パスワードが「123456」で iDRAC6 へのログイン権限のある「John」という新しいユーザーを追加する方法を示しています。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

新規ユーザーを検証するには、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

RAC6 ユーザーに権限を与える

ユーザーに特定の管理者権限（役割ベース）を与えるには、**cfgUserAdminPrivilege** プロパティを、表 13-2 に示した値から構成されるビットマスクに設定します。

表 13-2 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
iDRAC6 へのログイン	0x00000001
iDRAC6 の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
仮想コンソールへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100

たとえば、ユーザーに **iDRAC の設定**、**ユーザーの設定**、**ログのクリア**、**仮想コンソールへのアクセス** の各権限を与えるには、0x00000002、0x00000004、0x00000008、0x00000010 の値を追加してビットマップ 0x0000002E を構成します。続いて、次のコマンドを入力して権限を設定します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

RACADM を使った SSH キーのアップロード、表示、削除

アップロード

アップロードモードでは、キーファイルをアップロードしたり、コマンドラインでキーテキストをコピーしたりできます。キーのアップロードとコピー操作を同時に行うことはできません。

ローカル RACADM を使用する場合：

```
racadm sshpkauth -i <2 ～ 16> -k <1 ～ 4> -f <ファイル名>
```

telnet/ssh RACADM を使用する場合：

```
racadm sshpkauth -i <2 ～ 16> -k <1 ～ 4> -t

<キーテキスト>
```

例：

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

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

PK SSH 認証キーファイルが RAC に正常にアップロードされます。

△ **注意: telnet / ssh / serial RACADM では、ufilevオプションはサポートされていません。**

表示

表示モードでは、ユーザーが指定したキーまたはすべてのキーを表示できます。

```
racadm sshpkauth -i <2 ～ 16> -v -k <1 ～ 4>

racadm sshpkauth -i <2 ～ 16> -v -k all
```

削除

削除モードでは、ユーザーが指定したキーまたはすべてのキーを削除できます。

```
racadm sshpkauth -i <2 ～ 16> -d -k <1 ～ 4>
```

```
racadm sshpkauth -i <2 ～ 16> -d -k all
```

注意: この権限は通常、iDRAC の管理者ユーザーグループのメンバーに予約されています。ただし、「カスタム」ユーザーグループにこの権限を割り当てることもできます。この権限のあるユーザーは、他のユーザーの設定を変更できます。これには、ユーザーの削除や、ユーザーの SSH キーの管理などが含まれます。そのため、この権限の割り当てには注意が必要です。

サブコマンドのオプションについては、デルサポートサイト **support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』の「sshpkauth」を参照してください。

iDRAC6 ユーザーの削除

RACADM を使用する場合、iDRAC ユーザーの削除はできません。ユーザーは **cfgUserAdminEnable** オブジェクトでのみ無効にできます。コマンド構文は次のとおりです。

```
racadm config -g cfgUserAdmin -o cfgUserAdminEnable -I <インデックス>
```

user admins の管理の詳細については、デルサポートサイト **support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』を参照してください。

電子メール警告のテスト

iDRAC6 電子メール警告機能を使用すると、管理下サーバーで重要なイベントが発生したときに電子メール警告を受信できます。次の例は、電子メール警告機能をテストして、iDRAC6 が電子メール警告をネットワークを介して正しく送信できることを確認する方法を示しています。

```
racadm testemail -i 2
```

（-i 2 は電子メール警告テーブルのインデックスエントリの 2 番です）

メモ: 電子メール警告機能をテストする前に、SMTP と 電子メール警告のオプション が設定されていることを確認してください。詳細については、電子メール警告の設定を参照してください。

iDRAC6 SNMP トラップ警告機能のテスト

iDRAC6 SNMP トラップ警告機能を使用すると、管理下サーバーで発生したシステムイベントを受信するための SNMP トラップリスナーを設定できます。

次の例は、SNMP トラップ警告機能をテストする方法を示しています。

```
racadm testtrap -i 2
```

（-i 2 は電子メール警告テーブルのインデックスエントリの 2 番です）

メモ: iDRAC6 SNMP トラップ警告機能をテストする前に、SNMP とトラップのオプションが正しく設定されていることを確認してください。これらのオプションを設定するには、**testtrap** および **testemail** サブコマンドの説明を参照してください。詳細については、プラットフォームイベントトラップ（PET）の設定を参照してください。

iDRAC6 ネットワークプロパティの設定

使用可能なネットワークプロパティのリストを生成するには、次のように入力します。

```
racadm getconfig -g cfgLanNetworking
```

DHCP を使用して IP アドレスを取得するには、次のコマンドを使って **cfgNicUseDhcp** オブジェクトを記述し、この機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

コマンドは、<Ctrl><E> の入力を求められたときの iDRAC6 設定ユーティリティと同じ設定機能を提供します。iDRAC6 設定ユーティリティを使用したネットワークプロパティの設定の詳細については、「iDRAC6 LAN」を参照してください。

次に、LAN ネットワークプロパティを設定するコマンドの使用例を示します。

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

メモ: **cfgNicEnable** を **0** に設定すると、DHCP が有効の場合でも iDRAC6 LAN は無効になります。

IPMI オーバー LAN の設定

1. 次のコマンドを入力して、IPMI オーバー LAN を設定します。

   ```
   racadm config -g 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. 次のコマンドを入力して、IPMI チャネル権限をアップデートします。

      ```
      racadm config -g 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(**システム管理者**)

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

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

   b. 必要に応じて、次のようなコマンドを使用して IPMI LAN チャネルの暗号化キーを設定します。

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

      ```
      racadm config -g 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。

2. 次のコマンドを使用して、IPMI シリアルオーバー LAN(SOL)を設定します。

   ```
   racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
   ```

メモ: IPMI SOL 最小権限レベルは、IPMI SOL をアクティブにするために最低限必要な権限を指定します。詳細については、IPMI 2.0 規格を参照してください。

   a. 次のコマンドを使用して IPMI SOL の最小権限レベルをアップデートします。

      ```
      racadm config -g 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(**システム管理者**)

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

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
      ```

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

   b. 次のコマンドを使用して IPMI SOL のボーレートをアップデートします。

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

      <ボーレート> は 19200、57600、115200 bps のいずれかになります。

      たとえば、次のとおりです。

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
      ```

c. コマンドプロンプトで次のコマンドを入力して SOL を有効にします。

メモ: SOL は個々のユーザーに対して有効または無効にできます。

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable 1 -i <ID>
```

<ID> はユーザーの一意 ID です。

PEF の設定

各プラットフォーム警告に対し iDRAC6 が講じる処置を設定できます。表 13-3 は、可能な処置と RACADM でこれらを識別するための値のリストです。

表 13-3 プラットフォームイベントの処置

動作	値
処置は不要	0
電源オフ	1
再起動	2
電源の入れ直し	3

次のコマンドを使用して PEF 処置を設定します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <インデックス> <処置の値>
```

<インデックス> は PEF インデックス(「表 5-8」の「表 13-3」)で、<処置の値> は「」から取得した値です。

たとえば、プロセッサの重大なイベントが検出されたときに、PEF がシステムを再起動して IPMI 警告を送信できるようにするには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
```

PET の設定

1. 次のコマンドを使用してグローバル警告を有効にします。

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

2. 次のコマンドを使用して PET を有効にします。

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <インデックス> <0|1>
   ```

   <インデックス> は PET の送信先のインデックスで、0 は PET を無効に、1 は PET を有効にします。

   たとえば、PET をインデックス 4 で有効にするには、次のコマンドを入力します。

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

3. 次のコマンドを使用して PET ポリシーを設定します。

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <インデックス> <IP アドレス>
   ```

   <インデックス> は PET の送信先のインデックスで、<IP アドレス> は、プラットフォームイベント警告を受け取るシステムの宛先 IP アドレスです。

4. コミュニティ名の文字列を設定します。

   コマンドプロンプトで、次のコマンドを入力します。

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名前>
   ```

   <名前> は PET コミュニティ名です。

E-メール警告の設定

1. 次のコマンドを入力してグローバル警告を有効にします。

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

2. 次のコマンドを入力して電子メール警告を有効にします。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <インデックス> <0|1>
   ```

   <インデックス> は電子メール送信先のインデックスで、0 は電子メール警告を無効に、1 は電子メール警告を有効にします。電子メールの送信先インデックスとしては 1 ～ 4 の値を指定できます。

   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. 次のコマンドを使用して電子メールのオプションを設定します。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <電子メールアドレス>
   ```

   1 は電子メール送信先のインデックスで、<電子メールアドレス> は、プラットフォームイベント警告を受け取る送信先電子メールアドレスです。

4. SMTP 電子メールサーバーを設定するには、次のコマンドを入力します。

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP 電子メールサーバーの IP アドレス>
   ```

5. カスタムメッセージを設定するには、次のコマンドを入力します。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <インデックス> <カスタムメッセージ>
   ```

   <インデックス> は電子メール送信先のインデックスで、<カスタムメッセージ> はカスタムメッセージです。

6. 必要に応じて、次のコマンドを使用して設定した電子メール警告をテストします。

   ```
   racadm testemail -i <インデックス>
   ```

   <インデックス> は、テストする電子メール送信先のインデックスです。

IP フィルタ(IpRange)の設定

IP アドレスフィルタ(または IP 範囲チェック)を使用すると、ユーザーが特定した範囲内にある IP アドレスのクライアントワークステーションや管理ワークステーションからのみ iDRAC6 へのアクセスを許可できます。その他のすべてのログイン要求は拒否されます。

IP フィルタは着信ログインの IP アドレスを、次の **cfgRacTuning** プロパティで指定する IP アドレス範囲と比較します。

- 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。結果が同じ場合は、着信ログイン要求に iDRAC6 へのアクセスが許可されます。この範囲外の IP アドレスからのログイン要求にはエラーが返されます。

次の式の値がゼロに等しい場合は、ログインに進みます。

```
cfgRacTuneIpRangeMask & (<着信 IP アドレス> ^ cfgRacTuneIpRangeAddr)
```

& は数量のビットワイズ AND で ^ はビットワイズ XOR です。

cfgRacTuning プロパティの詳細リストについては、デルサポートサイト **support.dell.com/manuals** で『iDRAC6 管理者リファレンスガイド』の「cfgRacTuning」を参照してください。

表 13-4 IP アドレスフィルタ(IpRange)のプロパティ

プロパティ	説明
cfgRacTuneIpRangeEnable	IP アドレスのチェック機能を有効にします。
cfgRacTuneIpRangeAddr	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。 このプロパティはビットワイズ AND と **cfgRacTuneIpRangeMask** を使用して、許可する IP アドレスの上位ビットを決定します。IP アドレスの上位ビットにこのビットパターンが含まれるすべての IP アドレスにログインが許可されます。この範囲外の IP アドレスからのログインはエラーになります。各プロパティのデフォルト値は、192.168.1.0 ～ 192.168.1.255 のアドレス範囲からのログインを許可しています。
cfgRacTuneIpRangeMask	IP アドレスの有意ビット位置を定義します。マスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。

次の例では、ローカル RACADM を使用して IP フィルタを設定します。

メモ: RACADM と RACADM コマンドの詳細については、「RACADM コマンドラインインタフェースの使用」を参照してください。

1. 次の RACADM コマンドは 192.168.0.57 以外のすべての IP アドレスをブロックします。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

2. 連続する 4 つの IP アドレスにログインを限定するには（たとえば、192.168.0.212～192.168.0.215）、次のようにマスクの最下位の 2 ビットを除くすべてを選択します。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

範囲マスクの最後のバイトは 252 に設定されています。10 進数では 11111100b に相当します。

IP フィルタのガイドライン

IP フィルタを有効にする場合は、次のガイドラインに従ってください。

- **cfgRacTuneIpRangeMask** は必ずネットマスク形式で設定してください。最重要ビットがすべて（マスクのサブネットを定義する）1 で、下位ビットではすべて 0 になります。
- 必要な範囲の基底アドレスを **cfgRacTuneIpRangeAddr** の値として使用します。このアドレスの 32 ビットのバイナリ値は、マスクにゼロがある下位ビットがすべてゼロになります。

IP ブロックの設定

IP ブロックは、事前に選択した時間内に特定の IP アドレスからのログイン失敗回数が過剰になったのを動的に判断し、そのアドレスが iDRAC6 にログインするのをブロックします。

IP ブロックには次の機能が含まれます。

- 許可するログイン失敗回数（**cfgRacTuneIpBlkFailcount**）
- これらの失敗の時間枠（秒）（**cfgRacTuneIpBlkFailWindow**）
- 許可する合計失敗回数を超えてブロックされた IP アドレスのセッション確立が阻止される秒数（**cfgRacTuneIpBlkPenaltyTime**）

特定の IP アドレスからのログイン失敗が累積すると、それらは内部カウンタに登録されます。ユーザーがログインに成功すると、失敗履歴がクリアされて、内部カウンタがリセットされます。

メモ: クライアント IP アドレスからのログイン試行が拒否されると、SSH クライアントに「ssh exchange identification: Connection closed by remote host（SSH ID: リモートホストが接続を閉じました）」というメッセージが表示される場合があります。

cfgRacTune プロパティの詳細リストについては、デルサポートサイト **support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』を参照してください。

表 13-5 に、ユーザー定義のパラメータを示します。

表 13-5 ログイン再試行制限（IP ブロック）のプロパティ

プロパティ	定義
cfgRacTuneIpBlkEnable	IP ブロック機能を有効にします。 一定時間内に（**cfgRacTuneIpBlkFailWindow**）1 つの IP アドレスからの失敗が連続すると（**cfgRacTuneIpBlkFailCount**）、以降そのアドレスからのセッション確立試行がすべて一定の時間（**cfgRacTuneIpBlkPenaltyTime)**）拒否されます。
cfgRacTuneIpBlkFailCount	ログイン試行を拒否するまでの IP アドレスのログイン失敗回数を設定します。
cfgRacTuneIpBlkFailWindow	失敗した試行がカウントされる時間枠（秒）。失敗回数がこの制限値を超えると、カウンタはリセットされます。
cfgRacTuneIpBlkPenaltyTime	ログイン失敗回数の制限を超えた IP アドレスからのログイン試行を拒否する時間を秒で指定します。

IP ブロックを有効にする

次の例では、クライアントが 1 分間に 5 回ログイン試行に失敗した場合に、5 分間このクライアント IP アドレスのセッション確立を阻止します。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

次の例は、1 分以内に失敗が 3 回を超えた場合に、1 時間ログイン試行を阻止します。

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

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

ローカル RACADM を使用した iDRAC6 Telnet および SSH サービスの設定

Telnet/SSH コンソールは、RACADM コマンドを使用してローカル（管理下サーバー上）で設定できます。

メモ: この項のコマンドを実行するには、**iDRAC6 の設定** 権限が必要です。

メモ: iDRAC6 で Telnet または SSH 設定を変更した場合、既存のすべてのセッションは、警告なしに終了します。

ローカル RACADM から Telnet/SSH コンソールを有効にするには、管理下サーバーにログインし、コマンドプロンプトで次のコマンドを入力します。

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Telnet または SSH サービスを無効にするには、値を 1 から 0 に変更します。

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

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

iDRAC6 の Telnet ポート番号を変更するには、次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <新しいポート番号>
```

たとえば、Telnet ポートをデフォルトの 22 から 8022 に変更するには、次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

使用可能な全 RACADM CLI コマンドのリストは、「RACADM コマンドラインインタフェースの使用」を参照してください。

リモートおよび SSH/Telnet RACADM

リモート RACADM はクライアント側のユーティリティで、管理ステーションから帯域外ネットワークインタフェースを使用して実行できます。管理下システムに接続して、リモートコンソールまたは管理ステーションから RACADM サブコマンドを実行できるリモート機能のオプション（**-r**）があります。リモート機能を使用するには、有効なユーザー名（**-u** オプション）、パスワード（**-p** オプション）、および iDRAC6 の IP アドレスが必要です。SSH/Telnet RACADM とは、SSH または Telnet プロンプトから RACADM コマンドを使用することを指します。

同時に実行できるリモート RACADM の最大セッション数は 4 です。これらのセッションは独立しており、Telnet および SSH セッションとは別です。iDRAC6 は 4 つの RACADM セッションに加えて、4 つの SSH セッションと 4 つの Telnet セッションを同時にサポートできます。

メモ: RACADM のリモート機能を使用する前に、iDRAC6 の IP アドレスを設定します。

メモ: リモートシステムにアクセスしているシステムのデフォルト証明書ストアに iDRAC6 証明書がない場合は、RACADM コマンドを入力したときにメッセージが表示されます。

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (セキュリティ警告：証明書が無効です - 証明書の名前が無効かサイト名と一致しません)

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors. (実行を継続します。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 リモート機能を使用する場合は、次に示すようなファイル操作に関連して RACADM サブコマンドを使用するフォルダへの書き込み権限が必要になります。

```
racadm getconfig -f <ファイル名>
```

または

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

リモート RACADM の使用方法

```
racadm -r <iDRAC6 IP アドレス> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>

racadm -i -r <iDRAC6 IP アドレス> <サブコマンド> <サブコマンドオプション>
```

たとえば、次のとおりです。

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

iDRAC6 の HTTPS ポート番号をデフォルトポート(443)以外のカスタムポートに変更した場合は、次の構文を使用します。

```
racadm -r <iDRAC6 IP アドレス>:<ポート> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>

racadm -i -r <iDRAC6 IP アドレス>:<ポート> <サブコマンド> <サブコマンドオプション>
```

リモート RACADM のオプション

表 13-6 に、リモート RACADM コマンドのオプションを一覧にします。

表 13-6 RACADM コマンドのオプション

オプション	説明
-**r** <raclpAddr>	コントローラのリモート IP アドレスを指定します。
-**r** <raclpAddr>**:**<ポート番号>	iDRAC6 のポート番号がデフォルトポート(443)でない場合は、<ポート番号> を使用してください。
-**i**	インタラクティブにユーザーのユーザー名とパスワードを問い合わせるように RACADM に指示します。
-**u** <ユーザー名>	コマンドのトランザクションの認証に使用するユーザー名を指定します。-**u** オプションを使用すると、-**p**p オプションも必要になり、-**i** オプション(インタラクティブ)は使用できなくなります。
-**p** <パスワード>	コマンドのトランザクションを認証するパスワードを指定します。-**p**オプションを使用すると、-**i** オプションは使用できなくなります。
-S	RACADM が無効な証明書エラーをチェックするように指定します。RACADM は無効な証明書を検出した場合にコマンドの実行を停止して、エラーメッセージを表示します。

---

iDRAC6 設定ファイルの使用

iDRAC6 設定ファイルは、iDRAC6 データベースの代表値が含まれたテキストファイルです。RACADM **getconfig** サブコマンドを使用して iDRAC6 の現在の値が含まれた設定ファイルを生成できます。ファイルを編集し、RACADM **config -f** サブコマンドを使用してファイルを iDRAC6 にロードし直すか、設定を他の iDRAC6 にコピーできます。

iDRAC6 設定ファイルの作成

設定ファイルは、プレーンテキストファイルです。有効なファイル名なら何でも使用できますが、推奨される拡張子は **.cfg** です。

設定ファイルの特徴は以下のとおりです。

- テキストエディタで作成可能
- RACADM **getconfig** サブコマンドで iDRAC6 から取得
- RACADM **getconfig** サブコマンドで iDRAC6 から取得して編集

RACADM **getconfig** コマンドで設定ファイルを取得するには、次のコマンドを入力します。

```
racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> getconfig -f myconfig.cfg
```

このコマンドは、現在のディレクトリにファイル **myconfig.cfg** を作成します。

設定ファイルの構文

メモ: Windows の **Notepad** や Linux の **vi** など、プレーンテキストエディタで設定ファイルを編集します。**racadm** ユーティリティは ASCII テキストのみを解析します。フォーマットすると、パーサが混乱して iDRAC6 のデータベースが壊れる可能性があります。

この項では設定ファイルのフォーマットについて説明します。

- # で始まる行はコメントです。

  コメントは、行の最初の列から開始する必要があります。その他の列にある # の文字は、単に # 文字として処理されます。

例:

```
#

# This is a comment (これはコメントです。)

[cfgUserAdmin]

cfgUserAdminPrivilege=4
```

- すべてのグループエントリは、**[** と **]** の文字で囲む必要があります。

  グループ名を示す開始の **[** 文字は、一列目で始まる必要があります。このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。設定データはグループに分類されます。これについては、デルサポートサイト **support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』の定義を参照してください。

  次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

  例:

```
[cfgLanNetworking](グループ名)

cfgNicIpAddress=192.168.1.1(オブジェクト名)
```

- パラメータは、object、=、値の間に空白を入れずに「object=値」のペアとして指定します。

  値の後の空白スペースは無視されます。値の文字列内にあるスペースは変更されません。= の右側の文字はすべてそのまま解釈されます(たとえば 2 番目の =、または# 、[、] など)。

  インデックス付きグループの内容を表示するには、次のコマンドを使用します。

```
racadm getconfig -g <グループ名> [-i <インデックス>]
```

- インデックス付きグループの場合、オブジェクトアンカーは [ ] の組の後にくる最初のオブジェクトでなければなりません。次は、現在のインデックス付きグループの例です。

```
[cfgUserAdmin]

cfgUserAdminIndex=11
```

- パーサーがインデックス付きのグループを検出した場合、グループのインデックスはアンカーとして使用されます。インデックス付きグループ内のオブジェクトが変更された場合は、インデックス値にも関連づけられます。

  たとえば、次のとおりです。

```
[cfgUserAdmin]

# cfgUserAdminIndex=11

cfgUserAdminUserName=

# cfgUserAdminPassword=********  (Write-Only)

cfgUserAdminEnable=0

cfgUserAdminPrivilege=0x00000000

cfgUserAdminIpmiLanPrivilege=15

cfgUserAdminIpmiSerialPrivilege=15

cfgUserAdminSolEnable=0
```

- インデックスは読み取り専用で、変更できません。インデックス付きグループのオブジェクトは、そのインデックスに拘束され、オブジェクトの値に対する有効な設定は、その特定のインデックスにのみ適用されます。
- インデックス付きグループのそれぞれには、事前に定義されたインデックスのセットがあります。詳細については、デルサポートサイト **support.dell.com / manuals** で『iDRAC 管理者リファレンスガイド』を参照してください。

設定ファイルの iDRAC6 IP アドレスの変更

設定ファイル内の iDRAC6 IP のアドレスを変更するには、不要な **<**変数**>=**<値> のエントリをすべて削除します。IP アドレス変更に関連する 2 つの **<**変数**>**=<値> エントリを含め、"[" と "]" が付いた実際の変数グループのラベルのみが残ります。

たとえば、次のとおりです。

```
#

# Object Group (オブジェクトグループ) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110
```

```
cfgNicGateway=10.35.10.1
```

このファイルは次のようにアップデートされます。

```
#

# 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
```

iDRAC6 への設定ファイルのロード

`racadm config -f` <ファイル名> コマンドは、有効なグループとオブジェクト名が存在し、構文ルールに従っていることを検証するために設定ファイルを解析します。ファイルにエラーがなければ、このファイルの内容で iDRAC6 データベースがアップデートされます。

メモ: 構文のみを検証し、iDRAC6 データベースをアップデートしない場合は、**config** サブコマンドに **-c** オプションを追加します。

設定ファイルのエラーには、検出された行番号のフラグと、その問題を説明した簡単なメッセージが付きます。設定ファイルで iDRAC6 をアップデートする前に、すべてのエラーを修正する必要があります。

メモ: **racresetcfg** サブコマンドを使用すると、データベースと iDRAC6 NIC の設定は元のデフォルト設定にリセットされ、ユーザーとユーザー設定がすべて削除されます。`root`（ルート）ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。

`racadm config -f` <ファイル名> コマンドを実行する前に、`racresetcfg` サブコマンドを 実行して iDRAC6 をデフォルト設定にリセットできます。ロードする設定ファイルに目的のオブジェクト、ユーザー、インデックス、その他のパラメータがすべて含まれていることを確認してください。

設定ファイルで iDRAC6 をアップデートするには、次のコマンドを実行します。

```
racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> config -f myconfig.cfg
```

コマンドが完了したら、RACADM **getconfig** サブコマンドを実行すると、アップデートが正常に終了したことを確認できます。

複数の iDRAC6 の設定

設定ファイルを使用すると、同じプロパティを持つ別の iDRAC6 を設定できます。複数の iDRAC6 を設定するには、次の手順に従ってください。

1. 他の iDRAC6 に複製する iDRAC6 の設定から設定ファイルを作成します。次のコマンドを入力します。

   ```
   racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> getconfig -f <ファイル名>
   ```

   <ファイル名> は **myconfig.cfg** など、iDRAC6 のプロパティを保存するファイルの名前です。

   以下の例は、リモート RACADM コマンドを使用して複数の iDRAC6 を設定する方法を紹介しています。管理ステーションでバッチファイルを作成し、バッチファイルからリモート `racadm` コマンドを呼び出します。

   たとえば、次のとおりです。

   ```
   racadm -r <サーバー IP 1> -u <ユーザー> -p <パスワード> config -f myconfig.cfg

   racadm -r <サーバー IP 2> -u <ユーザー> -p <パスワード> config -f myconfig.cfg

   ...
   ```

   詳細については、iDRAC6 設定ファイルの作成を参照してください。

   メモ: 設定ファイルによっては、他の iDRAC6 にファイルをエクスポートする前に変更する必要のある固有の iDRAC6 情報（静的 IP アドレスなど）が含まれています。

2. 前の手順で作成した設定ファイルを編集し、コピーしない設定を削除またはコメントアウトします。

3. 設定する iDRAC6 がある管理下サーバーのそれぞれにアクセスできるネットワークドライブに、編集した設定ファイルをコピーします。

4. 各 iDRAC6 に次の設定を行います。

   a. 管理下サーバーにログインし、コマンドプロンプトを開始します。

b. iDRAC6 の設定をデフォルト設定から変更するには、次のコマンドを入力します。

```
racadm racreset
```

c. 次のコマンドを使用して、設定ファイルを iDRAC6 にロードします。

```
racadm -r <リモート iDRAC6 IP> -u <ユーザー> -p <パスワード> config -f <ファイル名>
```

<ファイル名> は、作成した設定ファイルの名前です。ファイルが作業ディレクトリにない場合は、完全修飾パスを含めてください。

d. 次のコマンドを入力して、設定済みの iDRAC6 をリセットします。

```
racadm reset
```

目次ページに戻る

目次ページに戻る

WS-MAN インタフェースの使用

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

Web Services for Management(WS-MAN)は、システム管理に使用される Simple Object Access Protocol(SOAP)ベースのプロトコルです。WS-MAN は、ネットワークでデータの共有とやり取りを行うデバイスの相互運用可能なプロトコルを提供します。iDRAC6 は WS-MAN を使用して、Distributed Management Task Force(DMTF)の Common Information Model (CIM)ベースの管理情報を伝送します。CIM 情報は、管理下システムで操作可能なセマンティックスや情報の種類を定義します。Dell が組み込まれたサーバープラットフォーム管理インタフェースはプロファイルに分類され、各プロファイルは個々の管理ドメインや機能領域に固有のインターフェイスを定義しています。さらに、Dell はモデルやプロファイルの拡張を多数定義することで、追加機能用のインタフェースを提供しています。

WS-MAN を介して入手できるデータは、DMTF プロファイルと Dell 拡張プロファイルにマッピングされた iDRAC6 計装インタフェースによって提供されます。

WS 管理の機能

WS-Management の仕様は、管理アプリケーションと管理下リソースの相互運用性を促進します。ウェブサービスの規格と使用要件のコアセットを識別して、あらゆるシステム管理の要となる共通操作を明らかにすることで、WS-Management は以下のことができます。

- 管理リソースの存在を検出し、リソース間を移動する
- 設定や動的な値など、個々の管理リソースを取得、設定、作成、削除する
- 大容量テーブルやログなど、コンテナやコレクションの内容を列挙する
- 強力に型付けされた入出力パラメータを使用して特定の管理手段を実行する

対応 CIM プロファイル

表 16-1 対応 CIM プロファイル

標準 DMTF
1. ベースサーバー ホストサーバーを表す CIM クラスを定義します。
2. ベースメトリック 管理下要素用に取り込まれたメトリックスをモデル化して制御する機能を提供する CIM クラスを定義します。
3. サービスプロセッサ サービスプロセッサをモデル化する CIM クラスを定義します。
4. USB リダイレクト USB リダイレクトに関する情報を記述する CIM クラスを定義します。キーボード、ビデオ、マウス装置を USB デバイスとして管理する場合は、このプロファイルを使用する必要があります。
5. 物理的資産 管理要素の物理資産を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して、物理トポロジだけでなく、ホストサーバーとそのコンポーネントの FRU 情報を表します。
6. SM CLP 管理ドメイン 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。
7. 電源状況管理 電源制御操作の CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーの電源制御操作を実行します。
8. CLP サービス CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して独自の CLP を実装します。
9. IP インタフェース 管理下システムの IP インタフェースを表す CIM クラスを定義します。
10. DHCP クライアント DHCP クライアントとそれに関連付けられた機能や設定を表す CIM クラスを定義します。
11. DNS クライアント 管理下システムの DNS クライアントを表す CIM クラスを定義します。
12. ログ記録

異なるログの種類を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してシステムイベントログ（SEL）と iDRAC6 RAC ログを表します。

13. 役割ベースの認証
役割を表す CIM 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 アカウント権限を定義します。

14. SMASH コレクション
CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して独自の CLP を実装します。

15. プロファイル登録
プロファイルの実装をアドバタイズする 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。

16. 簡易 ID 管理
ID を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して iDRAC6 のアカウントを定義します。

17. イーサネットポート
管理下システムの Ethernet ポート、それに関連付けられたコントローラ、および Ethernet インタフェースを表す CIM クラスを定義します。ポートの物理面との関連付けとプロファイル実装バージョンの情報はこのプロファイルでモデル化されます。

18. センサー
管理下システムのセンサーを説明する CIM クラスの定義に使用されます。また、センサーと監視されるデバイス間の関係を説明する関連クラスを定義します。

Dell g

1. Active Directory クライアント
iDRAC6 Active Directory クライアントおよび Active Directory グループのローカル権限を設定する CIM と Dell 拡張クラスを定義します。

2. 仮想メディア
iDRAC6 仮想メディアを設定する CIM と Dell 拡張クラスを定義します。USB リダイレクトプロファイルを拡張します。

3. OS 導入
OS 導入機能の設定を表す CIM クラスと Dell 拡張クラスを定義します。サービスプロセッサが提供する OS 導入機能の操作によって OS 導入アクティビティをサポートする機能を追加することで、参照プロファイルの管理機能を拡張します。

4. ソフトウェアインベントリ
現在インストールされている BIOS 、コンポーネントのファームウェア、診断、Unified Server Configurator、およびドライバパックのバージョンを表す CIM と Dell 拡張を定義します。また、ロールバックおよび再インストール目的で、Lifecycle Controller で利用できる BIOS およびファームウェアアップデートイメージのバージョンを表します。

5. ソフトウェアアップデート
BIOS、診断、ドライバパック、コンポーネント、Lifecycle Controller のファームウェアの更新目的で、サービスクラスおよびメソッドを表す CIM と Dell 拡張を定義します。アップデートメソッドは、CIFS、NFS、FTP、HTTP ネットワーク共有場所、そして Lifecycle Controller のアップデートイメージからのアップデートをサポートしています。アップデートリクエストは、ジョブとして計画され、アップデートに適用する再起動の処理方法の選択肢と共に、すぐにあるいは後で実行するようにスケジュールできます。

6. ジョブ制御
アップデートリクエストによって生成されるジョブを管理するための CIM と Dell 拡張を定義します。ジョブを作成、削除、変更、そして 1 回の再起動で複数のアップデートを実行するために、ジョブキューに統合させることもできます。

7. LC 管理
自動検出と部品交換 Lifecycle Controller 機能を管理する目的で、属性の取得および設定を行うための CIM と Dell 拡張を定義します。

8. 持続ストレージ
Dell のプラットフォームで仮想フラッシュメディアのパーティションを管理するために、CIM および Dell 拡張クラスを定義します。

9. シンプル NIC
NIC ネットワークコントローラの設定を表すために、CIM および Dell 拡張クラスを定義します。

10. BIOS と起動の管理
Dell の BIOS 属性を表し、ホストの起動順序を設定するために、CIM および Dell の拡張クラスを定義します。

11. シンプル RAID
ホストの RAID ストレージの設定を表すために、CIM および Dell 拡張クラスを定義します。

12. iDRAC カード
iDRAC6 インベントリ情報を表すために、CIM および Dell 拡張クラスを定義します。

13. メモリ
ホストの DIMM インベントリ情報を表すために、CIM および Dell 拡張クラスを定義します。

14. CPU
ホストの CPU インベントリ情報を表すために、CIM および Dell 拡張クラスを定義します。

15. システム情報
ホストプラットフォームのインベントリ情報を表すために、CIM および Dell 拡張クラスを定義します。

16. PCI デバイス
ホストの PCI デバイスのインベントリ情報を表すために、CIM および Dell 拡張クラスを定義します。

17. ビデオ
ホストのビデオカードのインベントリ情報を表すために、CIM および Dell 拡張クラスを定義します。

iDRAC6 WS-MAN の実装は、ポート 443 上で SSL を使用して送信のセキュリティを確保し、またベーシックおよびダイジェスト認証をサポートしています。ウェブサービスのインタフェースは、Windows WinRM や Powershell CLI などのクライアントインフラストラクチャ、WSMANCLI などのオープンソースのユーティリティ、および次のようなアプリケーションプログラミング環境を利用して使うこともできます
Microsoft .NET.

そのほか、実装ガイド、ホワイトペーパー、プロファイル、MOF、コード例などが デルエンタープライズテクノロジーセンター **www.delltechcenter.com** から入手可能です。詳細については、以下も参照してください。

- DMTF ウェブサイト **www.dmtf.org/standards/profiles/**
- WS-MAN リリースノートまたは Readme ファイル。

目次ページに戻る

目次ページに戻る

iDRAC6 Enterprise の使用
SM-CLP コマンドラインインタフェース

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

本項では、iDRAC6 に組み込まれている Server Management Workgroup(SMWG)Server Management Command Line Protocol(SM-CLP)について説明します。

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

iDRAC6 SM-CLP は DMTF と SMWG が提唱するプロトコルで、システム管理 CLI 実装の標準となっています。その原動力は、システム管理コンポーネントの標準化の基盤となることを目標に定義された SMASH アーキテクチャです。SMWG SM-CLP は DMTF が提唱する全体的な SMASH 作業のサブコンポーネントです。

SM-CLP は、ローカルの RACADM コマンドラインインタフェースが提供する機能のサブセットを別のアクセスパスで提供します。SM-CLP は iDRAC6 内で実行され、RACADM は管理下サーバー上で実行されます。また、RACADM は Dell 専用のインタフェースであるのに対し、SM-CLP は業界標準のインタフェースです。

メモ: iDRAC6 SM-CLP プロパティデータベース、WS-MAN クラスと SM-CLP ターゲット間のマッピング、およびデル実装の詳細については、**www.delltechcenter.com** のデルエンタープライズテクノロジセンターで『iDRAC6 CIM Element Mapping』と『iDRAC6 SM-CLP Property Database』の文書を参照してください。『iDRAC6 CIM 要素のマッピング』マニュアルに記載されている情報は、DMTF プロファイルと、それらのプロファイルの Dell 拡張で指定しています。WSMAN の構成については、**http://www.dmtf.org/standards/profiles/** の DMTF プロファイルと MOF に記載されています。また、Dell 拡張は **http://www.delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions** で入手できます。

SM-CLP を使用したシステム管理

iDRAC6 SM-CLP を使用すると、以下のシステム機能をコマンドラインから管理できます。

- サーバーの電源管理 - システムのオン、シャットダウン、再起動
- システムイベントログ(SEL)管理 - SEL レコードの表示やクリア
- iDRAC6 ユーザーアカウントの管理
- Active Directory 設定
- iDRAC6 LAN の設定
- SSL 証明書署名要求(CSR)の生成
- 仮想メディア設定

---

iDRAC6 SM-CLP のサポート

SM-CLP は iDRAC6 ファームウェアからホストされ、Telnet 接続と SSH 接続をサポートしています。iDRAC6 SM-CLP インタフェースは DMTF 組織が提供する SM-CLP 規格バージョン 1.0 に基づいています。

以下の項では、iDRAC6 からホストされる SM-CLP 機能の概要について説明します。

メモ: SM-CLP セッションを Telnet/SSH を使用して確立し、ネットワークの切断によってセッションが正しく終了しなかった場合に、「最大接続数に達した」というメッセージが表示されることがあります。これを解決するには、新しい接続を試みる前に、ウェブ GUI の **システム** → **リモートアクセス** → **iDRAC6**→ **ネットワーク / セキュリティ** → **セッション** で SM-CLP セッションを終了してください。

メモ: iDRAC6 は最大 4 つの Telnet セッションと 4 つの SSH セッションを同時にサポートします。ただし、それら 8 つのセッション中 1 つだけが SM-CLP を使用できます。つまり、iDRAC6 がサポートしているのは一度に 1 つの SM-CLP セッションのみです。

SM-CLP セッションの開始方法

- SSH/Telnet を使用して iDRAC6 に接続すると、CLI(コンソール)が開きます。
- ドル記号のプロンプトで「smclp」と入力して、SM-CLP コンソールを開始します。

構文:

```
telnet <iDRAC6 の IP アドレス>

$ (the CLI prompt is displayed (CLI プロンプトが表示されます) )
```

```
$smclp （at the CLI prompt, type smclp (CLI プロンプトで smclp と入力します）)
```

SM-CLP の機能

SM-CLP 仕様は、CLI を使用した単純なシステム管理に使用できる標準的な SM-CLP バーブの共通セットを提供しています。

SM-CLP はバーブとターゲットの概念を発展させて、CLI を使用したシステム設定機能を提供します。バーブは、実行する操作を示し、ターゲットは操作の実行対象となるエンティティ(またはオブジェクト)です。

以下は SM-CLP コマンドラインの構文です。

<バーブ> [<オプション>] [<ターゲット>] [<プロパティ>]

表 15-1 は、iDRAC6 CLI がサポートするバーブ、各コマンドの構文、およびバーブがサポートするオプションのリストです。

表 15-1 サポートされている SM-CLP CLI バーブ

バーブ	説明	オプション
CD	シェルを使用して管理下システムのアドレス領域を移動します。 構文: cd [オプション] [ターゲット]	-default、-examine、-help、-output、-version
delete	オブジェクトのインスタンスを削除します。 構文: delete [オプション] [ターゲット]	-examine、-help、-output、-version
exit	SM-CLP シェルのセッションを終了します。 構文: exit [オプション]	-help、-output、-version
help	SM-CLP コマンドのヘルプを表示します。 help	-examine、-help、-output、-version
reset	ターゲットをリセットします。 構文: reset [オプション] [ターゲット]	-examine、-help、-output、-version
set	ターゲットのプロパティを設定します。 構文: set [オプション] [ターゲット] <プロパティ名>=<値>	-examine、-help、-output、-version
show	ターゲットのプロパティ、バーブ、およびサブターゲットを表示します。 構文: set [オプション] [ターゲット] <プロパティ名>=<値>	-all、-default、-display、-examine、-help、-level、-output、-version
start	ターゲットを起動します。 構文: start [オプション] [ターゲット]	-examine、-force、-help、-output、-version
stop	ターゲットをシャットダウンします。 構文: stop [オプション] [ターゲット]	-examine、-force、-help、-output、-version、-wait
version	ターゲットのバージョン属性を表示します。 構文: version [オプション]	-examine、-help、-output、-version

表 15-2 は、SM-CLP オプションについて説明しています。表に示されているように、一部のオプションには省略形があります。

表 15-2 サポートされている SM-CLP オプション

SM-CLP オプション	説明

-all、-a	実行可能な機能のすべてを実行するようにバーブに指示します。
-destination	dump コマンドのイメージを保存する場所を指定します。 構文: -destination <URI>
-display、-d	コマンド出力をフィルタします。 構文: -display <プロパティ | ターゲット | バーブ>[, <プロパティ | ターゲット | バーブ>]*
-examine、-x	コマンドを実行せずにコマンド構文を確認するようにコマンドプロセッサに指示します。
-force, -f	正常に終了できない場合は、このオプションを使用して、ターゲットシステムの強制終了を実行します。 構文: stop -force <target>
-help、-h	バーブのヘルプを表示します。
-level、-l	指定ターゲット下の追加レベルでターゲットで動作するようバーブに指示します。 構文: -level <番号|すべて>
-output、-o	出力のフォーマットを指定します。 構文: -output format=<テキスト | clpcsv | キーワード | clpxml> または -output format=<テキスト | clpcsv | キーワード | clpxml>
-version、-v	SM-CLP のバージョン番号を示します。

MAP アドレス領域の移動

メモ: SM-CLP アドレスパスでスラッシュ(/)とバックスラッシュ(\)は置き換え可能です。ただし、コマンドラインの最後のバックスラッシュは次の行のコマンドに続き、コマンドが解析されると無視されます。

SM-CLP で管理できるオブジェクトは Manageability Access Point(MAP)アドレス領域と呼ばれる階層空間に分類されたターゲットで表されます。アドレスパスは、アドレス領域のルートからアドレス領域のオブジェクトへのパスを指定します。

ルートターゲットは、スラッシュ(/)またはバックスラッシュ(\)で表されます。これは、iDRAC6 にログインするときのデフォルトの開始ポイントです。cd バーブを使用してルートから移動します。

たとえば、システムイベントログ(SEL)で 3 番目のレコードに移動するには、次のコマンドを入力します。

```
->cd /admin1/system1/logs1/log1/record3
```

ターゲットなしで cd バーブを入力し、アドレス領域内の現在の場所を検索します。省略形 . .と . の機能は Windows および Linux の場合と同様で、. . は、親レベルを示し、. は、現在のレベルを示します。

ターゲット

SM-CLP で使用可能なターゲット一覧は、**www.delltechcenter.com** のデルエンタープライズテクノロジセンターで SM-CLP マッピングの文書を参照してください。

---

show バーブ の使用

ターゲットの詳細を理解するには、show バーブを使用します。このバーブは、その場所で許可されているターゲットのプロパティ、サブターゲット、および SM-CLP バーブのリストを表示します。

-display オプションの使用

show -display オプションを使用すると、コマンドの出力を 1 つまたは複数のプロパティ、ターゲット、バーブに制限できます。たとえば、現在の場所のプロパティとターゲットのみを表示する場合は、次のコマンドを使用します。

```
show -display properties,targets
```

特定のプロパティのみを表示するには、次のコマンドのように修飾します。

```
show -d properties=(ユーザー ID、名前) /admin1/system1/sp1/oemdcim_mfaaccount1
```

1 つのプロパティのみを表示する場合、括弧は省略できます。

-level オプションの使用

show -level オプションは、指定ターゲットの下の他のレベルに **show** を実行します。アドレス空間のターゲットとプロパティをすべて表示するには、**-l all** オプションを使用します。

-output オプションの使用

-output オプションは、SM-CLP バーブの出力の 4 つのフォーマット（**テキスト**、**clpcsv**、**キーワード**、**clpxml**）の 1 つを指定します。

デフォルトのフォーマットは **テキスト** で、最も読みやすい出力です。**clpcsv** フォーマットはカンマ区切りの値のフォーマットで、表計算プログラムへの読み込みに適しています。**キーワード** フォーマットは、キーワード=値 のペアを 1 行に 1 つずつのリストとして出力します。**clpxml** フォーマットは、**応答** XML 要素を含む XML ドキュメントです。DMTF は **clpcsbv** および **clpxml** フォーマットを指定しており、これらの仕様は DMTF ウェブサイト（**www.dmtf.org**）で参照できます。

次の例は、SEL の内容を XML で出力する方法を示しています。

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

---

iDRAC6 SM-CLP の例

以下のサブセクションでは、SSH インタフェースを使用して iDRAC6 にログインし、SM-CLP セッションを開始して以下の操作を実行する方法の例を示します。

- サーバーの電源管理
- SEL の管理
- MAP ターゲットのナビゲーション
- システムプロパティの表示

サーバーの電源管理

表 15-3 は、SM-CLP を使用して管理下サーバーの電源管理操作を実行する例を示しています。

「smclp」と入力して SM-CLP コンソールを開始します。

表 15-3 サーバーの電源管理操作

操作	構文
SSH インタフェースを使用して iDRAC6 にログインする	>ssh 192.168.0.120 >login: root >password: SM-CLP コンソールを開始するには、「smclp」と入力します。
サーバーの電源を切る	->stop /admin1/system1 system1 successfully stopped
電源オフの状態からサーバーの電源を入れる	->start /admin1/system1 system1 successfully started
サーバーを再起動する	->reset /admin1/system1 RESET successful for system1

SEL 管理

表 15-4 は、SM-CLP を使用して、管理下システムで SEL 関連の操作を実行する例を示しています。

MAP ターゲットのナビゲーション

表 15-4 SEL の管理操作

操作	構文
SEL	->show -d targets,properties,verbs /admin1/system1/logs1/log1

の表示	**Might return:** Targets: record1/ record2/... Properties: OverwritePolicy=7 LogState=4 CurrentNumberOfRecords=60 MaxNumberOfRecords=512 ElementName=Record Log 1 HealthState=5 EnabledState=2 RequestedState=12 EnabledDefault=2 TransitioningToState=12 InstanceID=DCIM: SEL Log OperationalStatus={2} Verbs: show exit version CD help
SEL レコードの表示	->show /admin1/system1/logs1/log1/record4 **以下が返されます。** ufip=/admin1/system1/logs1/log1/record4 Associations:LogManagesRecord=>/admin1/system1/logs1/log1 Properties: RecordData=*0.0.65*4 2*1245152621*65 65*4*31*0*true*111*1*255*255* RecordFormat=*IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*IPMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI_GeneratorID*IPMI_EvMRev*IPMI_Se Description=:0:Assert:OEM specific ElementName=DCIM System Event Log Entry InstanceID=DCIM:SEL LOG:4 LogInstanceID=idrac:Unknown:Unknown SEL Log LogName=DCIM System Event Log Entry RecordID=DCIM:SEL LOG:4 CreationTimeStamp=20090616114341.000000+000
	Verbs: show exit version CD help delete
SEL のクリア	->delete /admin1/system1/logs1/log1/record* **次のメッセージを返します。** Records deleted successfully. (レコードの削除に成功しました。)

表 15-5 は、**cd** バーブを使用して MAP をナビゲートする例を示しています。すべての例で、最初のデフォルトターゲットは / であると想定されます。

表 15-5 Map ターゲットのナビゲーション操作

操作	構文
システムターゲットまでナビゲートして再起動する	->cd admin1/system1 ->reset **メモ:** 現在のデフォルトターゲットは **/** です。
SEL ターゲットまでナビゲートしてログレコードを表示する	->cd admin1 ->cd system1 ->cd logs1 ->cd log1 ->show **is equivalent to** ->cd admin1/system1/logs1/log1 ->show
現在のターゲットを表示する	->cd .
1 つ上のレベルへ移動する	->cd ..
シェルを終了する	->exit

目次ページに戻る

目次ページに戻る

iVMCLI を使用したオペレーティングシステムの導入

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

統合仮想メディアコマンドラインインタフェース(iVMCLI)ユーティリティは、管理ステーションからリモートシステムの iDRAC6 に仮想メディアの機能を提供するコマンドラインインタフェースです。iVMCLI とスクリプト方式を使用すると、ネットワーク内の複数のリモートシステムにオペレーティングシステムを導入できます。

本項では、企業ネットワークに iVMCLI ユーティリティを統合する方法について説明します。

作業を開始する前に

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

リモートシステム要件

- 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 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 システムのイメージファイルの作成

Linux システム用にブータブルイメージファイルを作成するには、データ複製ユーティリティ(dd) を使用します。

このユーティリティを実行するには、コマンドプロンプトを開いて次のように入力します。

```
dd if=<入力デバイス> of=<出力ファイル>
```

例:

```
dd if=/dev/sdc0 of=mycd.img
```

Windows システム用のイメージファイルの作成

Windows イメージファイル用のデータ複製ユーティリティを選択するときには、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ブータブル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。

   設定済みブータブル導入イメージファイルがない場合は、このファイルを作成します。オペレーティングシステムの導入手順に使用されるプログラムやスクリプトをすべて含めます。

   たとえば、Microsoft Windows オペレーティングシステムを導入するには、Microsoft Systems Management Server(SMS)で使用されている導入方法に似たプログラムをイメージファイルに含めることができます。

   イメージファイルを作成するときは、以下の操作を行ってください。

   - 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、展開イメージを「読み取り専用」とマークする

- 次のいずれかの手順を実行してください。
  - **IPMItool** と仮想メディアコマンドラインインタフェース(iVMCLI)を既存のオペレーティングシステム導入アプリケーションに統合します。このユーティリティの使用の手引きとして **ivmdeploy** 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 **ivmdeploy** スクリプトを使用します。

メモ: **ivmdeploy** は内部で **iVMCLI** と **ipmitool** を使用します。このツールを使用するには、IPMI オーバー LAN 権限が必要です。また、**ivmdeploy** スクリプトを使用する場合は、仮想メディアが連結状態でなければなりません。

オペレーティングシステムの導入

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

始める前に、iVMCLI ユーティリティに含まれている **ivmdeploy** サンプルスクリプトを確認してください。このスクリプトは、ネットワーク内のリモートシステムにオペレーティングシステムを導入する手順を詳しく示しています。

以下は、ターゲットのリモートシステムにオペレーティングシステムを導入する手順の概要です。

1. **ip.txt** テキストファイルに導入されるリモートシステムの iDRAC6 の IP アドレス(1 行に 1 個の IP アドレス)を一覧表示します。
2. ブータブルオペレーティングシステム CD または DVD をクライアントのメディアドライブに挿入します。
3. コマンドラインで **ivmdeploy** を実行します。

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

```
ivmdeploy -r ip.txt -u <iDRAC ユーザー> -p <iDRAC パスワード> -c {<iso9660-img> | <パス>}
```

ここで、

- <iDRAC ユーザー> は iDRAC6 のユーザー名(たとえば **root**)です。
- <iDRAC パスワード> は iDRAC6 ユーザーのパスワード(たとえば **calvin**)です。
- <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。
- <パス> は、オペレーティングシステムインストール CD または DVD に含まれるデバイスのパスです。

ivmdeploy スクリプトは、コマンドラインオプションを **iVMCLI** ユーティリティに渡します。これらのオプションの詳細については、「コマンドラインオプション」を参照してください。このスクリプトの **-r** オプションの処理方法は、**iVMCLI -r** オプションとは若干異なります。**-r** オプションの引数が既存のファイル名である場合、スクリプトは指定したファイルから iDRAC6 IP アドレスを読み取り、各行につき **iVMCLI** ユーティリティを一度実行します。**-r** オプションの引数がファイル名でない場合は、単一の iDRAC6 のアドレスになります。この場合、**-r** は **iVMCLI** ユーティリティで説明されている通りに機能します。

ivmdeploy スクリプトは、CD/DVD または CD/DVD ISO9660 イメージからのインストールのみをサポートしています。フロッピーディスクまたはフロッピーディスクイメージからのインストールが必要な場合は、**iVMCLI -f** オプションを使用するようにスクリプトを変更してください。

仮想メディアコマンドラインインタフェースユーティリティの使用

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

iVMCLI ユーティリティは次の機能を提供します。

メモ: 読み取り専用のイメージファイルを仮想化するとき、複数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、その物理ドライブには一度に 1 つのセッションしかアクセスできなくなる。

- 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
- Secure Socket Layer(SSL)を使用した iDRAC6 通信のセキュリティ保護

ユーティリティを実行する前に、iDRAC6 に対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。

注意: iVMCLI コマンドラインユーティリティを実行する際は、対話フラグ「-ij」を利用することをお勧めします。多くの Windows および Linux オペレーティングシステムでは、他のユーザーがプロセスを確認する際、ユーザー名とパスワードが平文のまま表示されるため、上記を行うことで、ユーザー名とパスワードの秘密性が保たれ、セキュリティが強化されます。

オペレーティングシステムがシステム管理者権限、オペレーティングシステムに固有の権限またはグループメンバーシップをサポートしている場合は、iVMCLI コマンドを実行するためにはシステム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 システムの場合は、iVMCLI ユーティリティのパワーユーザー権限が必要です。

Linux システムでは、システム管理者権限がなくても、**sudo** コマンドを使って iVMCLI ユーティリティにアクセスできます。このコマンドは、一元管理下でシステム管理者以外にアクセス権を与え、すべてのユーザーコマンドをログに記録します。iVMCLI グループにユーザーを追加または編集する場合、システム管理者は **visudo** コマンドを使用します。システム管理者権限がないユーザーは、**sudo** コマンドを iVMCLI コマンドライン(または iVMCLI スクリプト)のプレフィックスとして追加することでリモートシステムの iDRAC6 へのアクセス権を取得し、このユーティリティを実行できます。

iVMCLI ユーティリティのインストール

iVMCLI ユーティリティは、Dell OpenManage システム管理ソフトウェアキットに含まれている『Dell Systems Management Tools and Documentation DVD』に収録されています。ユーティリティをインストールするには、DVD をシステムに挿入し、画面に表示される指示に従います。

『Dell Systems Management Tools and Documentation DVD』には、診断、ストレージ管理、リモートアクセスサービス、RACADM ユーティリティなど最新のシステム管理ソフトウェア製品が含まれています。この DVD には、システム管理ソフトウェアに関する最新の製品情報を記載した Readme ファイルも入っています。

『Dell Systems Management Tools and Documentation DVD』には、iVMCLI と RACADM ユーティリティを使用してソフトウェアを複数のリモートシステムに導入する方法を示すサンプルスクリプト **ivmdeploy** も収録されています。

メモ: ivmdeploy スクリプトは、インストール時にその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、そのディレクトリ内のすべてのファイルをコピーしてください。

コマンドラインオプション

iVMCLI インタフェースは、Windows と Linux システムで共通しています。このユーティリティのオプションは RACADM ユーティリティのオプションと同じです。たとえば、iDRAC6 の IP アドレスを指定するオプションでは、RACADM ユーティリティと iVMCLI ユーティリティで同じ構文が必要です。

iVMCLI コマンド形式は次のとおりです。

`iVMCLI [パラメータ] [オペレーティングシステムシェルオプション]`

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

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

- 何らかの理由で iVMCLI 接続が終了した。
- 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 でタスクマネージャを使うと処理を終了できます。

メモ: iVMCLI コマンドを使用するとき、パラメータ値の単語間にスペースがある場合は、パラメータ全体に引用符を使用する必要があります。たとえば、システムの DVD イメージをサーバーのオペレーティングシステムに接続する次のコマンドを見てみましょう。
F:\idrac>ivmcli -r 10.35.155.117 -u root -p calvin -c c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso

-c はパラメータの 1 つで、**c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso** は 'documents and settings' と 'my documents' にスペースを含むパラメータ値です。したがって、イメージファイルの完全修飾パスには引用符が使用されます。この引用符が無ければ、コマンドの実行に失敗します。次のコマンドも無効です。

C:\"documents and settings"\.....

iVMCLI パラメータ

iDRAC6 IP アドレス

`-r <iDRAC IP アドレス>[:<iDRAC SSL ポート>]`

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

<iDRAC の IP アドレス> は有効な一意の IP アドレスまたは iDRAC6 の動的ドメイン命名システム(DDNS)名です(サポートされている場合)。<iDRAC SSL ポート> を省くと、ポート 443(デフォルトポート)が使用されます。iDRAC6 のデフォルト SSL ポートを変更した場合を除いて、オプションの SSL ポートは不要です。

iDRAC6 ユーザー名

`-u <iDRAC ユーザー名>`

このパラメータは仮想メディアを実行する iDRAC6 ユーザー名を指定します。

<iDRAC ユーザー名> 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。

iDRAC6 ユーザーパスワード

`-p <iDRAC ユーザーパスワード>`

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

iDRAC6 の認証に失敗すると、エラーメッセージが表示されてコマンドが終了します。

フロッピー / ディスクデバイスまたはイメージファイル

`-f {<デバイス名> | <イメージファイル>}`

ここで、<デバイス名> は有効なドライブ文字（Windows システム）またはマウント可能ファイルシステムパーティション番号などを含む有効なデバイスファイル名（Linux システム）です。<イメージファイル> は有効なイメージファイルのファイル名とパスです。

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

たとえば、イメージファイルは次のように指定します。

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

`-f /tmp/myfloppy.img`（Linux システム）

イメージファイルが書き込み保護されていない場合は、仮想メディアがそのファイルに書き込むことができます。上書きしてはならないフロッピーイメージファイルへの書き込みを禁止するように、オペレーティングシステムを設定してください。

たとえば、デバイスは次のように指定します。

`-f a:\`（Windows システム）

`-f /dev/sdb4 # 4th partition on device /dev/sdb`（デバイス上の 4 番目のパーティション /dev/sdb）（Linux システム）

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

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

CD / DVD デバイスまたはイメージファイル

`-c {<デバイス名> | <イメージファイル>}`

この場合、<デバイス名> は有効な CD/DVD ドライブ文字（Windows システム）または有効な CD/DVD デバイスファイル名（Linux システム）で、<イメージファイル> は有効な ISO-9660 イメージファイルのファイル名とパスです。

このパラメータは、仮想 CD/DVD-ROM メディアとなる
デバイスまたはファイルを指定します。

イメージファイルはたとえば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）

デバイスはたとえば次のように指定します。

`-c d:\`（Windows システム）

`-c /dev/cdrom`（Linux システム）

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

スイッチオプションしかない場合を除いて、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。

ルート CA 証明書の検証

-S

このパラメータは iDRAC の CA 証明書が有効かどうかを示すパラメータです。証明書が有効でない場合は、iVMCLI セッションは終了し、証明書が有効でないことを示すエラーメッセージが表示されます。証明書が有効であれば、iVMCLI セッションが確立します。

バージョン表示

-v

このパラメータは iVMCLI ユーティリティのバージョンを表示するために使用します。その他の非スイッチオプションが提供されていない場合、コマンドはエラーメッセージなしで終了します。

ヘルプの表示

-h

このパラメータは iVMCLI ユーティリティのパラメータの概要を表示します。スイッチ以外のオプションが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。

マニュアル表示

-m

このパラメータは、使用可能なオプションすべてに関する説明などが記載された iVKMCLI ユーティリティの詳細「マニュアルページ」を表示します。

暗号化データ

-e

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

iVMCLI オペレーティングシステムシェルオプション

iVMCLI のコマンドラインでは、次のオペレーティングシステムの機能を使用できます。

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

  たとえば、「より大」記号(>)の後にファイル名を入力すると、指定したファイルが iVMCLI 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。

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

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

iVMCLI の戻りコード

0 = エラーなし

1 = 接続できない

2 = iVMCLI コマンドラインエラー

3 = RAC ファームウェア接続の切断

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

目次ページに戻る

目次ページに戻る

iDRAC6 設定ユーティリティの使用

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

概要

iDRAC6 設定ユーティリティは、iDRAC6 と管理下システムのパラメータを表示して設定できる起動前の設定環境です。具体的には、以下のことが可能です。

- iDRAC6 と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(LAN)を設定するか、有効と無効を切り替える
- 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
- システムサービスの有効と無効を切り替えるか、キャンセルする
- 自動検出機能を有効または無効にするか、プロビジョニングサーバーを設定する
- 仮想メディアデバイスを連結または分離する
- VFlash を有効または無効にする
- スマートカードログインとシングルサインオンを有効または無効にする
- システムデバイスを設定する
- システム管理者のユーザー名とパスワードを変更する
- iDRAC6 の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。

iDRAC6 設定ユーティリティを使用して実行できるタスクは、ウェブインタフェース、SM-CLP コマンドラインインタフェース、ローカルおよびリモート RACADM コマンドラインインタフェースなど、iDRAC6 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でも実行できます。また、基本ネットワーク設定の場合は、iDRAC6 の初期設定時に iDRAC6 LCD でも実行できます。

---

iDRAC6 設定ユーティリティの起動

初回、または iDRAC6 をデフォルト設定にリセットした後で iDRAC6 設定ユーティリティにアクセスするには、iDRAC6 仮想コンソールに接続しているコンソールを使用する必要があります。

1. iDRAC6 KVM コンソールに接続しているキーボードで、<Print Screen> を押して **iDRAC6 仮想コンソールの On Screen Configuration and Reporting(OSCAR)**メニューを表示します。 上下の方向キーを使用してサーバーが実装されているスロットを強調表示し、Enter キーを押します。
2. サーバーの前面にある電源ボタンを押してサーバーの電源を入れるか、再起動します。
3. リモートアクセス設定するには `Press <Ctrl-E> for Remote Access Setup within 5 sec.....` (5 秒以内に <Ctrl><E> キーを押してください.....) というメッセージが表示されたら、すぐに Ctrl キーを押しながら E キーを押します。iDRAC6 設定ユーティリティが表示されます。

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

最初の 2 行に、iDRAC6 ファームウェアと一次バックプレーンファームウェアのリビジョンに関する情報が表示されます。リビジョンレベルは、ファームウェアアップグレードが必要かどうかの決定に役立ちます。

iDRAC6 ファームウェアは、ウェブインタフェースや SM-CLP など、ファームウェアの外部インタフェースに関連する部分です。一次バックプレーンファームウェアは、サーバーのハードウェア環境とインタフェースし、それを監視するファームウェア部分です。

---

iDRAC6 設定ユーティリティの使用

ファームウェアのリビジョンメッセージの下の iDRAC6 設定ユーティリティの残り部分は、上下の方向キーを使用してアクセスできるメニュー項目です。

- 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** などの選択可能な値がある場合は、左右の方向キー、スペース キーを押して値を選択します。
- 編集できない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。

- iDRAC6 設定ユーティリティを使い終わったら、<Esc> キーを押して 終了 メニューを表示します。このメニューから、変更の保存または破棄を選択するか、ユーティリティに戻ることができます。

以下の項では、iDRAC6 設定ユーティリティの各メニュー項目について説明します。

iDRAC6 LAN

左右の方向キーとスペースキーを使用して **オン** または **オフ** を選択します。

iDRAC6 LAN は、デフォルトで無効になっています。ウェブインタフェース、SM-CLP コマンドラインインタフェースへの Telnet/SSH アクセス、仮想コンソール、仮想メディアなど、iDRAC6 の機能を使用するには、LAN を有効にする必要があります。

LAN を無効にすると、次の警告が表示されます。

`iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF. (LAN チャネルをオフにすると、iDRAC 帯域外インタフェースは無効になります。)`

このメッセージは、LAN を無効にすると、iDRAC6 HTTP、HTTPS、Telnet、または SSH ポートに直接接続してアクセスする機能だけでなく、管理ステーションから iDRAC6 に送信された IPMI メッセージなどの帯域外管理ネットワークトラフィックも受信できないことを通知します。ただし、ローカル RACADM インタフェースは引き続き使用でき、iDRAC6 LAN の再設定に使用することができます。

`C"L[bZ[WNAA±sB`

IPMI オーバー LAN

左右の方向キーとスペースキーを使って **オン** または **オフ** を選択します。**オフ** を選択すると、iDRAC6 は LAN インタフェース経由で着信する IPMI メッセージを受け入れません。

オフ を選択すると、警告メッセージが表示されます。

任意のキーを押してメッセージをクリアし、続行してください。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ら、<Esc> キーを押して、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	
MAC アドレス	これは、iDRAC6 ネットワークインタフェースの MAC アドレスで、編集できません。
VLAN を有効にする	**オン** / **オフ** を表示します。**オン** を選択すると、iDRAC6 の仮想 LAN フィルタが有効になります。
VLAN ID	1 ～ 4094 の VLAN ID の値を表示します。
VLAN	0 ～ 7 の VLAN の優先順位を表示します。
iDRAC6 名の登録	iDRAC6 名を DNS サービスに登録するには、**オン** を選択します。DNS でユーザーが iDRAC6 名を検索できないようにするには、**オフ** を選択します。
iDRAC6 名	**iDRAC 名の登録** を **オン** に設定すると、<Enter> キーを押して **現在の DNS iDRAC 名** テキストフィールドを編集できます。iDRAC6 名の編集が終了したら Enter キーを押します。前のメニューに戻るには、<Esc> キーを押します。iDRAC6 名は有効な DNS ホスト名でなければなりません。
DHCP からのドメイン名	ネットワーク上の DHCP サービスからドメイン名を取得するには、**オン** を選択します。ドメイン名を指定するには、**オフ** を選択します。
ドメイン名	**DHCP からのドメイン名** が **オフ** の場合、<Enter> キーを押して、**現在のドメイン名** テキストフィールドを編集します。編集を終えたら Enter キーを押します。前のメニューに戻るには、<Esc> キーを押します。ドメイン名は、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 警告を有効にする	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** に設定した場合は、PET LAN 警告の転送先となる IP アドレスを入力します。
IPv4 の設定	IPv4 接続のサポートを有効または無効にします。
IPv4	IPv4 プロトコルのサポートを **有効** または **無効** に指定します。 デフォルトは 有効 です。
RMCP+ 暗号キー	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** 項目が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** に設定した場合は、iDRAC6 に割り当てる IP アドレスを入力します。

	デフォルトは **192.168.0.120** です。
サブネットマスク	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得したサブネットマスクアドレスが表示されます。 **IP アドレスソース** を **静的** に設定した場合は、iDRAC6 のサブネットマスクを入力します。デフォルトは **255.255.255.0** です。
デフォルトゲートウェイ	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイの IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定した場合は、デフォルトゲートウェイの IP アドレスを入力します。デフォルトは **192.168.0.1** です。
DHCP からの DNS サーバー	ネットワーク上の DHCP サービスから DNS サーバーアドレスを取得するには、**オン** を選択します。下記の DNS サーバーアドレスを指定するには、**オフ** を選択します。
DNS サーバー 1	**DHCP からの DNS サーバー** が **オフ** の場合、最初の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	**DHCP からの DNS サーバー** が **オフ** の場合、2 番目の DNS サーバーの IP アドレスを入力します。
IPv6 の設定	
IPv6	IPv6 接続のサポートを有効または無効にします。
IPv6 アドレスソース	**AutoConfig（自動設定）** または **静的** を選択します。**AutoConfig（自動設定）** を選択すると、**IPv6 アドレス 1**、**プレフィックス長**、**デフォルトゲートウェイ** フィールドの値は DHCP から取得されます。 **静的** を選択すると、**IPv6 アドレス 1**、**プレフィックス長**、**デフォルトゲートウェイ** フィールドが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** に設定した場合は、iDRAC6 に割り当てる IP アドレスを入力します。
プレフィックス長	IPv6 アドレスのプレフィックス長を設定します。この値は、1 ～ 128 です。
デフォルトゲートウェイ	**IP アドレスソース** を **AutoConfig（自動設定）** に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイの IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定した場合は、デフォルトゲートウェイの IP アドレスを入力します。
IPv6 リンクローカルアドレス	これは、iDRAC6 ネットワークインタフェースの編集不可の **IPv6 リンクローカルアドレス** です。
IPv6 アドレス 2 ～ 15	これは、iDRAC6 ネットワークインタフェースの編集不可の **IPv6 アドレス 2～IPv6 アドレス 15** です。
DHCPv6 からの DNS サーバー	ネットワーク上の DHCP サービスから DNS サーバーアドレスを取得するには、**オン** を選択します。下記の DNS サーバーアドレスを指定するには、**オフ** を選択します。
DNS サーバー 1	**DHCP からの DNS サーバー** を **オフ** にした場合は、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** を **オフ** にした場合は、最初の DNS サーバーの IP アドレスを入力します。

仮想メディアの設定

仮想メディア

左右の方向キー を使用して **自動連結**、**接続**、または **切断** 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、**仮想コンソール** セッション中に使用できるようになります。
- **分離** を選択すると、ユーザーは **仮想コンソール** 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。
- **自動連結** を選択した場合は、仮想メディアセッションが開始されると、仮想メディアデバイスは自動的にサーバーに接続されます。

メモ: 仮想メディア機能で USB フラッシュドライブを使用するには、BIOS 設定ユーティリティで **USB フラッシュドライブのエミュレーションタイプ** を **ハードディスク** に設定してください。サーバー起動中に <F2> キーを押して、BIOS 設定ユーティリティにアクセスしてください。**USB フラッシュドライブのエミュレーションタイプを 自動** に設定すると、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。

vFlash

左右の方向キーを使用して **有効** または **無効** を選択します。

- **有効** - vFlash をパーティション管理に使用できます。
- **無効** - vFlash をパーティション管理に使用できません。

注意: 複数のパーティションを使用または連結している場合は、vFlash を無効にできません。

vFlash の初期化

vFlash カードを初期化するには、このオプションを選択します。初期化操作によって、SD カード上の既存のデータと既存のパーティションがすべて削除されます。1 つまたは複数のパーティションが使用中または連結している場合は、初期化操作を実行できません。このオプションは、256 MB より大きいサイズのカードが iDRAC Enterprise カードスロットにあり、vFlash が有効になっている場合にのみアクセス可能です。

Enter を押して vFlash SD カードを初期化します。

次のような理由で初期化操作に失敗する可能性もあります。

- 現在 SD カードがない。
- 現在 vFlash を別のプロセスが使用中である。
- vFlash が有効になっていない。
- SD カードが書き込み禁止になっている。
- 現在 1 つまたは複数のパーティションが使用されている。
- 現在 1 つまたは複数のパーティションが連結している。

vFlash のプロパティ

<Enter> を押すと、SD カードの以下のプロパティが表示されます。

- **名前** - サーバーの vFlash SD カードスロットに挿入されている vFlash SD カードの名前を表示します。それが Dell の SD カードであれば、vFlash SD カードと表示されます。Dell の SD カードでない場合は、SD カードと表示されます。
- **サイズ** - vFlash SD カードのサイズをギガバイト(GB)で表示します。
- **空き容量** - vFlash SD カードの空き容量をメガバイト(MB)で表示します。この空き容量を使用して、vFlash SD カードにさらにパーティションを作成できます。SD カードの場合、空き容量は 256MB と表示されます。
- **書き込み禁止** - vFlash SD カードが書き込み禁止かどうかを表示します。
- **正常性** - vFlash SD カード全体の正常性状態を表示します。次の状態があります。
  - 正常
  - 警告
  - 重要

<Esc> を押して終了します。

スマートカード / SSO

このオプションは、**スマートカードログオン** および **シングルサインオン** 機能を設定します。選択できるオプションは、**有効** と **無効** です。

メモ: **シングルサインオン** 機能を有効にすると、**スマートカードログオン** 機能は無効になります。

システムサービス

システムサービス

左右の方向キーを使用して **有効** または **無効** を選択します。有効にすると、一部の iDRAC6 機能を Lifecycle Controller から設定できます。詳細については、デルサポートサイト **support.dell.com / manuals** にある『Lifecycle Controller ユーザーガイド』を参照してください。

メモ: このオプションを変更すると、**保存** して **終了** した後、新しい設定を適用するために、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

上下の方向キー を使用して **はい** または **いいえ** を選択します。

はい を選択した場合は、Lifecycle Controller の全セッションが終了し、**保存** と **終了** を選択すると、新しい設定を適用するためにサーバーが再起動します。

再起動時のシステムインベントリの収集

起動中にインベントリを収集するには、**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 Lifecycle Controller ユーザーガイド』を参照してください。

メモ: このオプションを変更すると、設定を保存し、iDRAC6 設定ユーティリティを終了した後に、サーバーが再起動します。

LAN ユーザー設定

LAN ユーザーは iDRAC6 のシステム管理者アカウントで、デフォルトでは **ルート** です。LAN ユーザー設定のサブメニューを表示するには、Enter キーを押します。LAN ユーザーの設定を終えて <Esc> キーを押すと、前のメニューに戻ります。

表 18-2 LAN ユーザー設定画面

項目	説明
自動検出	自動検出機能は、ネットワークでプロビジョニングされていないシステムを自動的に検出します。さらに、初期資格情報をセキュアに確立して、これらの検出されたシステムを管理できるようにします。この機能を使用すると、iDRAC6 がプロビジョニングサーバーを見つけることができます。iDRAC6 とプロビジョニングサービスのサーバーは相互に認証します。リモートプロビジョニングサーバーはユーザーの資格情報を送信して、iDRAC6 にユーザーアカウントを作成させます。ユーザーアカウントが作成されると、リモートコンソールは、検出プロセスで指定された資格情報を使用して iDRAC6 と WSMAN 通信を確立し、オペレーティングシステムをリモート導入するためのセキュアな命令を iDRAC6 に送ります。 オペレーティングシステムのリモート導入の詳細については、デルサポートウェブサイト **support.dell.com / manuals** にある『Dell Lifecycle Controller ユーザーガイド』を参照してください。 自動検出を手動で有効にする前に、**iDRAC6 設定ユーティリティ** の別のセッションで、以下の操作を行ってください。 • NIC を有効にする(ブレードサーバー) • IPv4 を有効にする(ブレードサーバー) • DHCP を有効にする • DHCP からドメイン名を取得する • システム管理者アカウント(アカウント番号 2) を無効にする • DHCP から DNS サーバーアドレスを取得する • DHCP からドメイン名を取得する 自動検出機能を有効にするには、**有効** を選択します。このオプションはデフォルトで **無効** になっています。自動検出機能を **有効** にした Dell システムを注文した場合、Dell システムの iDRAC6 は リモートログインのデフォルトの資格情報なしで DHCP を有効にして出荷されます。
自動検出(続き...)	Dell システムをネットワークに追加して自動検出機能を使用する前に、以下を確認してください。 • Dynamic Host Configuration Protocol(DHCP)サーバー / ドメイン名システム(DNS)が設定されている。 • プロビジョニングウェブサービスがインストール、設定、登録されている。
プロビジョニングサーバー	このフィールドは、プロビジョニングサーバーを設定するのに使用します。プロビジョニングサーバーのアドレスは、IPv4 アドレスまたはホスト名の組み合わせにできます。アドレスは、255 文字を超えてはなりません。各アドレスまたはホスト名は、カンマで区切ります。 自動検出機能を有効にした場合、自動検出プロセスの完了後、将来のリモートプロビジョニングを可能にするために、設定されたプロビジョニングサーバーからユーザー資格情報が取得されます。 詳細については、デルサポートサイト **support.dell.com / manuals** にある『Dell Lifecycle Controller ユーザーガイド』を参照してください。
アカウントアクセス	**有効** を選択すると、システム管理者アカウントが有効になります。管理者アカウントを無効にする場合、または自動検出が有効になっている場合は、**無効** を選択します。
IPMI LAN 権限	**システム管理者**、**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	管理者アカウントの新しいパスワードを入力します。入力した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 **パスワードを入力する** フィールドに入力した文字と一致しない場合はメッセージが表示され、パスワードを再度入力する必要があります。

デフォルトに戻す

デフォルトに戻す メニュー項目を使用すると、iDRAC6 設定項目がすべて出荷時のデフォルトに戻されます。これは、システム管理者のユーザーパスワードを忘れた場合や iDRAC6 をデフォルト設定から再設定する場合に必要になる可能性があります。

メモ: iDRAC6 ネットワークはデフォルトで無効になっています。iDRAC6 設定ユーティリティで iDRAC6 ネットワークを有効にするまでは、ネットワーク上で iDRAC6 の設定を変更できません。

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

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

< NO (Cancel) > (<いいえ(キャンセル)...>)

< YES (Continue) > (<はい(続行)>)
```

iDRAC6 をデフォルトに戻すには、**はい** を選択して、Enter キーを押します。

この操作に失敗すると、次のエラーメッセージが表示されます。

- リセットコマンドの実行に失敗しました。後でもう一度行ってください。iDRAC はビジー状態です。
- 設定をデフォルト値に復元できませんでした。タイムアウトです。
- リセットコマンドを送信できません。後でもう一度行ってください。iDRAC はビジー状態です。

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 個のメッセージを保持します。

SEL メッセージを表示するには、**システムイベントログの表示** を選択して Enter キーを押します。移動方法:

- 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。

<Esc> キーを押すと、システムイベントログ が終了します。

メモ: iDRAC6 設定ユーティリティまたは iDRAC6 ウェブインタフェースでのみ SEL をクリアできます。

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

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

iDRAC6 設定ユーティリティの終了

iDRAC6 設定の変更を終えて <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 Enter キーを押すと、変更が維持されます。この操作に失敗すると、次のいずれかのメッセージが表示されます。
  - iDRAC6 Communication Failure-Displayed if iDRAC is not accessible. (iDRAC6 通信の失敗 - iDRAC にアクセスできない場合に表示されます。)
  - Some of the settings cannot be applied-Displayed when few settings cannot be applied. (一部の設定を適用できません - 設定のいくつかを適用できない場合に表示されます。)
- **変更を保存せずに終了** を選択して Enter キーを押すと、変更は保存されません。
- **セットアップへ戻る** を選択して Enter キーを押すと、iDRAC6 設定ユーティリティに戻ります。

目次ページに戻る

目次ページに戻る

管理下システムのリカバリとトラブルシューティング

Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers バージョン 3.0 ユーザーガイド

ここでは、iDRAC6 ユーティリティを使用して、リモート管理下システムの診断とトラブルシューティングに関連するタスクを実行する方法について説明します。以下のトピックが含まれています。

- 問題の兆候 - 問題の診断に導くメッセージやその他のシステムの問題の兆候を見つけるのに役立ちます。
- 不具合解決ツール - システムのトラブルシューティングに使用できる iDRAC6 ツールについて説明します。
- トラブルシューティングとよくあるお問い合わせ(FAQ) - 遭遇する可能性のある一般的な状況に対する回答を提供します。

ユーザーとシステムの安全優先

本項で説明する手順を実行するには、シャーシ、Dell PowerEdge システム、またはその他のハードウェアモジュールを操作する必要があります。このガイドおよびその他のシステムマニュアルで説明されている以外の方法でシステムハードウェアを修理しないでください。

△ **注意: 修理作業の多くは、認定されたサービス技術者のみが行うことができます。製品マニュアルで許可されている、もしくはオンライン / 電話によるサービスおよびサポートチームによって指示されたトラブルシューティングと簡単な修理のみを行ってください。デルで認められていない修理による損傷は、保証の対象となりません。製品に付属しているマニュアルの「安全にお使いいただくために」をお読みになり、指示に従ってください。**

問題の兆候

ここでは、システムに問題がある可能性を示す兆候について説明します。

LED インジケータ

シャーシまたはシャーシに実装されているコンポーネントの LED は、通常、システム上の問題の初期兆候を示します。次のコンポーネントおよびモジュールには状態 LED があります。

- シャーシ LCD モニタ
- サーバー
- ファン
- CMC
- I/O モジュール
- 電源ユニット

シャーシ LCD の単独 LED は、システムコンポーネント全体の状態を示します。LCD で青色の LED が点灯している場合は、システム内で検知されているエラー状態がないことを示します。LCD で黄色の LED が点滅している場合は、1 つまたは複数のエラー状態が検知されたことを示します。

シャーシ LCD で黄色の LED が点滅している場合は、LCD メニューを使用してエラーのあるコンポーネントを特定できます。LCD の使い方については、『Dell Chassis Management Controller ファームウェアユーザーガイド』を参照してください。

表 19-1 に、Dell PowerEdge システムの LED が表す意味を説明します。

表 19-1 ブレードサーバーの LED インジケータ

LED インジケータ	意味
緑色に点灯(電源ボタンのみ)	サーバーの電源が入っている状態です。緑色の LED が点灯していない場合は、サーバーの電源が入っていないことを示します。
青色に点灯	iDRAC6 は正常に動作しています。
黄色に点滅	iDRAC6 がエラー状態を検知したか、ファームウェアのアップデートを進行中である可能性があります。
青色に点滅	ユーザーがこのサーバーのロケータ ID をアクティブにした状態です。

ハードウェア問題の兆候

モジュールにハードウェアの不具合がある場合の兆候には、以下が含まれます。

- 電源が入らない

- ファンのノイズ
- ネットワーク接続の喪失
- バッテリー、温度、電圧、電源モニタのセンサー警告
- ハードドライブエラー
- USB メディアエラー
- 落下、浸水、その他の外部要因による物理的損傷

このような問題が発生した場合は、損傷を点検し、以下の方法で問題の解決を試みてください。

- モジュールを抜き差しして、再起動する
- モジュールをシャーシ内の別のベイに挿入する
- ハードドライブまたは USB キーを交換する
- 電源およびネットワークケーブルを再接続 / 交換する

これらの手順で問題が解決されない場合、『ハードウェアオーナーズマニュアル』で個々のハードウェアデバイスのトラブルシューティング情報を参照してください。

その他の問題の兆候

表 19-2 問題の兆候

チェック項目：	処置：
システム管理ソフトウェアからの警告メッセージ	システム管理ソフトウェアのマニュアルを参照してください。
システムイベントログのメッセージ	システムイベントログ（SEL）の確認 を参照してください。
起動時 POST コードのメッセージ	POST コードの確認 を参照してください。
前回クラッシュ画面のメッセージ	前回のシステムクラッシュ画面の表示 を参照してください。
LCD のサーバー状態画面の警告メッセージ	サーバー状態画面でのエラーメッセージの確認 を参照してください。
iDRAC6 ログのメッセージ	iDRAC6 ログの表示 を参照してください。

問題解決ツール

ここでは、システムの問題を診断する場合、特にリモートで問題解決を試みる場合に役立つ iDRAC6 ユーティリティについて説明します。

- システム正常性の確認
- エラーメッセージに対するシステムイベントログの確認
- POST コードの確認
- 前回クラッシュ画面の表示
- 最近の起動順序の表示
- LCD 上のサーバー状態画面のエラーメッセージを確認
- iDRAC6 ログの表示
- システム情報の表示
- シャーシ内の管理下サーバーの識別
- 診断コンソールの使用
- リモートシステムの電源管理

システム正常性の確認

iDRAC6 ウェブインタフェースにログインすると、**システム概要** 画面にシステムコンポーネントの正常性の状態が示されます。表 19-3 に、システム正常性インジケータの意味を示します。

表 19-3 サーバー正常性のインジケータ

インジケータ	説明
	緑のチェックマークは、正常（通常）状態を示します。
	感嘆符の入った黄色の三角形は、警告（非重要）状態を示します。

	赤い X は、重要（エラー）状態を示します。
	疑問符のアイコンは、不明な状態を示します。

サーバーの正常性 画面上のコンポーネントをクリックすると、そのコンポーネントに関する情報が表示されます。バッテリー、温度、電圧、電源モニタに対してはセンサーの読み取り値が表示されます。不具合の診断に役立ててください。iDRAC6 と CMC の情報画面には、現在の状態と設定に関する情報が表示されます。

システムイベントログ（SEL）の確認

SEL ログ 画面には、管理下サーバーで発生したイベントのメッセージが表示されます。

システムイベントログ を表示するには、次の手順を実行してください。

1. **システム** をクリックし、**ログ** タブをクリックします。
2. **システムイベントログ** をクリックして **システムイベントログ** 画面を表示します。

   システムイベントログ 画面には、システム正常性インジケータ（「表 19-3」を参照）、タイムスタンプ、イベントの説明が表示されます。
3. 適切な **システムイベントログ** ボタンをクリックして続行します（「表 19-4」を参照）。

表 19-4 SEL ボタン

ボタン	操作
印刷	**ウィンドウでの表示順に SEL を**印刷します。
ログのクリア	**SEL** をクリアします。 **メモ: ログのクリア** ボタンは、**ログのクリア** 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、選択したディレクトリに **SEL** を保存できます。 **メモ:** Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト **support.microsoft.com** から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。 **メモ:** Internet Explorer を使用しているとき、**名前を付けて保存** を使用して SEL のログを保存できない場合は、ブラウザの設定が原因の可能性があります。この問題を解決するには： 1. Internet Explorer で、**ツール**→ **インターネット オプション** → **セキュリティ** の順に選択し、ダウンロードするゾーンを選択します。たとえば、iDRAC デバイスがローカルイントラネット上にある場合は、**ローカル イントラネット** を選択して **レベルのカスタマイズ**... をクリックします。 2. **セキュリティ設定** ウィンドウの **ダウンロード** で、次のオプションが有効になっていることを確認します。 ○ ファイルのダウンロード時に自動的にダイアログを表示 ○ ファイルのダウンロード **注意: iDRAC へのアクセスに使用されるコンピュータの安全を確保するために、その他 で アプリケーションと安全でないファイルの起動 オプションを有効以外にする必要があります。**
更新	**SEL** 画面を再ロードします。

POST コードの確認

POST コード 画面には、オペレーティングシステムの起動前の最後のシステム POST コードが表示されます。POST コードはシステム BIOS から返される進行状況を示すコードで、電源オンリセットからの起動順序の異なる段階を示し、システム起動に関するあらゆるエラーを診断できます。

メモ: LCD モニタまたは『ハードウェアオーナーズマニュアル』の POST コードメッセージ番号の説明文を参照してください。

POST コードを表示するには、次の手順を実行してください。

1. **システム**、**ログ** タブ、**POST コード** の順にクリックします。

   POST コード 画面には、システム正常性のインジケータ（「表 19-3」を参照）、16 進コード、コードの説明が表示されます。
2. 適切な **POST コード** ボタンをクリックして続行します（「表 19-5」を参照）。

表 19-5 POST コードのボタン

ボタン	操作
印刷	**POST コード 画面**を印刷します。
更新	**POST コード 画面**を再ロードします。

前回のシステムクラッシュ画面の表示

メモ: 前回クラッシュ画面機能は Server Administrator と iDRAC6 ウェブインタフェースで設定する必要があります。この機能を設定する手順については、「管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定」を参照してください。

前回のクラッシュ画面 には、システムクラッシュ前に発生したイベントに関する情報を含む最新クラッシュ画面が表示されます。最後にシステムがクラッシュしたときのイメージは、iDRAC6 の持続的なストアに保存され、リモートからアクセスできます。

前回クラッシュ画面 を表示するには、次の手順を実行してください。

- **システム、ログ** タブ、**前回クラッシュ画面** の順にクリックします。

前回クラッシュ画面 には、表 19-6 に示すボタンが表示されます。

メモ: 保存されているクラッシュ画面がない場合、**保存** と **削除** ボタンは表示されません。

表 19-6 前回のクラッシュ画面のボタン

ボタン	操作
印刷	**前回のクラッシュ画面** を印刷します。
保存	ポップアップウィンドウが開き、選択したディレクトリに **前回クラッシュ画面** を保存できます。
削除	**前回のクラッシュ画面** を削除します。
更新	**前回のクラッシュ画面** を再ロードします。

メモ: 自動リカバリタイマーの変動により、システムリセットタイマーの値が高すぎる値で設定されている場合は、**前回クラッシュ画面** をキャプチャできない可能性があります。デフォルト設定は 480 秒です。Server Administrator または IT Assistant でシステムリセットタイマーを 60 秒に設定して、**前回クラッシュ画面** が正しく機能することを確認します。詳細については、「管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定」を参照してください。

最も最近の起動順序の表示

起動に問題がある場合は、**起動キャプチャ** 画面で最後の 3 回の起動順序時に発生した画面アクティビティを表示できます。起動画面の再生は、1 フレーム / 秒の速度で実行されます。iDRAC6 は起動時に 50 フレームを記録します。

表 19-7 に、使用可能な制御操作を示します。

メモ: 再生された起動キャプチャ順序を表示するには、Administrator 権限が必要です。

表 19-7 起動キャプチャオプション

ボタン / オプション	説明
起動順序の選択	ロードして再生する起動順序を選択できます。 - 起動キャプチャ 1 - 最も最近の起動順序をロードします。 - 起動キャプチャ 2 - 起動キャプチャ 1 の前に起きた、2 番目に最近の起動順序をロードします。 - 起動キャプチャ 3 - 起動キャプチャ 2 の前に起きた、3 番目に最近の起動順序をロードします。
名前を付けて保存	現在のシーケンスのすべての起動キャプチャイメージを含む圧縮 .zip ファイルを作成します。この操作を実行するには、Administrator 権限が必要です。
前の画面	再生コンソールに前の画面がある場合は、それを表示します。
再生	再生コンソールの現在の画面からスクリーンプレイを開始します。
一時停止	再生コンソールに表示されている現在の画面でスクリーンプレイを一時停止します。
停止	スクリーンプレイを停止して、起動順序の最初の画面をロードします。
次の画面	再生コンソールに次の画面がある場合は、それを表示します。
印刷	画面に表示されている起動キャプチャイメージを印刷します。
更新	起動キャプチャ画面を再ロードします。

サーバー状態画面でのエラーメッセージの確認

LED が黄色に点滅し、特定のサーバーにエラーが発生している場合、LCD 上のメインサーバー状態画面にエラーが発生したサーバーが橙色で強調表示されます。LCD ナビゲーションボタンを使用して、エラーが発生したサーバーを強調表示し、中央のボタンをクリックします。2 行目にエラーおよび警告メッセージが表示されます。下記の表には、すべてのエラーメッセージと各エラーの重要度が示されています。

表 19-8 サーバー状態画面

重要度	メッセージ	原因
警告	System Board Ambient Temp: Temperature sensor for System Board, warningevent (システム基板の周辺温度: システム基板の温度センサー、警告イベント)	サーバー周辺温度が警告しきい値を超えました。
重要	System Board Ambient Temp: Temperature sensor for System Board, failure event (システム基板の周辺温度: システム基板の温度センサー、エラーイベント)	サーバー周辺温度がエラーしきい値を超えました。
重要	System Board CMOS Battery: Battery sensor for System Board, failed wasasserted (システム基板の CMOS バッテリー: システム基板のバッテリーセンサー、エラーがアサートされました。)	CMOS バッテリーがないか、電圧がありません。
警告	System Board System Level: Current sensor for System Board, warning event (システム基板のシステムレベル: システム基板の電流センサー、警告イベント)	電流 が警告しきい値を超えました。
重要	System Board System Level: Current sensor for System Board, failure event (システム基板のシステムレベル: システム基板の電流センサー、エラーイベント)	電流 がエラーしきい値を超えました。
重要	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU <番号> <電圧センサー名>: CPU <番号> の電圧センサー、状態アサートがアサートされました。)	電圧が許容範囲を超えています。
重要	System Board <voltage sensor name>: Voltage sensor for System Board, state asserted was asserted (システム基板 <電圧センサー名>: システム基板の電圧センサー、状態アサートがアサートされました。)	電圧が許容範囲を超えています。
重要	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU <番号> <電圧センサー名>: CPU <番号> の電圧センサー、状態アサートがアサートされました。)	電圧が許容範囲を超えています。
重要	CPU<number> Status: Processor sensor for CPU<number, IERR was asserted (CPU <番号> 状態: CPU <番号> のプロセッサセンサー、IERR がアサートされました。)	CPU エラー
重要	CPU<number> Status: Processor sensor for CPU<number>, thermal tripped was asserted (CPU <番号> 状態: CPU <番号> のプロセッサセンサー、IERR がアサートされました。)	CPU が過熱状態
重要	CPU<number> Status: Processor sensor for CPU<number, configuration error was asserted (CPU <番号> 状態: CPU <番号> のプロセッサセンサー、IERR がアサートされました。)	不正なプロセッサタイプまたは間違った位置に取り付けられています。
重要	CPU<number> Status: Processor sensor for CPU<number>, presence was deasserted (CPU <番号> 状態: CPU <番号> のプロセッサセンサー、IERR がアサートされました。)	必要な CPU が見つからないか、ありません。
重要I	System Board Video Riser: Module sensor for System Board, device removed was asserted (システム基板ビデオライザー: システム基板のモジュールセンサー、デバイスの取り外しがアサートされました。)	必要なモジュールが取り外されました。
重要	Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted (メザニン B <スロット番号> 状態: メザニン B <スロット番号> のアドインカードセンサー、インストールエラーがアサートされました。)	IO ファブリックに間違ったメザニンカードが取り付けられています。
重要	Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted (メザニン B <スロット番号> 状態: メザニン B <スロット番号> のアドインカードセンサー、インストールエラーがアサートされました。)	I/O ファブリックに間違ったメザニンカードが取り付けられています。
重要	Backplane Drive <number>: Drive Slot sensor for Backplane, drive removed (バックプレーンドライブ <番号>: バックプレーンのドライブスロットセンサー、ドライブが取り外されました。)	ストレージドライブが取り外されました。
重要	Backplane Drive <number>: Drive Slot sensor for Backplane, drive fault was asserted (バックプレーンドライブ <番号>: バックプレーンのドライブスロットセンサー、ドライブ障害がアサートされました。)	ストレージドライブに障害が発生しました。
重要	System Board PFault Fail Safe: Voltage sensor for System Board, state asserted was asserted (システム基板 PFault フェールセーフ: システム基板の電圧センサー、状態アサートがアサートされました。)	システム基板の電圧が異常レベルに達した場合に、このイベントが生成されます。
重要	System Board OS Watchdog: Watchdog sensor for System Board, timer expired was asserted (システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、タイマー期限切れがアサートされました。)	iDRAC6 ウォッチドッグタイマーが期限切れで、処置が設定されていません。
重要	System Board OS Watchdog: Watchdog sensor for System Board, reboot was asserted (システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、再起動がアサートされました。)	iDRAC6 ウォッチドッグがシステムのクラッシュ(ホストからの応答がないためのタイマー期限切れ)を検知し、再起動の処置が設定されています。
重要	System Board OS Watchdog: Watchdog sensor for System Board, power off was asserted (システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、電源オフがアサートされました。)	iDRAC6 ウォッチドッグがシステムのクラッシュ(ホストからの応答がないためのタイマー期限切れ)を検知し、電源を切る処置が設定されています。
重要	System Board OS Watchdog: Watchdog sensor for System Board, power cycle was asserted (システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、電源の入れ直しがアサートされました。)	iDRAC6 ウォッチドッグがシステムのクラッシュ(ホストからの応答がないためのタイマー期限切れ)を検知し、電源の入れ直しが設定されています。
重要	System Board SEL: Event Log sensor for System Board, log full was asserted (システム基板 SEL: システム基板のイベントログセンサー、ログがいっぱいであることがアサートされました。)	SEL デバイスは、SEL がいっぱいになる前に 1 つしかエントリを追加できないことを検出しました。
警告	ECC Corr Err: Memory sensor, correctable ECC (<DIMM Location>) was asserted (ECC 修正可能エラー: メモリセンサー、訂正可能な ECC (<DIMM の位置>)がアサートされました。)	訂正可能 ECC エラー数が重要レートに達しました。
重要	ECC Uncorr Err: Memory sensor, uncorrectable ECC(<DIMM Location>) was asserted (ECC 訂正不能エラー: メモリセンサー、訂正不可 ECC (<DIMM の位置>)がアサートされました。)	訂正不可 ECC エラーが検知されました。
重要	I/O Channel Chk: Critical Event sensor, I/O channel check NMI was asserted (I/O チャネルチェック: 重要なイベントセンサー、I/O チャネルチェック NMI がアサートされました。)	I/O チャネルに重要な割り込みが発生しています。
重要	PCI Parity Err: Critical Event sensor, PCI PERR was asserted (PCI パリティエラー: 重要なイベントセンサー、PCI PERR がアサートされました。)	PCI バスにパリティエラーが検知されました。
Critical	PCI System Err: Critical Event sensor, PCI SERR (PCI システムエラー: 重大イベントセンサー、PCI SERR) (<Slot number or PCI Device ID>) was asserted ((<スロット番号または PCI デバイス ID>)がアサートされました。)	デバイスにより、PCI エラーが検知されました。
重要	SBE Log Disabled: Event Log sensor, correctable memory error logging disabled was asserted (SBE ロ	ログされるシングルビットエラーの数が多すぎると、シン

	グ無効: イベントログセンサー、訂正可能なメモリエラーのログ無効がアサートされました。)	グルビットエラーのログは無効になります。
重要	Logging Disabled: Event Log sensor, all event logging disabled was asserted (ログ無効: イベントログセンサー、すべてのイベントログ無効がアサートされました。)	すべてのエラーログは無効になります。
リカバリ不可	CPU Protocol Err: Processorsensor, transition to non-recoverable was asserted (CPU プロトコルエラー: プロセッサセンサー、リカバリ不可への状態移行がアサートされました。)	プロセッサプロトコルがリカバリ不可の状態になりました。
リカバリ不可	CPU Bus PERR: Processor sensor, transition to non-recoverable wasasserted (CPU プロトコルエラー: プロセッサセンサー、リカバリ不可への状態移行がアサートされました。)	プロセッサバス PERR がリカバリ不可の状態になりました。
リカバリ不可	CPU Init Err: Processor sensor, transition to non-recoverable wasasserted (CPU プロトコルエラー: プロセッサセンサー、リカバリ不可への状態移行がアサートされました。)	プロセッサ初期化がリカバリ不可の状態になりました。
リカバリ不可	CPU Machine Chk: Processor sensor, transition to non-recoverable was asserted (CPU プロトコルエラー: プロセッサセンサー、リカバリ不可への状態移行がアサートされました。)	プロセッサマシンチェックがリカバリ不可の状態になりました。
重要	Memory Spared: Memory sensor, redundancy lost (メモリスペア: メモリセンサー、冗長性喪失) (<DIMM Location>) was asserted ((<DIMM の位置>)がアサートされました。)	メモリスペアの冗長性が無くなりました。
重要	Memory Mirrored: Memory sensor, redundancy lost (メモリミラー: メモリセンサー、冗長性喪失) (<DIMM Location>) was asserted ((<DIMM の位置>)がアサートされました。)	メモリミラーの冗長性が無くなりました。
重要	Memory RAID: Memory sensor, redundancy lost (メモリ RAID: メモリセンサー、冗長性喪失) (<DIMM Location>) was asserted ((<DIMM の位置>)がアサートされました。)	RAID メモリの冗長性が無くなりました。
警告	Memory Added: Memory sensor, presence (<DIMM Location>) was deasserted (メモリ追加: メモリセンサー、メモリの存在(<DIMM の位置>)がアサート解除されました。)	増設されたメモリモジュールが取り外されました。
警告	Memory Removed: Memory sensor, presence (<DIMM Location>) was deasserted (メモリ除去: メモリセンサー、メモリの存在(<DIMM の位置>)がアサート解除されました。)	メモリモジュールが取り外されました。
重要	Memory Cfg Err: Memory sensor, configuration error (メモリ構成エラー: メモリセンサー、構成エラー) (<DIMM Location>) was asserted (<DIMM の位置>)がアサートされました。)	システムのメモリ構成が正しくありません。
警告	Mem Redun Gain: Memory sensor, redundancy degraded (メモリ冗長性低下: メモリセンサー、冗長性低下) (<DIMM Location>) was asserted ((<DIMM の位置>)がアサートされました。)	メモリの冗長性は低下しましたが、喪失されていません。
重要	PCIE Fatal Err: Critical Event sensor, bus fatal error was asserted (PCIE 致命的エラー: 重要なイベントセンサー、バスの致命的エラーがアサートされました。)	PCIE バスに致命的なエラーが検知されました。
重要	Chipset Err: Critical Event sensor, PCI PERR was asserted (チップセットエラー: 致命的なイベントセンサー、PCI PERR がアサートされました。)	チップエラーが検出されました。
警告	Mem ECC Warning: Memory sensor, transition to non-critical from OK (<DIMM Location>) was asserted (メモリ ECC 警告: メモリセンサー、OK から 非重要 (<DIMM の場所>)への状態移行がアサートされました。)	訂正可能な ECC エラー率が通常率より増加しました。
重要	Mem ECC Warning: Memory sensor, transition to critical from less severe (<DIMM Location>) was asserted (メモリ ECC 警告: メモリセンサー、OK から 非重要 (<DIMM の場所>)への状態移行がアサートされました。)	訂正可能な ECC エラー率が重要な率に達しました。
重要	POST Err: POST sensor, No memory installed (POST エラー: POST センサー、メモリ非搭載)	システム基板にメモリが搭載されていません。
重要	POST Err: POST sensor, Memory configuration error (POST エラー: POST センサー、メモリ構成エラー)	メモリが検出されましたが、構成不能です。
重要	POST Err: POST sensor, Unusable memory error (POST エラー: POST センサー、使用不可メモリエラー)	メモリが構成されましたが、使用できません。
重要	POST Err: POST sensor, Shadow BIOS failed (POST エラー: POST センサー、シャドウ BIOS にエラーが発生しました。)	システム BIOS シャドウの障害
重要	POST Err: POST sensor, CMOS failed (POST エラー: POST センサー、CMOS にエラーが発生しました。)	CMOS の障害
重要	POST Err: POST sensor, DMA controller failed (POST エラー: POST センサー、DMA コントローラにエラーが発生しました。)	DMA コントローラの障害
重要	POST Err: POST sensor, Interrupt controller failed (POST エラー: POST センサー、割り込み信号コントローラにエラーが発生しました。)	割り込み信号コントローラの障害
重要	POST Err: POST sensor, Timer refresh failed (POST エラー: POST センサー、タイマー更新に失敗しました。)	タイマー更新エラー
重要	POST Err: POST sensor, Programmable interval timer error (POST エラー: POST センサー、設定可能インターバルタイマーエラー)	設定可能インターバルタイマーのエラー
重要	POST Err: POST sensor, Parity error (POST エラー: POST センサー、パリティエラー)	パリティエラー
重要	POST Err: POST sensor, SIO failed (POST エラー: POST センサー、SIO にエラーが発生しました。)	SIO の障害
重要	POST Err: POST sensor, Keyboard controller failed (POST エラー: POST センサー、キーボードコントローラにエラーが発生しました。)	キーボードコントローラの障害
重要	POST Err: POST sensor, System management interrupt initialization failed (POST エラー: POST センサー、システム管理割り込みの初期化に失敗しました。)	SMI(システム管理割り込み)の初期化エラー。
重要	POST Err: POST sensor, BIOS shutdown test failed (POST エラー: POST センサー、BIOS シャットダウンテストに失敗しました。)	BIOS シャットダウンテストエラー
重要	POST Err: POST sensor, BIOS POST memory test failed (POST エラー: POST センサー、BIOS POST メモリテストに失敗しました。)	BIOS POST メモリテストエラー
重要	POST Err: POST sensor, Dell remote access controller configuration failed (POST エラー: POST センサー、Dell リモートアクセスコントローラの設定に失敗しました。)	DRAC(Dell Remote Access Controller)の設定エラー
重要	POST Err: POST sensor, CPU configuration failed (POST エラー: POST センサー、CPU 設定に失敗しました。)	CPU 設定エラー
重要	POST Err: POST sensor, Incorrect memory configuration (POST エラー: POST センサー、不正メモリ設定エラー。)	メモリ設定が正しくありません。
重要	POST Err: POST sensor, POST failure (POST エラー: POST センサー、POST にエラーが発生しました。)	ビデオ初期化後の一般エラー
重要	Hdwar version err: Version Change sensor, hardware incompatibility was asserted (ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性がアサートされました。)	互換性のないハードウェアが検知されました。
重要	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware) was asserted (ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性(BMC ファームウェア)がアサートされました。)	ハードウェアはファームウェアとの互換性がありません。
重要	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware and CPU mismatch) was asserted (ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性(BMC ファ	CPU はファームウェアとの互換性がありません。

	ームウェアと CPU の不一致）がアサートされました。）	
重要	Mem Overtemp: Memory sensor, correctable ECC <DIMM Location> was asserted (メモリ過熱: メモリセンサー、訂正可能な ECC <DIMM の位置> がアサートされました。)	メモリモジュールの過熱
重要	Mem Fatal SB CRC: Memory sensor, uncorrectable ECC was asserted (メモリ致命的 SB CRC: メモリセンサー、訂正不可の ECC がアサートされました。)	South Bridge メモリ障害
重要	Mem Fatal NB CRC: Memory sensor, uncorrectable ECC was asserted (メモリ致命的 NB CRC: メモリセンサー、訂正不可の ECC がアサートされました。)	North Bridge メモリ障害
重要	WatchDog Timer: Watchdog sensor, reboot was asserted (ウォッチドッグタイマー: ウォッチドッグセンサー、再起動がアサートされました。)	ウォッチドッグタイマーがシステムを再起動させました。
重要	WatchDog Timer: Watchdog sensor, timer expired was asserted (ウォッチドッグタイマー: ウォッチドッグ センサー、タイマー期限切れがアサートされました。)	ウォッチドッグタイマーが期限切れになりましたが、処置されていません。
警告	Link Tuning: Version Change sensor, successful software or F/W change was deasserted (リンクチューニング: バージョン変更センサー、ソフトウェアまたは ファームウェアの変更がアサート解除されました。)	正常な NIC 操作を可能にするリンクチューニング設定のアップデートに失敗しました。
警告	Link Tuning: Version Change sensor, successful hardware change <device slot number> was deasserted (リンクチューニング: バージョン変更センサー、ハードウェアの変更 <デバイスのスロット番号> がアサート解除されました。)	正常な NIC 操作を可能にするリンクチューニング設定のアップデートに失敗しました。
重要	LinkT/FlexAddr: Link Tuning sensor, failed to program virtual MAC address (Bus # Device # Function #) was asserted (リンクチューニング/フレックスアドレス: リンクチューニングセンサー、仮想 MAC アドレス（バス # デバイス # 機能 #）の設定の失敗がアサートされました。)	このデバイスでは、フレックスアドレスを設定できません。
重要	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz <location>) wasasserted (リンクチューニング / フレックスアドレス: リンクチューニングセンサー、デバイスオプション ROM によるリンクチューニングまたはフレックスアドレス（メザニン <位置>）のサポートの失敗がアサートされました。)	オプション ROM がフレックスアドレスまたはリンクチューニングをサポートしていません。
重要	LinkT/FlexAddr: Link Tuning sensor, failed to get link tuning or flex address data from BMC/iDRAC6 was asserted (リンクチューニング / フレックスアドレス: リンクチューニングセンサー、BMC/iDRAC6 からのリンクチューニングまたはフレックスアドレスデータの取得の失敗がアサートされました。)	BMC/iDRAC6 からリンクチューニングまたはフレックスアドレス情報の取得に失敗しました。
重要	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or FlexAddress (Mezz XX) was asserted (リンクチューニング / フレックスアドレス: リンクチューニングセンサー、デバイスオプション ROM によるリンクチューニングまたはフレックスアドレス（メザニン XX）のサポートの失敗がアサートされました。)	このイベントは、NIC 用の PCI デバイスオプション ROM がリンクチューニングまたはフレックスアドレス設定機能をサポートしない場合に生成されます。
重要	LinkT/FlexAddr: Link Tuning sensor, failed to program the virtual MAC address (<location>) was asserted (リンクチューニング / フレックスアドレス: リンクチューニングセンサー、仮想 MAC アドレス（<場所>）の設定の失敗がアサートされました。)	このイベントは、指定された NIC デバイスの仮想 MAC アドレスの設定に BIOS が 失敗した場合に生成されます。
重要	I/O Fatal Err: Fatal IO Group sensor, fatal IO error (<location>) (I/O 致命的エラー: 致命的 IO グループセンサー、致命的 IO エラー（<場所>))	このイベントは、CPU IERR に関連して生成され、CPU IERR の原因となったデバイスを示します。
警告	PCIE NonFatal Er: Non Fatal I/O Group sensor, PCIe error (<location>) (PCIE 非致命的エラー: 非致命的な I/O グループセンサー、PCIe エラー（<場所>))	このイベントは CPU IERR に関連して生成されます。

iDRAC6 ログの表示

iDRAC6 **ログ** は持続的なログで、iDRAC6 ファームウェアで管理されています。ログにはユーザーの処置（ログイン、ログアウト、セキュリティポリシーの変更など）と iDRAC6 が発行する警告のリストが含まれています。ログは iDRAC6 ファームウェアのアップデート後に消去されます。

システムイベントログ（SEL）には管理下サーバーで発生したイベントのレコードが保存され、**iDRAC6 ログ** には iDRAC6 で発生したイベントのレコードが保存されます。

iDRAC6 **ログ**にアクセスするには、以下の手順を実行してください。

- **システム** → **リモートアクセス** →**iDRAC6** → **ログ** の順にクリックします。**iDRAC6 ログ** 画面が表示されます。この画面には「表 19-9」に一覧表示されている情報が表示されます。

表 19-9 iDRAC6 ログ情報

フィールド	説明
日時	日時（12 月 19 日 16:55:47 など）。 iDRAC6 のクロックは、iDRAC6 の初期化時に管理下サーバーのクロックから設定されます。iDRAC6 が起動したときに管理下サーバーがオフになっていると、ブレードがあるシャーシの CMC から iDRAC6 のクロックが設定されます。 **メモ:** iDRAC6 の時刻の情報源は、iDRAC6 初期化時の管理下サーバーの電源状況によって異なるので、管理下サーバーの時刻を CMC の時刻と同じに設定しておく必要があります。システムと CMC の時刻が一致しないと、iDRAC の初期化イベントの後、iDRAC6 のログに矛盾した時刻が報告される可能性があります。
ソース	イベントを引き起こしたインタフェース
説明	イベントの短い説明と iDRAC6 にログインしたユーザー名。

iDRAC6 ログボタンの使用

iDRAC6 **ログ** 画面には以下のボタンがあります（「表 19-10」を参照）。

表 19-10 iDRAC6 ログボタン

ボタン	操作
印刷	iDRAC6 **ログ** 画面を印刷します。
ログのクリア	iDRAC6 **ログ** のエントリをクリアします。 **メモ:** **ログのクリア** ボタンは、**ログのクリア** 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウを開き、選択したディレクトリに iDRAC6 の **ログ** を保存できます。 **メモ:** Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト **support.microsoft.com** から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。
更新	iDRAC6 **ログ** 画面を再ロードします。

システム情報の表示

システム詳細 画面には、次のシステムコンポーネントに関する情報が表示されます。

- メインシステムエンクロージャ
- Integrated Dell Remote Access Controller 6(iDRAC6)-Enterprise

システム情報にアクセスするには、**システム** → **プロパティ**→**システム詳細** の順にクリックします。

システム概要、メインシステムエンクロージャ、および iDRAC6 の詳細については、「管理下システムのリカバリとトラブルシューティング 」を参照してください。

シャーシ内の管理下サーバーの識別

Dell PowerEdge M1000e シャーシには、最大 16 台のサーバーを収容できます。シャーシ内の特定のサーバーを見つけるには、iDRAC6 ウェブインタフェースを使用してサーバーの青色の点滅 LED をオンにします。LED をオンにする際、LED が点滅している間にシャーシに到達できるように LED を点滅させる秒数を指定できます。**0** を入力すると、LED は無効にするまで点滅し続けます。

サーバーを識別するには、次の手順に従ってください。

1. **システム** → **リモートアクセス** →**iDRAC6** → **トラブルシューティング** の順にクリックします。
2. **識別** 画面で **サーバーの識別** を選択します。
3. **サーバータイムアウトの識別** フィールドに、LED を点滅させる秒数を入力します。無効にするまで点滅させる場合は **0** を入力します。
4. **適用** をクリックします。

サーバー上の青色の LED が指定した秒数ほど点滅します。

0 を入力して LED を点滅させ続ける場合は、次の手順を実行してこれを無効にできます。

1. **システム** → **リモートアクセス** →**iDRAC6** → **トラブルシューティング** の順にクリックします。
2. **識別** 画面で **サーバーの識別** を選択解除します。
3. **適用** をクリックします。

診断コンソールの使用

iDRAC6 には、Microsoft Windows または Linux ベースのシステムのツールに類似したネットワーク診断ツールが標準装備されています(「表 19-11」を参照)。iDRAC6 ウェブインタフェースを使用して、ネットワークのデバッグツールにアクセスできます。

iDRAC をリセットするには、**iDRAC6 のリセット** をクリックします。iDRAC で通常の起動処理が実行されます。

診断コンソール 画面にアクセスするには、次の手順を実行してください。

1. **システム** → **iDRAC6** → **トラブルシューティング** の順にクリックします。
2. **診断コンソール** タブを選択します。

表 19-11 に、**診断コンソール** 画面に入力できるコマンドを示します。コマンドを入力して **送信** をクリックします。デバッグの結果が **診断コンソール** 画面に表示されます。

クリア ボタンをクリックして、前のコマンドで表示した結果をクリアします。

診断コンソール 画面を更新するには、**更新** をクリックします。

表 19-11 診断コマンド

コマンド	説明
arp	ARP(Address Resolution Protocol)テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を印刷します。
ping <IP アドレス>	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。宛先 IP アドレスをこのオプションの右側のフィールドに入力してください。現在のルーティングテーブルの内容に基づいて、ICMP(インターネットコントロールメッセージプロトコル)エコーパケットが宛先 IP アドレスに送信されます。
ping6 <IPv6 アドレス>	送信先の IPv6 アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。送信先の IPv6 アドレスをこのオプションの右側のフィールドに入力する必要があります。ICMP(インターネットコントロールメッセージプロトコル)エコーパケットは、現在のルーティングテーブルの内容に基づいて宛先の IPv6 アドレスに送信されます。
traceroute <**IP アドレス**>	IP ネットワークでパケットが通る経路を調べるために使用します。
traceroute6 <**IPv6 アドレス**>	IPv6 ネットワークでパケットが通る経路を調べるために使用します。
gettracelog	iDRAC6 トレースログ を表示します。詳細については、デルサポートサイト **support.dell.com / manuals** で『iDRAC6 管理者リファレンスガイド』の「gettracelog 」を参照してください。

リモートシステム の電源管理

iDRAC6 では、管理下サーバーの電源管理操作をリモートで実行できます。再起動時と電源の投入および切断時に、オペレーティングシステムからシャットダウンを正しく実行するには、**電源管理** 画面を使用します。

メモ: 電源管理処置を実行するには、**サーバー処置コマンドの実行** 権限が必要です。ユーザー権限の設定方法については、「iDRAC6 ユーザーの追加と設定」を参照してください。

1. **システム** をクリックし、**電源管理** → **電源制御** タブをクリックします。
2. **電源制御処置** を選択します(例:**システムをリセットする(ウォームブート)**)。

   表 19-12 に、電源制御操作について説明します。
3. 選択した操作を実行するには、**適用** をクリックします。

表 19-12 電源制御操作

システムの電源を入れる	システムの電源をオンにします(システムの電源がオフのときに電源ボタンを押すのと同じ)。
システムの電源を切る	システムの電源をオフにします(システムの電源がオンのときに電源ボタンを押すのと同じ)。
NMI(Non-Masking Interrupt)	オペレーティングシステムに高レベルの割り込みを送信し、重要な診断またはトラブルシューティング動作を可能にするためにシステム動作を一時停止させます。
正常なシャットダウン	オペレーティングシステムを正常にシャットダウンし、システムの電源を切ります。これには、システムによる電源管理を可能にする ACPI(Advanced Configuration and Power Interface)対応のオペレーティングシステムが必要です。 **メモ:** サーバーソフトウェアが応答しなくなった場合やシステム管理者として Windows のローカルコンソールにログインしていない場合は、オペレーティングシステムの正常なシャットダウンができないことがあります。そのような場合には、Windows の正常なシャットダウンではなく強制再起動を指定する必要があります。また、Windows OS のバージョンによっては、iDRAC6 からトリガされた場合にシャットダウンの動作を変更するポリシーがシャットダウンプロセスの周囲に設定されている場合があります。Microsoft のマニュアルで、ローカルコンピュータポリシー「シャットダウン:ログインなしでシステムのシャットダウンを許可する」を参照してください。
システムをリセットする(ウォームブート)	電源を切らずにシステムを再起動します(ウォームブート)。
システムの電源を入れ直す(コールドブート)	電源を切ってからシステムを再起動します(コールドブート)。

詳細については、電源モニタおよび電源管理を参照してください。

トラブルシューティングとよくあるお問い合わせ(FAQ)

表 19-13 に、トラブルシューティングについてよくあるお問い合わせ(FAQ)を掲載します。

表 19-13 トラブルシューティングとよくあるお問い合わせ(FAQ)

質問	回答
サーバー上の LED が黄色で点滅中です。	SEL でメッセージを確認し、SEL をクリアすると、LED の点滅が停止します。 iDRAC6 ウェブインタフェースを使用する場合: • 「システムイベントログ(SEL)の確認」を参照してください。 SM-CLP を使用する場合: • SEL 管理 を参照してください。 iDRAC6 設定ユーティリティを使用する場合: • システムイベントログメニュー を参照してください。
サーバー上で青色の LED が点滅しています。	ユーザーがサーバーのロケータ ID をアクティブにした状態です。シャーシ内のサーバーを識別するのに役立つ信号です。この機能については、「シャーシ内の管理下サーバーの識別」を参照してください。
iDRAC6 の IP アドレスはどのようにして検索しますか。	**CMC ウェブインタフェースを使用する場合:** 1. **シャーシ** → **サーバー** の順にクリックし、**セットアップ** タブをクリックします。 2. **導入** をクリックします。 3. 表示されるテーブルからサーバーの IP アドレスを読み取ります。 **仮想コンソールから以下の操作を行います。** • サーバーを再起動し、<Ctrl><E> キーを押して **iDRAC6 設定ユーティリティ** を開始します。 • BIOS POST 中に表示される IP アドレスを確認します。 • OSCAR の「Dell CMC」コンソールを選択してローカルシリアル接続経由で CMC にログインします。CMC RACADM コマンドはこの接続から発行できます。全 CMC RACADM サブコマンドのリストは、『Dell Chassis Management Controller システム管理者リファレンスガイド』を参照してください。 • iDRAC6 の IP アドレスを表示するには、ローカル RACADM **getsysinfo** コマンドを使用します。

	たとえば、次のとおりです。
	
	`$ racadm getniccfg -m server-1`
	
	`DHCP Enabled = 1`
	`IP Address = 192.168.0.1`
	`Subnet Mask = 255.255.255.0`
	`Gateway = 192.168.0.1`
	
	ローカル RACADM を使用する場合:
	
	コマンドプロンプトで次のコマンドを入力します。
	
	`racadm getsysinfo`
	
	LCD を使用する場合:
	
	1. メインメニューで **サーバー** を強調表示し、チェックボタンを押します。
	2. IP アドレスを検索するサーバーを選択し、チェックボタンを押します。

CMC の IP アドレスを見つける方法を教えてください。	**iDRAC6 ウェブインタフェースを使用する場合:**
	
	• **システム** → **リモートアクセス** → **CMC** の順にクリックします。
	
	CMC **概要** 画面に CMC の IP アドレスが表示されます。
	
	仮想コンソールから以下の操作を行います。
	
	• OSCAR の「Dell CMC」コンソールを選択してローカルシリアル接続経由で CMC にログインします。CMC RACADM コマンドはこの接続から発行できます。全 CMC RACADM サブコマンドのリストは、『Dell Chassis Management Controller システム管理者リファレンスガイド』を参照してください。
	
	`$ racadm getniccfg -m chassis`
	
	`NIC Enabled = 1`
	`DHCP Enabled = 1`
	`Static IP Address = 192.168.0.120`
	`Static Subnet Mask = 255.255.255.0`
	`Static Gateway = 192.168.0.1`
	`Current IP Address = 10.35.155.151`
	`Current Subnet Mask = 255.255.255.0`
	`Current Gateway = 10.35.155.1`
	`Speed = Autonegotiate`
	`Duplex = Autonegotiate`
	
	メモ: 上記の操作はリモート RACADM で実行することもできます。

iDRAC6 ネットワーク接続が機能しません。	• LAN ケーブルが CMC に接続されていることを確認してください。 • NIC の設定、IPv4 または IPv6 の設定、および静的または DHCP がネットワークで有効になっていることを確認してください。
サーバーをシャーシに挿入し、電源ボタンを押したので	• サーバーがパワーアップするまで、iDRAC6 の初期化に最大 2 分かかります。

すが、何も起こりません。	• CMC の電力バジェットを確認してください。シャーシの電力バジェットを超えている可能性があります。
iDRAC6 のシステム管理者ユーザー名とパスワードを忘れました。	iDRAC6 をデフォルト設定に復元する必要があります。 1. サーバーを再起動し、プロンプトが表示されたら <Ctrl><E> キーを押して **iDRAC6 設定ユーティリティ** を開始します。 2. **iDRAC6 設定ユーティリティ** メニューで、**デフォルトにリセット** を強調表示して <Enter> キーを押します。 **メモ:** また、`racadm racresetcfg` を発行してローカル RACADM から iDRAC6 をリセットすることもできます。 詳細については、「デフォルトに戻す」を参照してください。
サーバースロット名の変更方法を教えてください。	1. CMC ウェブインタフェースにログインします。 2. **シャーシ** ツリーを開き、**サーバー** をクリックします。 3. **セットアップ** タブをクリックします。 4. 該当するサーバーの行に、新しいスロット名を入力します。 5. **適用** をクリックします。
iDRAC6 ウェブインタフェースから仮想コンソールのセッションを開始すると、ActiveX セキュリティポップアップが表示されます。	iDRAC6 が信用済みサイトでない可能性があります。仮想コンソールのセッションを開始するたびにセキュリティポップアップが表示されるのを防ぐには、クライアントのブラウザで以下のように iDRAC6 を信頼済みサイトのリストに追加してください。 1. **ツール** → **インターネットオプション**→ **セキュリティ**→ **信頼済みサイト** の順にクリックします。 2. **サイト** をクリックして iDRAC6 の IP アドレスまたは DNS 名を入力します。 3. **追加** をクリックします。 4. **カスタムレベル** をクリックします。 5. **セキュリティ設定** ウィンドウで **署名なしの ActiveX Controls のダウンロード** で **プロンプト** を選択します。
仮想コンソールのセッションを開始したとき、ビューアの画面は空白です。	**仮想メディア** 権限があっても、**仮想コンソール** 権限がない場合は、仮想メディア機能にアクセスできるようにビューアを起動できますが、管理下サーバーのコンソールは表示されません。
起動中 iDRAC6 が応答していません。	サーバーを取り外し、挿入し直してください。 iDRAC6 がアップグレード可能なコンポーネントとして表示されているかどうか CMC ウェブインタフェースを確認します。表示されている場合は、「CMC を使用した iDRAC6 ファームウェアのアップデート」の手順に従ってください。 問題が解決されない場合は、テクニカルサポートにお問い合わせください。
管理下サーバーの起動を試行すると、電源インジケータは緑色ですが POST またはビデオが表示されません。	これは、次の状態である場合に発生します。 • メモリがインストールされていない、またはアクセス不可能である。 • CPU がインストールされていない、またはアクセス不可能である。 • ビデオライザーカードが不在、または接続が不適切である。 また、iDRAC6 ウェブインタフェースまたは LCD で iDRAC6 ログのエラーメッセージも確認してください。

目次ページに戻る