Integrated Dell Remote Access Controller 6（iDRAC6）バージョン 1.95 ユーザーズガイド

メモおよび注意

メモ：コンピュータを使いやすくするための重要な情報を説明しています。

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

本書で使用されている商標：Dell™、DELL ロゴ、OpenManage™、PowerEdge™ は Dell Inc. の商標です。Microsoft®、Windows®、Windows Server®、.NET®、Internet Explorer®、Windows Vista®、Active Directory® は米国およびその他の国における Microsoft Corporation の商標または登録商標です。Red Hat® と Red Hat Enterprise Linux® は 米国およびその他の国における Red Hat, Inc. の登録商標です。SUSE® は Novell Corporation の登録商標です。Intel® と Pentium® は米国およびその他の国における Intel Corporation の登録商標です。UNIX® は米国およびその他の国における The Open Group の登録商標です。Java® は米国およびその他の国における Oracle またはその子会社の登録商標です。

2013 - 03

目次

1 iDRAC6 の概要 19

このリリースの新機能 **19**

iDRAC6 Express の管理機能 **19**

iDRAC6 Enterprise および vFlash メディア **21**

対応プラットフォーム **24**

対応 OS **24**

対応ウェブブラウザ **24**

対応リモートアクセス接続 **25**

iDRAC6 のポート **25**

その他の必要マニュアル **26**

デルサポートサイトからの文書へのアクセス **28**

2 iDRAC6 を使い始めるにあたって 29

3 iDRAC6 の基本インストール 31

作業を開始する前に **31**

iDRAC6 Express/Enterprise ハードウェアの取り付け **31**

iDRAC 6 を使用するためのシステムの設定 **32**

ソフトウェアのインストールと設定の概要 **34**
iDRAC6 ソフトウェアのインストール 34
iDRAC6 の設定 34

管理下システムへのソフトウェアのインストール. . . . **35**

管理ステーションへのソフトウェアのインストール. **35**
Linux 管理ステーションでの RACADM のインストールと削除 36
RACADM のインストール 36
RACADM のアンインストール. 36

iDRAC6 ファームウェアのアップデート **37**
作業を開始する前に. 37
iDRAC6 ファームウェアのダウンロード. 37
ウェブベースのインタフェースを使用した iDRAC6 ファームウェアのアップデート. 38
RACADM を使用した iDRAC6 ファームウェアのアップデート 38
Windows および Linux 対応オペレーティングシステム用の Dell Update Packages を使用した iDRAC6 ファームウェアのアップデート 38

対応ウェブブラウザの設定. **39**
iDRAC6 ウェブインタフェースに接続するためのウェブブラウザの設定 39
信頼されているドメインのリスト 39
ウェブインタフェースの日本語版の表示. 40

4 ウェブインタフェースを使用した iDRAC6 の設定 43

ウェブインタフェースへのアクセス. **43**
ログイン. 44
ログアウト 45
複数のブラウザタブとウィンドウの使用. 45

iDRAC6 NIC の設定 **46**
ネットワークと IPMI LAN の設定 46
IP フィルタおよび IP ブロックの設定 51

プラットフォームイベントの設定 **52**
プラットフォームイベントフィルタ（PEF）の設定 53
プラットフォームイベントトラップ（PET）の設定 54
E- メールアラートの設定 55
ウェブインタフェースを使った IPMI の設定 56

iDRAC6 ユーザーの設定 **58**

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 **58**
SSL（セキュアソケットレイヤー） 58
証明書署名要求（CSR） 59
ウェブインタフェースを介した SSL へのアクセス 59
証明書署名要求の生成 60
サーバー証明書のアップロード 61

Active Directory の設定と管理 **62**

汎用 LDAP の設定と管理 **65**

iDRAC6 サービスの設定 **66**

iDRAC6 ファームウェア / システムサービスリカバリイメージのアップデート **69**
iDRAC6 ファームウェアのロールバック 70

リモートシスログ **71**

最初の起動デバイス **72**

リモートファイル共有 **73**

内蔵デュアル SD モジュール **75**
GUI を使って内蔵デュアル SD モジュールを表示する 76

5 iDRAC6 の詳細設定 79

作業を開始する前に **79**

リモート SSH/Telnet 経由でシリアル出力を表示するための iDRAC6 設定 **79**

iDRAC6 で SSH/Telnet を有効にする設定 80

Telnet または SSH を使用したテキストコンソールの起動 80

Telnet コンソールの使用 81

セキュアシェル（SSH）の使用 82

起動中に Linux にシリアルコンソールを設定する方法 84

シリアル接続のための iDRAC6 の設定 **88**

ダイレクト接続基本モードとダイレクト接続ターミナルモードの iDRAC の設定 90

RAC シリアルインタフェース通信モードとシリアルコンソールの間の切り替え 91

シリアルコンソールの DB-9 またはヌルモデムケーブルの接続 **93**

管理ステーションのターミナルエミュレーションソフトウェアの設定 **93**

Linux Minicom にシリアルコンソールエミュレーションを設定する方法 94

シリアルコンソール用ハイパーターミナルの設定 95

シリアルと端末モードの設定 **96**

IPMI と iDRAC6 シリアルの設定 96

ターミナルモードの設定 97

iDRAC6 のネットワーク設定 **98**

ネットワーク経由の iDRAC6 へのアクセス **99**

RACADM のリモート使用 **100**

RACADM 構文概要 101

RACADM オプション 102

racadm リモート機能の有効 / 無効化 **102**

RACADM サブコマンド 102
RACADM エラーメッセージについてよくある お問い合わせ（FAQ）. 105

複数の iDRAC6 コントローラの設定 106
iDRAC6 設定ファイルの作成. 107
構文解析規則 108
iDRAC6 IP アドレスの変更. 110
iDRAC6 ネットワークプロパティの設定. 110

ネットワークセキュリティについてよくある お問い合わせ（FAQ）. 112

6 iDRAC6 ユーザーの追加と設定 115

ウェブインタフェースを使用した iDRAC6 ユーザーの設定 115
iDRAC6 ユーザーの追加と設定 115
SSH 経由の公開キー認証 120
iDRAC6 ウェブインタフェースを使った SSH キーのアップロード、表示、削除 122
RACADM を使った SSH キーのアップロード、表示、削除 123

RACADM ユーティリティを使用した iDRAC6 ユーザーの設定 124
作業を開始する前に 125
iDRAC6 ユーザーの追加 126
iDRAC6 ユーザーの削除 127
iDRAC6 ユーザーに権限を与える 127

7 iDRAC6 ディレクトリサービスの使用 129

Microsoft Active Directory での iDRAC6 の使用. 129

iDRAC6 用に Microsoft Active Directory 認証を有効にするための必要条件 130
ドメインコントローラの SSL を有効にする . . . 131

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 131
iDRAC6 ファームウェア SSL 証明書のインポート 132

サポートされている Active Directory の認証機構 **133**

拡張スキーマ Active Directory の概要 **134**
Active Directory スキーマ拡張 134
iDRAC スキーマ拡張の概要 134
Active Directory オブジェクトの概要 134
拡張スキーマを使用した権限の蓄積 136

CMC にアクセスするための拡張スキーマ Active Directory の設定 **137**
Active Directory スキーマの拡張. 137
Microsoft 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 143
Microsoft Active Directory への iDRAC ユーザーと権限の追加 144
iDRAC6 ウェブベースのインタフェースを使用した Microsoft Active Directory と拡張スキーマの設定. 146
RACADM を使用した拡張スキーマの Microsoft Active Directory の設定 148

標準スキーマの Active Directory の概要. **151**
シングルドメインとマルチドメインのシナリオ 152

iDRAC6 にアクセスするための標準スキーマ Microsoft Active Directory の設定 **152**
iDRAC6 ウェブインタフェースを使用した標準スキーマの Microsoft Active Directory の設定. 153
RACADM を使用した標準スキーマの Microsoft Active Directory の設定 156

設定のテスト **159**

汎用 LDAP ディレクトリサービス **160**

ログイン構文（ディレクトリサービス vs ローカルユーザー）. 160
iDRAC6 ウェブベースの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 . . . 160
RACADM を使用した汎用 LDAP ディレクトリサービスの設定 163

Active Directory についてよくあるお問い合わせ（FAQ）. 164

8 iDRAC6 に対するシングルサインオンまたはスマートカードログインの設定 169

Kerberos 認証について. 169

Active Directory SSO とスマートカード認証の必要条件 170

Microsoft Active Directory SSO の使用 172
SSO を使用できるように iDRAC6 を設定する 173
SSO を使用して iDRAC6 にログインする 174

スマートカード認証の設定 174
ローカル iDRAC6 ユーザーに対するスマートカードログオンの設定 174
Active Directory ユーザーに対するスマートカードログオンの設定 175
iDRAC6 を使ったスマートカードの設定. 176
スマートカードを使用した iDRAC6 へのログイン 177
Active Directory スマートカード認証を使用した iDRAC6 へのログイン 178

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. 178

SSO についてよくあるお問い合わせ（FAQ）. 180

9 GUI 仮想コンソールの使用 183

概要 **183**

仮想コンソールの使用 **183**
管理ステーションの設定 184
ブラウザのキャッシュのクリア 185
仮想コンソールと仮想メディアアプリケーションに基づく ActiveX 用の Internet Explorer ブラウザ設定 186
サポートされている画面解像度とリフレッシュレート 187
iDRAC6 ウェブインタフェースでの仮想コンソールの設定 188
仮想コンソールセッションの開始 189
仮想コンソールのプレビュー 191

iDRAC6 仮想コンソールの使用（Video Viewer） **192**
ローカルサーバービデオの有効または無効 . . . 196

仮想コンソールと仮想メディアページのリモート起動 **197**
URL フォーマットを使用したコンソールの起動 197
一般的なエラーシナリオ 198

仮想コンソールについてよくあるお問い合わせ（FAQ） **199**

10 WS-MAN インタフェースの使用 203

対応 CIM プロファイル **203**

11 iDRAC6 SM-CLP コマンドラインインタフェースの使用 207

iDRAC6 SM-CLP のサポート **207**

SM-CLP の機能 **208**

SM-CLP の使用 208
SM-CLP のターゲット 209

12 VMCLI を使用したオペレーティング システムの導入 215

作業を開始する前に **215**
リモートシステム要件 215
ネットワーク要件. 215

ブータブルイメージファイルの作成 **215**
Linux システムのイメージファイルの作成. . . . 216
Windows システムのイメージファイルの作成. 216

導入の準備 **216**
リモートシステムの設定 216

オペレーティングシステムの導入 **217**

VMCLI ユーティリティの使用 **218**
VMCLI ユーティリティのインストール 219
コマンドラインオプション. 219
VMCLI パラメータ 220
VMCLI オペレーティングシステムシェルオプション 223

13 Intelligent Platform Management Interface の設定 225

ウェブベースインタフェースを使った IPMI の設定. **225**

RACADM CLI を使った IPMI の設定 **226**

IPMI リモートアクセスシリアルインタフェースの使用 **229**

ウェブベースインタフェースを使用したシリアルオーバー LAN の設定. **230**

14 仮想メディアの設定と使用 231

概要 **231**
Windows ベースの管理ステーション 232
Linux ベースの管理ステーション. 232

仮想メディアの設定 **233**

仮想メディアの実行 **234**
サポートされている仮想メディア設定 234
仮想メディアからの起動 236
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 237
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 238

仮想メディアについてよくあるお問い合わせ (FAQ) **239**

15 vFlash SD カードの設定と vFlash パーティションの管理 245

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 **246**

RACADM を使用した vFlash または標準 SD カードの設定 **248**
vFlash または標準 SD カードのプロパティの 表示 248
vFlash または標準 SD カードを有効または 無効にする 248
vFlash または標準 SD カードの初期化 248
vFlash または標準 SD カードの最後の状態の 取得 249
vFlash または標準 SD カードのリセット. 249

iDRAC6 ウェブインタフェースを使用した vFlash パーティションの管理 **249**
空のパーティションの作成 250

イメージファイルを使ったパーティションの作成. 251
パーティションのフォーマット 253
使用可能なパーティションの表示 254
パーティションの変更 256
パーティションの連結と分離. 256
既存のパーティションの削除. 257
パーティション内容のダウンロード 258
パーティションからの起動. 258

RACADM を使った vFlash パーティションの管理. . . . 259
パーティションの作成 260
パーティションの削除 261
パーティションの状態の取得. 261
パーティション情報の表示. 261
パーティションからの起動. 261
パーティンションの連結と分離 262
パーティションの変更 262

よくあるお問い合わせ（FAQ). 262

16 電源の監視と管理. 263

電力インベントリ、電力バジェット、電力制限. 263

電源監視 263

電源の設定と管理 264

電源装置の正常性状態の表示 264
ウェブインタフェースの使用. 264
RACADM の使用. 265

電力バジェットの表示. 266
ウェブインタフェースの使用. 266
RACADM の使用. 266

電力バジェットのしきい値 266
ウェブインタフェースの使用. 267

RACADM の使用 267

電源監視の表示 **268**
ウェブインタフェースの使用 268
RACADM の使用 270

サーバーに対する電源制御操作の実行 **270**
ウェブインタフェースの使用 270
RACADM の使用 271

17 iDRAC6 設定ユーティリティの使用 273

概要 **273**

iDRAC6 設定ユーティリティの起動 **273**

iDRAC6 設定ユーティリティの使用 **274**
iDRAC6 LAN 274
IPMI Over LAN 275
LAN Parameters 275
仮想メディアの設定 279
スマートカードのログオン 280
システムサービス設定 280
LCD の設定 281
LAN ユーザー設定 282
デフォルトに戻す 282
システムイベントログメニュー 282
iDRAC6 設定ユーティリティの終了 285

18 監視とアラート管理 287

管理下システムに前回クラッシュ画面のキャプチャを設定する方法 **287**

Windows の自動再起動オプションを無効にする **288**
Windows 2008 Server の自動再起動オプションを無効にする 288

Windows Server 2003 の自動再起動オプションを無効にする 288

プラットフォームイベントの設定 288

プラットフォームイベントフィルタ（PEF）の設定 289

PET の設定 290

E- メールアラートの設定 291

E- メールアラートのテスト 293

RAC SNMP トラップアラート機能のテスト 293

SNMP 認証についてよくあるお問い合わせ（FAQ）. . . 293

19 管理下システムのリカバリとトラブルシューティング 295

リモートシステムのトラブルシューティングの第一歩 295

リモートシステムの電源管理 296

iDRAC6 ウェブインタフェースからの電源制御処置の選択 296

iDRAC6 CLI からの電源制御処置の選択 296

システム情報の表示 296

メインシステムシャーシ 297

Remote Access Controller 298

システムインベントリ 300

システムイベントログ（SEL）の使用 301

コマンドラインを使ってシステムログを表示する 302

作業メモの使用 303

POST 起動ログの使用 304

前回システムクラッシュ画面の表示 305

20 iDRAC6 の修復とトラブルシューティング 307

RAC ログの使用 **307**

コマンドラインの使用 **308**

診断コンソールの使用 **308**

サーバーの識別機能の使用 **309**

トレースログの使用 **309**

racdump の使用 **310**

coredump の使用 **310**

21 センサー 311

バッテリプローブ **311**

ファンプローブ **311**

シャーシイントルージョンプローブ **311**

電源装置プローブ **311**

リムーバブルフラッシュメディアプローブ **312**

電力監視プローブ **312**

温度プローブ **312**

電圧プローブ **312**

22 セキュリティ機能の設定 313

iDRAC6 システム管理者用のセキュリティオプション **314**

iDRAC6 ローカル設定を無効にする 314

iDRAC6 仮想コンソールを無効にする 315

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 **316**
SSL（セキュアソケットレイヤー）. 316
証明書署名要求（CSR）. 317
SSL メインメニューへのアクセス 317
証明書署名要求の生成 318
サーバー証明書の表示 319

セキュアシェル（SSH）の使用 **319**

サービスの設定. **320**

iDRAC6 の追加のセキュリティオプションを有効にする **322**
iDRAC6 GUI を使ったネットワークセキュリティの設定 326

索引 329

1

iDRAC6 の概要

Integrated Dell Remote Access Controller6（iDRAC6）はシステム管理ハードウェアおよびソフトウェアのソリューションで、Dell PowerEdge システムのリモート管理機能、クラッシュしたシステムのリカバリ機能、電源制御機能などを提供します。

iDRAC6 は、リモート監視 / 制御システムに、システムオンチップの内蔵マイクロプロセッサを採用しています。iDRAC6 は、管理下 PowerEdge サーバーと同じシステム基板に搭載します。サーバーオペレーティングシステムはアプリケーションの実行に関与し、iDRAC6 はオペレーティングシステム外のサーバー環境および状態の監視と管理に関与します。

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

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

このリリースの新機能

- DIMM 構成および PCI カードのサポート（詳細については、リリースノートを参照してください）。
- Internet Explorer 10 ブラウザのサポート。
- デフォルトの証明書署名要求（CSR）暗号化キーの長さを 2048 ビットに変更。

iDRAC6 Express の管理機能

iDRAC6 Express は次の管理機能を提供します。

- ダイナミックドメイン名システム（DDNS）の登録。
- ウェブインタフェース、およびシリアル、Telnet、または SSH 接続経由でのサーバー管理コマンドラインプロトコル（SM-CLP）のコマンドラインを使用したリモートシステム管理と監視。

- Microsoft Active Directory 認証のサポート — 拡張スキーマまたは標準スキーマを使用して iDRAC6 のユーザー ID とパスワードを Active Directory で一元管理。
- Lightweight Directory Access Protocol（LDAP）ベースの認証をサポートするための汎用ソリューション — この機能は、お使いのディレクトリサービスへのスキーマ拡張を必要としません。
- 監視 のためのシステム情報やコンポーネントのステータスへのアクセス。
- システムイベントログ、iDRAC6 ログ、およびクラッシュした、または応答のないシステムの最後のクラッシュ画面（オペレーティングシステムの状態とは無関係のもの）へのアクセス。
- GUI または CLI を介した Lifecycle Controller ログへのワークノートの追加オプション。
- Dell OpenManage Server Administrator または Dell OpenManage IT Assistant からの iDRAC6 ウェブインタフェースの起動。
- E- メールメッセージまたは SNMP トラップによる管理下ノードの不具合の可能性のアラート。
- 管理コンソールからのシャットダウンやリセットなどのリモート電源管理機能。
- Intelligent Platform Management Interface（IPMI）のサポート。
- ウェブインタフェースを介したセキュアなリモートシステム管理。
- パスワードレベルのセキュリティ管理によるリモートシステムへの不正アクセスの防止。
- 役割ベースの権限による異なるシステム管理タスク用の割り当て可能パーミッション。
- IPv6 アドレスを使用した iDRAC6 ウェブインタフェースにアクセスできる IPv6 サポート、iDRAC NIC IPv6 アドレスの指定、IPv6 SNMP アラートの宛先を設定するための宛先番号の指定。
- Web Services for Management（WS-MAN）プロトコルを使用したネットワークからのアクセスが可能な管理。
- システム管理 CLI の実装標準を提供するサーバー管理コマンドラインプロトコル（SM-CLP）のサポート。
- ファームウェアロールバックおよびリカバリによる、希望するファームウェアイメージからの起動（またはイメージへのロールバック）。

iDRAC6 Express の詳細については、**dell.com/support/manualss** にある『ハードウェアオーナーズマニュアル』を参照してください。

iDRAC6 Enterprise および vFlash メディア

vFlash メディア装備の iDRAC6 は、RACADM、仮想コンソール、仮想メディア機能、専用 NIC、および vFlash（オプションの Dell vFlash メディアカードを使用）のサポートを追加します。vFlash を使用すると、vFlash メディアに緊急用の起動イメージと診断ツールを保存できます。iDRAC6 Enterprise および vFlash メディアの詳細については、**dell.com/support/manualss** 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。

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

表 1-1. iDRAC6 の機能リスト

機能	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise（vFlash 装備）
インタフェースと標準サポート				
IPMI 2.0	✓	✓	✓	✓
ウェブベースの GUI	✗	✓	✓	✓
SNMP	✗	✓	✓	✓
WSMAN	✗	✓	✓	✓
SMASH-CLP（SSH のみ）	✗	✓	✓	✓
RACADM コマンドライン（SSH とローカル）	✗	✓	✓	✓
RACADM コマンドライン（リモート）	✗	✗	✓	✓
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	✗	✗	✓	✓

表 1-1. iDRAC6 の機能リスト （続き）

機能	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise （vFlash 装備）
セキュリティと認証				
役割ベースの権限	✓	✓	✓	✓
ローカルユーザー	✓	✓	✓	✓
SSL 暗号化	✓	✓	✓	✓
Active Directory	✗	✓	✓	✓
汎用 LDAP のサポート	✗	✓	✓	✓
2 要素認証 [1]	✗	✓	✓	✓
シングルサインオン	✗	✓	✓	✓
PK 認証（SSH 用）	✗	✗	✓	✓
リモート管理と改善				
リモートファームウェアアップデート	✓[2]	✓	✓	✓
サーバーの電源制御	✓[2]	✓	✓	✓
シリアルオーバー LAN（プロキシ使用）	✓	✓	✓	✓
シリアルオーバー LAN（プロキシなし）	✓	✓	✓	✓
電力上限	✓	✓	✓	✓
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 [3]	✗	✗	✓	✓
仮想コンソール [3]	✗	✗	✓	✓
仮想コンソール共有 [3]	✗	✗	✓	✓

表 1-1. iDRAC6 の機能リスト （続き）

機能	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise （vFlash 装備）
リモート仮想コンソールの起動	✗	✗	✓	✓
vFlash	✗	✗	✗	✓
監視				
センサー監視と警告	✓[2]	✓	✓	✓
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	✗	✓	✓	✓
リモートシスログ	✗	✗	✓	✓
Lifecycle Controller				
Unified Server Configurator	✓[4]	✓	✓	✓
リモートサービス（WS-MAN を使用）	✗	✓	✓	✓
部品交換	✗	✗	✗	✓

[1] 2 要素認証には Internet Explorer が必要です。

[2] 機能はウェブインタフェースでなく IPMI からのみ使用できます。

[3] 仮想コンソールと仮想メディアは Java と Active-X プラグインを使って使用できます。

[4] BMC を使って使用できる統合サーバーコンフィギュレータは、オペレーティングシステムのインストールと診断に限定されています。

✓= 対応 ✗= 未対応

iDRAC6 には次のセキュリティ機能があります。

- シングルサインオン、二要素認証、公開キー認証。
- Active Directory（オプション）、LDAP 認証（オプション）、またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証。
- システム管理者が各ユーザーに特定の権限を設定できる、役割ベース認証。
- ウェブベースのインタフェースまたは SM-CLP を使用したユーザー ID とパスワードの設定。
- SM-CLP およびウェブインタフェースで SSL 3.0 規格を使用した 128 ビットと 40 ビットの暗号化のサポート（128 ビットが認められていない国の場合）。
- ウェブインターフェースまたは SM-CLP を使用したセッションタイムアウトの設定（秒単位）。
- 設定可能な IP ポート（該当する場合）。

  メモ : Telnet は SSL 暗号化をサポートしていません。
- 暗号化されたトランスポート層を使用する SSH でのセキュリティ強化。
- IP アドレスごとのログイン失敗数の制限による、制限を超えた IP アドレスのログインの阻止。
- iDRAC6 に接続するクライアントの IP アドレス範囲を制限する機能。

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、**dell.com/support/manuals** にある iDRAC6 Readme ファイルおよび『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

最新情報については、**dell.com/support/manuals** にある iDRAC6 Readme ファイルおよび『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

最新情報については、**dell.com/support/manuals** にある『iDRAC6 1.95 リリースノート』および『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 : 重大なセキュリティの欠陥があるため、SSL 2.0 のサポートは中止になりました。ブラウザを正しく動作させるには、SSL 3.0 対応に設定する必要があります。Internet Explorer 6.0 はサポートされていません。

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	• 10 Mbps/100 Mbps イーサネット • DHCP のサポート • SNMP トラップと E- メールによるイベント通知 • iDRAC6 設定、システム起動、リセット、電源投入、シャットダウンコマンドなどの操作に使用する SM-CLP（Telnet、SSH、RACADAM）コマンドシェルのサポート • IPMItool や ipmishell などの IPMI ユーティリティのサポート

iDRAC6 のポート

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

表 1-3. iDRAC6 サーバーリスニングポート

ポート番号	機能
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	仮想コンソールキーボード / マウス、仮想メディアサービス、仮想メディアセキュアサービス、仮想コンソールビデオ

* 設定可能なポート

表 1-4. iDRAC6 クライアントポート

ポート番号	機能
25	SMTP
53	DNS
68	DHCP で割り当てた IP アドレス

表 1-4. iDRAC6 クライアントポート （続き）

ポート番号	機能
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

このガイドの他に、デルサポートサイト **dell.com/support/manuals** にある次のドキュメントにもシステム内の iDRAC6 のセットアップと操作に関する追加情報が記載されています。

- iDRAC6 オンラインヘルプでは、ウェブインタフェースの使用法について詳しく説明されています。
- 『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』には、RACADM サブコマンド、サポートされているインタフェース、および iDRAC6 プロパティデータベースグループとオブジェクト定義に関する情報が記載されています。
- 『Dell Lifecycle Controller ユーザーガイド』は、Unified Server Configurator（USC）、Unified Server Configurator – Lifecycle Controller Enabled（USC – LCE）、およびリモートサービスについて説明しています。
- iDRAC6 および IPMI インタフェースについては、『Dell OpenManage Baseboard Management Controller ユーティリティユーザーズガイド』を参照してください。
- 『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を説明しています。
- 『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 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。
- 『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。

次のシステムドキュメントにも、iDRAC6 をインストールするシステムについての詳細が記載されています。

- iDRAC6 のインストールについては、『ハードウェアオーナーズマニュアル』を参照してください。
- システムに同梱の「安全にお使いいただくために」には、安全および規制に関する重要な情報が記載されています。規制の詳細については、**dell.com/regulatory_compliance** にある法規制順守の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。
- ラックソリューションに同梱の『ラック取り付けガイド』では、システムをラックに取り付ける方法について説明しています。
- 『はじめに』では、システムの機能、システムのセットアップ、および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。

デルサポートサイトからの文書へのアクセス

デルサポートサイトから文書にアクセスするには、次の手順を実行します。

1. **dell.com/support/manuals** にアクセスします。
2. **サービスタグまたはエクスプレスサービスコードをお持ちですか？** セクションの **いいえ** で **すべてのデル製品のリストから選択する** を選択し、**続行** をクリックします。
3. **お使いの製品タイプを選択してください** セクションで、**ソフトウェア、モニタ、周辺機器およびアクセサリ** をクリックします。
4. **お使いのデル製システムを選択してください - ソフトウェア、モニタ、周辺機器およびアクセサリ** セクションで、**Software**（ソフトウェア）をクリックします。
5. **お使いのデル製システムを選択してください - Software** セクションで、次の中から必要なリンクをクリックします。

- Client System Management（クライアントシステム管理）
- Enterprise System Management（エンタープライズシステム管理）
- Remote Enterprise System Management（リモートエンタープライズシステム管理）
- Serviceability Tools

6. マニュアルを表示するには、必要な製品バージョンをクリックします。

または、次のリンクを使用してマニュアルに直接アクセスすることもできます。

- クライアントシステム管理マニュアル — **dell.com/OMConnectionsClient**
- エンタープライズシステム管理マニュアル — **dell.com/openmanagemanuals**
- リモートエンタープライズシステム管理マニュアル — **dell.com/esmmanuals**
- Serviceability Tools マニュアル — **dell.com/serviceabilitytools**

2

iDRAC6 を使い始めるにあたって

iDRAC6 を使用すると、システムがダウンしているときでもリモートで Dell システムの監視、トラブルシューティング、修復ができます。iDRAC6 は、仮想コンソール、仮想メディア、スマートカード認証、およびシングルサインオン（SSO）などの機能を提供します。

管理ステーション とは、システム管理者が iDRAC6 を備えた Dell システムをリモート管理するシステムを指します。監視されるシステムのことを、管理下システム と呼んでいます。

また、オプションで、管理ステーションと管理下システムに Dell OpenManage ソフトウェアをインストールできます。管理下システムソフトウェアなしでは RACADM をローカルで使用できず、iDRAC6 は前回のクラッシュ画面をキャプチャできません。

iDRAC6 をセットアップするには、次の一般的な手順に従います。

メモ : この手順はシステムによって異なります。この手順を実行するための詳細は、デルサポートサイト **dell.com/support/manuals** にあるお使いのシステム向けの『ハードウェアオーナーズマニュアル』を参照してください。

1. iDRAC6 のプロパティ、ネットワーク、ユーザーを設定します。iDRAC6 の設定には、iDRAC6 設定ユーティリティ、ウェブインタフェース、または RACADM を使用できます。
2. **（オプション）**Windows システムを使用している場合は、iDRAC6 にアクセスできるように Microsoft Active Directory を設定し、Active Directory ソフトウェア内で既存のユーザーに対して iDRAC6 ユーザー権限を追加したり制御できるようにします。
3. **（オプション）**スマートカード認証を設定します。スマートカードは企業のセキュリティをさらに強化します。
4. コンソールリダイレクトや仮想メディアなどのリモートアクセスポイントを設定します。
5. セキュリティ設定を指定します。
6. システム管理機能の効率を上げるためのアラートを設定します。
7. 標準ベースの IPMI ツールを使用してネットワーク上のシステムを管理するために、iDRAC6 Intelligent Platform Management Interface（IPMI）を設定します。

3

iDRAC6 の基本インストール

本項では、iDRAC6 のハードウェアとソフトウェアのインストールおよび設定方法について説明します。

作業を開始する前に

iDRAC6 ソフトウェアをインストールして設定する前に、システムに含まれていた次のアイテムがあることを確認してください。

- iDRAC6 ハードウェア（組み込まれているかまたはオプションキットに同梱）
- iDRAC6 インストール手順（本章に記載）
- 『Dell Systems Management Tools and Documentation DVD』

iDRAC6 Express/Enterprise ハードウェアの取り付け

メモ : iDRAC6 接続は USB キーボード接続をエミュレートします。そのため、システムを再起動したとき、キーボードが接続していなくても通知されません。

iDRAC6 Express/Enterprise は、事前にシステムに組み込まれているか、個別に取り付けることができます。システムに取り付けられている iDRAC6 の利用を開始するには、34 ページの「ソフトウェアのインストールと設定の概要」を参照してください。

iDRAC6 Express/Enterprise がシステムに取り付けられていない場合は、お使いのプラットフォームの『ハードウェアオーナーズマニュアル』でハードウェアの取り付け方法を参照してください。

iDRAC 6 を使用するためのシステムの設定

iDRAC6 を使用するようにシステムを設定するには、iDRAC6 設定ユーティリティを使用します。

iDRAC6 設定ユーティリティを実行するには、次の手順に従います。

1. システムの電源を入れるか、再起動します。
2. POST 中に画面の指示に従って <Ctrl><E> を押します。

   <Ctrl><E> キーを押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、もう一度システムを再起動し、この手順を実行してください。
3. LOM を設定します。
   a. 方向キーを使用して **LAN パラメータ** を選択し、<Enter> を押します。**NIC の選択** が表示されます。
   b. 方向キーを使用して、次のいずれかの NIC モードを選択します。
      - **専用** — このオプションは、リモートアクセスデバイスから iDRAC6 Enterprise 上の専用ネットワークインタフェースを使用できるようにする場合に選択します。このインタフェースは、ホストオペレーティングシステムと共有されず、管理トラフィックを別の物理ネットワークに転送することでアプリケーションのトラフィックから分離できます。このオプションは、システムに iDRAC6 Enterprise が搭載されている場合にのみ、利用可能です。iDRAC6 Enterprise カードを取り付けた後、**NIC の選択** を **専用** に変更してください。これは、iDRAC6 設定ユーティリティ、iDRAC6 ウェブインタフェース、または RACADM を使って行うことができます。
      - **共有** — このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスのネットワークインタフェースは、ホストオペレーティングシステムに NIC チームを設定すると、完全に機能します。リモートアクセスデバイスは、データの受信は NIC 1 と NIC 2 で行いますが、送信は NIC 1 からのみ行います。NIC 1 が故障すると、リモートアクセスデバイスにアクセスできなくなります。

- **フェールオーバー付きで共有（LOM2）**— このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスのネットワークインタフェースは、ホストオペレーティングシステムに NIC チームを設定すると、完全に機能します。リモートアクセスデバイスは、データの受信は NIC 1 と NIC 2 で行いますが、データの送信は NIC 1 からのみ行います。NIC 1 が故障した場合、リモートアクセスデバイスはすべてのデータ送信を NIC 2 にフェールオーバーします。リモートアクセスデバイスはデータの送信に引き続き NIC 2 を使用します。NIC 2 が故障した場合、リモート アクセス デバイスはすべての送受信を再び NIC 1 にフェールオーバーします。ただし、これは最初の NIC 1 の障害が修復されている場合に限ります。
- **フェールオーバー付きで共有（すべての LOM）**— このオプションは、ネットワークインタフェースをホストのオペレーティングシステムと共有する場合に選択します。リモートアクセスデバイスのネットワークインタフェースは、ホストオペレーティングシステムに NIC チームを設定すると、完全に機能します。リモートアクセスデバイスは、NIC 1、NIC 2、NIC 3、NIC 4 を介してデータを受信しますが、データの送信は NIC 1 からのみ行います。NIC 1 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 2 にフェイルオーバーします。NIC 2 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 3 にフェールオーバーします。NIC 3 が故障した場合、リモートアクセスデバイスはデータ送受信のすべてを NIC 4 にフェールオーバーします。NIC 4 が故障した場合、リモート アクセス デバイスはすべてのデータ伝送を NIC 1 にフェイルオーバーします。ただし、これは最初の NIC 1 の障害が修復されている場合に限ります。

4 DHCP または静的 IP アドレスソースを使用するようにネットワークコントローラ LAN パラメータを設定します。

   a 下方向キーを使って、**LAN パラメータ** を選択し、<Enter> を押します。

   b 上下の方向キーを使って、**IP アドレスソース** を選択します。

   c 左右の方向キーを使って、**DHCP**、**自動設定** または **静的** を選択します。

   d **静的** を選択した場合は、**IP アドレス、サブネットマスク、デフォルトゲートウェイ** をそれぞれ設定します。

   e <Esc> を押します。

5 <Esc> を押します。

6 **変更を保存して終了** を選択します。

ソフトウェアのインストールと設定の概要

本項では、iDRAC6 ソフトウェアのインストールと設定について概説します。iDRAC6 のソフトウェアコンポーネントの詳細については、35 ページの「管理下システムへのソフトウェアのインストール」を参照してください。

iDRAC6 ソフトウェアのインストール

iDRAC6 ソフトウェアをインストールするには：

1. iDRAC6 ソフトウェアを管理下システムにインストールします。35 ページの「管理下システムへのソフトウェアのインストール」を参照してください。
2. iDRAC6 ソフトウェアを管理ステーションにインストールします。35 ページの「管理ステーションへのソフトウェアのインストール」を参照してください。

iDRAC6 の設定

iDRAC6 を設定するには：

1. 次のいずれかの設定ツールを選択します。
   - ウェブインタフェース（43 ページの「ウェブインタフェースを使用した iDRAC6 の設定」を参照）
   - RACADM CLI（**dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照）
   - Telnet コンソール（81 ページの「Telnet コンソールの使用」を参照）

   メモ：複数の iDRAC6 設定ツールを同時に使用すると、不測の結果が生じることがあります。
2. iDRAC6 ネットワークを設定します。98 ページの「iDRAC6 のネットワーク設定」を参照してください。
3. iDRAC6 ユーザーを追加して設定します。115 ページの「iDRAC6 ユーザーの追加と設定」を参照してください。
4. ウェブインタフェースにアクセスするために、ウェブブラウザを設定します。39 ページの「対応ウェブブラウザの設定」を参照してください。
5. Microsoft Windows 自動再起動オプションを無効にします。288 ページの「Windows の自動再起動オプションを無効にする」を参照してください。
6. iDRAC6 ファームウェアをアップデートします。37 ページの「iDRAC6 ファームウェアのアップデート」を参照してください。

管理下システムへのソフトウェアのインストール

管理下システムへのソフトウェアのインストールは省略可能です。管理下システムソフトウェアなしでは RACADM をローカルで使用できず、iDRAC6 は前回のクラッシュ画面をキャプチャできません。

管理下システムソフトウェアをインストールするには、『Dell Systems Management Tools and Documentation DVD』で管理下システムにソフトウェアをインストールします。このソフトウェアのインストール手順については、デルサポートサイト **support.dell.com\manuals** にある『ソフトウェアクイックインストールガイド』を参照してください。

管理下システムソフトウェアは、Dell OpenManage Server Administrator の適切なバージョンから、選択したコンポーネントを管理下システムにインストールします。

メモ : iDRAC6 管理ステーションソフトウェアと iDRAC6 管理下システムソフトウェアを同じシステムにインストールしないでください。

管理下システムに Server Administrator がインストールされていない場合は、システムの前回クラッシュ画面の表示 や**自動回復** 機能は使用できません。

前回クラッシュ画面の詳細については、305 ページの「前回システムクラッシュ画面の表示」を参照してください。

管理ステーションへのソフトウェアのインストール

システムには、『Dell Systems Management Tools and Documentation DVD』が同梱されています。この DVD には、次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。

Server Administrator、IT Assistant、Unified Server Configurator の詳細については、デルサポートサイト **dell.com/support/manual** にある『Server Administrator ユーザーズガイド』、『IT Assistant ユーザーズガイド』、『Lifecycle Controller ユーザーズガイド』を参照してください。

Linux 管理ステーションでの RACADM のインストールと削除

リモート RACADM 機能を使用するには、Linux が稼動する管理ステーションに RACADM をインストールします。

メモ：『Dell Systems Management Tools and Documentation DVD』で **セットアップ** を実行すると、サポートされているすべてのオペレーティングシステム用の RACADM ユーティリティが管理ステーションにインストールされます。

RACADM のインストール

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

   ```
   mount /media/cdrom
   ```

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

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

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

RACADM のアンインストール

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

```
rpm -e <racadm パッケージ名 >
```

<racadm パッケージ名 > は RAC ソフトウェアのインストールに使用する rpm パッケージです。

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

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

iDRAC6 ファームウェアのアップデート

iDRAC6 ファームウェアをアップデートするには、次のいずれかの方法を使用します。

- ウェブインタフェース（38 ページの「ウェブベースのインタフェースを使用した iDRAC6 ファームウェアのアップデート」を参照）
- RACADM CLI（38 ページの「RACADM を使用した iDRAC6 ファームウェアのアップデート」を参照）
- Dell アップデートパッケージ（38 ページの「Windows および Linux 対応オペレーティングシステム用の Dell Update Packages を使用した iDRAC6 ファームウェアのアップデート」を参照）

作業を開始する前に

ローカル RACADM または Dell Update Packages を使用して iDRAC6 ファームウェアをアップデートする前に、次の手順を実行してください。この手順を実行しないと、アップデートに失敗することがあります。

1. 適切な IPMI と管理下ノードのドライバをインストールして有効にします。
2. システムで Windows オペレーティングシステムが稼動している場合は、**Windows Management Instrumentation**（WMI）サービスを有効にして起動します。
3. iDRAC6 Enterprise を使用し、システムで Intel EM64T 用 SUSE Linux Enterprise Server（バージョン 10）が稼動している場合は、**Raw** サービスを開始します。
4. 仮想メディアを切断してマウント解除します。

   メモ : iDRAC6 ファームウェアのアップデートが何らかの理由で中断されると、ファームウェアのアップデートを再び実行できるまでに最大 30 分間待たなければならない場合があります。
5. USB が有効になっていることを確認してください。

iDRAC6 ファームウェアのダウンロード

iDRAC6 ファームウェアをアップデートするには、デルサポートサイト **support.dell.com** から最新ファームウェアをダウンロードしてローカルシステムに保存します。

iDRAC6 ファームウェアパッケージには、次のソフトウェアコンポーネントが含まれています。

- コンパイルされた iDRAC6 ファームウェアコードとデータ
- ウェブベースのインタフェース、JPEG、およびその他のユーザーインタフェースのデータファイル
- デフォルト設定ファイル

ウェブベースのインタフェースを使用した iDRAC6 ファームウェアのアップデート

詳細については、69 ページの「iDRAC6 ファームウェア / システムサービスリカバリイメージのアップデート」を参照してください。

RACADM を使用した iDRAC6 ファームウェアのアップデート

CLI ベースの RACADM ツールを使用して、iDRAC6 ファームウェアをアップデートできます。管理下システムに Server Administrator をインストールしている場合は、ローカル RACADM を使用してファームウェアをアップデートしてください。

1. デルサポートサイト **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.d6
   ```

2. 次の RACADM コマンドを実行します。

   ```
   racadm fwupdate -pud c:\downloads\
   ```

   リモート RACADM および TFTP サーバーを使用して、ファームウェアをアップデートすることも可能です。

   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、TFTP サーバー IP アドレスを含む **firmimg.d6** が保存されている TFTP サーバー上の場所です。

   パス : **<***TFTP サーバー* ***IP>*** -d **<** *TFTP サーバー上のファームウェアイメージのパス* **>**

   - 実例 1：firmimg.d6 イメージが tftp ルートフォルダにある場合、パス：**<***TFTP サーバー* ***IP>***
   - 実例 2: firmimg.d6 イメージが tftp ルートのサブフォルダにある場合、パス：**<***TFTP サーバー* ***IP>*** -d **/<** *サブフォルダのパス* **>**

Windows および Linux 対応オペレーティングシステム用の Dell Update Packages を使用した iDRAC6 ファームウェアのアップデート

Windows および Linux の対応オペレーティングシステム用の Dell Update Package をデルサポートサイト **support.dell.com** からダウンロードして実行します。詳細については、デルサポートサイト **support.dell.com\manuals** にある『Dell Update Package ユーザーズガイド』を参照してください。

メモ : Linux で Dell Update Package ユーティリティを使用して iDRAC6 ファームウェアをアップデートする際は、コンソール上に次のメッセージが表示される場合があります。

```
usb 5-2: device descriptor read/64, error -71
```

```
usb 5-2: デバイス記述子がアドレス 2 を受け入れません（エラー -71）。
```

これらのエラーは表面的なものであり、無視しても構いません。これらのメッセージは、ファームウェアのアップデートプロセス中に USB デバイスがリセットされたためで、無害です。

対応ウェブブラウザの設定

次に、対応ウェブブラウザの設定手順を説明します。

iDRAC6 ウェブインタフェースに接続するためのウェブブラウザの設定

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

Internet Explorer ウェブブラウザをプロキシサーバーにアクセスするように設定するには、次の手順を実行します。

1. ウェブブラウザのウィンドウを開きます。
2. **ツール** をクリックして、**インターネットオプション** をクリックします。
3. **インターネットオプション** ウィンドウで **接続** タブをクリックします。
4. **ローカルエリアネットワーク（LAN）設定** で **LAN 設定** をクリックします。
5. **プロキシサーバーを使用** ボックスが選択されている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** ボックスを選択します。
6. **OK** を 2 度クリックします。

信頼されているドメインのリスト

ウェブブラウザから iDRAC6 ウェブインタフェースにアクセスするとき、信頼されたドメインのリストに iDRAC6 の IP アドレスがない場合は、この IP アドレスをリストに加えるように要求されることがあります。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 ウェブベースのインタフェースへの接続を再確立します。

ウェブインタフェースの日本語版の表示

Windows

iDRAC6 ウェブインタフェースは、次の Windows オペレーティングシステム言語でサポートされています。

- 英語
- フランス語
- ドイツ語
- スペイン語
- 日本語
- 簡体字中国語

Internet Explorer で iDRAC6 ウェブインタフェースのローカライズバージョンを表示するには、次の手順に従います。

1. **ツール** をクリックして、**インターネットオプション** を選択します。
2. **インターネットオプション** ウィンドウで **言語** をクリックします。
3. **言語設定** ウィンドウで **追加** をクリックします。
4. **言語の追加** ウィンドウでサポートされている言語を選択します。

   複数の言語を選択するには、<Ctrl> を押しながら選択します。
5. 優先言語を選択して **上に移動** をクリックし、その言語をリストの先頭に移動します。
6. **OK** をクリックします。
7. **言語設定** ウィンドウで **OK** をクリックします。

Linux/

Red Hat Enterprise Linux（バージョン 4）クライアントで簡体字中国語のグラフィカルユーザーインタフェース（GUI）を使って仮想コンソールを実行している場合は、ビューアのメニューとタイトルが文字化けすることがあります。この問題は、Red Hat Enterprise Linux（バージョン 4）簡体字中国語オペレーティングシステムにおけるエンコードエラーによるものです。この問題を解決するには、次の手順で現在のエンコード設定にアクセスして変更してください。

1. コマンド端末を開きます。
2. 「locale」と入力して、<Enter> を押します。次の出力が表示されます。

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
```

```
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3 値に「zh_CN.UTF-8」が含まれている場合は、変更する必要はありません。値に「zh_CN.UTF-8」が含まれていない場合は、手順 4 に進んでください。

4 **/etc/sysconfig/i18n** ファイルに移動します。

5 ファイルに次の変更を加えます。

現在のエントリ：

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

アップデート後のエントリ：

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

6 ログアウトしてから、オペレーティングシステムにログインします。

7 iDRAC6 を再起動します。

他の言語から簡体字中国語に切り替える場合は、この修正がまだ有効であることを確認してください。有効でない場合は、この手順を繰り返します。

iDRAC6 の詳細設定については、79 ページの「iDRAC6 の詳細設定」を参照してください。

4

ウェブインタフェースを使用した iDRAC6 の設定

iDRAC6 には、iDRAC6 プロパティとユーザーの設定、リモート管理タスクの実行、リモート（管理下）システムのトラブルシューティングを可能にするウェブインタフェースが備わっています。日常のシステム管理には、iDRAC6 ウェブインタフェースを使用してください。本章では、iDRAC6 のウェブインタフェースを使って一般的なシステム管理タスクを実行する方法について説明し、関連情報へのリンクも掲載しています。

ほとんどのウェブインタフェースの設定タスクは、RACADM コマンドまたは SM-CLP（Server Management-Command Line Protocol）を使用して実行することもできます。

ローカル RACADM コマンドは、管理下サーバーから実行できます。

SM-CLP および SSH/Telnet RACADM コマンドは、Telnet または SSH 接続によってリモートアクセス可能なシェルにて実行されます。SM-CLP の詳細については、207 ページの「iDRAC6 SM-CLP コマンドラインインタフェースの使用」を参照してください。RACADM コマンドの詳細については、デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』を参照してください。

△ **警告：「更新」をクリック、または F5 キーを押してブラウザを更新する場合は、ウェブグラフィカルユーザーインタフェース（GUI）セッションからログアウトしたり、「システム概要」ページにリダイレクトされることがあります。**

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。

   IPv4 アドレスを使用してウェブインタフェースにアクセスする場合は、手順 2 へ進みます。

   IPv6 アドレスを使用してウェブインタフェースにアクセスする場合は、手順 3 へ進みます。

2. IPv4 アドレスを使用してウェブインタフェースにアクセスするには、IPv4 が有効になっている必要があります。

   ブラウザの **アドレス** バーに、次のように入力します。

   `https://<iDRAC IPv4 アドレス>`

   次に、<Enter> キーを押します。

3 IPv6 アドレスを使用してウェブインタフェースにアクセスするには、IPv6 が有効になっている必要があります。

ブラウザの **アドレス** バーに、次のように入力します。

`https://[<iDRAC IPv6 アドレス>]`

次に、<Enter> キーを押します。

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

`https://<iDRAC IP アドレス>:<ポート番号>`

iDRAC IP アドレス は iDRAC6 用の IP アドレスで、*ポート番号* は HTTPS ポート番号です。

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

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

`https://<iDRAC IP アドレス>:<ポート番号>`

iDRAC IP アドレス は iDRAC6 用の IP アドレスで、*ポート番号* は HTTPS ポート番号です。

iDRAC6 **ログイン** ウィンドウが表示されます。

ログイン

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

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

ログインするには、次の手順に従ってください。

1 ユーザー名 フィールドに、次のいずれかを入力します。

- iDRAC6 ユーザー名。

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

- Active Directory ユーザー名。

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

2 パスワード フィールドに、iDRAC6 のユーザーパスワードまたは Active Directory のユーザーパスワードを入力します。パスワードでは大文字と小文字が区別されます。

3 ドメイン ドロップダウンボックスから、この iDRAC を選択して iDRAC6 ユーザーとしてログインするか、利用可能ないずれかのドメインを選択して Active Directory ユーザーとしてログインします。

メモ : Active Directory ユーザーの場合、ユーザー名の一部としてドメイン名を指定した場合は、ドロップダウンメニューから この iDRAC を選択します。

4 **OK** をクリックするか、<Enter> キーを押します。

ログアウト

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

2 ブラウザウィンドウを閉じます。

メモ : ログインするまで **ログアウト** ボタンは表示されません。

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

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

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

複数のブラウザタブとウィンドウの使用

新しいタブやウィンドウを開いたときのウェブブラウザの動作は、バージョンによって異なります。Microsoft Internet Explorer バージョン 7 およびバージョン 8 では、タブとウィンドウを開くオプションがあります。

タブは、最後に開いたタブの特性を継承します。

<Ctrl-T> を押してアクティブなセッションから新しいタブを開き、再度ログインします。

<Ctrl-N> を押して、アクティブなセッションから新規のブラウザウィンドウを開きます。すでに認証済みの資格情報でログインされます。

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。

また、タブのひとつにパワーユーザー権限でログインし、その後別のタブにシステム管理者としてログインすると、最初のログインの権限が両タブで取得されます。

Mozilla Firefox 3 のタブ動作は、Microsoft Internet Explorer バージョン 7 およびバージョン 8 と同じです。

表 4-1. 対応ブラウザでのユーザー権限動作

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

iDRAC6 NIC の設定

ここでは、iDRAC6 が設定済みで、ネットワーク上でアクセス可能であると想定しています。iDRAC6 ネットワークの初期設定については、34 ページの「iDRAC6 の設定」を参照してください。

ネットワークと IPMI LAN の設定

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

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

メモ : スパニングツリープロトコル（STP）を有効にして実行している場合は、PortFast または同様のテクノロジも、次のとおり有効になっていることを確認してください。
- iDRAC6 に接続しているスイッチのポート上
- iDRAC 仮想コンソールセッションを実行中の管理ステーションに接続しているポート上

メモ : POST 中にシステムが停止した場合は、「続行するには `F1` キー、システムセットアッププログラムを実行するには `F2` を押してください」というメッセージが表示される可能性があります。このエラーの原因としては、iDRAC6 との通信喪失を引き起こすネットワークストームイベントが考えられます。ネットワークストームがおさまった後、システムを再起動します。

1 **iDRAC の設定** → **ネットワーク / セキュリティ** → **ネットワーク** とクリックします。

2 **ネットワーク** ページでは、ネットワーク設定、共通 iDRAC6 設定、IPv4 設定、IPv6 設定、IPMI 設定、VLAN 設定を入力できます。これらの設定については、表 4-2、表 4-3、表 4-4、表 4-5、表 4-6、表 4-7 を参照してください。

3 必要な設定を入力した後、**適用** をクリックします。

ネットワークページで行った新規設定が保存されます。

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。

表 4-2. ネットワークの設定

設定	説明
NIC 選択	次の 4 つのモードから現在のモードを設定します。 • 専用 • 共有（LOM1） • フェールオーバー付きで共有（LOM2） • フェールオーバー付きで共有（すべての LOM） **メモ：専用** オプションは、iDRAC Enterprise カード用にしか使用できず、**すべての LOM のフェイルオーバーと共有** オプションは数個のシステムでしか使用できないことがあります。 **NIC の選択** が **共有** または フェイルオーバー付きで共有 モードの場合、iDRAC6 は同じ物理ポート経由でローカル通信を行いません。これは、ネットワークスイッチがパケットを受信したポートと同じポートからパケットを送信しないからです。 NIC の選択が **共有とフェイルオーバー**（LOM 2 またはすべての LOM）に設定されている場合は、LOM を別のネットワークブロードキャストドメインに接続しないことを推奨します。 iDRAC が共有モードに設定されている場合は、LOM をネットワークコントローラのアドインとチーミングしないことを推奨します。LOM 間のどのタイプのチームも、NIC 選択モードにかかわらず受け入れられます（共有 / 共有とフェイルオーバー LOM2/ 共有とフェイルオーバー全 LOM）。
MAC アドレス	ネットワークの各ノードを固有に識別するメディアアクセスコントロール（MAC）アドレスを表示します。
NIC を有効にする	選択すると、NIC が有効になり、このグループの残りのコントロールがアクティブになることを示します。NIC が無効になっている場合は、ネットワーク経由の iDRAC6 とのすべての通信がブロックされます。 デフォルトは、**オン** です。

表 4-2. ネットワークの設定 （続き）

設定	説明
オートネゴシエーション	**オン** に設定した場合は、最も近いルーターまたはスイッチと通信してネットワーク速度とモードを表示します。**オフ** に設定した場合は、ネットワーク速度と二重モードを手動で設定できます。 **NIC の選択** が **専用** に設定されて*いない*場合は、オートネゴシエーションは常に有効になります **（オン）**。 **メモ：**このサービスがオフのとき、内蔵 LOM ポートは最大速度 100Mbps をサポートします。このため、LOM とスイッチがオートネゴシエイションをサポートするように設定することで、システムの電源移行中の iDRAC の接続性を確保できます。
ネットワーク速度	ネットワーク環境に合わせて、ネットワーク速度を 100 Mb または 10 Mb に設定することができます。このオプションは、オートネゴシエーションが **オン** に設定されているときは使用できません。
二重モード	ネットワーク環境に合わせて、二重モードを全二重または半二重に設定することができます。**オートネゴシエーション が オン** の場合、このオプションは使用できません。
NIC MTU	NIC で最大転送ユニット（MTU）サイズを設定できます。

表 4-3. 共通設定

設定	説明
DNS に iDRAC を登録	DNS サーバーに iDRAC6 の名前を登録します。 デフォルトは **無効** です。
DNS iDRAC 名	**DNS に iDRAC を登録** が選択されている場合にのみ、iDRAC6 名を表示します。デフォルト名は idrac-サービス　タグで、サービス　タグは Dell サーバーのサービスタグ番号を示します。 例：idrac-00002
ドメイン名を自動設定	デフォルトの DNS ドメイン名を使用します。このチェックボックスがオフで、**DNS に iDRAC を登録** オプションがオンの場合は、**DNS ドメイン名** フィールドで DNS ドメイン名を変更します。 デフォルトは **無効** です。
DNS ドメイン名	デフォルトの **DNS ドメイン名** は空白です。**ドメイン名の自動設定** チェックボックスがオンになっている場合、この オプションは無効です。

表 4-4. IPv4 の設定

設定	説明
IPv4 を有効にする	NIC を有効にすると、IPv4 プロトコルサポートが選択され、このセクションの他のフィールドが有効に設定されます。
DHCP 有効	iDRAC6 に動的ホスト構成プロトコル（DHCP）サーバーから NIC 用の IP アドレスを取得するように指示します。デフォルトは **オフ** です。
IP アドレス	iDRAC6 の IC IP アドレスを指定します。
サブネットマスク	iDRAC6 NIC の静的 IP アドレスを入力または編集できます。この設定を変更するには、[DHCP を使用（NIC IP アドレス用）] チェックボックスをオフにします。
ゲートウェイ	ルーターまたはスイッチのアドレス この値は「ドット区切り」の形式です。例：192.168.0.1
DHCP を使用して DNS サーバーアドレスを取得する	**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオンにし、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、**優先 DNS サーバー** フィールドと **代替 DNS サーバー** フィールドに IP アドレスを入力します。 デフォルトは **オフ** です。 **メモ : DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスがオンの場合は、**優先 DNS サーバー** フィールドと **代替 DNS サーバー** フィールドに IP アドレスを入力できません。
優先 DNS サーバー	DNS サーバーの IP アドレス
代替 DNS サーバー	代替 DNS サーバーの IP アドレス

表 4-5. IPv6 の設定

設定	説明
IPv6 を有効にする	チェックボックスをオンにした場合は、IPv6 が有効になります。チェックボックスをオフにした場合は、IPv6 が無効になります。デフォルトは無効です。
自動構成有効	iDRAC6 で、動的ホスト構成プロトコル（DHCPv6）サーバーの IPv6 アドレスを取得できるようにするには、このボックスをオンにします。また、自動構成を有効にすると、IP アドレス 1、プレフィックス長、および IP ゲートウェイの静的な値を非アクティブにして削除します。

表 4-5. IPv6 （続き）の設定

設定	説明
IP アドレス 1	iDRAC NIC の IPv6 アドレスを設定します。この設定を変更するには、まず関連するチェックボックスをオフにして **自動設定** を無効にする必要があります。
プレフィックス長	IPv6 アドレスのプレフィックス長を設定します。この値は 1 ～ 128 です。この設定を変更するには、まず関連するチェックボックスをオフにして **自動設定** を無効にする必要があります。
ゲートウェイ	iDRAC NIC の静的ゲートウェイを設定します。この設定を変更するには、まず関連するチェックボックスをオフにして **自動設定** を無効にする必要があります。
リンクのローカルアドレス	iDRAC6 NIC リンクのローカル IPv6 アドレスを指定します。
IP アドレス 2 ～ 15	追加の iDRAC6 NIC IPv6 アドレスがある場合は、それも指定します。
DHCP を使用して DNS サーバーアドレスを取得する	**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオンにし、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、**優先 DNS サーバー** フィールドと **代替 DNS サーバー** フィールドに IP アドレスを入力します。 デフォルトは オフ です。 **メモ : DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスがオンの場合は、**優先 DNS サーバー** フィールドと **代替 DNS サーバー** フィールドに IP アドレスを入力できません。
優先 DNS サーバー	優先 DNS サーバーの静的 IPv6 アドレスを設定します。この設定を変更するには、まず **DHCP を使用して DNS サーバーアドレスを取得する** をオフにする必要があります。
代替 DNS サーバー	代替 DNS サーバーの静的 IPv6 アドレスを設定します。この設定を変更するには、まず **DHCP を使用して DNS サーバーアドレスを取得する** をオフにする必要があります。

表 4-6. IPMI 設定

設定	説明
IPMI オーバー LAN を有効にする	このチェックボックスがオンになっていると、IPMI LAN チャネルが有効であることを示します。デフォルトは **オフ** です。

表 4-6. IPMI 設定

設定	説明
チャネル権限レベルの制限	LAN チャネル上で許可されるユーザーの最小権限レベルを設定します。**システム管理者、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	暗号キーの文字形式の設定では、0 ～ 20 の 16 進数の文字を使用します（空白は使用できません）。デフォルト設定は、すべてゼロです。

表 4-7. VLAN の設定

設定	説明
VLAN ID 有効	有効である場合、一致する仮想 LAN（VLAN）ID トラフィックのみが受け入れられます。
VLAN ID	802.1g フィールドの VLAN ID フィールド。VLAN ID の有効値を入力します（1 ～ 4094 の値を指定する必要があります）。
優先度	802.1g フィールドの 優先度 フィールド。0 ～ 7 の値を入力して、VLAN ID の優先度を設定します。

IP フィルタおよび IP ブロックの設定

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

1. **iDRAC の設定** → **ネットワーク / セキュリティ** をクリックしてから、**ネットワーク** タブをクリックして **ネットワーク** ページを開きます。
2. **詳細設定** をクリックして、ネットワークセキュリティ設定を行います。
   表 4-8 で、**ネットワークセキュリティ ページの設定** について説明します。
3. 設定後、**適用** をクリックします。
   ネットワークセキュリティ ページに追加された新規設定を保存します。

表 4-8. ネットワークセキュリティページの設定

設定	説明
IP 範囲有効	IP 範囲のチェック機能を有効します。これにより、iDRAC にアクセスできる IP アドレスの範囲を定義できます。デフォルトは **オフ** です。

表 4-8. ネットワークセキュリティページの設定 （続き）

設定	説明
IP 範囲のアドレス	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。可能な IP アドレスの上位部分を決定するため、この値は IP 範囲サブネットマスクとビット単位で AND されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインには失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0 ～ 192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。デフォルトは **255.255.255.0** です。
IP ブロック有効	事前に選択した時間枠で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。デフォルトは **オフ** です。
IP ブロックエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。デフォルトは **10** です。
IP ブロックのエラーウィンドウ	ここで指定した時間枠（秒）内に IP ブロックエラーカウントが制限値を超えると、IP ブロックペナルティ時間がトリガされます。デフォルトは **3600** です。
IP ブロックのペナルティ時間	ログイン失敗回数が制限値を超えた IP アドレスからのログインを拒否する時間を秒で指定します。デフォルトは **3600** です。

プラットフォームイベントの設定

プラットフォームイベントの設定では、特定のイベントメッセージに対して iDRAC6 が選択した処置を実行するように設定します。処置には、処置の必要なし、システムの再起動、システムの電源を入れなおす、システムの電源を切る、アラートの生成（プラットフォームイベントトラップ [PET]、E- メール）があります。

表 4-9 に、フィルタ可能なプラットフォームイベントを示します。

表 4-9. プラットフォームイベントフィルタ

索引	プラットフォームイベント
1	ファン重要アサート
2	バッテリ警告アサート
3	バッテリ重要アサート

表 4-9. プラットフォームイベントフィルタ （続き）

索引	プラットフォームイベント
4	電圧重要アサート
5	温度警告アサート
6	温度重要アサート
7	侵入重要アサート
8	冗長性低下
9	冗長性喪失
10	プロセッサ警告アサート
11	プロセッサ重要アサート
12	プロセッサ不在重要アサート
13	電源供給警告アサート
14	電源供給重要アサート
15	電源供給不在重要アサート
16	イベントログ重要アサート
17	ウォッチドッグ重要アサート
18	システム電源警告アサート
19	システム電源重要アサート
20	リムーバブルフラッシュメディア不在情報アサート
21	リムーバブルフラッシュメディア重要アサート
22	リムーバブルフラッシュメディア警告アサート

プラットフォームイベント（たとえば、バッテリ警告アサート）が発生すると、システムイベントが生成され、システムイベントログ（SEL）に記録されます。このイベントが、有効になっているプラットフォームイベントフィルタ（PEF）と一致し、アラート（PET または E- メール）を生成するようにフィルタを設定している場合は、1 つまたは複数の設定されている送信先に PET または E- メールアラートが送信されます。

同じプラットフォームイベントフィルタで別の処置（システムの再起動など）を実行するように設定すると、その処置が実行されます。

プラットフォームイベントフィルタ（PEF）の設定

メモ : プラットフォームイベントトラップまたは E- メールアラートを設定する前に、プラットフォームイベントフィルタを設定してください。

1 対応ウェブブラウザを使ってリモートシステムにログインします。43 ページの「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** → **アラート** → **プラットフォームイベント** を順にクリックします。

3 **プラットフォームのイベントフィルタ設定** で、**有効** オプションを選択して **プラットフォームのイベントフィルタアラート** を有効にします。

メモ : 設定されている有効な送信先（PET または E- メール）にアラートを送信するためには、**プラットフォームイベントフィルタアラートを有効にする** を有効にする必要があります。

4 **プラットフォームのイベントフィルタリスト** の表で、設定するフィルタに対して次を行います。

- 次の処置の 1 つを選択します。
  - システムの再起動
  - システムのパワーサイクル
  - システムの電源を切る
  - 処置の必要なし
- **一般アラート** 列で、チェックボックスを選択してアラート生成を有効にするか、チェックボックスを選択解除してアラート生成を無効にします。

メモ : 設定されている有効な宛先（PET）にアラートを送信するためには、**アラートの生成** を有効にする必要があります。

5 **適用** をクリックします。設定が保存されます。

プラットフォームイベントトラップ（PET）の設定

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

1 対応ウェブブラウザを使ってリモートシステムにログインします。

2 53 ページの「プラットフォームイベントフィルタ（PEF）の設定」の手順を実行したことを確認してください。

3 **システム** → **アラート** → **トラップ設定** の順にクリックします。

4 IPv4 **送信先リスト** または **IPv6 送信先リスト** で、**送信先番号**に対して次を行って IPv4 または IPv6 SNMP アラート送信先を設定します。

a **状態** チェックボックスを選択または選択解除します。チェックボックスがオンになっていると、アラート受信用の IP アドレスが有効になっていることを示しています。チェックボックスがオフの場合は、アラート受信用の IP アドレスが無効になっていることを示しています。

b **送信先 IPv4 アドレス** または **送信先 IPv6 アドレス** に有効なプラットフォームイベントトラップ送信先の IP アドレスを入力します。

c **テストトラップ** で **送信** をクリックしてアラートを設定します。

メモ : テストトラップを送信するには、ユーザーアカウントに **テストアラート** 権限が必要です。詳細については、表 6-6 を参照してください。

指定した変更は、IPv4 または IPv6 の**送信先リスト**に表示されます。

5 **コミュニティ文字列** フィールドに iDRAC SNMP コミュニティ名を入力します。

メモ : 送信先コミュニティ文字列は iDRAC6 コミュニティ文字列と同じである必要があります。

6 **適用** をクリックします。設定が保存されます。

メモ : プラットフォームのイベントフィルタを無効にすると、問題が発生しているそのセンサーに関連するトラップも無効になります。**プラットフォームのイベントフィルタアラートの有効化** オプションが有効になっていると、「不良な状態から正常な状態へ」の処理にかかわるトラップが常に生成されます。たとえば、**リムーバブルフラッシュメディア不在情報アサートフィルタ** の **アラートの生成** オプションを無効にし SD カードを取り出すと、関連するトラップは表示されません。SD カードを再度挿入すると、トラップが生成されます。一方、**プラットフォームイベントフィルタアラートの有効化** オプションを有効にすると、SD カードを取り外すか挿入するときにトラップが生成されます。

E- メールアラートの設定

メモ : メールサーバーが Microsoft Exchange Server 2007 である場合、iDRAC から E- メールアラートを受け取るためには、そのメールサーバー用に iDRAC ドメイン名が設定されていることを確認してください。

メモ : E- メールアラートは IPv4 および IPv6 の両方のアドレスをサポートしています。

1 対応ウェブブラウザを使ってリモートシステムにログインします。

2 53 ページの「プラットフォームイベントフィルタ（PEF）の設定」の手順を実行したことを確認してください。

3 **システム** → **アラート** → **E- メールアラート設定** の順にクリックします。

4 **送信先の E- メールアドレス** の表で次を行って、**E- メールアラート番号**の受信先アドレスを設定します。

a **状態** チェックボックスを選択または選択解除します。チェックボックスがオンになっていると、アラート受信用の E- メールアドレスが有効になっていることを示しています。チェックボックスがオフの場合は、アラートメッセージ受信用の E- メールアドレスが無効になっていることを示しています。

b **送信先 E- メールアドレス** フィールドに有効な E- メールアドレスを入力します。

c **E- メールの説明** フィールドに短い説明を入力します。

5 **テスト E- メール** で **送信** をクリックし、設定した E- メールアラートをテストします。

6 **SMTP（E- メール）サーバー IP アドレス** フィールドで、設定に使用される SMTP サーバーの有効な IP アドレスまたは FQDN（完全修飾ドメイン名）を入力します。

メモ : テストメールの送信に成功するには、**SMTP（E- メール）サーバー IP アドレス**は、**E- メールアラート設定** ページで設定する必要があります。SMTP サーバーは設定した IP アドレスを使用して iDRAC6 と通信し、プラットフォームイベントが発生したときに E- メールアラートを送信します。

7 **適用** をクリックします。設定が保存されます。

ウェブインタフェースを使った IPMI の設定

1 対応ウェブブラウザを使ってリモートシステムにログインします。

2 IPMI オーバー LAN を設定します。

a **システム** ツリーで、**iDRAC の設定** をクリックします。

b **ネットワーク / セキュリティ** タブをクリックして **ネットワーク** をクリックします。

c **ネットワーク** ページの **IPMI 設定** で **IPMI オーバー LAN を有効にする** を選択して **適用** をクリックします。

d 必要に応じて IPMI LAN チャネル権限を更新します。

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

IPMI 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。

暗号化キー フィールドの **IPMI LAN 設定** に暗号化キーを入力して、**適用** をクリックします。

メモ : 暗号鍵は 40 文字までの偶数の 16 進数で指定します。

3 IPMI シリアルオーバー LAN （SOL）を設定します。

a **システム** ツリーで、**iDRAC の設定** をクリックします。

b **ネットワーク / セキュリティ** タブをクリックして、**シリアルオーバー LAN** をクリックします。

c **シリアルオーバー LAN** ページで **シリアルオーバー LAN を有効にする** を選択します。

d IPMI SOL ボーレートを更新します。

メモ : シリアルコンソールを LAN 経由でリダイレクトするには、SOL ボーレートが管理下システムのボーレートと同じであることを確認してください。

e **ボーレート** ドロップダウンメニューをクリックして、適切なボーレートを選択し、**適用** をクリックします。

f 最低限必要な権限を更新します。このプロパティは、**シリアルオーバー LAN** 機能を使うために 最低限必要なユーザー権限を定義します。

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

g **適用** をクリックします。

4 IPMI シリアルを設定します。

a **ネットワーク / セキュリティ** タブで、**シリアル** をクリックします。

b **シリアル** メニューで、IPMI シリアル接続モードを適切な設定に変更します。

IPMI シリアル の **接続モードの設定** ドロップダウンメニューで適切なモードを選択します。

c IPMI シリアルボーレートを設定します。

ボーレート ドロップダウンメニューをクリックして、適切なボーレートを選択し、**適用** をクリックします。

d **チャネル特権レベルの制限** と **フロー制御** を設定します。

e **適用** をクリックします。

f 管理下システムの BIOS セットアッププログラムでシリアル MUX が正しく設定されていることを確認します。

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

IPMI シリアルが端末モードの場合は、次の設定を追加できます。

- 削除制御
- エコー制御
- 行編集

- 改行シーケンス
- 改行シーケンスの入力

これらのプロパティの詳細については、IPMI 2.0 規格を参照してください。ターミナルモードコマンドの追加情報については、**dell.com/support/manuals** の『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

iDRAC6 ユーザーの設定

詳細については、115 ページの「iDRAC6 ユーザーの追加と設定」を参照してください。

SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保

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

- SSL（セキュアソケットレイヤー）
- 証明書署名要求（CSR）
- ウェブインタフェースを介した SSL へのアクセス
- CSR の生成
- サーバー証明書のアップロード
- サーバー証明書の表示

SSL（セキュアソケットレイヤー）

iDRAC6 には、業界標準の SSL セキュリティプロトコルを使用してネットワーク上で暗号化データを送信するように設定されたウェブサーバーが含まれています。公開キーと秘密キーの暗号化技術を基盤とする SSL は、ネットワークでの盗聴を防ぐためにクライアントとサーバー間に認証された暗号化通信を提供する技術として広く普及しています。

SSL 対応システムは、次のタスクを実行できます。

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

暗号化プロセスは高度なデータ保護を提供します。iDRAC6 では、北米のインターネットブラウザで一般的に使用されている最も安全な暗号化方式である 128 ビットの SSL 暗号化標準を採用しています。

iDRAC6 のウェブサーバーは、デフォルトで Dell の署名入り SSL デジタル証明書（サーバー ID）を提供します。インターネット上で高いセキュリティを確保するには、ウェブサーバーの SSL 証明書を、著名な認証局によって署名された証明書で置き換えてください。署名された証明書を取得するには、まず、iDRAC6 ウェブインタフェースを使用して企業情報を掲載した証明書署名要求（CSR）を生成します。生成した CSR を VeriSign や Thawte などの 認証局（CA）に送信します。

証明書署名要求（CSR）

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

認証局（CA）は、IT 業界で認知されたビジネス組織で、信頼性の高い審査、身元確認、その他の重要なセキュリティ要件を満たしています。CA には、Thawte や VeriSign などがあります。CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ基準を満たしていれば、ネットワークやインターネット上でトランザクションを行う申請者を個別に識別するデジタル署名付き証明書を発行します。

CA が CSR を承認して証明書を送信したら、それを iDRAC6 ファームウェアにアップロードします。iDRAC6 ファームウェアに保管されている CSR 情報は、証明書に記載されている情報と一致する必要があります。

ウェブインタフェースを介した SSL へのアクセス

1. **iDRAC の設定** → **ネットワーク / セキュリティ** とクリックします。
2. **SSL** をクリックして **SSL** ページを開きます。

SSL ページを使用して次のいずれかのオプションを実行します。

- CA に送信する証明書署名要求（CSR）を生成する。CSR 情報は iDRAC6 ファームウェアに保存されています。
- サーバー証明書をアップロードする。
- サーバー証明書を表示する

表 4-10 では、上記の **SSL** ページのオプションについて説明しています。

表 4-10. SSL ページのオプション

フィールド	説明
証明書署名要求（CSR）の生成	このオプションにより、CA に送信する安全なウェブ証明書を要求するための CSR を生成できます。 **メモ：**新しい CSR は、ファームウェアにある古い CSR を上書きします。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。
サーバー証明書のアップロード	このオプションにより、会社が保有する既存の証明書をアップロードし、iDRAC6 へのアクセス制御に利用できます。 **メモ：**iDRAC6 で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER でエンコードされた証明書は受け入れられません。新しい証明書をアップロードすると、iDRAC6 て受信したデフォルトの証明書が置き換えられます。
サーバー証明書の表示	このオプションにより、既存のサーバー証明書を表示できます。

証明書署名要求の生成

1. **SSL** ページで、**証明書署名要求（CSR）の生成** を選択し、**次へ** をクリックします。
2. **証明書署名要求（CSR）の生成** ページで、各 CSR 属性の値を入力します。表 4-11 では、CSR 属性について説明しています。
3. **生成** をクリックして CSR を作成し、お使いのローカルコンピュータへダウンロードして、指定のディレクトリに保存します。
4. **SSL メインメニューに戻る** をクリックして SSL ページに戻ります。

表 4-11. 証明書署名要求（CSR）属性の生成

フィールド	説明
共通名	証明される名前（通常は **xyzcompany.com** のような iDRAC のドメイン名）。英数字、ハイフン、ピリオドが有効です。
組織名	この組織に関連付けられた名前（たとえば「XYZ Corporation」）。英数字、ハイフン、ピリオドが有効です。
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、ピリオドが有効です。

表 4-11. 証明書署名要求（CSR）属性の生成 （続き）

フィールド	説明
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、ハイフン、ピリオドが有効です。
状態名	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、ハイフン、ピリオドが有効です。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。
E- メール	CSR に関連付けられている E- メールアドレス。組織の E- メールアドレスまたは CSR に関連付ける E- 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。

サーバー証明書のアップロード

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

   サーバー証明書のアップロード ページが表示されます。

2. **ファイルパス** フィールドの **値** フィールドに証明書のパスを入力するか、**参照** をクリックして証明書ファイルに移動します。

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

3. **適用** をクリックします。
4. **SSL メインメニューに戻る** をクリックして **SSL メインメニュー** ページに戻ります。

サーバー証明書の表示

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

   サーバー証明書の表示 ページは、iDRAC へアップロードしたサーバー証明書を表示します。

   表 4-12 に、**証明書** テーブルに表示されるフィールドと関連する説明を記載してします。

2. **SSL メインメニューに戻る** をクリックして **SSL メインメニュー** ページに戻ります。

表 4-12. 証明書情報

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	対象者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

Active Directory の設定と管理

このページでは、Active Directory 設定の設定と管理ができます。

メモ : Active Directory を使用または設定するには、**iDRAC の設定**権限が必要です。

メモ : Active Directory の機能を設定または使用する前に、Active Directory サーバーと iDRAC6 が通信できるように設定されていることを確認してください。

メモ : Active Directory 設定の詳細および拡張スキーマまたは標準スキーマによる Active Directory の設定方法については、129 ページの「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 の設定と管理 ページにアクセスするには、次の手順を実行してください。

1. **iDRAC の設定** → **ネットワーク / セキュリティ** とクリックします。
2. **Active Directory** をクリックして **Active Directory の設定と管理** ページを開きます。

   表 4-13 に、**Active Directory の設定と管理** ページのオプションを示します。
3. **Active Directory の設定** をクリックして Active Directory を設定します。詳細な設定の情報は、129 ページの「iDRAC6 ディレクトリサービスの使用」を参照してください。
4. **テスト設定** をクリックして、指定した設定を使用した Active Directory 設定のテストを行います。テスト設定オプションの使用についての詳細は、129 ページの「iDRAC6 ディレクトリサービスの使用」を参照してください。

表 4-13. Active Directory の設定と管理 ページのオプション

属性	説明
共通設定	
Active Directory が有効	Active Directory が有効か無効かを指定します。
シングルサインオンが有効	シングルサインオンが有効か無効かを指定します。有効の場合は、ユーザー名やパスワードなどのドメインユーザー資格情報を入力せずに、iDRAC6 にログインできます。チェックボックスを選択して、サインオンを有効にします。
スキーマの選択	Active Directory で標準スキーマが使用されているか拡張スキーマが使用されているかを指定します。 **メモ：**このリリースでは、Active Directory が拡張スキーマ用に設定されていると、スマートカードベースの 2 要素認証（TFA）機能はサポートされません。シングルサインオン（SSO）機能は標準と拡張スキーマの両方でサポートされています。
ユーザードメイン名	この値は最大 40 個のユーザードメインエントリを保持します。設定した場合、ログインユーザーが選択できるユーザードメイン名のリストがログインページのプルダウンメニューに表示されます。設定しなかった場合でも、Active Directory ユーザーは ユーザー名 @ ドメイン名、ドメイン名 / ユーザー名、または ドメイン名 \ ユーザー名 の形式でユーザー名を入力すると、ログインできます。
タイムアウト	Active Directory クエリが完了するまで待つ時間（秒）を指定します。デフォルト値は 120 秒です。
DNS を使用したドメインコントローラのルックアップ	**DNS を使用したドメインコントローラのルックアップ** 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、一つずつ接続を試みます。 **拡張スキーマ** を選択した場合、これらは iDRAC6 デバイスオブジェクトと関連オブジェクトが存在するドメインコントローラのアドレスです。**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。

表 4-13. Active Directory の設定と管理 ページのオプション （続き）

属性	説明
ドメインコントローラーサーバーアドレス 1-3（FQDN または IP）	ドメインコントローラーの完全修飾ドメイン名（FQDN）または IP アドレスを指定します。3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。拡張スキーマを選択した場合、これらは iDRAC6 デバイスオブジェクトと関連オブジェクトが存在するドメインコントローラーのアドレスです。標準スキーマを選択した場合、これらはユーザーアカウントとロールグループが存在するドメインコントローラのアドレスです。
証明書検証が有効	iDRAC6 は Active Directory への接続中に、セキュアソケットレイヤ（SSL）を使用します。デフォルト設定では、iDRAC6 はセキュリティソケットレイヤ（SSL）のハンドシェーク中、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ーのセキュリティソケットレイヤ（SSL）サーバー証明書を検証し、強力なセキュリティを提供します。テスト目的の場合や、システム管理者が SSL（セキュリティソケットレイヤ）証明書を検証せずにセキュリティ境界内のドメインコントローラーを信頼することにした場合は、証明書の検証を無効にできます。このオプションは、証明書の検証を有効にするか無効にするかを指定します。
Active Directory CA 証明書	
証明書	すべての ドメインコントローラーの SSL（セキュリティソケットレイヤ）サーバー証明書に署名する認証局の証明書。
拡張スキーマの設定	**iDRAC 名**：Active Directory 内の iDRAC を一意に 識別する名前を指定します。この値はデフォルトでは NULL になっています。 **iDRAC ドメイン名**：Active Directory iDRAC オブジェクトが存在するドメインの DNS 名（文字列）。この値はデフォルトでは NULL になっています。 これらの設定は、拡張 Active Directory スキーマで iDRAC を使用するように設定されている場合にのみ表示されます。

表 4-13. Active Directory の設定と管理 ページのオプション （続き）

属性	説明
標準スキーマ設定	**グローバルカタログサーバーアドレス 1-3（FQDN または IP）**：グローバルカタログサーバーの完全修飾ドメイン名（FQDN）または IP アドレスを指定します。3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。ユーザーアカウントと役割グループが異なるドメインにある場合に限り、標準スキーマにグローバルカタログサーバーが必要です。 **役割グループ**：iDRAC6 に関連する役割グループのリストを指定します。 **グループ名** ：iDRAC6 に関連付けられている Active Directory の役割グループを識別する名前を指定します。 **グループドメイン**：グループドメインを指定します。 **グループ特権**：グループ特権レベルを指定します。 これらの設定は、標準 Active Directory スキーマで iDRAC を使用するように設定されている場合にのみ表示されます。 DNS の**ルックアップグローバルカタログサーバー** 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、一つずつ接続を試みます。ユーザーアカウントと役割グループが異なるドメインにある場合に限り、標準スキーマにグローバルカタログサーバーが必要です。

汎用 LDAP の設定と管理

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。汎用 LDAP ディレクトリサービスについては、160 ページの「汎用 LDAP ディレクトリサービス」を参照してください。

iDRAC6 サービスの設定

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

1. **iDRAC の設定** → **ネットワーク / セキュリティ** とクリックします。**サービス** タブをクリックして **サービス** 設定ページを表示します。
2. 必要に応じて、次のサービスを設定します。
   - ローカル設定 ー表 4-14 を参照。
   - ウェブサーバー — ウェブサーバーの設定については 表 4-15 を参照。
   - SSH — SSH 設定については 表 4-16 を参照。
   - Telnet — Telnet 設定については 表 4-17 を参照。
   - リモート RACADM — リモート RACADM 設定については 表 4-18 を参照。
   - SNMP — SNMP 設定については 表 4-19 を参照。
   - 自動システムリカバリ（ASR）エージェント — ASR エージェント設定については 表 4-20 を参照。
3. **適用** をクリックして **サービス** ページの設定を適用します。

表 4-14. ローカル設定

設定	説明
オプション ROM を使用して iDRAC ローカル設定を無効にする	オプションの ROM を使用して iDRAC のローカル設定を無効にします。オプションの ROM は BIOS 内にあり、BMC および iDRAC の設定を可能にするユーザーインタフェースエンジンを提供します。オプションの ROM は、<Ctrl+E> を押してセットアップモジュールを開始するよう指示します。
RACADM を使用して iDRAC ローカル設定を無効にする	ローカル RACADM を使用した iDRAC のローカル設定を無効にします。

表 4-15. ウェブサーバーの設定

設定	説明
有効	iDRAC ウェブサーバーを有効または無効にします。チェックボックスがオンの場合は、ウェブサーバーが有効であることを示します。デフォルトは **有効** です。
最大セッション数	このシステムで同時に許可される最大ウェブサーバーセッション数。このフィールドは編集できません。最大同時セッション数は 5 です。

表 4-15. ウェブサーバーの設定 （続き）

設定	説明
アクティブセッション数	システムの現在のセッション数（**最大セッション数** 以下）。このフィールドは編集できません。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更はすぐに適用され、現在のウェブインタフェースセッションが終了します。ウェブサーバーもリセットされます。新しいウェブインタフェースセッションが始まるまで数分お待ちください。タイムアウト範囲は 60 ～ 10800 秒です。デフォルト値は 1800 秒です。
HTTP ポート番号	ブラウザ接続で iDRAC6 が通信するポート。デフォルトは **80** です。
HTTPS ポート番号	セキュアなブラウザ接続で iDRAC6 が通信するポート。デフォルトは **443** です。

表 4-16. SSH の設定

設定	説明
有効	SSH を有効または無効にします。チェックボックスがオンの場合は、SSH が有効になります。
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。このフィールドは編集できません。 **メモ：**iDRAC6 は、最大 2 つの SSH セッションを同時にサポートします。
アクティブセッション数	システムの現在の SSH 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	セキュアシェルのアイドルタイムアウト（秒）。タイムアウト範囲は 60 ～ 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 4-17. Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。チェックボックスがオンの場合は、Telnet が有効になります。

表 4-17. Telnet の設定 （続き）

設定	説明
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。このフィールドは編集できません。 **メモ：**iDRAC6 は、最大 2 つの Telnet セッションを同時にサポートします。
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（**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	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 4-18. リモート RACADM の設定

設定	説明
有効	リモート RACADM を有効または無効にします。チェックボックスをオンにすると、リモート RACADM が有効になります。
アクティブセッション数	システムの現在の RACADM セッション数。このフィールドは編集できません。

表 4-19. 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。使用される SNMP コミュニティ文字列を定義します。コミュニティ名は最大 31 文字（スペースなし）まで指定できます。デフォルトは **public** です。

表 4-20. 自動システムリカバリエージェントの設定

設定	説明
有効	自動システムリカバリエージェントを有効または無効にします。選択した場合、自動システムリカバリエージェントが有効になります。

iDRAC6 ファームウェア / システムサービスリカバリイメージのアップデート

メモ : iDRAC6 ファームウェアのアップデートが完了する前に中断されるなどにより、iDRAC6 のファームウェアが破損した場合は、iDRAC6 ウェブインタフェースを使用して iDRAC6 を修復できます。

メモ : ファームウェアアップデートは、デフォルトで現在の iDRAC6 設定を保持します。アップデートプロセス中、iDRAC6 設定を工場出荷時のデフォルト設定にリセットできるオプションが用意されています。設定を工場出荷時のデフォルト設定に設定する場合は、iDRAC6 設定ユーティリティを使用してネットワークを設定する必要があります。

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

2 **i DRAC の設定** をクリックし、次に **アップデート** タブをクリックします。

3 **アップロード / ロールバック（手順 3 の 1）** ページで、**参照** をクリックして **support.dell.com** からダウンロードしたファームウェアイメージかシステムサービスリカバリイメージを選択します。

メモ : Firefox を実行している場合は、**ファームウェアイメージ** フィールドにテキストカーソルは表示されません。

たとえば、次のとおりです。

`C:\Updates\V1.0\<` *イメージ名* `>.`

または

`\\192.168.1.10\Updates\V1.0\<` *イメージ名* `>`

デフォルトのファームウェアイメージ名は **firmimg. d6** です。

4 **アップロード** をクリックします。

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

プロセスが完了するまで次のメッセージが表示されます。

ファイルアップロード中

5 **ステータス（ページ** 3 の 2）ページで、アップロードしたイメージファイルに対する検証結果が表示されます。

- システムリカバリイメージファイルのアップロードに成功し、すべての検証チェックに合格すると、システムリカバリイメージファイル名が表示されます。ファームウェアイメージをアップロードした場合は、現在のファームウェアと新しいファームウェアバージョンが表示されます。

  または

- イメージのアップロードに失敗した場合や、検証チェックに合格しなかった場合は、該当するエラーメッセージが表示され、アップデートが **アップロード / ロールバック（手順 1/3）**ページに戻ります。iDRAC6 のアップグレードを再試行するか、**キャンセル** をクリックして iDRAC を通常の動作モードにリセットします。

6 ファームウェアイメージの場合、**設定の保存** は既存の iDRAC6 設定を保存または消去するオプションを提供します。このオプションは、デフォルトでは選択されています。

メモ : 設定の保存 チェックボックスをオフにすると、iDRAC6 はデフォルト設定にリセットされます。デフォルト設定では、静的 IPv4 アドレスで LAN が有効になっています。iDRAC6 ウェブインタフェースにログインできない場合もあります。BIOS POST 時に、iDRAC6 設定ユーティリティを使用して、LAN 設定を再設定する必要があります。

7 **アップデート** をクリックして、アップデートプロセスを開始します。

8 **アップデート中（手順 3 の 3）**ページに、アップデートの状況が表示されます。アップグレードの進行状況は、**進行状況** 列にパーセントで表示されます。

メモ : アップデートモードでは、このページから移動してもアップデートプロセスはバックグラウンドで継続されます。

ファームウェアアップデートが成功した場合、iDRAC6 は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC6 に再接続する必要があります。エラーが発生した場合、該当するエラーメッセージが表示されます。

システムサービスリカバリのアップデートに成功または失敗した場合は、該当するステータスメッセージが表示されます。

iDRAC6 ファームウェアのロールバック

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

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

システム → **i DRAC の設定** とクリックし、次に **アップデート** タブをクリックします。

2 **アップロード / ロールバック（手順 3 の 1）**ページで、**ロールバック** をクリックします。現在およびロールバックのファームウェアバージョンが **ステータス（手順 3 の 2）**ページに表示されます。

設定の保存 で、iDRAC6 の既存の設定を保存するか消去するかを指定できます。このオプションは、デフォルトでは選択されています。

メモ : 設定の保存 チェックボックスをオフにすると、iDRAC6 はデフォルト設定にリセットされます。デフォルト設定では LAN は有効になっています。iDRAC6 ウェブインタフェースにログインできない場合もあります。BIOS POST 時に iDRAC6 設定ユーティリティを使用するか、RACADM コマンド（ローカルサーバー上で利用可能）を使用して LAN 設定を再設定する必要があります。

3 **アップデート** をクリックして、ファームウェアアップデートプロセスを開始します。

アップデート中（手順 3 の 3） ページに、ロールバック動作の状況が表示されます。進行度が **進行状況** 列にパーセントで表示されます。

メモ : アップデートモードでは、このページから移動してもアップデートプロセスはバックグラウンドで継続されます。

ファームウェアアップデートが成功した場合、iDRAC6 は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC6 に再接続する必要があります。

リモートシスログ

iDRAC6 Enterprise は、RAC 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る機能であるリモートシスログを提供します。中央ログからサーバーファームログのすべてを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（User Datagram Protocol）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。

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 4-21 はリモートシスログの設定一覧です。

表 4-21. リモートシスログの設定

属性	説明
リモートシスログ有効	指定したサーバーのシスログの転送とリモートキャプチャを有効にするには、このオプションを選択します。シスログが有効になると、新しいログエントリがシスログサーバーに送信されます。
シスログサーバー 1 ～ 3	SEL ログや RAC ログなどの iDRAC6 のログメッセージをログ記録するリモートシスログサーバーのアドレスを入力します。シスログサーバーのアドレスには英数字、「-」、「.」、「:」、および「_」記号を使用できます。
ポート番号	リモートシスログサーバーのポート番号を入力します。ポート番号は 1 ～ 65535 の範囲で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] ; デフォルトは 0

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer1 < サーバー名 1> ; デフォルトは空白

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer2 < サーバー名 2>; デフォルトは空白

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer3 < サーバー名 3>; デフォルトは空白

racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPort
< ポート番号 >; デフォルトは 514
```

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、**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。

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 4-22 は、**最初の起動デバイス** の設定をリストしています。

表 4-22. 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。
一回限りの起動	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 リモートファイル共有（RFS）機能を使うと、ネットワーク共有上にある ISO または IMG イメージファイルを指定し、ネットワークファイルシステム（NFS）または共通インターネットファイルシステム（CIFS）を使ってそれを CD/DVD またはフロッピーとしてマウントすることで、管理下サーバーのオペレーティングシステムから仮想ドライブとして使用できるようにすることができます。

CIFS 共有イメージパスのフォーマットは次のとおりです。

//<IP アドレスまたはドメイン名>/<イメージへのパス>

NFS 共有イメージパスのフォーマットは次のとおりです。

<IP アドレス>:/<イメージへのパス>

メモ : NFS を使用する場合、大文字と小文字の区別がなされるイメージファイル拡張子を含め、正確な < *イメージへのパス* > を指定するようにしてください。

メモ : *<IP アドレス>* には IPv4 アドレスを指定する必要があります。IPv6 アドレスは現在サポートされていません。

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

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

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

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

iDRAC6 ウェブインタフェースを介してリモートファイル共有を有効にするには、次のようにします。

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 ウェブインタフェースにログインします。
3. **システム** → **リモートファイル共有** タブの順に選択します。
   リモートファイル共有 画面が表示されます。

表 4-23 はリモートファイル共有の設定一覧です。

表 4-23. 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。
ステータス	**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 ...** ：共有への接続中です。

接続 をクリックして RFS に接続します。接続が確立されたら、**接続** 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*`>`

オプションは、次のとおりです。

- `-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

メモ : ユーザー名と**パスワード**の最大文字数は 40 文字で、**イメージファイルパス** は 511 文字です。これら 3 つのフィールドには、次を除く英数字と特殊文字を含むすべての文字を使用できます。

- '（一重引用符）
- "（二重引用符）
- ,（カンマ）
- <（より小さい）
- >（より大きい）

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、別の SD を最初の SD カードの内容のミラーとして使うことで、ハイパーバイザー SD の冗長性を提供します。2 番目の SD カードは、システム BIOS 設定の **内蔵デバイス** 画面で **冗長性** オプションを **ミラーモード** に設定することで他の SD カードと共に IDSDM に設定できます。IDSDM 用の BIOS オプション の詳細については、デルサポートサイト **dell.com/support/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 設定の **内蔵デバイス** 画面の **内蔵 USB ポート** オプションを **オン** にする必要があります。これを **オフ** に設定すると、IDSDM は起動デバイスとしてシステムから認識されません。

2 枚の SD カードのうちの一方をマスターにできます。たとえば、AC 電源がシステムから取り外されている間に IDSDM に 2 枚の SD カードが取り付けられた場合、SD1 がアクティブまたはマスターカードと見なされます。SD2 はバックアップカードで、すべての IDSDM 書き込みは両方のカードで行われますが、読み取りは SD1 のみで行われます。いつでも SD1 が故障するか取り外されると、SD2 は自動的にアクティブ（マスター）カードになります。ミラーモードでは vFlash SD カードは無効になります。

表 4-24. IDSDM の状態

IDSDM - ミラーモード	SD1 カード	SD2 カード	vFlash SD カード
有効	アクティブ	アクティブ	非アクティブ
無効	アクティブ	非アクティブ	アクティブ

iDRAC を使うと、IDSDM の状態、正常性、可用性を表示できます。

SD カードの冗長性状態とエラーイベントは SEL にログされ、LCD 画面に表示されて、PET アラートが生成されます（アラートが有効になってる場合）。

GUI を使って内蔵デュアル SD モジュールを表示する

1. iDRAC ウェブ GUI にログインします。
2. **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、次の 2 つのセクションが表示されます。

- **内蔵デュアル SD モジュール** — IDSDM が冗長モードのときにのみ表示されます。冗**長性状態が 完全** として表示されます。このセクションがない場合、カードは非冗長モード状態です。有効な**冗長性状態**の表示は次の通りです。
  - **完全** — SD カード 1 と 2 が正しく機能しています。
  - **喪失** — SD カードの一方または両方が正しく機能していません。
- **内蔵 SD モジュール状態** — SD1、SD2、vFlash カードの次の情報を含む SD カード状態を表示します。
  - 状態：
    -  — カードに異常がないことを示します。
    -  — カードがオフラインか書き込み禁止になっていることを示します。
    -  — アラートが発行されたことを示します。
  - 場所 — SD カードの場所を示します。

– オンライン状態 — SD1、SD2、vFlash カードは、表 4-25 に表示されている状態のいずれかになります。

表 4-25. SD カードの状態

SD カード	状態	説明
SD1 または SD2	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	カードは SD 読み取り / 書き込み要求を受け取る準備ができています。
	スタンバイ	カードがセカンダリカードです。SD 書き込みすべてのコピーを受け取っています。
	失敗	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 カードを検出できません。
	オフライン	起動時のカード識別（CID）署名は、不揮発性（NV）ストレージ値や進行中のコピー動作のコピー先とは異なります。
	書き込み禁止	カードは、SD カード上の物理ラッチによって書き込み禁止になっています。IDSDM では、書き込み禁止になっているカードは使用できません。
vFlash	アクティブ	カードは SD 読み取り / 書き込み要求を受け取る準備ができています。
	不在	SD カードを検出できません。

5

iDRAC6 の詳細設定

本項では、iDRAC6 の詳細設定について説明します。システム管理の知識が豊富なユーザーや、特定のニーズに応じて iDRAC6 環境をカスタマイズしたいユーザーは、本項をお読みになることをお勧めします。

作業を開始する前に

DRAC6 ハードウェアとソフトウェアの基本インストールと設定が完了していることを前提とします。詳細については、31 ページの「iDRAC6 の基本インストール」を参照してください。

リモート SSH/Telnet 経由でシリアル出力を表示するための iDRAC6 設定

次の手順を実行して、iDRAC6 でリモートシリアルコンソールを設定できます。

まず、BIOS を設定して、シリアルコンソールを有効にします。

1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に **<F2>** を押します。

   `<F2> = System Setup`
3. スクロールダウンし、**シリアル通信** を選択して **<Enter>** を押します。
4. **シリアル通信** 画面のオプションを次のように設定します。

   シリアル通信 `....com2` からのシリアルリダイレクト付きでオン に設定

   メモ : シリアルポートアドレス フィールドのシリアル device2 も com1 に設定されている限り、シリアル通信を **com1 からのシリアルリダイレクト付きでオン** に設定できます。

   シリアルポートアドレス `....` シリアルデバイス `1 = com1`、シリアルデバイス `2 = com2`

   外部シリアルコネクタ `....` シリアルデバイス `1`

   フェイルセーフボーレート `....115200`

   リモートターミナルタイプ `....vt100/vt220`

   起動後のリダイレクト `....` 有効

   次に、**変更を保存** を選択します。

5 **セットアップユーティリティ** を終了してシステムセットアッププログラムの設定を完了するには、<Esc> を押してください。

iDRAC6 で SSH/Telnet を有効にする設定

次に、iDRAC6 を設定して ssh/Telnet を有効にします。これは RACADM または iDRAC6 ウェブインタフェースからできます。

RACADM を使用して iDRAC6 で ssh/Telnet を有効にするには、次のコマンドを実行します。

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
```

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

リモートでも RACADM コマンドを実行できます。100 ページの「RACADM のリモート使用」を参照してください。

iDRAC6 のウェブインタフェース を使用して iDRAC6 で ssh/Telnet を有効にするには、次の手順に従います。

1 **システム** ツリーを展開して、**iDRAC の設定** をクリックします。
2 **ネットワーク / セキュリティ** タブをクリックして **サービス** をクリックします。
3 **SSH** または **Telnet** セクションの下にある **有効** を選択します。
4 **変更の適用** をクリックします。

次に、Telnet または SSH 経由で iDRAC6 に接続します。

Telnet または SSH を使用したテキストコンソールの起動

管理ステーションのターミナルソフトウェアから Telnet または SSH 経由で iDRAC6 にログインした後、Telnet/SSH コマンドの **console com2** を使用して、管理下システムのテキストコンソールをリダイレクトできます。一度に 1 つの **console com2** クライアントのみサポートされています。

管理下システムのテキストコンソールに接続するには、iDRAC6 コマンドプロンプトを開いて（Telnet または SSH セッションを通して表示）、次のように入力します。

```
console com2
```

`console -h com2` コマンドは、キーボードからの入力またはシリアルポートからの新しい文字を待つ前にシリアル履歴バッファの内容を表示します。

履歴バッファのデフォルト（最大）サイズは 8192 文字です。この値は、次のコマンドを使って小さくすることができます。

```
racadm config -g cfgSerial -o cfgSerialHistorySize
< 数値 >
```

起動中に Linux にコンソールダイレクトを設定するには、84 ページの「起動中に Linux にシリアルコンソールを設定する方法」を参照してください。

Telnet コンソールの使用

Windows XP または Microsoft Windows 2003 での Telnet の実行

管理ステーションで Windows XP または Windows 2003 が稼動している場合は、iDRAC6 Telnet セッションで文字の問題が発生する可能性があります。この問題はログインのフリーズとして表れ、Return キーが応答せず、パスワードプロンプトが表示されません。

この問題を解決するには、Microsoft のサポートウェブサイト **support.microsoft.com** から修正プログラム hotfix 824810 をダウンロードします。詳細については、Microsoft 技術情報の記事 824810 を参照してください。

Windows 2000 での Telnet の実行

管理ステーションで Windows 2000 が稼動している場合は、<F2> キーを押して BIOS セットアップにアクセスすることはできません。この問題は、Microsoft から無償でダウンロードできる UNIX 3.5 用の Windows サービスに同梱されている Telnet クライアントを使用すると解決できます。**microsoft.com/downloads/** にアクセスして、*Windows Services for UNIX 3.5* を検索してください。

Microsoft Telnet で Telnet 仮想コンソールを有効にする方法

メモ : Microsoft オペレーティングシステム上の一部の Telnet クライアントでは、BIOS 仮想コンソールを VT100/VT220 エミュレーションに設定した場合に BIOS セットアップ画面が正しく表示されないことがあります。この問題が発生した場合は、BIOS 仮想コンソールを ANSI モードに変更して表示を更新します。BIOS セットアップメニューでこの手順を実行するには、**仮想コンソール** ? **リモートターミナルの種類** ? **ANSI** を選択します。

メモ : クライアント VT100 エミュレーションウィンドウを設定するときにテキストを正しく表示するには、リダイレクトされた仮想コンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定してください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

1. **Windows コンポーネントサービス** で **Telnet** を有効にします。
2. 管理ステーションの iDRAC6 に接続します。

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

   `telnet <`*IP アドレス*`>:<`*ポート番号*`>`

   IP アドレスは iDRAC6 の IP アドレスで、ポート番号は Telnet ポート番号です（新しいポートを使用している場合）。

Telnet セッション用の Backspace キーの設定

一部の Telnet クライアントでは、<Backspace> キーを使用すると予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> キーを使用できるように設定するには、次の手順を実行してください。

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

   ```
   telnet
   ```

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

   ```
   set bsasdel
   ```

   次のメッセージが表示されます。

   ```
   Backspace が Delete として送信されます。
   ```

Linux Telnet セッションで <Backspace> キーを使用できるように設定するには、次の手順を実行してください。

1. コマンドプロンプトを開いて、次のように入力します。

   ```
   stty erase ^h
   ```
2. コマンドプロンプトで、次のように入力します。

   ```
   telnet
   ```

セキュアシェル（SSH）の使用

システムのデバイスとデバイス管理がセキュアであることは不可欠です。組み込み接続デバイスは多くのビジネスプロセスの中核となっています。これらのデバイスが危険に曝されると、ビジネスリスクが生じる可能性があるため、コマンドラインインタフェース（CLI）のデバイス管理ソフトウェアに新しいセキュリティ要件が求められます。

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セッションですが、セキュリティ面で Telnet より優れています。iDRAC6 は、パスワード認証付きの SSH バージョン 2 をサポートしています。iDRAC6 ファームウェアをインストールまたはアップデートすると、iDRAC6 上の SSH が有効になります。

管理ステーション上では、PuTTY または OpenSSH を使用して、管理下システムの iDRAC6 に接続できます。ログイン中にエラーが発生すると、セキュアシェルクライアントでエラーメッセージが表示されます。メッセージのテキストはクライアントによって異なり、iDRAC6 で制御することはできません。

メモ : OpenSSH は Windows の VT100 または ANSI ターミナル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）。

一度に最大 2 つの SSH セッションのみがサポートされます。デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』で説明されているように、セッションタイムアウトは cfgSsnMgtSshIdleTimeout プロパティで制御されています。

iDRAC6 で SSH を有効にするには、次のように入力します。

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

SSH ポートを変更するには、次のように入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort
< ポート番号 >
```

cfgSerialSshEnable と cfgRacTuneSshPort プロパティの詳細については、デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』を参照してください。

iDRAC6 SSH の実装では、表 5-1 に示すように複数の暗号化スキームがサポートされています。

表 5-1. 暗号化スキーム

スキーマの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024（ランダム）ビット（NIST 仕様）
対称暗号	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128

表 5-1. 暗号化スキーム （続き）

スキーマの種類	スキーム
メッセージの整合性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	• パスワード

メモ : SSHv1 はサポートされていません。

起動中に Linux にシリアルコンソールを設定する方法

次は、Linux GRand Unified Bootloader（GRUB）に固有の手順です。別のブートローダを使用する場合も、同様の変更が必要になる可能性があります。

メモ : クライアント VT100 エミュレーションウィンドウを設定するときにテキストを正しく表示するには、リダイレクトされた仮想コンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定してください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

/etc/grub.conf ファイルを次のように編集します。

1. ファイルの 全般設定 セクションを見つけて、次の 2 行を追加します。

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2. カーネル行に次の 2 つにオプションを追加します。

```
kernel .............console=ttyS1,115200n8r
console=tty1
```

3. **/etc/grub.conf** に `splashimage` ディレクティブがある場合は、コメントアウトします。

表 5-2 に、この手順で説明する変更を示したサンプル **/etc/grub.conf** ファイルがあります。

表 5-2. サンプルファイル：/etc/grub.conf

```
# grub.conf （作成者： anaconda）
#
# このファイルに変更を加えた後 grub を再実行する
# 必要はありません。
# 通知：/boot パーティションがありません。 これは
```

表 5-2. サンプルファイル：/etc/grub.conf （続き）

```
#           すべてのカーネルと initrd パスが / に相対パスであること
を意味します。例：
#           root (hd0,0)
#           kernel /boot/vmlinuz-version ro root=/dev/sda1
#           initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server(2.4.9-e.3smp)
   root(hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=
ide-scsi console=ttyS0 console=ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up(2.4.9-e.3)
   root(hd0,00)
  kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

/etc/grub.conf ファイルを編集するときは、次のガイドラインに従ってください。

1. GRUB のグラフィカルインタフェースを無効にして、テキストベースのインタフェースを使用します。そうしないと、RAC 仮想コンソールで GRUB 画面が表示されません。グラフィカルインタフェースを無効にするには、`splashimage` で始まる行をコメントアウトします。
2. RAC シリアル接続を介して仮想コンソールセッションを開始する GRUB オプションを複数有効にするには、すべてのオプションに次の行を追加します。

   ```
   console=ttyS1,115200n8r console=tty1
   ```

   表 5-2 に、`console=ttyS1,57600` を最初のオプションにのみ追加した例を示します。

起動後の仮想コンソールへのログインを有効にする

/etc/inittab ファイルを次のように編集します。

COM2 シリアルポートに `agetty` を設定する新しい行を追加します。

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

表 5-3 に、新しい行を追加したサンプルファイルを示します。

表 5-3. サンプルファイル：/etc/innitab

```
#
# inittab  このファイルは INIT プロセスで特定ランレベルのシステムを
#          セットアップする方法を記述します。
#
# 作成者： Miquel van Smoorenburg
#          RHS Linux 用に修正：Marc Ewing、Donnie Barnes
#
# デフォルトランレベル。RHS が使用するランレベル：
#   0 - 停止（この値に initdefault を設定しないでください）
#   1 - シングルユーザーモード
#   2 - マルチユーザー、NFS なし（ネットワークがない場合は
#       3 と同じ）
#   3 - フルマルチユーザーモード
#   4 - 未使用
#   5 - X11
#   6 - 再起動（この値に initdefault を設定しないでください）
#
id:3:initdefault:

# システムの初期化。
si::sysinit:/etc/rc.d/rc.sysinit


l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

表 5-3. サンプルファイル：/etc/innitab （続き）

```
# 各ランレベルで実行するもの。
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# UPS から停電が知らされたら、数分間分の
# 電源が残っていることを仮定します。シャットダウンを 2 分間後にスケ
ジュールします。
# 電源が取り付けられており UPS が接続して
# 正しく動作していることを前提とします。
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System
Shutting Down"
# シャットダウンの前に電源が復元した場合は、割り込んでキャンセルします。
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored;
Shutdown Cancelled"


# gettys を標準ランレベルで実行します。
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# xdm をランレベル 5 で実行します。
# xdm i が別のサービスになりました。
x:5:respawn:/etc/X11/prefdm -nodaemon
```

/etc/securetty ファイルを下記のように編集します。

COM2 用のシリアル tty の名前の新しい行を追加します。

```
ttyS1
```

表 5-4 に、新しい行を追加したサンプルファイルを示します。

表 5-4. サンプルファイル：/etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

メモ：IPMI ツールを使用するシリアルコンソールでは、ブレークキーシーケンス（~B）を使用して、Linux **Magic SysRq** キーコマンドを実行します。

シリアル接続のための iDRAC6 の設定

シリアル接続経由での iDRAC6 への接続には、次のいずれかのインタフェースを使用できます。

- iDRAC6 CLI
- ダイレクト接続基本モード
- ダイレクト接続ターミナルモード

このいずれかのインタフェースを使用するようにシステムを設定するには、次の手順を実行してください。

1 **BIOS** を設定して、シリアル接続を有効にします。

a システムの電源を入れるか、再起動します。

b 次のメッセージが表示された直後に <F2> を押します。

```
<F2> = System Setup
```

c スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。

d **シリアル通信** 画面で次のように設定します。

外部シリアルコネクタ .... リモートアクセスデバイス

e **変更を保存** を選択します。

f **セットアップユーティリティ** を終了してシステムセットアップ プログラムの設定を完了するには、<Esc> を押します。

2 DB-9 またはヌルモデムケーブルを管理ステーションから管理下ノードサーバーに接続します。93 ページの「シリアルコンソールの DB-9 またはヌルモデムケーブルの接続」を参照してください。

3 管理ステーションのターミナルエミュレーションソフトウェアにシリアル接続が設定されていることを確認します。93 ページの「管理ステーションのターミナルエミュレーションソフトウェアの設定」を参照してください。

4 シリアル接続が有効になるように iDRAC6 を設定します。これは RACADM または iDRAC6 のウェブインタフェースからできます。

RACADM を使用して iDRAC6 でシリアル接続を有効にするには、次のコマンドを実行します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

iDRAC6 のウェブインタフェースを使用して iDRAC6 でシリアル接続を有効にするには、次の手順に従います。

1 **システム** ツリーを展開して、**iDRAC の設定** をクリックします。

2 **ネットワーク / セキュリティ** タブをクリックして **シリアル** をクリックします。

3 **RAC シリアル** セクションの下にある **有効** を選択します。

4 **変更の適用** をクリックします。

元の設定でシリアルに接続した場合は、ログインプロンプトが表示されます。iDRAC6 ユーザー名とパスワードを入力します（デフォルト値は、それぞれ `root` と `calvin` です）。

このインタフェースから、RACADM などの機能を実行できます。たとえば、システムイベントログ を表示するには、次の RACADM コマンドを入力します。

```
racadm getsel
```

ダイレクト接続基本モードとダイレクト接続ターミナルモードの iDRAC の設定

RACADM を使用して次のコマンドを実行し、iDRAC6 コマンドラインインタフェースを無効にします。

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

この後、次の RACADM コマンドを実行し、ダイレクト接続基本モード を有効にします。

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 1
```

または、次の RACADM コマンドを実行し、ダイレクト接続ターミナルモード を有効にします。

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 0
```

iDRAC6 ウェブインタフェースを使用して同じ操作を実行できます。

1. **システム** ツリーを展開して、**iDRAC の設定** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **シリアル** をクリックします。
3. **RAC シリアル** セクションの下にある **有効** を選択解除します。

   ダイレクト接続基本モードの設定

   IPMI シリアル セクションの下にある **接続モード設定** ドロップダウンメニューを **ダイレクト接続基本モード** に変更します。

   直接接続端末モードの設定

   IPMI シリアル セクションの下にある **接続モード設定** ドロップダウンメニューを **ダイレクト接続ターミナルモード** に変更します。
4. **変更の適用** をクリックします。
   ダイレクト接続基本モードとダイレクト接続ターミナルモードの詳細については、96 ページの「シリアルと端末モードの設定」を参照してください。

ダイレクト接続基本モードでは、シリアル接続から直接 ipmish などのツールを使用できます。たとえば、IPMI 基本モードから ipmish を使用してシステムイベントログを印刷するには、次のコマンドを実行します。

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin
sel get
```

ダイレクト接続ターミナルモードでは、iDRAC6 に ASCII コマンドを発行できます。たとえば、ダイレクト接続ターミナルモードでサーバーの電源をオンまたはオフにするには、

1 ターミナルエミュレーションソフトウェアから iDRAC6 に接続します。

2 次のコマンドを入力し、ログインします。

```
[SYS PWD -U root calvin]
```

次の応答が表示されます。

```
[SYS]

[OK]
```

3 次のコマンドを入力し、ログインが成功したことを確認します。

```
[SYS TMODE]
```

次の応答が表示されます。

```
[OK TMODE]
```

4 サーバーの電源をオフにするには（サーバーの電源はすぐに切れます）、次のコマンドを入力します。

```
[SYS POWER OFF]
```

5 サーバーの電源をオンにするには（サーバーの電源はすぐに入ります）、次のコマンドを入力します。

```
[SYS POWER ON]
```

RAC シリアルインタフェース通信モードとシリアルコンソールの間の切り替え

iDRAC6 では、RAC シリアルインタフェース通信モードとシリアルコンソールの切り替えができる Esc キーシーケンスがサポートされています。

この動作を使用できるようにシステムを設定するには、次の手順を実行します。

1 システムの電源を入れるか、再起動します。

2 次のメッセージが表示された直後に <F2> を押します。

```
<F2> = System Setup
```

3 スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。

4 **シリアル通信** 画面で次のように設定します。

シリアル通信 -- com2 のシリアルリダイレクトでオン に設定

メモ：シリアルポートアドレス フィールドの **シリアルデバイス 2** も com1 に設定されている限り、**シリアル通信** フィールドを **com1 のシリアルリダイレクトでオン** に設定できます。

シリアルポートアドレス -- シリアルデバイス 1 = com1、シリアルデバイス 2 = com2

外部シリアルコネクタ -- シリアルデバイス 2

フェイルセーフボーレート 115200

リモートターミナルの種類 ...vt100/vt220

起動後のリダイレクト ... 有効

次に、**変更を保存** を選択します。

5 **セットアップユーティリティ** を終了してシステムセットアップ プログラムの設定を完了するには、<Esc> を押します。

管理下システムの外部シリアルコネクタと管理ステーションのシリアルポートをヌルモデムケーブルで接続します。

管理ステーション上のターミナルエミュレーションプログラム（ハイパーターミナルまたは Tera Term）を使用すると、管理下サーバーの起動シーケンスの進行状態に基づいて、POST 画面またはオペレーティングシステムの画面が表示されます。これは設定によって異なり、Windows では SAC、Linux では Linux テキストモード画面がそれぞれ表示されます。管理ステーションのターミナル設定をボーレート -115200、データ –8 ビット、パリティ - なし、ストップ -1 ビット、およびフロー制御 - なしに設定します。

シリアルコンソールモードのときに RAC シリアルインタフェース通信モードに切り替えるには、次のキーシーケンスを使用してください。

```
<Esc> +<Shift> <9>
```

上述のキーシーケンスを使用すると、「iDRAC ログイン」プロンプト（RAC が「RAC シリアル」モードに設定されている場合）、またはターミナルコマンドを発行できる「シリアル接続」モード（RAC が「IPMI シリアルダイレクト接続ターミナルモード」に設定されている場合）に移動します。

RAC シリアルインタフェース通信モードのときにシリアルコンソールモードに切り替えるには、次のキーシーケンスを使用してください。

```
<Esc> +<Shift> <q>
```

ターミナルモードのときにシステム COM2 ポートへの接続に切り替える場合には、次のコマンドを使用します。

```
<Esc> +<Shift> <q>
```

システム COM2 ポートに接続している場合にターミナルモードに戻るには、次のコマンドを使用します。

```
<Esc> +<Shift> <9>
```

シリアルコンソールの DB-9 またはヌルモデムケーブルの接続

シリアルテキストコンソールを使って DRAC/MC にアクセスするには、管理下システム上の COM ポートに DB-9 ヌルモデムケーブルを接続します。ヌルモデムケーブルで接続が機能するには、対応するシリアル通信設定を CMOS セットアップで行う必要があります。DB-9 ケーブルのすべてが、この接続に必要なピン割り当て / 信号を持っているわけではありません。この接続に使用する DB-9 ケーブルは、表 5-5 の仕様に従っている必要があります。

メモ : DB-9 ケーブルは BIOS テキスト仮想コンソールにも使用できます。

表 5-5. DB-9 ヌルモデムケーブルに必要なピン割り当て

信号名	DB-9 ピン（7 ピン）	DB-9 ピン（ワークステーションピン）
FG（筐体接地）	–	–
TD（送信データ）	3	2
RD（受信データ）	2	3
RTS（送信要求）	7	8
CTS（送信可）	8	7
SG（信号用接地）	5	5
DSR（データセットレディ）	6	4
CD（データキャリア検出）	1	4
DTR（データ端末レディ）	4	1 と 6

管理ステーションのターミナルエミュレーションソフトウェアの設定

iDRAC6 は、次のいずれかの種類のターミナルエミュレーションソフトウェアを実行している管理ステーションからのシリアルまたは Telnet テキストコンソールをサポートしています。

- Xterm の Linux Minicom
- Hilgraeve の HyperTerminal Private Edition（バージョン 6.3）
- Xterm の Linux Telnet
- Microsoft Telnet

使用するターミナルソフトウェアを設定するには、次の項の手順に従ってください。Microsoft Telnet を使用する場合、設定は不要です。

Linux Minicom にシリアルコンソールエミュレーションを設定する方法

Minicom は Linux 用のシリアルポートアクセスユーティリティです。次の手順は、Minicom のバージョン 2.0 に有効です。他のバージョンでは若干異なる場合がありますが、必要な基本設定は同じです。他のバージョンの Minicom の設定については、95 ページの「シリアルコンソールエミュレーションに必要な Minicom の設定」を参照してください。

Minicom バージョン 2.0 にシリアルコンソールエミュレーションを設定する方法

メモ : Telnet コンソールを表示する場合は、テキストが正しく表示されるように、Linux インストールのデフォルトのコンソールではなく、Xterm ウィンドウの使用をお勧めします。

1. 新しい Xterm セッションを開始するには、コマンドプロンプトで `xterm &` と入力します。
2. Xterm ウィンドウで、矢印キーをウィンドウの右下隅に移動してウィンドウのサイズを 80 x 25 に変更します。
3. Minicom の設定ファイルがない場合には、次の手順に進んでください。

   Minicom の設定ファイルがある場合は、`minicom <`*`Minicom 設定ファイル名`*`>` と入力し、手順 17 に進んでください。
4. Xterm コマンドプロンプトで、`minicom -s` と入力します。
5. **シリアルポートのセットアップ** を選択し、<Enter> を押します。
6. <a> を押して、該当するシリアルデバイスを選択します（例：**/dev/ttyS0**）。
7. <e> を押して、**速度 / パリティ / ビット** オプションを **57600 8N1** に設定します。
8. <f> を押して、**ハードウェアフロー制御** を **はい** に設定し、**ソフトウェアフロー制御** を **いいえ** に設定します。
9. **シリアルポートの設定** メニューを終了するには、<Enter> を押します。
10. **モデムとダイヤル** を選択して、<Enter> を押します。
11. **モデムダイヤルとパラメータのセットアップ** メニューで、<Backspace> を押して **初期化**、**リセット**、**接続**、**切断** 設定をクリアすると、設定が空白になります。
12. <Enter> を押して、それぞれの空白値を保存します。
13. 指定のフィールドをすべてクリアする場合は、<Enter> を押して **モデムダイヤルとパラメータのセットアップ** メニューを終了します。
14. **セットアップを config_name として保存** を選択して、<Enter> を押します。
15. **Minicom から終了** を選択して、<Enter> を押します。

16 コマンドシェルプロンプトで、`minicom <Minicom 設定ファイル名>` と入力します。

17 Minicom ウィンドウを 80 x 25 に拡大するには、ウィンドウの隅をドラッグします。

18 <Ctrl+a>、<z>、<x> を押して、Minicom を終了します。

メモ : シリアルテキスト仮想コンソールに Minicom を使用して管理下システムの BIOS を設定する場合は、Minicom で色をオンにすると便利です。色をオンにするには、`minicom -c on` コマンドを入力します。

Minicom ウィンドウにコマンドプロンプトが表示されることを確認します。コマンドプロンプトが表示されたら、接続が確立され、**connect** シリアルコマンドを使用して管理下システムのコンソールに接続できます。

シリアルコンソールエミュレーションに必要な Minicom の設定

表 5-6 に従って Minicom を設定します。

表 5-6. シリアルコンソールエミュレーションに必要な Minicom の設定

設定の説明	必要な設定
速度 / パリティ / ビット	57600 8N1
ハードウェアフロー制御	あり
ソフトウェアフロー制御	なし
ターミナルエミュレーション	ANSI
モデムダイヤルとパラメータの設定	**初期化**、**リセット**、**接続**、**切断** 設定をクリアして空白にします。
ウィンドウのサイズ	80 x 25（サイズ変更するには、ウィンドウの隅をドラッグする）

シリアルコンソール用ハイパーターミナルの設定

HyperTerminal は、Microsoft Windows のシリアルポートアクセスユーティリティです。仮想コンソール画面のサイズを正しく設定するには、Hilgraeve の HyperTerminal Private Edition バージョン 6.3 を使用します。

警告 : Microsoft Windows オペレーティングシステムのすべてのバージョンに Hilgraeve の HyperTerminal ターミナルエミュレーションソフトウェアが含まれています。ただし、同梱のバージョンでは仮想コンソールに必要な機能が十分に提供されません。このため、代わりにエディション 6.3 を使用するか、VT100/VT220 または ANSI エミュレーションモードをサポートするターミナルエミュレーションソフトウェアを使用してください。システムの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例として、Hilgraeve の HyperTerminal Private があります。

HyperTerminal にシリアルコンソールを設定するには、次の手順を実行してください。

1. HyperTerminal プログラムを起動します。
2. 新しい接続名を入力して、**OK** をクリックします。
3. **使用する接続方法：**の隣で、DB-9 ヌルモデムケーブルを接続した管理ステーション上の COM ポート（たとえば COM1）を選択し、**OK** をクリックします。
4. 表 5-7 に示した COM ポート設定を指定します。
5. **OK** をクリックします。
6. **ファイル** → **プロパティ** をクリックして、**設定** タブをクリックします。
7. **Telnet ターミナル ID：**を **ANSI** に設定します。
8. **ターミナル設定** をクリックして、**画面の行数** を **26** に設定します。
9. **列数** を **80** に設定して、**OK** をクリックします。

表 5-7. 管理ステーション COM ポート設定

設定の説明	必要な設定
速度	57600
データビット	8
パリティ	なし
終了ビット	1
フロー制御	ハードウェア

シリアルと端末モードの設定

IPMI と iDRAC6 シリアルの設定

1. **システム** ツリーを展開して、**iDRAC の設定** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **シリアル** をクリックします。
3. IPMI のシリアル設定を指定します。
   IPMI シリアル設定については、表 5-8 を参照してください。
4. iDRAC6 のシリアル設定
   iDRAC6 シリアル設定については、表 5-9 を参照してください。
5. **変更を適用** をクリックして、IPMI および iDRAC6 シリアルの変更を適用します。
6. **シリアル** ページの適切なボタンをクリックして続行します。**シリアル設定** ページの設定の説明は、『*iDRAC6 オンラインヘルプ*』を参照してください。

表 5-8. IPMI シリアル設定

設定	説明
接続モードの設定	• ダイレクト接続基本モード - IPMI シリアル基本モード • ダイレクト接続ターミナルモード - IPMI シリアルターミナルモード
ボーレート	• データ速度を設定します。**9600 bps**、**19.2 kbps**、**57.6 kbps**、または **115.2 kbps** から選択します。
フロー制御	• なし — ハードウェアフロー制御オフ • RTS/CTS — ハードウェアフロー制御オン
チャネル権限レベルの制限	• 管理者 • オペレータ • ユーザー

表 5-9. iDRAC6 シリアル設定

設定	説明
有効	iDRAC6 シリアルコンソールを有効または無効にします。オン = 有効、オフ = 無効
タイムアウト	回線が切断される前の最大アイドル時間（秒）。範囲は 60 ～ 1920 秒です。デフォルトは 300 秒です。タイムアウト機能を無効にするには、0 秒を使用します。
リダイレクト有効	仮想コンソールを有効または無効にします。オン = 有効、オフ = 無効
ボーレート	外部シリアルポート上のデータ速度。値は **9600 bps**、**19.2 kbps**、**57.6 kbps**、**115.2 kbps** から選択できます。デフォルトは **57.6 kbps** です。
Esc キー	<Esc> キーを指定します。デフォルトは ^\ です。
履歴バッファサイズ	仮想コンソールに書き込まれた最後の文字を保持するシリアル履歴バッファのサイズ。最大値およびデフォルト値 = 8192 文字
ログインコマンド	有効なログイン後に実行する iDRAC6 コマンドライン。

ターミナルモードの設定

1. **システム** ツリーを展開して、**iDRAC の設定** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **シリアル** をクリックします。
3. **シリアル設定** ページで **ターミナルモード設定** をクリックします。

4 ターミナルモード設定を指定します。
ターミナルモードの設定の説明は、表 5-10 を参照してください。

5 **変更の適用** をクリックします。

6 **ターミナルモード設定** ページの適切なボタンをクリックして続行します。**ターミナルモード設定** ページボタンの説明は、『iDRAC6 オンラインヘルプ』を参照してください。

表 5-10. ターミナルモード設定

設定	説明
ライン編集	ライン編集を有効または無効にします。
削除制御	次のいずれかを選択します。 • **iDRAC は、<bksp> または <del> を受け取ると、<bksp><sp><bksp> 文字を出力します** — • **iDRAC は、<bksp> または <del> を受け取ると、<del> 文字を出力します** —
エコー制御	エコーを有効または無効にします。
ハンドシェイク制御	ハンドシェークを有効または無効にします。
新しいラインシーケンス	**None**、**<CR-LF>**、**<NULL>**、**<CR>**、**<LF-CR>**、または **<LF>** を選択します。
新しいラインシーケンスの入力	**<CR>** または **<NULL>** を選択します。

iDRAC6 のネットワーク設定

警告 : iDRAC6 のネットワーク設定を変更すると、現在のネットワーク接続が切断される可能性があります。

iDRAC6 のネットワーク設定には、次のいずれかのツールを使用します。

- ウェブベースのインタフェース — 46 ページの「iDRAC6 NIC の設定」を参照してください。
- RACADM CLI — デルサポートサイト **support.dell.com/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』の cfgLanNetworking を参照してください。
- iDRAC6 設定ユーティリティ — 32 ページの「iDRAC 6 を使用するためのシステムの設定」を参照してください。

メモ : Linux 環境で iDRAC6 を導入する場合は、36 ページの「RACADM のインストール」を参照してください。

ネットワーク経由の iDRAC6 へのアクセス

iDRAC6 を設定した後、次のいずれかのインタフェースを使って管理下システムにリモートアクセスできます。

- ウェブインタフェース
- RACADM
- Telnet コンソール
- SSH
- IPMI

表 5-11 に、各 iDRAC6 インタフェースを示します。

表 5-11. iDRAC6 インタフェース

インタフェース	説明
ウェブインタフェース	グラフィカルユーザーインタフェースを使って iDRAC6 へのリモートアクセスを提供します。ウェブインタフェースは iDRAC6 ファームウェアに組み込まれており、管理ステーション上の対応ウェブブラウザから NIC インタフェースを通してアクセスします。
RACADM	コマンドラインインタフェースを使って iDRAC6 にリモートアクセスできます。RACADM は iDRAC6 IP アドレスを使って RACADM コマンドを実行します。 **メモ :** racadm リモート機能オプションは、管理ステーションでのみサポートされています。詳細については、100 ページの「RACADM のリモート使用」を参照してください。 **メモ :** racadm リモート機能を使用する場合は、次に示すようなファイル操作に関連して RACADM サブコマンドを使用するフォルダへの書き込み権限が必要になります。 `racadm getconfig -f <` *ファイル名* `>` または `racadm sslcertupload -t 1 -f c:\cert\cert.txt` サブコマンド
Telnet コンソール	iDRAC6 へアクセスを提供し、**電源オフ、電源オン、パワーサイクル、ハードリセット**などのコマンドを含んだシリアルおよび RACADM コマンドをサポートしています。 **メモ :** Telnet はセキュアなプロトコルではなく、パスワードを含むすべてのデータをプレーンテキストで送信します。機密情報を送信する場合は、SSH インタフェースを使用してください。
SSH インタフェース	高度なセキュリティ用の暗号化トランスポート層を使った Telnet コンソールと同じ機能を提供します。

表 5-11. iDRAC6 インタフェース （続き）

インタフェース	説明
IPMI インタフェース	iDRAC6 を通してリモートシステムの基本管理機能にアクセスできます。このインタフェースには IPMI オーバー LAN、IPMI オーバーシリアル、シリアルオーバー LAN が含まれます。詳細については、**support.dell.com\manuals** にある『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

メモ : iDRAC6 のデフォルトユーザー名は root、デフォルトパスワードは calvin です。

iDRAC6 NIC 経由で iDRAC6 のウェブインタフェースにアクセスするには、対応するウェブブラウザか、Server Administrator または IT Assistant を使用します。

Server Administrator を使用して iDRAC6 リモートアクセスインタフェースにアクセスするには、次の手順に従います。

- Server Administrator を起動します。
- Server Administrator ホームページの左ペインにあるシステムツリーで、**システム** → **メインシステムシャーシ** → **リモートアクセスコントローラ** の順にクリックします。

詳細については、『Server Administrator ユーザーズガイド』を参照してください。

RACADM のリモート使用

メモ : RACADM のリモート機能を使用する前に、iDRAC6 の IP アドレスを設定します。iDRAC6 の設定方法の詳細と関連文書については、31 ページの「iDRAC6 の基本インストール」を参照してください。

RACADM には、管理下システムに接続し、リモート仮想コンソールまたは管理ステーションから RACADM サブコマンドを実行できるリモート機能オプション（**-r**）があります。リモート機能を使用するには、有効なユーザー名（**-u** オプション）、パスワード（**-p** オプション）、および iDRAC6 IP アドレスが必要です。

メモ : リモートシステムにアクセスしているシステムのデフォルト証明書ストアに iDRAC6 証明書がない場合は、RACADM コマンドを入力したときにメッセージが表示されます。iDRAC6 証明書の詳細については、58 ページの「SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保」を参照してください。

セキュリティアラート：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

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。

セキュリティアラート：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 はコマンドの実行を続行しません。

エラー：指定した IP アドレスで iDRAC6 に接続できません

Linux システムでは、リモート RACADM を使った証明書の検証に成功するためには、次の中間手順を必ず実行してください。

1 DER フォーマットの証明書を PEM フォーマットに変換します（openssl cmdline ツールを使用）。

```
openssl x509 -inform pem -in
<yourdownloadedderformatcert.crt> -outform pem -out
<outcertfileinpemformat.pem> -text
```

2 管理ステーション上でデフォルト CA 証明書バンドルの場所を見つけます。たとえば、RHEL5 64 ビットでは、/etc/pki/tls/cert.pem です。

3 PEM フォーマットの CA 証明書を管理ステーションの CA 証明書の後に追加します。

たとえば、cat コマンドを使用します。

```
- cat testcacert.pem >> cert.pem
```

RACADM 構文概要

```
racadm -r <iDRAC6 IP アドレス> -u <ユーザー名> -p <パスワード>
<サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <iDRAC6 IP アドレス> <サブコマンド> <サブコマンドオプション>
```

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>
```

RACADM オプション

表 5-12 に、RACADM コマンドのオプションを示します。

表 5-12. racadm コマンドオプション

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）と異なる場合は、< *ポート番号* > を使用します。
-i	インタラクティブにユーザーのユーザー名とパスワードを問い合わせるように RACADM に指示します。
-u < *ユーザー名* **>**	コマンドのトランザクションの認証に使用するユーザー名を指定します。**-u** オプションを使用すると、**-pp** オプションも必要になり、**-i** オプション（インタラクティブ）は使用できなくなります。
-p < *パスワード* **>**	コマンドのトランザクションを認証するパスワードを指定します。**-p** オプションを使用すると、**-i** オプションは使用できなくなります。
-S	RACADM が無効な証明書エラーをチェックするように指定します。RACADM は無効な証明書を検出した場合にコマンドの実行を停止して、エラーメッセージを表示します。

racadm リモート機能の有効 / 無効化

メモ : これらのコマンドはローカルシステムで実行することをお勧めします。

RACADM リモート機能はデフォルトでは有効になっています。無効になっている場合は、次の RACADM コマンドを入力して有効にします。

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

リモート機能を無効にするには、次のように入力します。

```
racadm config -g cfgRacTuning -o
cfgRacTuneRemoteRacadmEnable 0
```

RACADM サブコマンド

表 5-13 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。構文および有効なエントリを含む RACADM サブコマンドの詳細リストについては、デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』を参照してください。

RACADM サブコマンドを入力するときは、コマンドに racadm のプレフィックスを付けてください。

```
racadm help
```

表 5-13. RACADM サブコマンド

コマンド	説明
help	iDRAC6 サブコマンドを一覧にします。
help < *サブコマンド*>	指定したサブコマンドの使用ステートメントを一覧にします。
arp	ARP テーブルの内容を表示します。ARP エントリの追加や削除はできません。
clearasrscreen	前回の ASR（クラッシュ）画面をクリアします（前回の青色画面）。
clrraclog	iDRAC6 のログをクリアします。ログがクリアされたときのユーザーと時間を示すエントリが 1 つ作成されます。
config	iDRAC6 を設定します。
getconfig	現在の iDRAC6 設定のプロパティを表示します。
coredump	前回の iDRAC6 コアダンプを表示します。
coredumpdelete	iDRAC6 に保存されているコアダンプを削除します。
fwupdate	iDRAC6 ファームウェアアップデートを実行、または状態を表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsysinfo	iDRAC6 とシステムの一般情報を表示します。
getractime	iDRAC6 の時刻を表示します。
ifconfig	現在の iDRAC6 の IP 設定を表示します。
netstat	ルーティングテーブルと現在の接続を表示します。
ping	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。
setniccfg	コントローラの IP 設定を指定します。
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 に既にあるキーを表示したりできます。
getniccfg	コントローラの現在の IP 設定を表示します。
getsvctag	システムのサービスタグを表示します。
racdump	iDRAC6 のステータスと状態情報をデバッグ用にダンプします。
racreset	iDRAC6 をリセットします。
racresetcfg	iDRAC6 をデフォルト設定にリセットします。

表 5-13. RACADM サブコマンド （続き）

コマンド	説明
serveraction	管理下システムの電源管理を行います。
getraclog	iDRAC6 のログを表示します。
clrsel	システムイベントログのエントリをクリアします。
gettracelog	iDRAC6 トレースログ を表示します。 -i と一緒に使用した場合は、iDRAC6 のトレースログ内のエントリ数を表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
sslcertupload	CA 証明書またはサーバー証明書を iDRAC6 にアップロードします。
sslcertdownload	CA 証明書をダウンロードします。
sslcertview	iDRAC6 で CA 証明書またはサーバー証明書を表示します。
sslkeyupload	SSL キーをクライアントから iDRAC6 にアップロードします。
testtrap	トラップの設定をチェックするには、iDRAC6 に iDRAC6 NIC 経由でテスト SNMP トラップを送信させます。
vmdisconnect	仮想メディア接続を強制終了します。
closessn	デバイス上の通信セッションを閉じます。
getsel	SEL エントリを表示します。
krbkeytabupload	Kerberos keytab ファイルをアップロードします。
localConRedirDisable	サーバーコンソールを無効化します。サーバービデオポートからのビデオ出力はありません。
testemail	RAC の E- メールアラート機能をテストします。
usercertupload	ユーザー証明書またはユーザー CA 証明書をクライアントから iDRAC6 にアップロードします。
usercertview	iDRAC6 上にあるユーザー証明書またはユーザー CA 証明書を表示します。
vflashsd	vflash SD カードを初期化するかその状態を取得します。
vflashpartition	初期化された vFlash SD カード上のパーティションの作成、削除、一覧表示、または状態表示を行います。

RACADM エラーメッセージについてよくあるお問い合わせ（FAQ）

（racadm racreset コマンドを使用して）iDRAC6 リセットを実行した後、コマンドを発行すると次のメッセージが表示されます。

エラー：指定した IP アドレスで RAC に接続できません。

このメッセージは何を意味しますか？

iDRAC6 のリセットが完了してから、別のコマンドを発行してください。

racadm コマンドやサブコマンドを使用すると、原因不明のエラーが発生します。

RACADM コマンドやサブコマンドを使用するとき、次のようなエラーが 1 つまたは複数発生することがあります。

- ローカル RACADM エラーメッセージ — 構文、入力ミス、名前の誤りなどの問題。
- リモート RACADM エラーメッセージ — IP アドレスの誤り、ユーザー名の誤り、パスワードの誤りなどの問題。

システムから iDRAC6 IP アドレスを ping した後で、iDRAC6 を専用モードと共有モードを切り替えると、応答がありません。

システムの ARP テーブルをクリアしてください。

リモート RACADM は SUSE Linux Enterprise Server（SLES）11 SP1 から iDRAC への接続に失敗します。

公式 openssl と libopenssl バージョンをインストールしたことを確認してください。次に示すコマンドを実行して、RPM パッケージをインストールします。

```
rpm -ivh --force < ファイル名 >
```

ここで、< ファイル名 > は openssl または libopenssl rpm パッケージファイルです。

たとえば、次のとおりです。

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-
30.22.21.1.x86_64.rpm
```

複数の iDRAC6 コントローラの設定

RACADM を使用すると、同じプロパティで 1 つまたは複数の iDRAC6 コントローラを設定できます。グループ ID と オブジェクト ID を使って特定の iDRAC6 コントローラをクエリすると、RACADM は取得した情報から **.cfg** 設定ファイルを作成します。ファイル名は **racadm.cfg** などのユーザー指定です。ファイルを 1 つまたは複数の iDRAC6 にエクスポートすると、同じプロパティを使用してコントローラを最短時間で設定できます。

メモ : 設定ファイルによっては、他の iDRAC6 にファイルをエクスポートする前に変更が必要な固有の iDRAC6 情報（静的 IP アドレスなど）が含まれています。

複数の iDRAC6 コントローラを設定するには、次の手順を実行してください。

1. RACADM を使用して、適切な設定が含まれているターゲット iDRAC6 にクエリします。

   メモ : 生成された **.cfg** ファイルにはユーザーパスワードは含まれていません。

   コマンドプロンプトを開いて、次のように入力します。

   ```
   racadm getconfig -f myfile.cfg
   ```

   メモ : getconfig -f を使った iDRAC6 設定のファイルへのリダイレクトは、ローカルまたはリモート RACADM インタフェースでのみサポートされています。

2. テキストエディタを使用して、設定ファイルに変更を加えます（**オプション**）。
3. 新しい設定ファイルを使用して、ターゲット iDRAC6 を変更します。

   コマンドプロンプトで、次のように入力します。

   ```
   racadm getconfig -f myfile.cfg
   ```

4. 設定されたターゲット iDRAC6 をリセットします。

   コマンドプロンプトで、次のように入力します。

   ```
   racadm racreset
   ```

`getconfig -f racadm.cfg` サブコマンドは iDRAC6 の設定を要求し、**racadm.cfg** ファイルを生成します。必要に応じて、ファイルに別の名前を付けることもできます。

getconfig コマンドを使用すると、次のような操作ができます。

- グループのすべての設定プロパティを表示する（グループ名とインデックスで指定）
- ユーザーのすべての設定プロパティをユーザー名別に表示する

config サブコマンドは、この情報を他の iDRAC6 にロードします。**config** を使用して、ユーザーとパスワードのデータベースを Server Administrator に同期させます。

初期設定ファイルの **racadm.cfg** ユーザーが命名します。次の例では、設定ファイルの名前は **myfile.cfg** です。このファイルを作成するには、コマンドプロンプトで次のように入力します。

```
racadm getconfig -f myfile.cfg
```

警告 : このファイルはテキストエディタで編集することをお勧めします。RACADM ユーティリティは ASCII テキストの構文解析を使用します。フォーマットすると、パーサーが混乱して RACADM データベースが破損する可能性があります。

iDRAC6 設定ファイルの作成

iDRAC6 設定ファイル **<** *ファイル名* **>.cfg** は、`racadm racadm config -f <` *ファイル名* `>.cfg` コマンドと共に使用します。この設定ファイルを使用して設定ファイルを作成し（**.ini** ファイルと同様）、このファイルから iDRAC6 を設定できます。ファイル名は自由に指定でき、最後に **.cfg** を付ける必要もありません（ただし、この項ではその命名法を使用しています）。

.cfg ファイルは次の方法で用意できます。

- 作成済み
- `racadm getconfig -f <` *ファイル名* `>.cfg` コマンドで取得する
- `racadm getconfig -f <` *ファイル名* `>.cfg` コマンドで取得してから編集する

メモ : getconfig コマンド の情報は、デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』の getconfig コマンド を参照してください。

.cfg ファイルは、最初に解析が行われ、有効なグループとオブジェクト名があるかどうか、いくつかの単純な構文規則が守られているかどうかが検証されます。エラーはエラーが検出された行番号でフラグ指定され、その問題を説明した簡単なメッセージがあります。ファイル全体の正確性について解析され、すべてのエラーが表示されます。**.cfg** ファイルにエラーが見つかった場合は、iDRAC6 に書き込みコマンドは送信されません。設定する前に、すべてのエラーを訂正する必要があります。**-c** オプションは **config** サブコマンドで使用できます。これは構文を検証するのみで、iDRAC6 への書き込みは行いません。

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

- パーサがインデックス付きグループを見つけた場合、その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の変更はすべて、インデックス値にも関連付けられます。

  たとえば、次のとおりです。

  ```
  [cfgUserAdmin]

  # cfgUserAdminIndex=11

  cfgUserAdminUserName=
  ```

```
# cfgUserAdminPassword=******** （書き込み専用）
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インデックスに結合されており、その下に一覧表示され、オブジェクトの有効な設定値はそのインデックスにのみ適用されます。
- 各インデックス付きグループには事前定義されたインデックスセットが用意されています。詳細については、デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』を参照してください。
- **racresetcfg** サブコマンドを使って iDRAC6 を元のデフォルトに戻し、`racadm config -f <`*ファイル名*`>.cfg` コマンドを実行します。**.cfg** ファイルにすべての必要オブジェクト、ユーザー、インデックス、およびその他のパラメータが入っていることを確認します。

△ **警告：racresetcfg サブコマンドを使用すると、データベースと iDRAC6 NIC は元のデフォルトの設定にリセットされ、ユーザーとユーザー設定はすべて削除されます。root ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。**

構文解析規則

- 「#」で始まる行はすべてコメントとして扱われます。

  コメント行は一列目から記述する*必要*があります。その他の列にある「#」の文字は単に # という文字として扱われます。

  一部のモデムパラメータでは # をその文字列内に含むことができます。エスケープ文字は必要ありません。`racadm getconfig -f <`*ファイル名*`>.cfg` コマンドで **.cfg** を生成し、エスケープ文字を追加せずに、`racadm config -f <`*ファイル名*`>.cfg` コマンドを異なる iDRAC6 上で実行します。

  例：

```
#
# これはコメントです。
[cfgUserAdmin]
```

cfgUserAdminPageModemInitString=< モデム初期化文字列 # コメントではありません >

- すべてのグループエントリは [と] の文字で囲む必要があります。

  グループ名を示す開始の [文字は一列目になければなりません。このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。設定データは、デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』に定義されているように、グループ化されています。

  次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

  例：

  [cfgLanNetworking] -{ *グループ名* }

  cfgNicIpAddress=143.154.133.121 { *オブジェクト名* }

- すべてのパラメータは、「object（オブジェクト）」、「=」、または「value（値）」の間に空白を入れずに「object=value」のペアとして指定されます。

  値の後にあるスペースは無視されます。値の文字列内にあるスペースは変更されません。'=' の右側の文字はそのまま使用されます（例：2 番目の '='、または '#'、'[',']' など）。これらの文字は、有効なモデムチャットスクリプト文字です。

  上記の例を参照してください。

  racadm getconfig -f < *ファイル名* >.cfg コマンドは、インデックスオブジェクトの前にコメントを置くため、ユーザーは使用されているコメントをここで参照できます。

  インデックス付きグループの内容を表示するには、次のコマンドを使用します。

  racadm getconfig -g < *グループ名* > -i < *インデックス 1 ～ 16*>

- 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 "[ ]" の組み合わせの後に出現する最初のオブジェクトでなければなりません。次は、現在のインデックス付きグループの例です。

  [cfgUserAdmin]

  cfgUserAdminIndex=11

  racadm getconfig -f <***myexample***>.cfg と入力すると、現在の iDRAC6 設定用の **.cfg** ファイルが構築されます。この設定ファイルは、固有の **.cfg** ファイルの使用例または開始点として利用できます。

iDRAC6 IP アドレスの変更

設定ファイルの iDRAC6 IP アドレスを変更する場合は、不要な < *変数*>= **値** のエントリをすべて削除します。IP アドレスの変更に関する < *値*>= **値** エントリを含む実際の変数グループのラベルと "[" と "]" だけが残ります。

たとえば、次のとおりです。

```
#
#  オブジェクトグループ "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

このファイルは次のようにアップデートされます。

```
#
#  オブジェクトグループ "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# コメント、次の行は無視されます
cfgNicGateway=10.35.9.1
```

racadm config -f myfile.cfg コマンドは、このファイルを解析して、行番号ごとにエラーを特定します。ファイルが正しければ、該当するエントリがその内容で更新されます。さらに、前の例の **getconfig** コマンドを使用して、更新を確認できます。

このファイルを使用して会社全体の変更をダウンロードしたり、ネットワーク上で新しいシステムを設定したりできます。

メモ :「Anchor」は内部用語です。ファイルには使用しないでください。

iDRAC6 ネットワークプロパティの設定

使用可能なネットワークプロパティのリストを生成するには、次のように入力します。

```
racadm getconfig -g cfgLanNetworking
```

DHCP を使用して IP アドレスを取得するには、次のコマンドを使って **cfgNicUseDhcp** オブジェクトを記述し、この機能を有効にします。

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

このコマンドは、起動時に **<Ctrl><E>** の入力を求められたときの **iDRAC6** 設定ユーティリティと同じ設定機能を提供します。**iDRAC6** 設定ユーティリティを使用したネットワークプロパティ設定の詳細については、**32** ページの「**iDRAC 6** を使用するためのシステムの設定」を参照してください。

次に、**LAN** ネットワークプロパティを設定するコマンドの使用例を示します。

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask
255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1
192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2
192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-
EK00002

racadm config -g cfgLanNetworking -o
cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName
MYDOMAIN
```

メモ : cfgNicEnable を **0** に設定すると、DHCP が有効の場合でも iDRAC6 LAN は無効になります。

iDRAC6 モード

iDRAC6 は、次の 4 つのモードのいずれかに設定できます。

- 専用
- 共有
- フェールオーバー付きで共有（LOM2）
- フェールオーバー付きで共有（すべての LOM）

表 5-14 に、各モードについて説明します。

表 5-14. iDRAC6 NIC の設定

モード	説明
専用	iDRAC6 は、ネットワークトラフィックに対して専用の NIC（RJ-45 コネクタ）と iDRAC MAC アドレスを使用します。
共有	iDRAC6 はプレーナで LOM1 を使用します。
フェールオーバー付きで共有（LOM2）	iDRAC6 は LOM1 と LOM2 をフェールオーバー用のチームとして使用します。このチームは iDRAC6 MAC アドレスを使用します。
フェールオーバー付きで共有（すべての LOM）	iDRAC6 は LOM1、LOM2、LOM3、LOM4 をフェールオーバー用のチームとして使用します。このチームは iDRAC6 MAC アドレスを使用します。

ネットワークセキュリティについてよくあるお問い合わせ（FAQ）

iDRAC6 のウェブベースインタフェースにアクセスするときに、SSL 証明書のホスト名が iDRAC6 のホスト名と一致しないというセキュリティ警告が表示されます。

iDRAC6 にはデフォルトの iDRAC6 サーバー証明書が含まれており、ウェブインタフェースのネットワークセキュリティとリモート RACADM 機能を確保します。この証明書を使用する場合には、ウェブブラウザにはセキュリティ警告が表示されます。これは、デフォルトの証明書が iDRAC6 のホスト名（たとえば IP アドレス）と一致しない **iDRAC6 デフォルト証明書** に対して発行されたためです。

このセキュリティ問題に対処するには、iDRAC6 の IP アドレスまたは iDRAC 名に発行された iDRAC6 サーバー証明書をアップロードします。証明書の発行に使用する証明書署名要求（CSR）を生成する場合には、CSR の共通名（CN）が（**証明書を IP に発行する場合**）iDRAC6 の IP アドレス（例：192.168.0.120）、または登録されている DNS iDRAC6 名（**証明書が登録済み iDRAC 名に発行された場合**）と一致することを確認してください。

CSR が登録されている DNS iDRAC6 名と一致することを確認するには、次の手順に従います。

1. **システム** ツリーで、**iDRAC の設定** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **ネットワーク** をクリックします。
3. **共通設定** テーブルで次の操作を行います。
   a. **DNS に iDRAC を登録** チェックボックスを選択します。
   b. **DNS iDRAC 名** フィールドに iDRAC6 名を入力します。
4. **変更の適用** をクリックします。

CSR の生成と証明書の発行については、316 ページの「SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保」を参照してください。

プロパティを変更すると、リモート RACADM とウエブベースのサービスを使用できなくなるのはなぜですか。

iDRAC6 ウェブサーバーがリセットした後、リモート RACADM サービスとウェブベースのインタフェースが使用できるようになるまでに時間がかかることがあります。

iDRAC6 ウェブサーバーは次のような場合にリセットします。

- iDRAC6 ウェブユーザーインタフェースを使ってネットワーク設定またはネットワークセキュリティのプロパティが変更された
- **cfgRacTuneHttpsPort** プロパティが変更された（ config -f *< 設定ファイル >* によって変更された場合を含む）
- **racresetcfg** が使われた
- iDRAC6 がリセットされた
- 新しい SSL サーバー証明書がアップロードされた

DNS サーバーで iDRAC6 を登録できない理由は何ですか。

一部の DNS サーバーは 31 文字以内の名前しか登録しません。

iDRAC6 ウェブインタフェースにアクセスすると、SSL 証明書が信頼できない認証局（CA）から発行されたというセキュリティ警告が表示されます。

iDRAC6 にはデフォルトの iDRAC6 サーバー証明書が含まれており、ウェブインタフェースのネットワークセキュリティとリモート RACADM 機能を確保します。この証明書は信頼できる CA によって発行されませんでした。このセキュリティ問題に対処するには、信頼できる CA（たとえば Microsoft 認証局、Thawte または Verisign）から発行された iDRAC6 サーバー証明書をアップロードしてください。証明書の発行の詳細については、316 ページの「SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保」を参照してください。

6

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維持するには、特定の管理者権限（または役割ベースの権限）を持つ一意のユーザーを作成します。セキュリティを強化するために、特定のシステムイベントが発生したときに特定のユーザーに電子メールでアラートを送るように設定することもできます。

ウェブインタフェースを使用した iDRAC6 ユーザーの設定

iDRAC6 ユーザーの追加と設定

iDRAC6 を使用してシステムを管理し、システムのセキュリティを確保するには、特定の管理者権限（役割ベースの権限）を持つ一意のユーザーを作成します。

iDRAC6 のユーザーを追加して設定するには、次の手順に従ってください。

メモ : iDRAC ユーザーを設定するには、**ユーザーの設定** 権限が必要です。

1. **iDRAC の設定** → **ネットワーク / セキュリティ** → **ユーザー** とクリックします。

   ユーザー ページ（表 6-1 を参照）には、iDRAC6 ユーザーの **ユーザー ID**、**状態**（有効 / 無効）、**ユーザー名**、**iDRAC**、**LAN**、**シリアルポート**、および **シリアルオーバー LAN**（有効 / 無効）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、この設定は変更できません。

2. **ユーザー ID** 列で、ユーザー ID をクリックします。

   ユーザーメインメニュー ページ（表 6-2 と 表 6-7 を参照）で、ユーザーの設定、ユーザー証明書の表示またはアップロード、信頼される認証局（CA）証明書のアップロード、セキュアシェル（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 キーの表示または削除ができます。

   ユーザーの設定 を選択して **次へ** をクリックすると、**ユーザー設定** ページが表示されます。

3. **ユーザー設定** ページで、次の項目を設定します。

   - 新規または既存の iDRAC ユーザーのユーザー名、パスワード、およびアクセス権。では、**一般ユーザー設定** について 表 6-3 説明しています。

- ユーザーの IPMI 権限。表 6-4 では、ユーザーの LAN 権限を設定するための **IPMI ユーザー権限** について説明しています。
- iDRAC ユーザー権限。表 6-5 では、**iDRAC のユーザー権限** について説明しています。
- iDRAC のグループアクセス権。表 6-6 では、**iDRAC グループ権限** について説明しています。

4 完了したら、**変更の適用** をクリックします。

5 **ユーザーページに戻る** をクリックして、ユーザーページに戻ります。

表 6-1. ユーザーの状態および権限

設定	説明
ユーザー ID	ユーザー ID 番号の連番リストを表示します。**ユーザー ID** の各フィールドには、事前設定された 16 個のユーザー ID 番号の 1 つが含まれています。このフィールドは編集できません。
状態	ユーザーのログイン状態（有効または無効）を表示します。（デフォルトでは無効になっています。） **メモ :** ユーザー 2 はデフォルトで有効になっています。
ユーザー名	ユーザーのログイン名を表示します。iDRAC6 ユーザー名は、最大 16 文字で指定できます。各ユーザーは一意のユーザー名を持つ必要があります。 **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。
iDRAC	ユーザー（システム管理者、オペレータ、読み取り専用、なし）を割り当てたグループ（権限レベル）を表示します。
LAN	ユーザー（システム管理者、オペレーター、読み取り専用、なし）を割り当てた IPMI LAN の権限レベルを表示します。
シリアルポート	ユーザー（システム管理者、オペレーター、読み取り専用、なし）を割り当てた IPMI シリアルポートの権限レベルを表示します。
シリアルオーバー LAN	IPMI シリアルオーバー LAN の使用を許可または拒否します。

表 6-2. スマートカード設定オプション

オプション	説明
ユーザー証明書のアップロード	ユーザー証明書を iDRAC6 にアップロードし、ユーザープロファイルにインポートできます。
ユーザー証明書の表示	iDRAC にアップロードされたユーザー証明書ページを表示します。
信頼される CA 証明書のアップロード	信頼される CA 証明書を iDRAC にアップロードして、ユーザープロファイルにインポートできます。
信頼される CA 証明書の表示	iDRAC にアップロード済みの信頼される CA 証明書を表示します。信頼される CA 証明書は、ユーザーに証明書を発行することを許可されている CA が発行したものです。

表 6-3. 一般ユーザー設定

ユーザー ID	16 個ある設定済みユーザー ID 番号の 1 つです。
ユーザーを有効にする	オンの場合は、iDRAC6 へのユーザーアクセスが有効であることを示します。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	最大 16 文字のユーザー名。次の文字がサポートされています。 • 0 ～ 9 • A ～ Z • a ～ z • 特殊文字：

+	%	)	'	>	:	$	[	|
!	&	=	*	,	-	{	]	§
#	(	?	<	;	_	}	\	

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。選択を解除すると、ユーザーの パスワード を変更できません。

表 6-3. 一般ユーザー設定 （続き）

新しいパスワード	16 文字以内の **パスワード** を入力します。文字は表示されず、マスクされます。次の文字がサポートされています。 • 0 ～ 9 • A ～ Z • a ～ z • 特殊文字：

+	&	?	>	-	}	|	を参照してください。
!	(	'	,	_	[		@
#	)	*	;	$	]	/	§
%	=	<	:	{	I	\	

新しいパスワードの確認	確認のために iDRAC ユーザーのパスワードを再入力します。

表 6-4. IPMI ユーザー権限

プロパティ	説明
LAN ユーザーに許可する最大権限	IPMI LAN チャネルでのユーザーの最大権限として、**システム管理者**、**オペレータ**、**ユーザー**、または **なし** のユーザーグループからいずれかを指定します。
許可する最大シリアルポートユーザー権限	IPMI シリアルチャネルでのユーザーの最大権限として、**システム管理者**、**オペレータ**、**ユーザー**、または **なし** のユーザーグループからいずれかを指定します。
シリアルオーバー LAN を有効にする	IPMI シリアルオーバー LAN を使用できます。選択すると、権限が有効になります。

表 6-5. iDRAC ユーザー権限

プロパティ	説明
役割	iDRAC ユーザーの最大権限として、**システム管理者**、**オペレータ**、**読み取り専用**、または **なし** のいずれかを指定します。**iDRAC グループ権限** については、表 6-6 を参照してください。
iDRAC へのログイン	iDRAC にログインできます。
iDRAC の設定	iDRAC を設定できます。

表 6-5. iDRAC ユーザー権限 （続き）

プロパティ	説明
ユーザーの設定	特定ユーザーのシステムアクセスを許可できるようにします。 **警告：この権限は通常、iDRAC の管理者役割のメンバーであるユーザー用に予約されていますが、オペレータ役割のユーザーにこの権限を割り当てることもできます。この権限を持つユーザーは、どのユーザーの構成も変更できます。これには、任意のユーザーの作成と削除、ユーザーの SSH キー管理などがあります。このため、この権限は慎重に割り当ててください。**
ログのクリア	iDRAC のログをクリアできます。
サーバー制御コマンドの実行	サーバー制御のコマンドを実行できるようにします。
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。
テストアラート	ユーザーがテストアラート（E- メールと PET）を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

表 6-6. iDRAC グループ権限

ユーザーグループ	許可する権限
管理者	**iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、アラートのテスト、診断コマンドの実行。**
オペレータ	**iDRAC へのログイン、iDRAC の設定、ユーザーの設定、ログのクリア、サーバー処置コマンドの実行、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、テストアラート、診断コマンドの実行** の各権限を任意に組み合わせて選択できます。
読み取り専用	**iDRAC へのログイン**
なし	権限の割り当てなし

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 を正しく設定して使用すれば、iDRAC6 へのログイン時にユーザ名またはパスワードを入力する必要がありません。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、次の点に気をつけてください。

- この機能は、RACADM および 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ます。iDRAC6 では、新しいキーを追加する前に、前のキーが削除されているかどうかの確認作業は行われません。新しいキーを追加すると、SSH インタフェースが有効な間、自動的に有効になります。

Windows 用の公開キーの生成

公開キーは、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 が稼動するクライアントの PuTTY キー生成アプリケーションを使用する方法と Linux が稼動するクライアントの *ssh-keygen* CLI 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について説明します。これらのツールの使用法の詳細については、アプリケーションヘルプを参照してください。

Windows クライアント用の PuTTY キー生成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. サポートされているキー生成アルゴリズムは RSA および DSA のみです。キーのビット数を入力します。ビット数は RSA では 768 ～ 4096 ビット、DSA では 1024 ビットで指定します。

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 [公開キーの保存] オプションを使用して公開キーをファイルに保存すると、後でアップロードできます。アップロードされるすべてのキーは、RFC4716 または openssh 形式である必要があります。そうしないと、そのキーを対象のフォーマットに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と小文字が区別されます。

ここで、

–t オプションでは *dsa* または *rsa* を指定できます。

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

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

手順に従ってください。コマンドを実行したら、公開ファイルをアップロードします。

警告 : ssh-keygen を使って Linux 管理ステーションから生成したキーは、4716 以外のフォーマットで指定されています。 `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` **を使って、キーを 4716 フォーマットに変換します。キーファイルのアクセス権を変更しないでください。上記の変換作業はデフォルトのアクセス権を使って実行します。**

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

公開キーをアップロードした後で、パスワードを入力せずに SSH 経由で iDRAC6 にログインできます。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 ユーザー名 @< *ドメイン* >

または

ssh ユーザー名 @<*IP アドレス* >

ここで、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 ユーザー名 @< *ドメイン*> racadm getversion

ssh ユーザー名 @< *ドメイン*> racadm getsel

iDRAC6 ウェブインタフェースを使った SSH キーのアップロード、表示、削除

1. **iDRAC の設定** → **ネットワーク / セキュリティ** → **ユーザー** とクリックします。**ユーザー** ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID をクリックします。**ユーザーメインメニュー** ページが表示されます。
3. **SSH キーの設定** オプションを使って、SSH キーをアップロード、表示、または削除します。

警告 : SSH キーのアップロード、表示、および削除の各機能は、「ユーザーの設定」ユーザー権限に基づきます。この権限を持つユーザーは、他のユーザーの SSH キーを設定することができます。この権限は慎重に与えてください。ユーザー権限の詳細については、115 ページの「iDRAC6 ユーザーの追加と設定」を参照してください。

表 6-7. SSH キーの設定

オプション	説明
SSH キーのアップロード	ローカルユーザーはセキュアシェル（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** ページの編集不可能な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、セキュアシェル（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 **SSH キーの表示 / 削除** ページの編集不可能なテキストボックスに表示されます。

表 6-8. 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。
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 6-9. 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。削除 オプションを選択し、**適用** をクリックして既存のキーを削除します。

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 RACADAM とリモート RACADM

```
racadm sshpkauth -i <2 ～ 16> -k <1 ～ 4> -f < ファイル名 >
racadm sshpkauth -i <2 ～ 16> -k <1 ～ 4> -t
< キーテキスト >
```

Telnet/SSH/ シリアル RACADM：

```
racadm sshpkauth -i <2 ～ 16> -k <1 ～ 4> -t
< キーテキスト >
```

例：

次のファイルを使って、有効なキーを最初のキースペース内の iDRAC6 ユーザー 2 にアップロードします。

```
$ 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。

警告：「キーテキスト」オプションはローカルおよびリモート RACADM でサポートされています。「ファイル」オプションは Telnet/ssh/ シリアル RACADM で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
```

サブコマンドオプションの情報は、デルサポートサイト **dell.com/support/manuals** にある『iDRAC6 および CMC コマンドライン リファレンスガイド』の `sshpkauth` サブコマンドを参照してください。

RACADM ユーティリティを使用した iDRAC6 ユーザーの設定

メモ：リモート Linux システム上で RACADM コマンドを実行するには、**root** ユーザーとしてログインする必要があります。

管理下システムに iDRAC6 エージェントでインストールされている RACADM コマンドラインを使用すると、単一または複数の iDRAC6 ユーザーを設定できます。

同じ設定を複数の iDRAC6 に対して指定する場合は、次のいずれかの操作を実行します。

- 本項の RACADM の例を参考にして、RACADM コマンドのバッチファイル を作成し、各管理下システム上でこのバッチファイルを実行します。
- iDRAC6 設定ファイルを、デルサポートサイト **dell.com/support/manuals** にある『iDRAC6 および CMC コマンドライン リファレンスガイド』の説明通りに作成し、同じ設定ファイルを使って各管理下システム上で **racadm config** サブコマンドを実行します。

作業を開始する前に

iDRAC6 のプロパティデータベースには、最大 16 のユーザーを設定できます。iDRAC6 ユーザーを手動で有効にする前に、現在のユーザーが存在するかどうかを確認します。新しい iDRAC6 を設定している場合や、**racadm racresetcfg** コマンドを実行した場合、現在のユーザーは `root` のみで、パスワードは `calvin` になります。**racresetcfg** サブコマンドは iDRAC6 をデフォルト値にリセットします。

警告 : racresetcfg コマンドを使用する場合は、注意が必要です。すべての 設定パラメータがデフォルト値に戻ります。それまでに行った変更がすべて失われます。

メモ : ユーザーは経時的に有効にしたり、無効にしたりできます。その結果、ユーザーが各 iDRAC6 に異なるインデックス番号を持つ場合があります。

コマンドプロンプトで次のコマンドを入力すると、ユーザーが存在するかどうかがわかります。

```
racadm getconfig -u < ユーザー名 >
```

または

1 ～ 16 までの各インデックスに、次のコマンドを 1 回ずつ入力することもできます。

```
racadm getconfig -g cfgUserAdmin -i < インデックス >
```

メモ : `racadm getconfig -f <myfile.cfg>` と入力して、iDRAC6 設定パラメータのすべてが含まれる **myfile.cfg** ファイルの表示や編集も行えます。

複数のパラメータとオブジェクト ID が現在値と一緒に表示されます。対象オブジェクトは次の 2 つです。

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

cfgUserAdminUserName オブジェクトに値がない場合は、**cfgUserAdminIndex** オブジェクトで示されるその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る場合は、そのインデックスがそのユーザー名で使用されています。

メモ : rracadm config サブコマンドを使用してユーザーを手動で追加または削除する場合は、**-i** オプションでインデックスを指定する必要があります。前の例で示した **cfgUserAdminIndex** オブジェクトに '**#**' 文字が含まれていることに注目してください。**racadm config -f racadm.cfg** コマンドを使用して、書き込むグループ / オブジェクトの数を指定する場合、インデックスは指定できません。最初に 使用可能なインデックスに新しいユーザーが追加されます。これにより、同じ設定で複数の iDRAC6 を設定する際の柔軟性が得られます。

iDRAC6 ユーザーの追加

新しいユーザーを RAC 設定に追加するには、基本的なコマンドをいくつか使用できます。通常は、次の手順を実行してください。

1. ユーザー名を設定します。
2. パスワードを設定します。
3. 次のユーザー権限を設定します。
   - iDRAC
   - LAN
   - シリアルポート
   - シリアルオーバー LAN
4. ユーザーを有効にします。

例

次の例では、パスワード「123456」と LOGIN 権限を持つ新しいユーザー名「John」を RAC に追加します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -
i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -
i 2 123456

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

確認するには、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john

racadm getconfig –g cfgUserAdmin –i 2
```

iDRAC6 ユーザーの削除

RACADM を使用している場合は、ユーザーを手動で個別に無効にする必要があります。設定ファイルを使用してユーザーを削除することはできません。

次の例は、iDRAC6 ユーザーを削除するときに使用できるコマンド構文です。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i
< インデックス > ""
```

二重引用符（""）のヌル文字列は、指定したインデックスのユーザー設定を削除して、出荷時のデフォルトに戻すように iDRAC6 に指示します。

iDRAC6 ユーザーに権限を与える

特定のシステム管理許可（ロールベースの権限）を持つユーザーを有効にするには、まず 125 ページの「作業を開始する前に」のステップを実行して使用可能なユーザーインデックスを探します。次に、新しいユーザー名とパスワードを使って次のコマンドラインを入力します。

メモ : 特定のユーザー権限に有効なビットマスク値のリストについては、デルサポートサイト **dell.com/support/manuals** にある『iDRAC6 および CMC コマンドラインリファレンスガイド』を参照してください。　デフォルトの権限値は 0 で、これはユーザーの権限が有効になっていないことを示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege
-i < インデックス > < ユーザー権限ビットマスク値 >
```

7

iDRAC6 ディレクトリサービスの使用

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 を使用して iDRAC6 ユーザーを認識する機能は、Microsoft Windows 2000、Windows Server 2003 および Windows Server 2008 オペレーティングシステムでサポートされています。

Microsoft Active Directory を使って、iDRAC6 にログインするユーザー認証を設定できます。システム管理者が各ユーザーに特定の権限を設定できる役割ベースの許可を与えることもできます。詳細については、次の各項を参照してください。

表 7-1 は、iDRAC6 Active Directory ユーザー権限を示しています。

表 7-1. iDRAC6 ユーザー権限

権限	説明
iDRAC へのログイン	iDRAC6 にログインできます。
iDRAC の設定	iDRAC6 を設定できます。
ユーザーの設定	特定ユーザーのシステムアクセスを許可できるようにします。
ログのクリア	iDRAC6 のログをクリアできます。
サーバー制御コマンドの実行	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	仮想コンソールを実行できます。
仮想メディアへのアクセス	仮想メディアを実行および使用できます。
テストアラート	テストアラート（E- メールと 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できます。

Active Directory を使用して、次のいずれかの方法で iDRAC6 にログインできます。

- ウェブインタフェース
- リモート RACADM
- シリアルまたは Telnet コンソール

ログイン構文は、3 つの方法にすべて共通です。

< *ユーザー名* @ *ドメイン* >

または

< *ドメイン* >\< *ユーザー名* > または < *ドメイン* >/< *ユーザ名* >

ユーザー名 は 1 ～ 256 バイトの ASCII 文字列です。

ユーザー名またはドメイン名に空白スペースと特殊文字（\、/、@ など）は使用できません。

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

ウェブインタフェースからログインし、ユーザードメインが設定されている場合、ウェブインタフェースのログイン画面のプルダウンメニューにすべてのユーザードメインが表示されます。プルダウンメニューからユーザードメインを選択する場合は、ユーザー名のみを入力します。**この iDRAC** を選択した場合、上記に記載されるログイン構文を使用して、Active Directory ユーザーとしてログインできます。

スマートカードまたはシングルサインオンを使用して iDRAC6 にログインすることもできます。詳細については、169 ページの「iDRAC6 に対するシングルサインオンまたはスマートカードログインの設定」を参照してください。

メモ : Windows 2008 Active Directory サーバーは、最長 256 文字の < *ユーザー名* >@< *ドメイン名* > 文字列のみをサポートしています。

iDRAC6 用に Microsoft Active Directory 認証を有効にするための必要条件

iDRAC6 で Active Directory 認証機能を使用するには、Active Directory インフラストラクチャがすでに導入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（PKI）メカニズムを使用して Active Directory に対して安全に認証するため、Active Directory のインフラストラクチャにも PKI を統合する必要があります。PKI の設定については、Microsoft のウェブサイトを参照してください。

すべてのドメインコントローラに対して正しく認証するには、iDRAC6 に接続するすべてのドメインコントローラでセキュアソケットレイヤー（SSL）を有効にする必要もあります。詳細については、131 ページの「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

iDRAC は Active Directory ドメインコントローラに対してユーザーを認証するとき、ドメインコントローラと SSL セッションを開始します。この時点で、ドメインコントローラは認証局（CA）によって署名された証明書を発行し、そのルート証明書も iDRAC にアップロードされます。つまり、iDRAC が（ルートまたは子ドメインコントローラにかかわらず）*どの* ドメインコントローラに対しても認証できるためには、ドメインコントローラがそのドメインの CA によって署名された SSL が有効な証明書を所有している必要があります。

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

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。

1. **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。
2. **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。
3. **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。
4. **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 : Windows 2000 が稼動するシステムの場合、またはスタンドアロン CA を使用している場合の手順は、次の手順とは異なる可能性があります。

1. Microsoft Enterprise CA サービスを実行しているドメインコントローラを見つけます。
2. **スタート** → **ファイル名を指定して実行** の順にクリックします。
3. **ファイル名を指定して実行** のフィールドに「mmc」と入力し、**OK** をクリックします。
4. **コンソール 1**（MMC）ウィンドウで、**ファイル**（Windows 2000 システムでは **コンソール**）をクリックし、**スナップインの追加 / 削除** を選択します。
5. **スナップインの追加と削除** ウィンドウで **追加** をクリックします。
6. **スタンドアロンスナップイン** ウィンドウで **証明書** を選択して **追加** をクリックします。

7 **コンピュータ アカウント**を選択して **次へ** をクリックします。

8 **ローカルコンピュータ** を選択して **完了** をクリックします。

9 **OK** をクリックします。

10 **コンソール 1** ウィンドウで、**証明書** フォルダを展開し、**パーソナル** フォルダを展開して、**証明書** フォルダをクリックします。

11 ルート CA 証明書を見つけて右クリックし、**すべてのタスク** を選択して **エクスポート** をクリックします。

12 **証明書のエクスポートウィザード**で **次へ** を選択し、**いいえ、秘密キーをエクスポートしない** を選択します。

13 **次へ** をクリックし、フォーマットとして **Base-64 エンコード X.509（.cer）** を選択します。

14 **次へ** をクリックし、システムのディレクトリに証明書を保存します。

15 手順 14 に保存した証明書を iDRAC にアップロードします。

RACADM を使って証明書をアップロードする場合は、146 ページの「iDRAC6 ウェブベースのインタフェースを使用した Microsoft Active Directory と拡張スキーマの設定」または 156 ページの「RACADM を使用した標準スキーマの Microsoft Active Directory の設定」を参照してください。

ウェブインタフェース を使って証明書をアップロードする場合は、146 ページの「iDRAC6 ウェブベースのインタフェースを使用した Microsoft Active Directory と拡張スキーマの設定」または 153 ページの「iDRAC6 ウェブインタフェースを使用した標準スキーマの Microsoft Active Directory の設定」を参照してください。

iDRAC6 ファームウェア SSL 証明書のインポート

メモ : Active Directory サーバーが SSL セッションの開始段階でクライアントを認証する設定になっている場合、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 セッションの開始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 が稼動している場合は、次の手順が異なる可能性があります。

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

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。iDRAC のコントローラにはすべて、デフォルトの自己署名付き証明書が付属しています。

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

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

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

   独自の証明書をインストールした場合は、その証明書に署名する CA が **信頼できるルート認証局** リストにあるかどうか確認してください。この 認証局 がリストにない場合は、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、保存する場所を指定します。
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 2 通りの方法で iDRAC6 へのユーザーアクセスを定義できます。1 つは、デル定義の Active Directory オブジェクトが追加された*拡張スキーマ*ソリューションを使用する方法です。もう一つは、Active Directory グループオブジェクトのみを使用する*標準スキーマ*ソリューションを使用する方法です。これらのソリューションの詳細については、以降の 各項を参照してください。

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

拡張スキーマソリューションを使用する場合の利点は次のとおりです。

- アクセス制御オブジェクトのすべてを Active Directory で管理できます。
- 異なる iDRAC6 でさまざまな権限レベルのユーザーアクセスを設定できます。

標準スキーマソリューションを使用する利点は、スキーマ拡張子が必要ないことです。必要なオブジェクトクラスはすべて、Active Directory スキーマの Microsoft のデフォルト設定で提供されています。

拡張スキーマ Active Directory の概要

拡張スキーマソリューションを使用する場合は、次の項で説明するように、Active Directory スキーマの拡張が必要になります。

Active Directory スキーマ拡張

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。企業は、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することができます。デルでは、スキーマを拡張して、リモート管理の認証と許可をサポートするために必要な変更を含めました。

既存の Active Directory スキーマに追加した属性やクラスは、それぞれ固有の ID で定義する必要があります。業界で一意の ID を保持するため、Microsoft では Active Directory オブジェクト識別子（OID）のデータベースを管理して、会社がスキーマに拡張を追加する場合、それらが他社と重複しないようにしています。デルでは、Microsoft の Active Directory のスキーマを拡張できるように、ディレクトリサービスに追加された属性とクラス用の固有の OID、固有の名前の拡張子、および固有のリンク属性 ID を受け取りました。

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

iDRAC スキーマ拡張の概要

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

Active Directory オブジェクトの概要

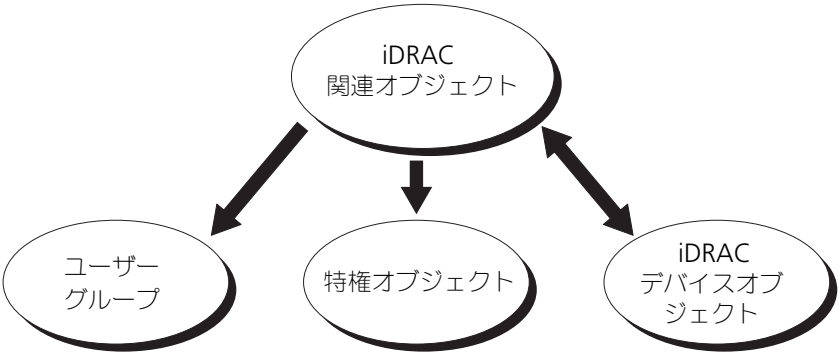
認証と許可のために Active Directory に統合するネットワーク上の物理 iDRAC につき、関連オブジェクトと RAC デバイスオブジェクトを少なくとも 1 つずつ作成しておきます。関連オブジェクトは必要な数だけ作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、iDRAC デバイスオブジェクトの数にも制限はありません。ユーザーと iDRAC デバイスオブジェクトは、企業内のどのドメインのメンバーでも構いません。

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

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

図 7-1 は、関連オブジェクトがすべての認証と認可に必要な関連付けを提供する仕組みを示しています。

図 7-1. Active Directory オブジェクトの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、iDRAC で認証と許可を実行するには、関連オブジェクトを少なくとも 1 つ作成する必要があり、Active Directory と統合するネットワーク上の iDRAC デバイスごとに iDRAC デバイスオブジェクトが 1 つ必要です。

関連オブジェクトに含むことができるユーザー、グループ、iDRAC デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる特権オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは、iDRACs デバイス上で 権限 を持つ ユーザー を接続します。

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

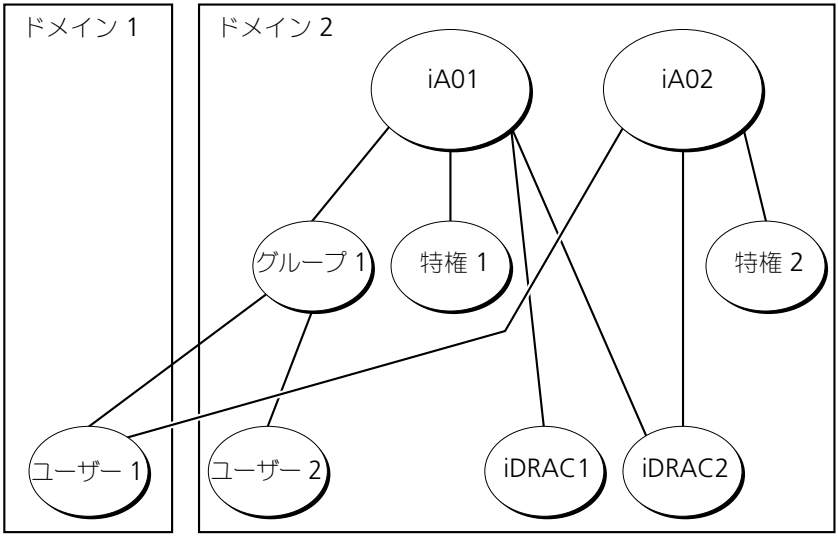
任意のドメインのユーザー、ユーザーグループ、またはネストされたユーザーグループを関連オブジェクトに追加できます。拡張スキーマソリューションは、Microsoft Active Directory によって許可されている複数のドメインにわたってネストされたユーザーグループやユーザーグループの種類をサポートしています。

拡張スキーマを使用した権限の蓄積

拡張スキーマ認証機構は、異なる関連オブジェクトを通して同じユーザーに関連付けられた異なる権限オブジェクトからの権限の蓄積をサポートしています。つまり、拡張スキーマ認証は権限を蓄積して、同じユーザーに関連付けられた異なる権限オブジェクトに対応して割り当てられた権限すべてのスーパーセットをユーザーに許可します。

図 7-2 に、拡張スキーマを使用した権限の蓄積例を示します。

図 7-2. ユーザーの権限の蓄積



この図は、2 つの関連オブジェクト iA01 と iA02 を示しています。ユーザー 1 は、両方の関連オブジェクトを通して、iDRAC2 に関連付けられています。したがって、ユーザー 1 には iDRAC2 で権限 1 と権限 2 のオブジェクトに設定された権限を組合わせて蓄積された権限が与えられます。

たとえば、権限 1 には、ログイン、仮想メディア、およびログのクリアの権限が割り当てられ、権限 2 には、iDRAC へのログイン、テスト、およびテストアラートの権限が割り当てられます。その結果、ユーザー 1 には、権限 1 と権限 2 の両方の権限を組み合わせた iDRAC へのログイン、仮想メディア、ログのクリア、iDRAC の設定、テストアラート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 では権限 1 と権限 2 を持っています。ユーザー 1 は、iDRAC1 では権限 1 だけを持っています。ユーザー 2 は、iDRAC1 と iDRAC2 の両方で権限 1 を持っています。また、この図によると、ユーザー 1 は異なるドメインに属することができ、ネストされたグループに関連付けることができます。

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

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

1. Active Directory スキーマを拡張します（137 ページの「Active Directory スキーマの拡張」を参照）。
2. Active Directory ユーザーとコンピュータスナップインを拡張します（143 ページの「Microsoft 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（144 ページの「Microsoft Active Directory への iDRAC ユーザーと権限の追加」を参照）。
4. iDRAC6 ウェブインタフェースまたは RACADM を使用して、iDRAC6 Active Directory プロパティを設定します（146 ページの「iDRAC6 ウェブベースのインタフェースを使用した Microsoft Active Directory と拡張スキーマの設定」または 148 ページの「RACADM を使用した拡張スキーマの Microsoft Active Directory の設定」を参照）。

Active Directory スキーマの拡張

重要： この製品のスキーマ拡張は、旧世代の Dell リモート管理製品とは異なります。新しいスキーマを拡張し、新しい Active Directory ユーザーとコンピュータ Microsoft 管理コンソール（MMC）スナップイン をディレクトリにインストールする必要があります。古いスキーマはこの製品には対応していません。

メモ： 新しいスキーマを拡張したり、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たりしても、以前の製品には効果がありません。

スキーマエクステンダおよび Active Directory ユーザーとコンピュータ MMC スナップイン拡張子は、『Dell Systems Management Tools and Documentation DVD』に収録されています。 インストールの詳細については、143 ページの「Microsoft 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 用の既存のスキーマの拡張および Active Directory ユーザーとコンピュータ MMC スナップインの詳細については、**dell.com/support/manuals** にある『Dell OpenManage インストールとセキュリティユーザーズガイド』を参照してください。

メモ : iDRAC 関連オブジェクトまたは iDRAC デバイスオブジェクトを作成する場合は、**Dell リモート管理オブジェクトの詳細設定** を選択してください。

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

次のいずれかの方法を使用してスキーマを拡張できます。

- 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

メモ : Remote_Management は DRAC4 や DRAC5 などの古いリモートアクセス製品上でスキーマを拡張するためのフォルダで、**Remote_Management_Advanced** は iDRAC6 上でスキーマを拡張するためのフォルダです。

LDIF ファイルを使用するには、**LDIF_Files** ディレクトリにある readme の説明を参照してください。Dell Schema Extender を使用して Active Directory スキーマを拡張するには、139 ページの「Dell Schema Extender の使い方」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 の使い方

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

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

   スキーマが拡張されます。スキーマ拡張を確認するには、Microsoft 管理コンソール（MMC）と Active Directory スキーマスナップインを使用して、次があることを確認します。

   - クラス（表 7-2 ～表 7-7 を参照）。
   - 属性（表 7-8）

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

表 7-2. Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられ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 7-3. dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.1
説明	Dell iDRAC デバイスを表します。iDRAC デバイスは、Active Directory で delliDRACDevice として設定する必要があります。この設定を使用して、iDRAC は LDAP（Lightweight Directory Access Protocol）クエリを Active Directory に送信できます。

表 7-3. dellRacDevice クラス （続き）

OID	1.2.840.113556.1.8000.1280.1.7.1.1
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 7-4. delliDRACAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.2
説明	Dell 関連オブジェクトを表します。この関連オブジェクトはユーザーとデバイスを連結します。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	**dellProductMembers** **dellPrivilegeMember**

表 7-5. dellRAC4Privileges クラス

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

表 7-6. dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	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 7-7. 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 7-8. Active Directory スキーマに追加された属性のリスト

属性名 / 説明	割り当てられた 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

表 7-8. Active Directory スキーマに追加された属性のリスト （続き）

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
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アラート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

表 7-8. Active Directory スキーマに追加された属性のリスト （続き）

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
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

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

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

『Dell Systems Management Tools and Documentation DVD』を使ってシステム管理ソフトウェアをインストールする場合、インストール手順中に **Active Directory ユーザーとコンピュータスナップイン** のオプションを選択するとスナップインを拡張できます。システム管理ソフトウェアのインストールの手順については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。64 ビット Windows オペレーティングシステムでは、スナップインのインストーラは **<DVD ドライブ >:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64** にあります。

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

Administrator Pack のインストール

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

詳細については、144 ページの「Microsoft Active Directory ユーザーとコンピュータのスナップインを開く」を参照してください。

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

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

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

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

   MMC が表示されます。

2. **コンソール 1** ウィンドウで、**ファイル**（または Windows 2000 が稼動するシステムでは **コンソール**）をクリックします。
3. **Add/Remove Snap-in**（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. **Close**（閉じる）をクリックして **OK** をクリックします。

Microsoft Active Directory への iDRAC ユーザーと権限の追加

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

- iDRAC デバイスオブジェクトの作成
- 権限オブジェクトの作成
- 関連オブジェクトの作成
- 関連オブジェクトの設定

iDRAC デバイスオブジェクトの作成

1. MMC **コンソールルート** ウィンドウでコンテナを右クリックします。
2. **新規** → **Dell リモート管理オブジェクトの詳細設定** の順に選択します。

   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、146 ページの「iDRAC6 ウェブベースのインタフェースを使用した Microsoft Active Directory と拡張スキーマの設定」の手順 A で入力する iDRAC 名と同一でなければなりません。
4. **iDRAC デバイスオブジェクト** を選択します。
5. **OK** をクリックします。

特権オブジェクトの作成

メモ : 特権オブジェクトは、関係する関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールのルート**（MMC）ウィンドウでコンテナを右クリックします。
2. **新規** → **Dell リモート管理オブジェクトの詳細設定** の順で選択します。
   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **特権オブジェクト** を選択します。
5. **OK** をクリックします。
6. 作成した特権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、ユーザーに与える権限を選択します。

関連オブジェクトの作成

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

1. **コンソールのルート**（MMC）ウィンドウでコンテナを右クリックします。
2. **新規** → **Dell リモート管理オブジェクトの詳細設定** の順で選択します。
   新規オブジェクト ウィンドウが開きます。
3. 新しいオブジェクトの名前を入力します。
4. **関連オブジェクト** を選択します。
5. **OK** をクリックします。

関連オブジェクトの設定

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

ユーザーのグループを追加できます。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。

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

特権の追加

1. **特権オブジェクト** タブを選択し、**追加** をクリックします。
2. 特権オブジェクト名を入力し、**OK** をクリックします。

定義されたユーザーまたはユーザーグループが利用できるネットワークに接続している iDRAC デバイスを 1 つ追加するには、**製品** タブをクリックします。関連オブジェクトには複数の iDRAC デバイスを追加できます。

iDRAC デバイスの追加

iDRAC デバイスを追加するには、次の手順を実行します。

1. **製品** タブを選択して **追加** をクリックします。
2. iDRAC デバイス名を入力して、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。

iDRAC6 ウェブベースのインタフェースを使用した Microsoft Active Directory と拡張スキーマの設定

1. サポートされているウェブブラウザのウィンドウを開きます。
2. iDRAC6 のウェブベースのインタフェースにログインします。
3. **iDRAC の設定** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** タブ → **Microsoft Active Directory** と進みます。
4. **Active Directory 設定と管理** ページの下にスクロールし、**Active Directory の設定** をクリックします。

   Active Directory の設定と管理手順 4 の 1 ページが開きます。
5. Active Directory の SSL 証明書を検証する場合は、**証明書設定** の下の **証明書検証を有効にする** を選択します。検証しない場合は、ステップ 9 へ進みます。
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 ÉN リックします。

   アップロードした Active Directory CA 証明書の情報が表示されます。
8. **（オプション：AD 認証用）Kerberos Keytab のアップロード** で、keytab ファイルのパスを入力するか、このファイルを参照します。**アップロード** をクリックします。Kerberos keytab が iDRAC6 にアップロードされます。
9. **次へ** をクリックします。**Active Directory の設定と管理手順 4 の 2 ページ**が開きます。

10 **Active Directory を有効にする** を選択します。

警告：このリリースでは、Active Directory が拡張スキーマ用に設定されていると、スマートカードベースの 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）機能は標準と拡張スキーマの両方でサポートされています。

11 **追加** をクリックして、ユーザードメイン名を入力します。

12 表示されるプロンプトにユーザードメイン名を入力し、**OK** をクリックします。

メモ：この手順はオプションです。ユーザードメインのリストを設定した場合は、ウェブインタフェースのログイン画面で表示されます。リストから選択すると、ユーザー名を入力するだけです。

13 **タイムアウト** フィールドに、iDRAC が Active Directory の応答を待つ時間を秒数で入力します。デフォルト値は 120 秒です。

14 次のオプションのいずれかを選択します。

a **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。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。または、**ドメインの指定** を選択し、DNS ルックアップで使用するドメイン名を入力します。iDRAC6 は接続が確立されるまで、各アドレス（DNS ルックアップによって返される最初の 4 つのアドレス）に対して、一つずつ接続を試みます。**拡張スキーマ** を選択した場合、iDRAC6 デバイスオブジェクトと関連オブジェクトはドメインコントローラに置かれます。

b **ドメインコントローラアドレスの指定** オプションを選択すると、iDRAC6 は指定された Active Directory ドメインコントローラのサーバーアドレスを使用できます。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の指定** オプションが選択されている場合は、3 つのアドレスの少なくとも 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** 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置かれているドメインコントローラーのアドレスです。

メモ：ドメインコントローラのサーバーアドレス 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（証明書の検証が有効な場合）の サブジェクト または サブジェクト代替名 フィールドに一致する必要があります。

15 **次へ** をクリックします。**Active Directory の設定と管理手順 4 の 3** ページが開きます。

16 スキーマの選択 で、拡張スキーマ をクリックします。

17 **次へ** をクリックします。**Active Directory の設定と管理手順 4 の 4** ページが開きます**。**

18 **拡張スキーマの設定** で、**iDRAC 名**および **iDRAC ドメイン名**を入力して iDRAC のデバイスオブジェクトを設定します。iDRAC ドメイン名は、iDRAC オブジェクトが作成されるドメインです。

19 Active Directory 拡張スキーマ**の**設定を保存するには、**完了** をクリックします。

iDRAC6 ウェブサーバーは、自動的に **Active Directory 設定と管理** ページに戻ります。

20 Active Directory 拡張スキーマの設定を確認するには、**設定のテスト** をクリックします。

21 Active Directory ユーザー名とパスワードを入力します。

テスト結果およびテストログが表示されます。詳細については、159 ページの「設定のテスト」参照してください。

メモ : Active Directory ログインをサポートするには、iDRAC 上で DNS サーバーが正しく設定されている必要があります。**iDRAC 設定** → **ネットワーク / セキュリティ** → **ネットワーク** ページの順にクリックし、手動で DNS サーバーを設定するか、DHCP を使用して DNS サーバーを取得します。

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

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

ウェブベースのインタフェースの代わりに RACADM CLI ツールを使用して、拡張スキーマで iDRAC6 Microsoft Active Directory 機能を設定するには、次のコマンドを使用します。

1 コマンドプロンプトを開き、次の RACADM コマンドを入力します。

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

racadm config -g cfgActiveDirectory -o cfgADType 1

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

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

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

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

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

メモ : 3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。拡張スキーマのオプションが選択されている場合、iDRAC デバイスが所在するドメインコントローラの FQDN または IP アドレスとなります。拡張スキーマモードでは、グローバルカタログサーバーは全く使用されません。

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

警告 : このリリースでは、Active Directory が拡張スキーマ用に設定されていると、スマートカードベースの 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）機能は標準と拡張スキーマの両方でサポートされています。

DNS ルックアップを使って Active Directory ドメインコントローラサーバーアドレスを取得するには、次に示すコマンドを入力します。

```
racadm config -g cfgActiveDirectory -o
cfgADDcSRVLookupEnable=1
```

- ログインユーザーのドメイン名で DNS ルックアップを実行するには、次に示すコマンドを入力します。

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupbyUserdomain=1
  ```

- DNS ルックアップで使用するドメイン名を指定するには、次に示すコマンドを入力します。

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <DNS ルックアップで使用するドメイン名>
  ```

SSL ハンドシェイク中の証明書の検証を無効にしたい場合は、次の RACADM コマンドを入力します。

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

この場合、CA 証明書をアップロードする必要はありません。

SSL ハンドシェイク中の証明書の検証を強制したい場合は、次の RACADM コマンドを入力します。

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

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

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

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

次の RACADM コマンドは任意で実行できます。詳細については、132 ページの「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 タイムアウトする前に Active Directory（AD）のクエリを待つ時間を秒数で指定するには、次に示すコマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADAuthTimeout
<秒数>
```

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

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

4 iDRAC で DHCP が無効な場合や、手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<プライマリ DNS IP アドレス>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
<セカンダリ DNS IP アドレス>
```

5 iDRAC6 ウェブインタフェースにログイン中にユーザー名を入力するだけで済むように、ユーザードメインのリストを設定する場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName -i
<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。

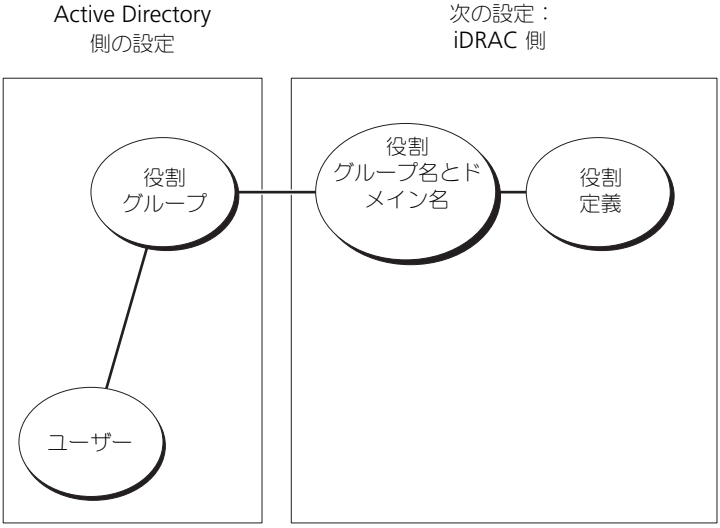
ユーザードメインの詳細については、160 ページの「汎用 LDAP ディレクトリサービス」を参照してください。

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

標準スキーマの Active Directory の概要

図 7-3 に示すように、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 7-3. Microsoft Active Directory と標準 スキーマで iDRAC の設定



Active Directory 側では、標準グループオブジェクトが役割グループとして使用されます。iDRAC6 へのアクセス権を持つユーザーは役割グループのメンバーとなります。指定した iDRAC6 へのアクセスをこのユーザーに与えるには、役割グループ名とそのドメイン名を特定の iDRAC6 で設定する必要があります。拡張スキーマソリューションとは異なり、役割と権限レベルは Active Directory でなく、各 iDRAC6 で定義されます。各 iDRAC について、最大 5 つまで役割グループを設定および定義できます。表 7-9 は、デフォルトの役割グループの権限を示しています。

メモ : 5 つの役割グループすべての役割グループ権限のデフォルトレベルは **なし** です。ドロップダウンボックスから役割グループデフォルト権限のうちひとつを選択する必要があります。

表 7-9. デフォルトのロールグループの権限

権限レベル	許可する権限	ビットマスク
管理者	**iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、アラートのテスト、診断コマンドの実行。**	0x000001ff
オペレータ	**iDRAC へのログイン、iDRAC の設定、サーバー制御コマンドの実行、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、アラートのテスト、診断コマンドの実行。**	0x000000f9
読み取り専用。	**iDRAC へのログイン**	0x00000001
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は、ドメインコントローラのアドレスのみを iDRAC6 で設定する必要があります。このような単一ドメインのシナリオでは、すべてのグループタイプがサポートされています。

ログインユーザーと役割グループのすべて、またはネストされたグループのいずれかが異なるドメインに属する場合は、iDRAC6 でグローバルカタログサーバーのアドレスを設定する必要があります。このようなマルチドメインのシナリオでは、すべての役割グループとネストされたグループがユニバーサルグループタイプであることが必要です。

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

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

1 Active Directory サーバー（ドメインコントローラ）で、**Active Directory ユーザーとコンピュータスナップイン** を開きます。

2 グループを作成するか、既存のグループを選択します。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 を使って、iDRAC6 上のグループの名前とドメイン名を設定します。詳細については、153 ページの「iDRAC6 ウェブインタフェースを使用した標準スキーマの Microsoft Active Directory の設定」および 156 ページの「RACADM を使用した標準スキーマの Microsoft 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た標準スキーマの Microsoft Active Directory の設定

1 サポートされているウェブブラウザのウィンドウを開きます。

2 iDRAC6 のウェブベースのインタフェースにログインします。

3 **iDRAC の設定** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** タブ → **Microsoft Active Directory** と進みます。

4 **Active Directory 設定と管理** ページの下にスクロールし、**Active Directory の設定** をクリックします。

Active Directory の設定と管理手順 4 の 1 ページが開きます。

5 Active Directory の SSL 証明書を検証する場合は、**証明書設定** の下の **証明書検証を有効にする** を選択します。検証しない場合は、ステップ 9 へ進みます。

6 **Active Directory CA 証明書のアップロード** で、証明書ファイルを参照します。

7 **アップロード** を ÉN リックします。

有効な Active Directory CA 証明書の情報が 表示されます。

8 **（オプション：AD 認証用）Kerberos Keytab のアップロード** で、keytab ファイルのパスを入力するか、このファイルを参照します。**アップロード** をクリックします。Kerberos keytab が iDRAC6 にアップロードされます。

9 **次へ** をクリックします。**Active Directory の設定と管理手順 4 の 2** ページが開きます。

10 **Active Directory を有効にする** を選択します。

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

12 **追加** をクリックして、ユーザードメイン名を入力します。

13 表示されるプロンプトにユーザードメイン名を入力し、**OK** をクリックします。

14 **タイムアウト** フィールドに、iDRAC が Active Directory の応答を待つ時間を秒数で入力します。デフォルト値は 120 秒です。

15 次のオプションのいずれかを選択します。

a **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。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。または、**ドメインの指定** を選択し、DNS ルックアップで使用するドメイン名を入力します。iDRAC6 は接続が確立されるまで、各アドレス（DNS ルックアップによって返される最初の 4 つのアドレス）に対して、一つずつ接続を試みます。**標準スキーマ** を選択した場合、これらはユーザーアカウントと役割グループはドメインコントローラに置かれます。

b **ドメインコントローラアドレスの指定** オプションを選択すると、iDRAC6 で指定された Active Directory ドメインコントローラのサーバーアドレスを使用できます。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の指定** オプションが選択されている場合は、3 つのアドレスの少なくとも 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。**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。

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サブジェクトまたはサブジェクト代替名のフィールドの値と一致する必要があります。

16 **次へ** をクリックします。**Active Directory の設定と管理手順 4 の 3** ページが開きます。

17 **スキーマの選択** で、**標準スキーマ** をクリックします。

18 **次へ** をクリックします。**Active Directory の設定と管理手順 4 の 4a** ページが開きます。

19 次のオプションのいずれかを選択します。

- **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。グローバルカタログサーバーのアドレス 1 ～ 3 は無視されます。iDRAC6 は接続が確立されるまで、各アドレス（DNS ルックアップによって返される最初の 4 つのアドレス）に対して、一つずつ接続を試みます。ユーザーアカウントと役割グループが異なるドメインにある場合に限り、標準スキーマにグローバルカタログサーバーが必要です。
- **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。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。

メモ : グローバルカタログサーバーのアドレス 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（証明書の検証が有効な場合）の サブジェクト または サブジェクト代替名 フィールドに一致する必要があります。

メモ : ユーザーアカウントと役割グループが異なるドメインにある場合、グローバルカタログサーバーは標準スキーマのみに必要です。また、このようなマルチドメインのシナリオで使用できるのは、ユニバーサルグループのみです。

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

Active Directory の設定と管理 手順 4 の 4b ページが開きます。

21 **役割グループ名** を指定します。

役割グループ名 は、Active Directory における iDRAC に関連付けられた役割グループを識別します。

22 役割グループのドメインとなる **役割グループドメイン** を指定します。

23 **役割グループの権限レベル** を選択して、**役割グループの権限** を指定します。たとえば、**システム管理者** を選択すると、そのアクセス権レベルのすべての権限が選択されます。

24 **適用** をクリックして、役割グループの設定を保存します。

iDRAC6 ウェブサーバーによって、設定が表示される手順 4 の 4b、**Active Directory 設定と管理** ページに自動的に戻ります。

25 必要に応じて、追加の役割グループを設定します。

26 **終了** をクリックし、**Active Directory の設定と管理** ページに戻ります。

27 Active Directory 標準スキーマの設定を確認するには、**設定のテスト** をクリックします。

28 iDRAC6 ユーザー名とパスワードを入力します。

テスト結果およびテストログが表示されます。詳細については、159 ページの「設定のテスト」参照してください。

メモ : Active Directory ログインをサポートするには、iDRAC 上で DNS サーバーが正しく設定されている必要があります。**iDRAC 設定 → ネットワーク / セキュリティ → ネットワーク** ページの順にクリックし、手動で DNS サーバーを設定するか、DHCP を使用して DNS サーバーを取得します。

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

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

ウェブインタフェースの代わりに RACADM CLI を使用して、標準スキーマの iDRAC Active Directory 機能を設定するには、次のコマンドを使用します。

1 コマンドプロンプトを開き、次の RACADM コマンドを入力します。

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

```
racadm config -g cfgActiveDirectory -o cfgADType 2
```

```
racadm config -g cfgStandardSchema -i < 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 < 特定のユーザー権限のビットマスク
番号 >
```

メモ : ビットマスク番号値については、デルサポートサイト **dell.com/support/manuals** にある『RACADM iDRAC6 および CMC コマンドラインリファレンスガイド』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 : 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サブジェクトまたはサブジェクト代替名のフィールドの値と一致する必要があります。

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

メモ : 3 つのアドレスのうち、少なくとも 1 つのアドレスを設定する必要があります。iDRAC6 は、接続が確立されるまで、設定されたアドレスに対して、一つずつ接続を試みます。標準スキーマでは、ユーザーアカウントと役割グループが存在するドメインコントローラのアドレスとなります。

DNS ルックアップを使って Active Directory ドメインコントローラサーバーアドレスを取得するには、次に示すコマンドを入力します。

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

- ログインユーザーのドメイン名で DNS ルックアップを実行するには、次に示すコマンドを入力します。

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

- DNS ルックアップで使用するドメイン名を指定するには、次に示すコマンドを入力します。

  `racadm config -g cfgActiveDirectory -o cfgADDcSRVLookupDomainName <`*DNS ルックアップで使用するドメイン名*`>`

グローバルカタログサーバーアドレスを指定するには、次に示すコマンドを入力します。

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

メモ : ユーザーアカウントと役割グループが異なるドメインにある場合、グローバルカタログサーバーは標準スキーマのみに必要です。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サブジェクトまたはサブジェクト代替名のフィールドの値と一致する必要があります。

DNS ルックアップを使って Active Directory グローバルカタログサーバーアドレスを取得するには、次に示すコマンドを入力します。

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

```
racadm config -g cfgActiveDirectory -o
cfgADGcRootDomain < ドメイン名 >
```

SSL ハンドシェイク中の証明書の検証を無効にしたい場合は、次の RACADM コマンドを入力します。

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

この場合、認証局（CA）の証明書をアップロードする必要はありません。

SSL ハンドシェイク中の証明書の検証を強制したい場合は、次の RACADM コマンドを入力します。

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

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

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

次の RACADM コマンドは任意で実行できます。詳細については、132 ページの「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 タイムアウトする前に Active Directory（AD）のクエリを待つ時間を秒数で指定するには、次に示すコマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADAuthTimeout
< 秒数 >
```

3 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
```

4 iDRAC6 で DHCP が無効になっている場合や、手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
< プライマリ DNS IP アドレス >
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
< セカンダリ DNS IP アドレス >
```

5 iDRAC6 ウェブインタフェースにログインするときにユーザー名だけの入力で済むように、ユーザードメインのリストを設定する場合は、次のコマンドを入力します。

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

最大 40 のユーザードメインをインデックス番号 1 ～ 40 で設定することが可能です。ユーザードメインの詳細については、160 ページの「汎用 LDAP ディレクトリサービス」を参照してください。

設定のテスト

設定が正常に動作するか確認する場合や、Active Directory ログインが失敗する問題を診断する必要がある場合は、iDRAC6 ウェブインタフェースから設定をテストできます。

iDRAC6 ウェブインタフェースで設定を完了したら、画面下部の **設定のテスト** をクリックします。テストを実行する場合は、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。結果ページの下部に詳細なテストログが表示されます。

いずれかの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、164 ページの「Active Directory についてよくあるお問い合わせ（FAQ）」を参照してください。

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

汎用 LDAP ディレクトリサービス

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 実装を汎用的にするには、異なるディレクトリサービス間の共通点を使って、ユーザーをグループ化してからユーザーとグループの関係をマップします。ディレクトリサービス固有の処置がスキーマです。たとえば、ユーザーとグループの間では、グループ、ユーザー、および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（ディレクトリサービス vs ローカルユーザー）

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。ログインユーザーはユーザー名のみを入力します（ドメイン名は入力しない）。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 が有効である場合、GUI ログインページのドロップダウンメニューには「この iDRAC」のみが表示されます。

メモ : openLDAP および OpenDS ベースのディレクトリサービスのユーザー名には、「<」および「>」文字は使用できません。

iDRAC6 ウェブベースの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 のウェブベースのインタフェースにログインします。
3. **iDRAC の設定** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** タブ → **汎用 LDAP ディレクトリサービス** の順に選択します。

   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。

   汎用 LDAP の設定と管理手順 3 の 1 ページが開きます。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場合は、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。

4 **証明書の設定** の **証明書検証を有効にする** を選択すると、証明書の検証が有効になります。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省略します。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の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。

警告 : 証明書の生成中に LDAP サーバー証明書のサブジェクトフィールドで、CN = LDAP FQDN を開く が設定されている（CN= openldap.lab など）ことを確認します。iDRAC6 の LDAP サーバーアドレスフィールドは、証明書の検証機能が動作するように同じ FQDN アドレスに一致するように設定します。

5 **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。

6 **アップロード** を ÉN リックします。

すべてのドメインコントローラのセキュアソケットレイヤ（SSL）サーバーの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。

7 **次へ** をクリックします。**汎用 LDAP の設定と管理手順 3 の 2** ページが開きます。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 : このリリースでは、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（SSO）機能は、汎用 LDAP ディレクトリサービスでサポートされていません。

8 次の情報を入力します。

- **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。

- 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。クリアされた場合、ログインユーザーが提供するユーザー名がグループのメンバーとの比較に使用されます。

- **LDAP サーバーアドレス** フィールドに、LDAP サーバーの完全修飾ドメイン名（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には、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交代で試みます。
- **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。
- **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。指定されていない場合は、匿名のバインドが使用されます。
- 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。
- **検索するベース DN** フィールドに、すべての検索が開始されるディレクトリのブランチの DN を入力します。
- **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。
- **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。
- **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。

9 **次へ** をクリックします。**汎用 LDAP の設定と管理手順 3 の 3a** ページが開きます。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。

メモ： このリリースでは、AD とは異なり、特殊文字（「@」、「\」、「/」）を使って LDAP ユーザーとローカルユーザーと区別する必要はありません。ログインする場合はユーザー名のみを入力します。ドメイン名は入力しないでください。

10 **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 3 の 3b ページが開きます。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。

11 **グループ DN** フィールドで、iDRAC6 に関連付けられている汎用 LDAP ディレクトリサービス内で役割グループを識別するグループを入力します。

12 **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。

13 **適用** をクリックして、役割グループの設定を保存します。

iDRAC6 ウェブサーバーによって、役割グループの設定が表示される**汎用 LDAP 設定と管理手順 3 の 3a ページ**に自動的に戻ります。

14 必要に応じて、追加の役割グループを設定します。

15 **終了** をクリックすると、**汎用 LDAP 設定と管理** の概要ページ に戻ります。

16 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。

17 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。

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

RACADM を使用した汎用 LDAP ディレクトリサービスの設定

```
racadm config -g cfgldap -o cfgLdapEnable 1
racadm config -g cfgldap -o cfgLdapServer <FQDN または IP アドレス>
racadm config -g cfgldap -o cfgLdapPort < ポート番号 >
racadm config -g cfgldap -o cfgLdapBaseDN dc=
common,dc=com
racadm config -g cfgldap -o
cfgLdapCertValidationenable 0
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupDN 'cn=everyone,ou=groups,dc=
common,dc=com'
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupPrivilege 0x0001
```

次のコマンドを使用して設定を表示します。

```
racadm getconfig -g cfgldap
racadm getconfig -g cfgldaprolegroup -i 1
```

RACADM を使ってログインできるかどうかを確認します。

```
racadm -r <iDRAC6 IP> -u user.1 -p password getractime
```

BindDN オプションをテストするための追加の設定

```
racadm config -g cfgldap -o cfgLdapBindDN "cn=
idrac_admin,ou=iDRAC_admins,ou=People,dc=common,dc=
com"
racadm config -g cfgldap -o cfgLdapBindPassword
password
```

メモ : ドメインネームサーバーを使用するように iDRAC6 を設定します。これは、iDRAC6 を LDAP サーバーアドレスで使用するように設定する LDAP サーバーホスト名を解決します。ホスト名は LDAP サーバーの証明書の「CN」または「サブジェクト」に一致する必要があります。

Active Directory についてよくあるお問い合わせ（FAQ）

Active Directory のログインに失敗しました。この問題はどのようにトラブルシュートできますか。

iDRAC6 は、ウェブインタフェースから診断ツールを提供しています。ウェブインタフェースから、システム管理者権限のあるローカルユーザーとしてログインします。**iDRAC の設定** → **N 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。Act**ive Directory 設定と管理** ページの下にスクロールし、**設定のテスト** をクリックします。テストユーザー名とパスワードを入力し、**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。問題の解決に役立つように、詳細なテスト結果がログに記録されます。Active Directory の**設定と管理** ページに戻ります。設定を変更し、テストユーザーが認証手順に合格するまでテストを再実行するには、ページの下までスクロールし、**Active Directory の設定** をクリックします。

証明書の検証を有効にしましたが、Active Directory のログインに失敗しました。GUI から診断を実行しましたが、テスト結果に次のエラーメッセージが表示されています。

ERROR（エラー）: Can't contact LDAP server（LDAP サーバーと通信できません）, error（エラー）:14090086:SSL routines（SSL ルーチン）:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed（証明書の検証に失敗しました）: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC（iDRAC に正しい認証局（CA）証明書がアップロードされていることを確認してください。）iDRAC の日付が証明書の有効期限内かどうか、また iDRAC で設定されたドメインコントローラのアドレスがディレクトリサーバーの証明書の件名と一致するかどうか確認してください。

何が問題なのでしょうか。どうすれば修正できますか。

証明書の検証が有効になっていると、iDRAC6 がディレクトリサーバーとの SSL 接続を確立したときに、iDRAC6 はアップロードされた CA 証明書を使用してディレクトリサーバーの証明書を検証します。認証の検証を失敗する最も一般的な理由として、次が挙げられます。

1. iDRAC6 の日付がサーバー証明書または CA 証明書の有効期限内ではない。証明書の iDRAC6 の日付と有効期限を確認してください。
2. iDRAC6 で設定されたドメインコントローラのアドレスがディレクトリサーバー証明書のサブジェクトまたはサブジェクト代替名と一致しない。IP アドレスを使用している場合は、次の質問と回答をお読みください。FQDN を使用している場合は、ドメインではなく、ドメインコントローラの FQDN を使用しているかどうか確認してください（たとえば、`example.com` ではなく、`servername.example.com` ）。

ドメインコントローラのアドレスに IP アドレスを使用していますが、証明書の検証に失敗します。何が問題なのでしょうか。

ドメインコントローラ証明書の サブジェクトまたはサブジェクト代替名 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 サブジェクトまたはサブジェクト代替名 フィールドにドメインコントローラの IP アドレスではなく、ホスト名を使用します。この問題は複数の方法で修正できます。

1. サーバー証明書のサブジェクトまたはサブジェクト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。
2. iDRAC6 で設定された IP アドレスと一致する IP アドレスをサブジェクトまたはサブジェクト代替名のフィールドで使用するようにサーバー証明書を再発行します。
3. SSL ハンドシェイク時に証明書の検証がなくても、このドメインコントローラを信頼する場合は、証明書の検証を無効にします。

マルチドメイン環境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 オブジェクトが属するドメインのドメインコントローラのホスト名（FQDN）または IP アドレスを使用します。

いつグローバルカタログアドレスを設定する必要がありますか。

拡張スキーマを使用している場合、グローバルカタログアドレスは使用されません。

標準スキーマを使用し、ユーザーと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、使用できるのはユニバーサルグループのみです。

標準スキーマを使用し、すべてのユーザーと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、ユーザーと役割グループがそのドメインにある場合は、権限が保存されます。

グローバルコントローラアドレスが設定されている場合は、iDRAC6 グローバルカタログのクエリを継続します。グローバルカタログから追加の権限が取得された場合は、これらの権限が蓄積されます。

iDRAC6 は、常に LDAP オーバー SSL を使用しますか。

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

設定のテスト 中、iDRAC6 は問題を特定するためにのみ、LDAP CONNECT を行いますが、不安定な接続では LDAP BIND を行いません。

iDRAC6 で、証明書の検証がデフォルトで有効になっているのはなぜですか。

iDRAC6 は、接続先となるドメインコントローラの身元を確認するために、強力なセキュリティ対策を実施しています。証明書を検証しないと、ハッカーはドメインコントローラになりすまし、SSL 接続を乗っ取る危険があります。証明書の検証なしに、自分のセキュリティ境界内のドメインコントローラをすべて信頼する場合は、GUI または CLI を使用して無効にすることもできます。

iDRAC6 は NetBIOS 名をサポートしていますか。

このリリースでは、サポートされていません。

Active Directory を使用して iDRAC6 にログインできない場合は、何を確認すればいいですか。

iDRAC6 ウェブベースのインタフェースの **Active Directory 設定と管理** ページの下部にある **設定のテスト** をクリックすると、問題を診断できます。次に、テスト結果で特定された問題を修正します。詳細については、159 ページの「設定のテスト」参照してください。

本項では、最もよくある問題について説明します。一般的に、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。

   ログインした後、次を行います。

   a. iDRAC6 **Active Directory 設定と管理** ページにある **Active Directory を有効にする** オプションが選択されていることを確認します。

   b. iDRAC6 ネットワーク設定 ページの DNS 設定が正しいことを確認します。

   c. 証明書の検証を有効にした場合は、iDRAC6 に正しい Active Directory ルート CA 証明書がアップロードされていることを確認します。iDRAC6 の日時が CA 証明書の有効期限内であることを確認します。

   d. 拡張スキーマを使用している場合は、**iDRAC6 名** と **iDRAC6 ドメイン名** が Active Directory の環境設定と一致していることを確認します。

      標準スキーマを使用している場合は、**グループ名** と **グループドメイン名** が Active Directory の環境設定と一致していることを確認します。
3. ドメインコントローラの SSL 証明書で、iDRAC6 の日付が SSL 証明書の有効期限内であることを確認します。

8

iDRAC6 に対するシングルサインオンまたはスマートカードログインの設定

本項では、iDRAC6 に対して、ローカルユーザーおよび Active Directory ユーザーのスマートカードログインの設定と Active Directory ユーザーのシングルサインオン（SSO）を設定する方法について説明します。

iDRAC6 は、Active Directory スマートカードおよび SSO ログインの Kerberos ベースの Active Directory 認証をサポートします。

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 SSO 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、Kerberos をデフォルト認証方式として採用しています。

iDRAC6 では、Kerberos を使用して Active Directory SSO と Active Directory スマートカードログインの 2 種類の認証方式をサポートしています。Active Directory SSO 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。これは、ローカルスマートカード認証の追加機能です。

iDRAC6 の時刻がドメインコントローラの時刻と異なる場合は、iDRAC6 の Kerberos 認証に失敗します。最大 5 分のオフセットが許可されています。認証を成功させるには、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。

Active Directory SSO とスマートカード認証の必要条件

Active Directory SSO とスマートカード認証両方の必要条件は、次のとおりです。

- iDRAC6 を Active Directory ログイン 用に設定します。詳細については、129 ページの「iDRAC6 ディレクトリサービスの使用」を参照してください。
- iDRAC6 を Active Directory のルートドメインにある コンピュータとして登録します。これには、次の操作を行います。
  - **a** **iDRAC の設定** → **ネットワーク / セキュリティ** タブ → **ネットワーク** サブタブとクリックします。
  - **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 iDRAC を登録する** を選択します。
  - **d** 有効な **DNS ドメイン名** を入力します。

    詳細については、iDRAC6 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 ネットワーク上の Kerberos 対応サービスとして 自らを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 ベースのサービスが、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るようにします。

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

iDRAC6 は Windows 以外のオペレーティングシステム搭載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先の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 -princ
HOST/dracname.domainname.com@DOMAINNAME.COM -mapuser
dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -
pass * -out c:\krbkeytab
```

iDRAC6 が Kerberos 認証に使用する暗号タイプは DES-CBC-MD5 です。プリンシパルタイプは KRB5_NT_PRINCIPAL です。サービスプリンシパル名がマッピングされているユーザーアカウントのプロパティで、**このアカウントに DES 暗号化を使用する** プロパティが有効になっている必要があります。

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。

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ため、安全な場所に保管してください。

ktpass ユーティリティの詳細については、Microsoft ウェブサイトを参照してください。
http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true

- iDRAC6 の時刻を Active Directory ドメインコントローラの時刻に同期する必要があります。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 >
  ```

- 拡張スキーマのシングルサインオンを有効にするためには、keytab ユーザーに対して **委任** タブで **任意のサービスへの委任でこのユーザーを信頼する（Kerberos のみ）** オプションが選択されていることを確認してください。このタブは、**ktpass** ユーティリティを使って keytab ファイルを作成した後にのみ使用可能になります。

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、次の手順を実行します。

1. Internet Explorer ウェブ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** → **ローカルイントラネット** の順に選択します。
3. **サイト** をクリックします。
4. 次のオプションのみを選択します。
   - 他のゾーンに含まれていないすべてのローカル（イントラネット）サイトを含める。
   - プロキシサーバーをバイパスするすべてのサイトを含める。
5. **詳細** をクリックします。
6. SSO 設定の一部である Weblogic Server インスタンスとして使用する相対ドメイン名（myhost.example.co など）をすべて追加します。
7. **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 用のブラウザ設定を行うには、次の手順を実行します。

1. Firefox ウェブブラウザを開きます。
2. アドレスバーで `about:config` と入力します。
3. **フィルタ** で `network.negotiate` と入力します。
4. iDRAC 名を network.negotiate-auth.trusted-uris に追加します（カンマ区切りリストを使用）。
5. iDRAC 名を network.negotiate-auth.delegation-uris に追加します（カンマ区切りリストを使用）。

Microsoft Active Directory SSO の使用

SSO 機能を使用すると、ワークステーションにログインした後、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、iDRAC6 に直接ログインできます。この機能を使用して iDRAC6 にログインするには、有効な Active Directory ユーザーアカウントを使用してシステムに既にログインしていることが条件となります。また、Active Directory 資格情報を使用して iDRAC6 にログインするようにユーザーアカウントを事前に設定しておく必要があります。キャッシュに格納された Active Directory 資格情報を使用して iDRAC6 にログインできます。

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、SSO を有効にできます。詳細については、169 ページの「Kerberos 認証について」を参照してください。iDRAC6 を SSO ログイン用に設定する前に、170 ページの「Active Directory SSO とスマートカード認証の必要条件」の項にリストされている手順を実行したことを確認してください。

SSO を使用できるように iDRAC6 を設定する

iDRAC ウェブインタフェースを使って SSO を使用できるように、次の手順に従って iDRAC6 を設定します。

1. iDRAC ウェブインタフェースにログインします。
2. **iDRAC の設定** → **ネットワーク / セキュリティ** タブ → **ディレクトリサービス** タブ → **Microsoft Active Directory** と移動します。
3. **Active Directory の設定** をクリックします。**Active Directory の設定と管理手順 1/4** ページが開きます。
4. Active Directory のルートドメインから取得した keytab を iDRAC6 にアップロードするには、次の手順に従います。これを行うには、**Kerberos Keytab のアップロード** で、keytab ファイルのパスを入力するか、同ファイルを**参照**します。**アップロード** をクリックします。Kerberos keytab が iDRAC6 にアップロードされます。keytab は、170 ページの「Active Directory SSO とスマートカード認証の必要条件」にリストされているタスクの実行中に作成したのと同じファイルです。
5. **次へ** をクリックします。**Active Directory の設定と管理手順 4 の 2** ページが開きます。
6. **シングルサインオンを有効にする** を選択して、SSO ログインを有効にします。
7. 最後のページが表示されるまで **次へ** をクリックします。Active Directory が標準スキーマを使用するように設定されている場合は、**Active Directory 設定と管理手順 4 の 4a** ページが開きます。Active Directory が標準スキーマを使用するように設定されている場合は、**Active Directory 設定と管理手順 4 の 4** ページが開きます。
8. 設定を適用するには、**完了** をクリックします。

RACADM の使用：

次の CLI RACADM コマンドを使用して keytab ファイルを iDRAC6 にアップロードできます。

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

< ファイル名 > は keytab ファイルの名前です。RACADM コマンドはローカルとリモートの両方の RACADM でサポートされています。

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 config -g cfgActiveDirectory -o cfgADSSOEnable 1
```

SSO を使用して iDRAC6 にログインする

1. Active Directory の有効なアカウントを使ってシステムにログインします。
2. iDRAC6 ウェブページにアクセスするには、次のように入力します。

   `https://<FQDN 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://<FQDN アドレス>:<ポート番号>`

   FQDN アドレス は iDRAC FQDN (idracdnsname.domain name) で、ポート番号 は HTTPS のポート番号です。

   メモ : FQDN の代わりに IP アドレスを使用すると、SSO に失敗します。

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

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

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

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** を有効にすることにより、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、これは最小限のセキュリティしか提供しません。

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。

ローカル iDRAC6 ユーザーに対するスマートカードログオンの設定

ローカル iDRAC6 ユーザーがスマートカードを使って iDRAC6 にログインするように設定できます。**iDRAC の設定** → **ネットワーク / セキュリティ** → **ユーザー** とクリックします。

ただし、ユーザーがスマートカードを使用して iDRAC6 にログインするには、まずユーザーのスマートカード証明書と、信頼される認証局（CA）の証明書を iDRAC6 にアップロードする必要があります。

メモ : スマートカードを設定する前に、CA 証明書の検証が有効になっていることを確認してください。

スマートカード証明書のエクスポート

ユーザーの証明書を取得するには、カード管理ソフトウェア（CMS）を使用して、スマートカードから Base64 符号化形式ファイルにスマートカード証明書をエクスポートします。CMS は通常、スマートカードのベンダーから入手できます。この符号化ファイルをユーザーの証明書として iDRAC6 にアップロードしてください。スマートカードのユーザー証明書を発行する信頼された認証局も、CA 証明書を Base64 エンコード形式でファイルにエクスポートする必要があります。ユーザー用の信頼された CA 証明書としてこのファイルをアップロードします。スマートカード証明書内でユーザーのユーザープリンシプル名（UPN）を形成するユーザー名を使用してユーザーを設定します。

メモ : iDRAC6 にログインするには、iDRAC6 で設定するユーザー名が、大文字と小文字の区別を含め、スマートカード証明書のユーザープリンシプル名（UPN）と同じでなければなりません。

たとえば、スマートカード証明書が「sampleuser@domain.com」というユーザーに発行された場合、ユーザー名は 「sampleuser」となります。

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

Active Directory スマートカードログオン機能を使用する前に、iDRAC6 に Active Directory ログインできるように設定されており、スマートカードが発行されたユーザーアカウントで iDRAC6 Active Directory ログインが有効になっていることを確認してください。

Active Directory のログオン設定が有効になっていることも確認してください。Active Directory ユーザーの設定方法については、129 ページの「iDRAC6 ディレクトリサービスの使用」を参照してください。また、Active Directory のルートドメインから取得した有効な keytab ファイルを iDRAC6 にアップロードして、iDRAC6 を Kerberos 対応サービスにする必要もあります。

Active Directory ユーザーがスマートカードを使って iDRAC6 にログインできるように設定するには、iDRAC6 管理者は DNS サーバーを設定して、Active Directory CA 証明書を iDRAC6 にアップロードし、Active Directory ログオンを有効にします。Active Directory ユーザーの設定方法については、129 ページの「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 を設定するには、**iDRAC の設定** → **ネットワーク / セキュリティ** → **ディレクトリサービス** → **Microsoft Active Directory** の順にクリックします。

メモ : スマートカードを設定する前に、CA 証明書の検証が有効になっていることを確認してください。

iDRAC6 を使ったスマートカードの設定

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

1. iDRAC6 ウェブインタフェースで、**iDRAC の設定** → **ネットワーク / セキュリティ** → タブ **スマートカード** の順に選択します。
2. スマートカードのログオン設定を指定します。
   表 8-1 に、**スマートカード** ページの設定を示します。
3. **適用** をクリックします。

表 8-1. スマートカードの設定

設定	説明
スマートカードログオンの設定	• **無効** — スマートカードログオンを無効にします。以降、グラフィカルユーザーインタフェース（GUI）からログインすると、通常のログインページが表示されます。セキュアシェル（SSH）、Telnet、シリアル、リモート RACADM を含むすべての帯域外インタフェースは、各々の状態を維持します。 • **有効** — スマートカードログオンを有効にします。変更を適用した後、ログアウトして、スマートカードを挿入し、**ログイン** をクリックしてスマートカード PIN を入力します。スマートカードログオンを有効にすると、SSH、Telnet、シリアル、リモート RACADM、IPMI over LAN などの CLI 帯域外インタフェースは単一要素認証しかサポートしていないため、これらはすべて無効になります。 • **リモート RACADM と共に有効にする** — スマートカードログオンとリモート RACADM を有効にします。その他の CLI 帯域外インタフェースがすべて無効になります。 **有効にする** または **リモート RACADM と共に有効にする** を選択すると、ウェブベースのインターフェースを使用する以降のログイン試行でスマートカード のログオンを要求されます。 **リモート RACADM と共に有効にする** は、iDRAC6 システム管理者がリモート RACADM コマンドを使ってスクリプトを実行する目的で iDRAC6 ウェブベースのインタフェースにアクセスする場合に限り、設定することをお勧めします。リモート RACADM を使用する必要がないときは、スマートカードログオンを **有効にする** 設定を選択してください。iDRAC6 のローカルユーザー設定や Active Directory の設定が完了していることを確認してから、スマートカードログオン を有効にしてください。 **メモ :** スマートカードログインでは、適切な証明書を使用してローカル iDRAC6 ユーザーを設定する必要があります。スマートカードログオンを Microsoft Active Directory ユーザーのログインに使用する場合は、そのユーザーの Active Directory ユーザー証明書を設定する必要があります。ユーザー証明書は、**ユーザー** ? **ユーザーメインメニュー** ページで設定できます。

表 8-1. スマートカードの設定 （続き）

設定	説明
スマートカードログオンの CRL チェックを有効にする	このチェックはスマートカードのローカルユーザーにのみ使用可能です。このオプションは、ユーザーのスマートカード証明書を失効させるために iDRAC6 で証明書失効リスト（CRL）をチェックする場合に選択します。証明書失効リスト（CRL）配信サーバーからダウンロードしたユーザーの iDRAC 証明書と照合してチェックします。 CRL 配信サーバーのリストがユーザーのスマートカード証明書に表示されています。 CRL が機能するには、ネットワーク構成の過程で iDRAC6 に DNS の有効な IP アドレスが設定されている必要があります。iDRAC6 の **iDRAC の設定** → **ネットワーク / セキュリティ** → **ネットワーク** で DNS の IP アドレスを設定できます。 次の場合には、ユーザーはログインできません。 • ユーザー証明書が CRL ファイルのリストで失効となっている。 • iDRAC6 が CRL 配信サーバーと通信できない。 • iDRAC6 が CRL をダウンロードできない。 **メモ :** このチェックに成功するには、**ネットワーク / セキュリティ** → **ネットワーク** ページで DNS サーバーの IP アドレスを正しく設定する必要があります。

スマートカードを使用した iDRAC6 へのログイン

iDRAC6 ウェブインタフェースは、スマートカードを使用するように設定されているすべてのユーザーに、スマートカードログオンページを表示します。

メモ : ユーザー用のスマートカードログオンを有効にする前に、iDRAC6 のローカルユーザーと Active Directory の設定が完了していることを確認してください。

メモ : ブラウザの設定によっては、この機能を初めて使用するときに Smart Card reader ActiveX プラグインのダウンロードとインストールを要求される場合があります。

1 https を使用して iDRAC6 のウェブページにアクセスします。

`https://<IP アドレス>`

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

`https://<IP アドレス>:<ポート番号>`

<IP 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、スマートカードを挿入するように求められます。

2 スマートカードをリーダーに挿入して **ログイン** をクリックします。

スマートカードの PIN を入力するように求められます。

3 ローカルスマートカードのスマートカード PIN を入力したとき、このユーザーがローカルで作成されていない場合は、ユーザーの Active Directory アカウントのパスワードを入力するように求められます。

メモ：スマートカードログオンの CTL チェックを有効にする が選択されている Active Directory ユーザーの場合は、CRL がダウンロードされ、ユーザーの証明書の CRL がチェックされます。証明書が CRL に失効と表示されているか、何らかの理由で CRL をダウンロードできない場合は、Active Directory を通したログインに失敗します。

これで、iDRAC6 にログインできます。

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

1 https を使用して iDRAC6 にログインします。

`https://<IP アドレス>`

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

`https://<IP アドレス>:<ポート番号>` ここで *IP アドレス* は iDRAC6 の IP アドレス、ポート番号 は HTTPS ポート番号になります。

iDRAC6 ログインページが表示され、スマートカードを挿入するように求められます。

2 スマートカードを挿入して、**ログイン** をクリックします。

PIN ポップアップダイアログボックスが表示されます。

3 パスワードを入力して、**OK** をクリックします。

Active Directory に設定した資格情報で iDRAC6 にログインします。

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

次は、スマートカードにアクセスできないときのデバッグに役立つヒントです。

ActiveX プラグインがスマートカードリーダーを検出しません

スマートカードが Microsoft Windows オペレーティングシステムでサポートされていることを確認します。Windows がサポートしているスマートカード暗号サービスプロバイダ（CSP）の数は限られています。

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

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。

ローカル iDRAC6 へのログインを無効にする

ローカルの iDRAC6 ユーザーがログインできない場合は、ユーザー名とユーザー証明書が iDRAC6 にアップロードされているかどうか確認します。iDRAC6 のトレースログに、エラーに関する重要なログメッセージが含まれていることがあります。ただし、セキュリティ上の理由から、エラーメッセージは意図的に曖昧になっている場合があります。

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

- Active Directory ユーザーとして iDRAC6 にログインできない場合は、スマートカードログオンを有効にしないで iDRAC6 にログインしてみてください。CRL チェックを有効にしている場合は、CRL チェックを有効にしないで Active Directory にログインしてみてください。iDRAC6 追跡ログには、CRL に失敗した場合の重要なメッセージが入っています。
- また、`racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0` コマンドを使用してローカル RACADM からスマートカードのログオンを無効にすることもできます。
- 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」が導入されていると、iDRAC6 認証 Active-X プラグインがインストールされません。Active–X プラグインを正しくインストールして実行するには、32 ビットバージョンの Microsoft Visual C++ 2005 SP1 再配布可能パッケージ（x86）を導入します。このパッケージは、Internet Explorer ブラウザで vKVM セッションを起動するのに必要です。
- エラーメッセージ「スマートカードプラグインをロードできません。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」というメッセージが表示された場合は、Microsoft Visual C++ 2005 SP1 再配布可能パッケージ（x86）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 **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。詳細については、表 8-2 を参照してください。

表 8-2. C++ 再配布可能パッケージの配布バージョン

再配布パッケージのファイル名	バージョン	リリース日	サイズ	説明
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 認証が機能するには、iDRAC6 とドメインコントローラサーバーの時刻の差が 5 分以内であることを確認してください。**RAC の時刻** は **システム** → **iDRAC の設定** → **プロパティ** → **iDRAC 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（分）>` たとえば、システムの時刻が GMT -6（米国 CST）で、時刻が 2PM であれば、iDRAC6 の時刻を GMT 時刻の 18:00 に設定します。その場合、上記のコマンドのオフセット値に 360 と入力する必要があります。また、*cfgRacTuneDaylightoffset* を使用すると、夏時間の調整ができます。この操作により、毎年 2 回夏時間の調整をするときに時刻を変更しなくても済みます。あるいは、上の例のオフセットに「300」を使用して誤差を見込みます。

SSO についてよくあるお問い合わせ（FAQ）

Windows Server 2008 R2 x64 では SSO のログインに失敗します。SSO を Windows Server 2008 R2 x64 で使用できるようにするにはどうすればよいですか。

1. ドメインコントローラとドメインポリシーに対して **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** を実行します。DES-CBC-MD5 暗号スイートを使用するようにコンピュータを設定します。これらの設定は、クライアントコンピュータまたはサービス、およびお使いの環境内のアプリケーションとの互換性に影響を与える場合があります。**Kerberos で許可された暗号化タイプの設定** ポリシーの設定は、**Computer Configuration\Security Settings\Local Policies\Security Options** にあります。

2 ドメインクライアントには更新された GPO が必要です。コマンドラインで `gpupdate /force` を入力し、古いキータブを `klist purge` cmd と入れ替えます。

3 GPO を更新したら、新しいキータブを作成します。

4 キータブを iDRAC6 にアップロードします。

これで、SSO を使用して iDRAC にログインできます。

Windows 7 と Windows Server 2008 R2 の AD ユーザーの SSO ログインに失敗します。これを解決するにはどうすればよいですか。

Windows 7 と Windows Server 2008 R2 の暗号化方式を有効にする必要があります。暗号化方式を有効にするには、次の手順を実行します。

1 システム管理者としてログインするか、管理者権限を持つユーザーとしてログインします。

2 **スタート** から **gpedit.msc** を実行します。**ローカルグループポリシーエディタ** ウィンドウが開きます。

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 すべてのオプションを有効にします。

6 **OK** をクリックします。これで、SSO を使用して iDRAC にログインできます。

拡張スキーマでは、次の追加設定を行います。

1 **ローカルグループポリシーエディタ** ウィンドウで、**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。

2 **ネットワークセキュリティ：NTLM の制限：リモートサーバーへの発信 NTLM トラフィック** を右クリックして **プロパティ** を選択します。

3 **すべて許可** を選択します。

4 **OK** をクリックして、**ローカルグループポリシーエディタ** ウィンドウを閉じます。

5 **スタート** から **cmd** を実行します。**コマンドプロンプト** ウィンドウが表示されます。

6 `gpupdate /force` コマンドを実行します。グループポリシーが更新されます。**コマンドプロンプト** ウィンドウを開きます。

7 **スタート** から **regedit** を実行します。**レジストリエディタ** ウィンドウが表示されます。

8 **HKEY_LOCAL_MACHINE**→ **System**→ **CurrentControlSet**→ **Control**→ **LSA** に移動します。

9 右ペインで、**新規** → **DWORD（32 ビット）値** を右クリックします。

10 新しいキーを **SuppressExtendedProtection** と名付けます。

11 **SuppressExtendedProtection** を右クリックして、**変更** をクリックします。

12 **値データ** フィールドに **1** を入力して **OK** をクリックします。

13 **レジストリ エディタ** ウィンドウを閉じます。これで、SSO を使用して iDRAC にログインできます。

iDRAC 用に SSO を有効にし、Internet Explorer を使って iDRAC にログインする場合に、SSO に失敗してユーザー名とパスワードの入力を求められます。解決方法を教えてください。

iDRAC の IP アドレスが **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** のリストに表示されていることを確認してください。リストに表示されていない場合は、SSO に失敗し、ユーザー名とパスワードの入力を求められます。**キャンセル** をクリックして、先に進んでください。

9

GUI 仮想コンソールの使用

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、ローカルのコンソールにリモートからグラフィックモードまたはテキストモードでアクセスできます。仮想コンソール機能を使用すると、1 つの場所から単一または複数の iDRAC6 システムを制御できます。

日常的なメンテナンスを各サーバーの前に座って行う必要はありません。デスクトップまたはラップトップコンピュータを使ってリモートからサーバーを管理できます。また、リモートから即座に他のユーザーと情報を共有することもできます。

仮想コンソールの使用

メモ : 仮想コンソールセッションを開いたとき、管理下サーバーはそのコンソールがリダイレクトされていることを示しません。

メモ : 仮想コンソールセッションが、管理ステーションから特定の iDRAC6 に対してすでに開かれている場合、同じ管理ステーションからその iDRAC6 に対して新しいセッションを開こうとすると失敗します。

メモ : 1 つの管理ステーションから複数の iDRAC6 コントローラに対して、仮想コンソールの複数のセッションを同時に開くことができます。

仮想コンソール ページでは、ローカルの管理ステーションのキーボード、ビデオ、およびマウスを使ってリモートシステムを管理し、リモート管理下サーバーでそのデバイスを制御できます。この機能を仮想メディア機能と併用すると、リモートでソフトウェアのインストールを実行できます。

仮想コンソールセッションに適用される規則

- 最大 4 つの仮想コンソールセッションが同時にサポートされます。すべてのセッションで、同じ管理下サーバーのコンソールが同時に表示されます。
- バージョン 1.5 以降では、複数リモートサーバーへの複数セッションを同じクライアントから開かれた順に実行できるようになりました。Java プラグインを使った仮想コンソールセッションが開いていると、ActiveX プラグインを使ってもう一つの仮想コンソールセッションを開くことができます。しかしながら、ActiveX ベースの仮想コンソールセッションが開いていると、Java プラグインを使う仮想コンソールをもう一つ開くことはできません。最初の仮想コンソールセッションを閉じてから、2 番目の仮想コンソールセッションを開く必要があります。

- 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。
- iDRAC6 への最初の仮想コンソールセッションは、フルアクセスのセッションとなります。2 人目のユーザーが仮想コンソールセッションを要求したら、最初のユーザーはそのことを知らされ、2 人目のユーザーに共有要求を送信するオプション（許可、拒否、読み取り専用として許可）が与えられます。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。最初のユーザーがその後の各ユーザーの共有要求に 30 秒の待ち時間内に応答しないと、`cfgRacTuneVirtualConsoleAuthorizeMultipleSessions` オブジェクト用に設定されている値に基づいて仮想コンソールへのアクセスが許可されます。このオブジェクトは、2 番目 /3 番目 /4 番目のセッションで使用するように設定されているプラグインタイプ（ActiveX または Java）には依存しません。このオブジェクトの詳細については、デルサポートサイト **dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

  メモ : この規則は、リモートまたはファームウェア（SSH または Telnet）RACADM にのみ適用可能で、ローカル RACADM には適用できません。

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、次の手順を実行してください。

1. 対応ウェブブラウザをインストールして設定します。詳細については、次の項を参照してください。
   - 24 ページの「対応ウェブブラウザ」
   - 39 ページの「対応ウェブブラウザの設定」
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。Internet Explorer ブラウザを使用している場合、コンソールビューア用に ActiveX コントロールが提供されています。JRE をインストールし、iDRAC6 ウェブインタフェースでコンソールビューアを起動前に設定すると、Firefox でも Java コンソールビューアを使用できます。
3. Internet Explorer（IE）を使用している場合、次の手順に従って、ブラウザが暗号化されたコンテンツをダウンロードできるようにします。
   - Internet Explorer で **ツール**→ **インターネットオプション**→ **詳細設定** の順に選択します。
   - **セキュリティ** までスクロールし、次のオプションをクリアします。
     暗号化されたページをディスクに保存しない

4 IE を使って Active-X プラグインを搭載した仮想コンソールセッションを起動する場合は、iDRAC6 IP またはホスト名が **信頼済みサイト** リストに追加されていることを確認してください。また、カスタム設定を **中低** にリセットするか、署名済みの Active-X プラグインをインストールできるように設定を変更する必要もあります。詳細については、186 ページの「仮想コンソールと仮想メディアアプリケーションに基づく ActiveX 用の Internet Explorer ブラウザ設定」を参照してください。

メモ : 64 ビット ActiveX プラグインは、Internet Explorer を使った仮想コンソールセッションの起動ではサポートされていません。

5 画面解像度は 1280x1024 ピクセル以上に設定することをお勧めします。

メモ : システムで Linux オペレーティングシステムが稼動している場合は、ローカルモニターで X11 コンソールが表示されないことがあります。Linux をテキストコンソールに切り替えるには、iDRAC6 仮想コンソール で <Ctrl><Alt><F1> キーを押します。

メモ :「`Expected: ;`」という Java Script コンパイルエラーが発生する場合があります。この問題を解決するには、JavaWebStart で **ダイレクト接続** を使用するようにネットワーク設定を調整します。**編集** → **プリファレンス** ? **全般** → **ネットワーク設定** の順に選択し、**ブラウザ設定を使用する** の代わりに **ダイレクト接続** を選択します。

ブラウザのキャッシュのクリア

仮想コンソールの操作中に問題（範囲外エラーや同期問題など）が発生した場合は、ブラウザのキャッシュをクリアして、システムに格納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。

メモ : ブラウザのキャッシュをクリアするには、システム管理者特権が必要です。

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 Video Viewer 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、**アドオンを有効または無効にする** をクリックします。**アドオンの管理** ウィンドウが表示されます。

3 **表示** ドロップダウンメニューから **Internet Explorer によって使用されているアドオン** を選択します。

4 *Video Viewer* アドオンを削除します。

IE8 の古いバージョンの Active-X ビューアをクリアするには、次の手順を行います。

1 Video Viewer 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、**アドオンを有効または無効にする** をクリックします。**アドオンの管理** ウィンドウが表示されます。

3 **表示** ドロップダウンメニューから **すべてのアドオン** を選択します。

4 *Video Viewer* アドオンを選択し、**詳細情報** リンクをクリックします。

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` または `javaws-uninstall` を実行します。

2 **Java キャッシュビューア** が表示されます。

3 iDRAC6 仮想コンソールクライアント というタイトルの項目を削除します。

仮想コンソールと仮想メディアアプリケーションに基づく ActiveX 用の Internet Explorer ブラウザ設定

本項では、ActiveX ベースの仮想コンソールと仮想メディアアプリケーションの起動と実行に必要な Internet Explorer ブラウザ設定について説明します。

メモ : ブラウザのキャッシュをクリアしてから、ブラウザ設定を指定します。詳細については、185 ページの「ブラウザのキャッシュのクリア」を参照してください。

Microsoft Windows オペレーティングシステムの共通設定

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** タブの順に選択します。

2 アプリケーションの実行に使用するゾーンを選択します。

3 **カスタム** をクリックします。Internet Explorer 8 を使用している場合は、**カスタムレベル** をクリックします。**セキュリティ設定** ウィンドウが表示されます。

4 **ActiveX コンソールとプラグイン** で、次を選択します。

- **署名付き ActiveX コントロールのダウンロード** の **プロンプト** オプション
- **ActiveX コントロールとプラグインの実行** の **有効** または**プロンプト** オプション
- **スクリプトが安全とマークされた ActiveX コントロールのスクリプト** の **有効** または**プロンプト** オプション
- **OK** をクリックし、もう一度 **OK** をクリックします。

Windows Vista または Newer Microsoft オペレーティングシステム用の追加設定

Windows Vista またはそれ以降のオペレーティングシステムの Internet Explorer ブラウザには、「保護モード」と呼ばれる追加のセキュリティ機能があります。

「保護モード」付きの Internet Explorer ブラウザでは、ActiveX アプリケーションを次のいずれかの方法で起動して実行できます。

- **プログラムファイル** → **Internet Explorer** の順に選択します。**iexplore.exe** を右クリックして、**管理者として実行** をクリックします。
- iDRAC IP アドレスを信頼済みサイトに追加します。これには、次の操作を行います。

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** → **信頼済みサイト** の順に選択します。
2. 信頼済みサイトゾーンに対して **保護モードを有効にする** オプションが選択されていないことを確認してください。または、iDRAC アドレスをイントラネットゾーン内のサイトに追加することもできます。イントラネットゾーンと信頼済みサイトゾーンでは、保護モードはデフォルトでオフになっています。
3. **サイト** をクリックします。
4. **次のウェブサイトをゾーンに追加する** フィールドに iDRAC のアドレスを追加し、**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。
6. 設定を有効にするために、ブラウザを閉じてから再起動します。

サポートされている画面解像度とリフレッシュレート

表 9-1 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 9-1. 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

iDRAC6 ウェブインタフェースでの仮想コンソールの設定

iDRAC6 の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、次の手順を実行してください。

1. iDRAC6 仮想コンソールを設定するには、**システム** → **コンソール / メディア** → **設定** の順にクリックします。
2. 仮想コンソールのプロパティを設定します。表 9-2 は、仮想コンソールの設定について説明しています。
3. 完了したら、**適用** をクリックして新しい設定を保存します。

表 9-2. 仮想コンソールの設定プロパティ

プロパティ	説明
有効	クリックして、仮想コンソールを有効または無効にします。このオプションが有効の場合は、仮想コンソールが有効であることを示します。デフォルト値は **有効** です。 **メモ :** 仮想コンソールの起動後に **有効** オプションをオンまたはオフにすると、既存の仮想コンソールセッションがすべて切断される可能性があります。
最大セッション数	仮想コンソールの最大セッション数（1 ～ 4）が表示されます。デフォルトは **2** です。
アクティブセッション数	アクティブなコンソールセッション数を表示します。このフィールドは読み取り専用です。
リモートプレゼンスポート	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。 **メモ :** 仮想コンソールの起動後に **リモートプレゼンスポート** の値を変更すると、既存の仮想コンソールセッションがすべて切断される可能性があります。

表 9-2. 仮想コンソールの設定プロパティ （続き）

プロパティ	説明
ビデオ暗号化有効	**チェックボックスがオン** の場合は、ビデオ暗号化が有効です。ビデオポートを経由するすべての トラフィックは、暗号化されます。 **チェックボックスがオフ** の場合は、ビデオ暗号化が無効です。ビデオポートを経由するトラフィックは暗号化されません。 デフォルトは、**暗号化** されます。暗号化を無効にすると、低速なネットワークパフォーマンスを改善できる場合があります。 **メモ：**仮想コンソールの起動後に **ビデオ暗号化有効** オプションをオンまたはオフにすると、既存の仮想コンソールセッションがすべて切断される可能性があります。
ローカルサーバービデオ有効	チェックボックスがオンの場合は、仮想コンソール中 iDRAC6 KVM モニターへの出力は無効になります。これにより、**仮想コンソール** を使って実行したタスクは、管理下サーバーのローカルモニターに表示されなくなります。
プラグインタイプ	設定するプラグインのタイプ。 • **ネイティブ**（Windows では ActiveX、Linux では Java プラグイン）— ActiveX ビューアは Internet Explorer でのみ機能します。 • **Java** — Java ビューアが起動します。

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、231 ページの「仮想メディアの設定と使用」を参照してください。

仮想コンソールセッションの開始

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が開始し、リモートシステムのデスクトップがビューアに表示されます。この仮想コンソール ビューアアプリケーションを使用すると、ローカル管理ステーションからリモートシステムのマウスとキーボードの機能を制御できます。

メモ：Windows Vista 管理ステーションから仮想コンソールを起動した場合、仮想コンソール再起動メッセージが表示される場合があります。これを回避するには、次の場所で適切なタイムアウト値を設定します。**コントロールパネル** → **電力オプション** → **節電機能** → **詳細設定** → **ハードディスク** → **< タイムアウト値 > 後にハードディスクをオフにする** と **コントロールパネル** → **電力オプション** → **高パフォーマンス** → **詳細設定** → **ハードディスク** → **< タイムアウト値 > 後にハードディスクをオフにする**。

ウェブインタフェースで仮想コンソールセッションを開くには、次の手順を実行してください。

1 **システム** → **コンソール / メディア** → **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 表 9-3 の情報を使用して、仮想コンソールセッションが利用可能であることを確認します。

表示されているプロパティ値の設定を変更する場合は、188 ページの「iDRAC6 ウェブインタフェースでの仮想コンソールの設定」を参照してください。

表 9-3. 仮想コンソール

プロパティ	説明
仮想コンソール有効	はい / いいえ（チェックボックスがオン \ チェックボックスがオフ）
ビデオ暗号化有効	はい / いいえ（チェックボックスがオン \ チェックボックスがオフ）
最大セッション数	サポートされている仮想コンソールの最大セッション数を表示します。
アクティブセッション数	現在アクティブな仮想コンソールのセッション数を表示します。
ローカルサーバービデオ有効	はい = 有効、いいえ = 無効。
リモートプレゼンスポート	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。
プラグインタイプ	**設定** ページで選択したプラグインのタイプを表示します。 **メモ :** 64 ビット Windows プラットフォームの場合、64 ビットバージョンの「Microsoft Visual C++ 2005 再配布可能パッケージ」が導入されていると、iDRAC6 認証 Active-X プラグインが正しくインストールされません。Active–X プラグインを正しくインストールして実行するには、32 ビットバージョンの Microsoft Visual C++ 2005 SP1 再配布可能パッケージ（x86）を導入します。このパッケージは、Internet Explorer ブラウザで vKVM セッションを起動するのに必要です。

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、231 ページの「仮想メディアの設定と使用」を参照してください。

3 仮想コンソールセッションが利用可能な場合は、**仮想コンソールおよび仮想メディア** ページで **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 : 次の手順の途中で **セキュリティアラート** 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、iDRAC6 仮想コンソール ビューアアプリケーションにリモートシステムのデスクトップが表示されます。

4 2 つのマウスポインタ（1 つはリモートシステム用、もう 1 つはローカルシステム用）がビューアウィンドウに表示されます。iDRAC6 仮想コンソールメニューの **ツール** で **単一カーソル** オプションを選択すると、1 つのカーソルに変更できます。

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** → **システムの概要** 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。イメージは 30 秒ごとに自動的に更新されます。

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おり、iDRAC6 Enterprise カードがあるときにのみ表示されます。

表 9-4 には、利用可能なオプションに関する情報が記載されています。

表 9-4. 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	このリンクをクリックして、仮想コンソールを起動します。 仮想メディアだけが有効になっている場合は、このリンクをクリックすると仮想メディアが起動します。 仮想コンソール権限がないか、仮想コンソールと仮想メディアが両方とも無効になっている場合は、このリンクは表示されません。
設定	このリンクをクリックすると、**コンソール / メディア設定** ページで仮想コンソールの設定を表示、編集できます。 **メモ :** 仮想コンソールの設定を編集するには、iDRAC の設定権限が必要です。
更新	このリンクをクリックすると、表示されている仮想コンソールイメージを更新できます。

iDRAC6 仮想コンソールの使用（Video Viewer）

iDRAC6 仮想コンソール（Video Viewer）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ため、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、iDRAC6 仮想コンソールが別のウィンドウで開始します。

メモ：iDRAC6 仮想コンソール（Video Viewer）を起動するには、システム管理者特権が必要です。

メモ：リモートサーバーの電源がオフになっていると、**信号がありません**というメッセージが表示されます。

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する先の iDRAC の DNS 名または IP アドレスが表示されます。iDRAC が DNS 名を持たない場合は、IP アドレスが表示されます。このサブコマンドのフォーマットは次の通りです。

`<DNS 名 / IPv6 アドレス / IPv4 アドレス>, <モデル>, User: <ユーザー名>, <fps>`

iDRAC 6 仮想コンソールは、マウスの同期、スナップショット、キーボードマクロ、仮想メディアへのアクセスなど、さまざまなコントロール調整機能を提供します。これらの機能の詳細については、**システム** ? **コンソール / メディア** の順にクリックし、**仮想コンソールおよび仮想メディア** GUI ページで **ヘルプ** をクリックします。

仮想コンソールセッションを開始し、iDRAC6 仮想コンソールが表示されたら、マウスポインタの同期が必要になる場合があります。

表 9-5 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 9-5. 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
「ピン」アイコン	-	「ピン」アイコンをクリックして、iDRAC6 仮想コンソール メニューバーをロックします。これにより、ツールバーが自動的に非表示にならなくなります。 **メモ：**これは、Active-X ビューア にのみ適用できます。Java プラグインには使用できません。

表 9-5. ビューアメニューバーの選択項目 （続き）

メニュー項目	項目	説明
仮想メディア	**仮想メディアの起動**	**仮想メディアセッション** が表示され、メインウィンドウ内のマッピングに使用できるデバイスがリストされます。ISO または IMG イメージを仮想化するには、**追加** をクリックしてからイメージファイルを選択します。メインウィンドウにマッピングできるデバイスのリストと共に選択したイメージファイルが表示されます。デバイスまたは am イメージを仮想化するには、テーブルの **マップ** 列にあるオプションをオンにします。デバイスはこの時点でサーバーにマッピングされます。マップ解除するには、チェックボックスをオフにします。 **詳細** をクリックすると、仮想デバイスとイメージが一覧表示されているパネルが開きます。各デバイスまたはイメージの読み取り書き込み操作も表示されます。
ファイル	**ファイルへの取り込み**	現在のリモートシステム画面を Windows 上の **.bmp** ファイルまたは Linux 上の **.png** ファイルにキャプチャします。ダイアログボックスが表示され、指定した場所にファイルを保存できます。 **メモ : .bmp** ファイル形式（Windows）または **.png** ファイル形式（Linux）は、ネイティブプラグインに対してのみ適用できます。Java プラグインは **.jpg** および **.jpeg** ファイル形式のみをサポートします。
	終了	コンソールの使用を終え、（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、**ファイル** メニューから **終了** を選択して **iDRAC6 仮想コンソール** ウィンドウを閉じます。
表示	**更新**	ビデオ仮想コンソールの表示を更新します。仮想コンソールはサーバーにリファレンスビデオフレームを要求します。
	全画面 / ウィンドウ表示	ビデオ仮想コンソールを全画面表示モードで表示します。全画面表示モードを終了するには、**ウィンドウ表示** をクリックします。
	ビデオに合わせる	ビデオ仮想コンソールのサイズをサーバーのビデオを表示するために最小限必要なサイズに変更します。このメニュー項目は、全画面表示モードにはありません。

表 9-5. ビューアメニューバーの選択項目 （続き）

メニュー項目	項目	説明
マクロ	• **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** • **Tab** • **Ctrl+Enter** • **SysRq** • **Alt+LShift+RShift+Esc** • **Ctrl+Alt+Backspace** • **Alt+F?**（ここで F? は F1-F12 キーを表す） • **Ctrl+Alt+F?**（ここで F? は F1-F12 キーを表す）	マクロを選択するか、マクロに指定されたホットキーを入力すると、リモートシステムでそのアクションが実行されます。

表 9-5. ビューアメニューバーの選択項目 （続き）

メニュー項目	項目	説明
ツール	**セッションオプション**	セッションオプション ウィンドウには、別のセッションビューアコントロール調整機能も用意されています。このウィンドウには **全般** タブと **マウス** タブがあります。 全般 タブからは **キーボードのパススルーモード** も管理できます。**すべてのキー入力をターゲットにパスする** を選択すると、管理ステーションのキー入力がリモートシステムにパスされます。 マウス タブには、**単一カーソル** と **マウスアクセラレータ** という 2 つのセクションが含まれています。**単一カーソル** 機能は一部のリモートオペレーティングシステムでのマウス配置問題をオフセットします。ビューアが **単一カーソル** モードに入ると、マウスポインタはビューアウィンドウ内にトラップされます。このモードを終了するには、終了キーを押します。単一カーソルモードから移動するには、このコントールを使用してキーを選択します。 **マウスアクセラレータ** は、お使いのオペレーティングシステムに応じて、マウスの性能を最適化します。
	単一カーソル	ビューアで単一カーソルモードを有効にします。このモードでは、クライアントのカーソルは表示されないため、サーバーのカーソルのみが表示されます。クライアントのカーソルもビューア内にトラップされます。ユーザーは、**セッション オプション**の **マウス** タブで指定した **終了キー** を押すまで、ビューアウィンドウの外でカーソルを使用することができません。
	統計	このメニューオプションでは、ビューアのパフォーマンス統計を表示するダイアログが起動します。表示される値は次のとおりです。 • フレームレート • 帯域幅 • 圧縮 • パケットレート

表 9-5. ビューアメニューバーの選択項目 （続き）

メニュー項目	項目	説明
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。 **メモ：**このオプションを使って正常なシャットダウンを行う前に、そのオペレーティングシステムのシャットダウンオプションが有効になっていることを確認してください。シャットダウンオプションを設定せずにオペレーティングシステムでこのオプションを使用すると、シャットダウン操作を実行せずに、管理下システムを再起動します。
	システムをリセットする（ウォームブート）	電源を切らずにシステムを再起動します。
	システムの電源を入れなおす（コールドブート）	システムの電源を切ってから再起動します。
ヘルプ	**内容と索引**	オンラインヘルプの表示方法に関する手順を示します。
	iDRAC6 仮想コンソールについて	**iDRAC6 仮想コンソール** バージョンを表示します。

ローカルサーバービデオの有効または無効

iDRAC6 ウェブインタフェースで、iDRAC6 仮想コンソールの接続を無効にするように iDRAC6 を設定できます。

管理下サーバーのコンソールへの排他的アクセスを確保する場合は、ローカルコンソールを無効にし、*また* **仮想コンソールの設定** ページ で **最大セッション数** を 1 に 再設定する必要があります。

メモ：サーバー上のローカルビデオを無効にする（オフにする）と、iDRAC6 仮想コンソールに接続しているモニタ、キーボード、マウスが無効になります。

ローカルコンソールを無効または有効にするには、次の手順に従ってください。

1. 管理ステーション上で、対応ウェブブラウザを開いて iDRAC6 にログインします。
2. **システム** ? **コンソール / メディア** ? **設定** の順にクリックします。
3. サーバー上でローカルビデオを無効にする（オフにする）には、**設定** ページで **ローカルサーバービデオ有効** チェックボックスをオフにしてから **適用** をクリックします。デフォルト値は オフ です。

メモ : ローカルサーバービデオをオンにした場合、オフにするには 15 秒かかります。

4 サーバー上でローカルビデオを有効にする（オンにする）には、**設定** ページで **ローカルサーバービデオを有効にする** チェックボックスをオンにしてから **適用** をクリックします。

仮想コンソールと仮想メディアページのリモート起動

仮想コンソール / 仮想メディアは、iDRAC6 ウェブ GUI から起動せずに、サポートされているブラウザに 1 つの URL を入力して起動します。お使いのシステムの構成に応じて、認証プロセス（ログインページ）を使用して手動で行われるか、仮想コンソール / 仮想メディアのビューアに自動的にリダイレクトされます。

SSO がシステムですでに設定されている場合、仮想コンソール / 仮想メディアの起動に URL フォーマットを使用することはできません。

仮想コンソールは、iDRAC6、LDAP および Active Directory でローカルに作成されたユーザーアカウントで起動できます。

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、Windows ベースのオペレーティングシステムではローカル、AD、SSO ログインしかサポートしていません。SC ログインはサポートされていません。

URL フォーマットを使用したコンソールの起動

ブラウザに `link<IP>/console` と入力した場合、ログイン設定に応じて、通常の手動ログイン手順でログインしてください。ログインに成功したら、仮想コンソール / 仮想メディアのビューが起動します。そうでない場合は、iDRAC6 GUI ホームページにリダイレクトされます。

iDRAC ウェブ GUI セッションは、vKVM ページのバックグラウンドに表示されます。

一度に起動できる仮想コンソールは 1 セッションのみです。

読み取り専用権限を持っている場合は、URL フォーマットを使用して仮想コンソールページだけを起動します。仮想メディアページは起動されません。

仮想コンソールが iDRAC6 で無効化されている場合でも、十分な権限を持つユーザーまたはシステム管理者は、引き続き仮想メディアを起動できます。十分な権限の詳細については、197 ページの「仮想コンソールと仮想メディアページのリモート起動」を参照してください。

一般的なエラーシナリオ

表 9-6 は、一般的なエラーシナリオ、エラー原因、および iDRAC6 の動作を示しています。

表 9-6. 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を入力しました。	*https://<IP>* が指定されている場合も同じ動作が起こり、ログインに失敗します。
iDRAC6 Enterprise Card がありません	iDRAC6 Enterprise Card がありません。そのため、仮想コンソール / 仮想メディアを使用できません。	iDRAC6 仮想コンソールビューアは起動されません。iDRAC6 GUI ホームページにリダイレクトされます。
特権が不十分です	仮想コンソールと仮想メディア権限がありません。	iDRAC6 仮想コンソール ビューアは起動されず、コンソール / メディア設定 GUI ページにリダイレクトされます。
仮想コンソール無効	仮想コンソールがシステムで無効になっています。	iDRAC6 仮想コンソール ビューアは起動されず、コンソール / メディア設定 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。

仮想コンソールについてよくあるお問い合わせ（FAQ）

表 9-7 は、よくあるお問い合わせとその回答です。

表 9-7. 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
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。	仮想コンソールと仮想メディアセッションは、ウェブセッションがログオフしてもアクティブのままになります。セッションからログアウトするには、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閉じてください。
サーバー上のローカルビデオがオフになっている場合に、新しいリモートコンソールビデオセッションを開始できますか。	はい。
ローカルビデオをオフにするように要求してからサーバー上のローカルビデオがオフになるまで 15 秒もかかるのはなぜですか。	ビデオがオフに切り替わる前に、ローカルユーザーが必要に応じて別の操作を実行できるように配慮されています。
ローカルビデオをオンにする場合に、遅延時間は発生しますか。	いいえ。ローカルビデオを **オン** にする要求を iDRAC6 が受信すると、ビデオは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。	ローカルコンソールを無効にすると、ローカルユーザーがビデオをオフにすることはできません。
ローカルユーザーがビデオをオンにすることもできますか。	ローカルコンソールを無効にすると、ローカルユーザーがビデオをオンにすることはできません。
ローカルビデオをオフに切り替えると、ローカルキーボードとマウスもオフになりますか。	いいえ
ローカルコンソールをオフにすると、リモートコンソールセッションのビデオはオフになりますか。	いいえ。ローカルビデオのオン / オフを切り替えても、リモートコンソールセッションには影響しません。

表 9-7. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）（続き）

質問	回答
iDRAC6 ユーザーがローカルサーバービデオをオン / オフにするために必要な権限は何ですか。	iDRAC6 の設定権限を持つユーザーであれば、ローカルコンソールをオン / オフにできます。
ローカルサーバービデオの現在のステータスを取得するには、どのようにしますか。	状態は iDRAC6 ウェブインタフェースの **仮想コンソールの設定** ページに表示されます。 RACADM CLI コマンドの `racadm getconfig -g cfgRacTuning` は、**cfgRacTuneLocalServerVideo** のオブジェクトにステータスを表示します。
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。iDRAC6 KVM クライアント上のスクロールバーも使ってみてください。
コンソールウィンドウが文字化けします。	Linux のコンソールビューアには UTF-8 文字コードが必要です。ロケールを確認し、必要に応じて文字コードをリセットしてください。
Linux テキストコンソール（Dell Unified Server Configurator（USC）、Dell Lifecycle Controller または Dell Unified Server Configurator Lifecycle Controller Enabled（USC-LCE））でマウスが同期しないのはどうしてですか。	仮想コンソールは USB マウスドライバを必要としますが、USB マウスドライバは X-Window オペレーティングシステムでしか使用できません。
マウスの同期の問題がまだ解決しません。	仮想コンソールセッションの開始前に、オペレーティングシステム用に正しいマウスが選択されていることを確認します。 iDRAC6 仮想コンソールクライアント上の iDRAC6 仮想コンソールメニューの **ツール** で **単一カーソル** オプションが選択されていることを確認します。デフォルトは、2 カーソルモードです。

表 9-7. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）（続き）

質問	回答
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中に、キーボードやマウスを使用できないのはなぜですか。	BIOS で仮想コンソールが有効になっているシステムで、Microsoft の対応オペレーティングシステムをリモートからインストールすると、EMS 接続メッセージが表示され、続行する前に **OK** を選択するように要求されます。リモートでマウスを使って **OK** を選択することはできません。ローカルシステムで **OK** を選択するか、リモートで管理下サーバーを再起動し、再インストールしてから、BIOS で仮想コンソールをオフにする必要があります。 このメッセージは、仮想コンソールが有効になったことをユーザーに通知するために、Microsoft によって生成されます。このメッセージが表示されないようにするには、オペレーティングシステムをリモートインストールする前に、必ず仮想コンソールを 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 のステータスが反映されないのはなぜですか。	iDRAC6 からアクセスした場合、管理ステーションの Num Lock インジケータは必ずしもリモートサーバーの Num Lock 状態と一致するとは限りません。Num Lock の状態は、管理ステーションの Num Lock の状態にかかわらず、リモートセッションが接続されたときのリモートサーバーの設定に依存します。
ローカルホストから仮想コンソール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ためです。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。
仮想コンソールセッションを実行するために必要な帯域幅はどれくらいですか。	良好なパフォーマンスを得るには、5 MB/ 秒の接続をお勧めします。最低限必要なパフォーマンスを得るためには、1 MB/ 秒の接続が必要です。
管理ステーションで仮想コンソールを実行するために最低限必要なシステム要件を教えてください。	管理ステーションには、256 MB 以上の RAM を搭載した Intel Pentium III 500 MHz プロセッサが必要です。

表 9-7. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）（続き）

質問	回答
iDRAC6 仮想コンソール Video Viewer 内に **「信号がありません」**のメッセージが表示されるのはなぜですか。	iDRAC6 仮想コンソール プラグインがリモートサーバーのデスクトップビデオを受信していない場合に、このメッセージが表示される場合があります。一般的に、これはリモートサーバーの電源がオフになると、この現象が発生します。リモートサーバーのビデオ受信の誤動作によって、このメッセージが表示される場合もあります。
iDRAC6 仮想コンソール Video Viewer に **「範囲外」**というメッセージが表示されるのはなぜですか。	ビデオをキャプチャするために必要なパラメータが、iDRAC6 がビデオをキャプチャできる範囲を超えている場合に、このメッセージが表示されます。ディスプレイの解像度やリフレッシュレートなどのパラメータが高すぎると、範囲外の状態が発生します。通常、パラメータの最大範囲は、ビデオのメモリサイズや帯域幅などの物理的な制限に基づいて設定されます。

10

WS-MAN インタフェースの使用

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、Distributed Management Task Force（DMTF）の Common Information Model（CIM）ベースの管理情報を伝達するために、WS-MAN を使用します。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 に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別に分類され、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、デルで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 を介して利用できるデータは、次の DMTF プロファイルおよび Dell 拡張プロファイルにマッピングされている iDRAC 計装インタフェースによって提供されます。

対応 CIM プロファイル

表 10-1. 標準 DMTF

標準 DMTF
1 ベースサーバー ホストサーバーを表す CIM クラスを定義します。
2 サービスプロセッサ iDRAC6 を表す CIM クラスの定義が記載されています。
3 物理資産 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ホストサーバーの FRU 情報を表示します。
4 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。
5 電源状況管理 電源制御操作の CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーの電源制御操作を実行します。
6 電源装置（バージョン 1.1） 電源装置を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーの電源装置を表し、消費電力の高低を示す電力消費量を説明します。

表 10-1. 標準 DMTF （続き）

標準 DMTF
7 CLP サービス CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して独自の CLP を実装します。
8 IP インタフェース
9 DHCP クライアント
10 DNS クライアント
11 Ethernet ポート 上記のプロファイルは、ネットワークスタックを表す CIM クラスを定義します。iDRAC6 は、これらのプロファイルを使用して iDRAC6 NIC の構成を表します。
12 ログ記録 異なるログの種類を表す CIM を定義します。iDRAC6 は、このプロファイルを使用してシステムイベントログ（SEL）と iDRAC6 RAC ログを表します。
13 ソフトウェアインベントリ インストールしたソフトウェアや利用可能なソフトウェアのインベントリの CIM クラスを定義します。iDRAC6 はこのプロファイルを使用して、現在インストールされている iDRAC6 ファームウェアバージョンのインベントリを TFTP プロトコルを使って実行します。
14 役割ベースの認証 役割を表す CIM を定義します。iDRAC6 は、このプロファイルを使用して iDRAC6 のアカウント特権を定義します。
15 ソフトウェアップデート 利用可能なソフトウェアアップデートのインベントリの CIM クラスを定義します。iDRAC6 はこのプロファイルを使用して、TFTP プロコルを使ってファームウェアアップデートのインベントリを実行します。
16 SMASH コレクション CLP の構成を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して独自の CLP を実装します。
17 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 を定義します。iDRAC6 は、この表で説明しているように、このプロファイルを使用して独自に実装したプロファイルをアドバタイズします。
18 ベースメトリック メトリックを表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用してホストサーバーのメトリックを表し、消費電力の高低を示す電力消費量を説明します。
19 簡易 ID 管理 ID を表す CIM クラスを定義します。iDRAC6 は、このプロファイルを使用して iDRAC6 のアカウントを定義します。
20 USB リダイレクト ローカル USB ポートのリモートリダイレクトを表す CIM を定義します。iDRAC6 は、このプロファイルを仮想メディアプロファイルと併せて使用し、仮想メディアを定義します。

表 10-1. 標準 DMTF （続き）

Dell 拡張
1 Dell Active Directory クライアントバージョン 2.0.0 iDRAC6 Active Directory クライアントおよび Active Directory グループのローカル権限を設定する CIM と Dell 拡張クラスを定義します。
2 Dell 仮想メディア iDRAC6 仮想メディアを設定する CIM と Dell 拡張クラスを定義します。USB リダイレクトプロファイルを拡張します。
3 Dell Ethernet ポート iDRAC6 NIC 用 NIC サイドバンドインターフェースを設定する CIM と Dell 拡張クラスを定義します。Ethernet ポートプロファイルを拡張します。
4 Dell 電力使用制御 ホストサーバーの電力バジェットを表したり、ホストサーバーの電力を設定 / 監視したりするための CIM と Dell 拡張クラスを定義します。
5 Dell 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。
6 Dell ジョブコントロール 設定ジョブを管理する CIM と Dell 拡張クラスを定義します。
7 Dell LC 管理プロファイル 自動検出などの Dell ライフサイクルコントローラの設定属性用に CIM と Dell 拡張クラスを定義します。このプロファイルは、パーツ交換、マザーボード交換、システムプロファイルのエクスポートおよびインポート、ネットワーク共有からの起動、および暗号化証明書の管理も有効化します。
8 Dell 持続的ストレージ Dell プラットフォームの vFlash SD カード上のパーティションを管理する CIM と Dell 拡張クラスを定義します。
9 Dell 簡易 NIC NIC ネットワークコントローラの設定を表す CIM と Dell 拡張クラスを定義します。
10 Dell BIOS および起動管理プロファイル Dell BIOS 属性を表し、ホストの起動順序を設定する CIM と Dell 拡張クラスを定義します。
11 Dell RAID プロファイル ホストの RAID ストレージの設定を表す CIM と Dell 拡張クラスを定義します。
12 Dell 電源プロファイル ホストの電源インベントリ情報を表示する CIM と Dell 拡張クラスを定義します。
13 Dell iDRAC カードプロファイル iDRAC6 インベントリ情報を表示する CIM と Dell 拡張クラスを定義します。このプロファイルは、iDRAC 属性とユーザーアカウントを設定するための表現と方法も提供します。
14 Dell ファンプロファイル ホストのファンインベントリ情報を表示する CIM と Dell 拡張クラスを定義します。

表 10-1. 標準 DMTF （続き）

Dell 拡張
15 Dell メモリプロファイル ホストの DIMM インベントリ情報を表示する CIM と Dell 拡張クラスを定義します。
16 Dell CPU プロファイル ホストの CPU インベントリ情報を表示する CIM と Dell 拡張クラスを定義します。
17 Dell システム情報プロファイル ホストプラットフォームインベントリ情報を表示する CIM と Dell 拡張クラスを定義します。
18 Dell PCI デバイスプロファイル ホストの PCI デバイスインベントリ情報を表示する CIM と Dell 拡張クラスを定義します。
19 Dell ビデオプロファイル ホストのビデオカードインベントリ情報を表示する CIM と Dell 拡張クラスを定義します。

iDRAC6 WS–MAN の実装は、伝送セキュリティ用にポート 443 で SSL を使用し、基本認証とダイジェスト認証をサポートしています。Windows WinRM および 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ユーティリティ、および Microsoft .NET などのアプリケーションプログラミング環境を活用することにより、ウェブサービスインタフェースを利用できます。

Dell Lifecycle Controller Remote Service の詳細については、次のマニュアルを参照してください。

- ユーザーズガイド
- リリースノート
- エラーメッセージおよびトラブルシューティングリスト

これらのマニュアルにアクセスするには、次の手順を実行します。

1. **dell.com/support/manuals** にアクセスします。
2. **ソフトウェア → システム管理 → Dell Unified Server Configurator および Lifecycle Controller** とクリックします。
3. 該当するバージョンをクリックして、特定のリリースに対するすべてのマニュアルを表示します。

Web Services インタフェースガイド（Windows および Linux）、プロファイルマニュアル、コードサンプル、ホワイトペーパー、およびその他の便利な情報には、**delltechcenter.com** で **OpenManage システム管理 → Lifecycle Controller** と進んでください。

詳細については、次の項も参照してください。

- DMTF ウェブサイト：**dmtf.org/standards/profiles/**
- WS–MAN リリースノートまたは Readme ファイル。

11

iDRAC6 SM-CLP コマンドライン インタフェースの使用

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

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

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

iDRAC6 SM-CLP のサポート

SM-CLP は iDRAC6 コントローラのファームウェアからホストされ、Telnet、SSH、およびシリアルベースのインタフェースをサポートしています。iDRAC6 SM-CLP インタフェースは、DMTF 機関が提供する SM-CLP 規格バージョン 1.0 に基づいています。iDRAC6 SM-CLP では、表 10-1 で説明されているすべてのプロファイルがサポートされます。

次の項では、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。

SM-CLP の機能

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

次にある SM-CLP コマンドライン構文の例を参照してください。

< バーブ > [< オプション >] [< ターゲット >] [< プロパティ >]

標準的な SM-CLP セッション中は、表 11-1 のリストにあるバーブを使って操作を実行できます。

表 11-1. システムでサポートされている CLI バーブ

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

SM-CLP の使用

正しい資格情報を使用して SSH（または Telnet）で iDRAC6 に接続します。SMCLP プロンプト（/admin1->）が表示されます。

SM-CLP のターゲット

表 11-2 は、上記の 表 11-1 で説明される操作をサポートするために SM-CLP から提供されるターゲットのリストです。

表 11-2. SM-CLP のターゲット

ターゲット	定義
admin1	管理ドメイン
admin1/profiles1	iDRAC6 の登録プロファイル
admin1/hdwr1	ハードウェア
admin1/system1	管理下システムターゲット
admin1/system1/redundancyset1	電源装置
admin1/system1/redundancyset1/pwrsupply*	管理下システムの電源装置
admin1/system1/sensors1	管理下システムセンサー
admin1/system1/capabilities1	管理下システム SMASH 収集機能
admin1/system1/capabilities1 pwrcap1	管理下システムの電力使用機能
admin1/system1/capabilities1 elecap1	管理下システムターゲット機能
admin1/system1/logs1	レコードログ収集ターゲット
admin1/system1/logs1/log1	システムイベントログ（SEL）のレコードエントリ
admin1/system1/logs1/log1/ÉåÉRÅ[Éh*	管理下システムの SEL レコードの個々のインスタンス
admin1/system1/settings1	管理下システムの SMASH 収集設定
admin1/system1/settings1 pwrmaxsetting1	管理下システムの最大電源割り当て設定
admin1/system1/settings1 pwrminsetting1	管理下システムの最小電源割り当て設定
admin1/system1/capacities1	管理下システム機能 SMASH 収集
admin1/system1/consoles1	管理下システムコンソール SMASH 収集
admin1/system1/usbredirectsap1	仮想メディア USB リダイレクト SAP
admin1/system1/usbredirectsap1/remotesap1	仮想メディア送信先 USB リダイレクト SAP
admin1/system1/sp1	サービスプロセッサ

表 11-2. SM-CLP のターゲット （続き）

ターゲット	定義
admin1/system1/sp1/timesvc1	サービスプロセッサ時間サービス
admin1/system1/sp1/capabilities1	サービスプロセッサ機能 SMASH 収集
admin1/system1/sp1/capabilities1/clpcap1	CLP サービス機能
admin1/system1/sp1/capabilities1/pwrmgtcap1	システムの電源状態管理サービス機能
admin1/system1/sp1/capabilities1/ipcap1	IP インタフェース機能
admin1/system1/sp1/capabilities1/dhcpcap1	DHCP クライアント機能
admin1/system1/sp1/capabilities1/NetPortCfgcap1	ネットワークポート構成機能
admin1/system1/sp1/capabilities1/usbredirectcap1	仮想メディア機能 USB リダイレクト SAP
admin1/system1/sp1/capabilities1/vmsapcap1	仮想メディア SAP 機能
admin1/system1/sp1/capabilities1/swinstallsvccap1	ソフトウェアインストールサービス機能
admin1/system1/sp1/capabilities1/acctmgtcap*	アカウント管理サービス機能
admin1/system1/sp1/capabilities1/adcap1	Active Directory 機能
admin1/system1/sp1/capabilities1/rolemgtcap*	ローカル役割ベースの管理機能
admin1/system1/sp1/capabilities/PwrutilmgtCap1	電力使用管理機能
admin1/system1/sp1/capabilities/metriccap1	メトリックサービス機能
admin1/system1/sp1/capabilities1/elecap1	複数要素認証機能
admin1/system1/sp1/capabilities1/lanendptcap1	LAN（Ethernet ポート）エンドポイント機能
admin1/system1/sp1/logs1	サービスプロセッサログ収集
admin1/system1/sp1/logs1/log1	システムレコードログ

表 11-2. SM-CLP のターゲット （続き）

ターゲット	定義
admin1/system1/sp1/logs1/log1/record*	システムログエントリ
admin1/system1/sp1/settings1	サービスプロセッサ設定収集
admin1/system1/sp1/settings1 clpsetting1	CLP サービス設定データ
admin1/system1/sp1/settings1 ipsettings1	IP インタフェース割り当て設定データ（静的）
admin1/system1/sp1/settings1 ipsettings1/staticipsettings1	静的 IP インタフェース割り当て設定データ
admin1/system1/sp1/settings1 ipsettings1/dnssettings1	DNS クライアント設定データ
admin1/system1/sp1/settings1 ipsettings2	IP インタフェース割り当て設定データ（DHCP）
admin1/system1/sp1/settings1 ipsettings2/dhcpsettings1	DHCP クライアント設定データ
admin1/system1/sp1/clpsvc1	CLP サーバープロトコルサービス
admin1/system1/sp1/clpsvc1 clpendpt*	CLP サーバープロトコルエンドポイント
admin1/system1/sp1/clpsvc1 tcpendpt*	CLP サーバープロトコル TCP エンドポイント
admin1/system1/sp1/jobq1	CLP サーバープロトコルジョブキュー
admin1/system1/sp1/jobq1/job*	CLP サーバープロトコルジョブ
admin1/system1/sp1/pwrmgtsvc1	電源状況管理サービス
admin1/system1/sp1/ipcfgsvc1	IP インターフェース設定サービス
admin1/system1/sp1/ipendpt1	IP インタフェースプロトコルエンドポイント
admin1/system1/sp1 ipendpt1/gateway1	IP インタフェースゲートウェイ
admin1/system1/sp1 ipendpt1/dhcpendpt1	DHCP クライアントプロトコルエンドポイント
admin1/system1/sp1 ipendpt1/dnsendpt1	DNS クライアントプロトコルエンドポイント

表 11-2. SM-CLP のターゲット （続き）

ターゲット	定義
admin1/system1/sp1/ipendpt1 dnsendpt1/dnsserver*	DNS クライアントサーバー
admin1/system1/sp1/NetPortCfgsvc1	ネットワークポート構成サービス
admin1/system1/sp1/lanendpt1	LAN エンドポイント
admin1/system1/sp1 lanendpt1/enetport1	Ethernet ポート
admin1/system1/sp1/VMediaSvc1	仮想メディアサービス
admin1/system1/sp1 VMediaSvc1/tcpendpt1	仮想メディア TCP プロトコルエンドポイント
admin1/system1/sp1/swid1	ソフトウェア識別
admin1/system1/sp1 swinstallsvc1	ソフトウェアインストールサービス
admin1/system1/sp1 account1-16	複数要素認証（MFA）アカウント
admin1/sysetm1/sp1/ account1-16/identity1	ローカルユーザー識別アカウント
admin1/sysetm1/sp1/ account1-16/identity2	IPMI 識別（LAN）アカウント
admin1/sysetm1/sp1/ account1-16/identity3	IPMI 識別（シリアル）アカウント
admin1/sysetm1/sp1/ account1-16/identity4	CLP 識別アカウント
admin1/system1/sp1/acctsvc1	MFA アカウント管理サービス
admin1/system1/sp1/acctsvc2	IPMI アカウント管理サービス
admin1/system1/sp1/acctsvc3	CLP アカウント管理サービス
admin1/system1/sp1/group1-5	Active Directory グループ
admin1/system1/sp1 group1-5/identity1	Active Directory 識別
admin1/system1/sp1/ADSvc1	Active Directory サービス
admin1/system1/sp1/rolesvc1	ローカルロールベース認証（RBA）サービス
admin1/system1/sp1/rolesvc1 Role1-16	ローカル役割

表 11-2. SM-CLP のターゲット （続き）

ターゲット	定義
admin1/system1/sp1/rolesvc1 Role1-16/privilege1	ローカル役割権限
admin1/system1/sp1/rolesvc1 Role17-21/	Active Directory 役割
admin1/system1/sp1/rolesvc1 Role17-21/privilege1	Active Directory 権限
admin1/system1/sp1/rolesvc2	IPMI RBA サービス
admin1/system1/sp1/rolesvc2 Role1-3	IPMI 役割
admin1/system1/sp1/rolesvc2 Role4	IPMI シリアルオーバー LAN（SOL）役割
admin1/system1/sp1/rolesvc3	CLP RBA サービス
admin1/system1/sp1/rolesvc3 Role1-3	CLP 役割
admin1/system1/sp1/rolesvc3 Role1-3/privilege1	CLP 役割権限
admin1/system1/sp1 pwrutilmgtsvc1	電源使用管理サービス
admin1/system1/sp1 pwrutilmgtsvc1/pwrcurr1	電源使用管理サービスの電力設定割り当て設定データ
admin1/system1/sp1/metricsvc1	メトリックサービス
/admin1/system1/sp1/metricsvc1/ cumbmd1	累積ベースメトリック定義
/admin1/system1/sp1/metricsvc1/ cumbmd1/cumbmv1	累積ベースメトリック値
/admin1/system1/sp1/metricsvc1/ cumwattamd1	累積ワット集約メトリック定義
/admin1/system1/sp1/metricsvc1/ cumwattamd1/cumwattamv1	累積ワット集約メトリック値
/admin1/system1/sp1/metricsvc1/ cumampamd1	累積アンペア集約メトリック定義
/admin1/system1/sp1/metricsvc1/ cumampamd1/cumampamv1	累積アンペア集約メトリック値

表 11-2. SM-CLP のターゲット （続き）

ターゲット	定義
/admin1/system1/sp1/metricsvc1/loamd1	低累積メトリック定義
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	低累積メトリック値
/admin1/system1/sp1/metricsvc1/hiamd1	高累積メトリック定義
/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*	高累積メトリック値
/admin1/system1/sp1/metricsvc1/avgamd1	平均累積メトリック定義
/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*	平均累積メトリック値

12

VMCLI を使用したオペレーティングシステムの導入

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

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

作業を開始する前に

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

リモートシステム要件

各リモートシステムで iDRAC6 が設定されている。

ネットワーク要件

ネットワーク共有に次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。

次の項では、Linux と Microsoft Windows システム用のイメージファイルの作成方法について説明します。

Linux システムのイメージファイルの作成

Linux システムのブータブルイメージファイルを作成するには、データ複製ユーティリティ（dd）を使用します。

ユーティリティを実行するには、コマンドプロンプトを開いて次のように入力します。

`dd if=<`*入力デバイス*`> of=<`*出力ファイル*`>`

たとえば、次のとおりです。

```
dd if=/dev/sdc0 of=mycd.img
```

Windows システムのイメージファイルの作成

Windows イメージファイル用のデータ複製ユーティリティを選択するときには、イメージファイルと CD/DVD のブートセクターをコピーするユーティリティを選んでください。

導入の準備

リモートシステムの設定

1. 管理ステーションからアクセスできるネットワーク共有フォルダを作成します。
2. オペレーティングシステムファイルをネットワーク共有フォルダにコピーします。
3. オペレーティングシステムをリモートシステムに導入する設定済みのブータブルな導入イメージファイルがある場合は、この手順をスキップしてください。

   設定済みのブータブルな導入イメージファイルがない場合は、このファイルを作成します。オペレーティングシステムの導入手順に使用されるプログラムやスクリプトをすべて含めます。

   たとえば、Windows オペレーティングシステムを導入する場合、イメージファイルには Microsoft Systems Management Server（SMS）で使用される導入方法と同様のプログラムを含めることができます。

   イメージファイルを作成するときは、次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手順を起動して実行するように、導入イメージを「読み取り専用」とマークする

4 次のいずれかの手順を実行してください。
   - 既存のオペレーティングシステム導入アプリケーションに **IPMItool** と VMCLI を組み込みます。ユーティリティを使用する際の手引きとして、**vm6deploy** サンプルスクリプトを使用します。
   - オペレーティングシステムの導入には、既存の **vm6deploy** スクリプトを使用します。

オペレーティングシステムの導入

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

始める前に、VMCLI ユーティリティに含まれているサンプル **vm6deploy** スクリプトを確認してください。このスクリプトは、ネットワーク内のリモートシステムにオペレーティングシステムを導入する手順を詳しく説明しています。

次は、ターゲットのリモートシステムにオペレーティングシステムを導入する手順の概要です。

1 **ip.txt** テキストファイルに、導入するリモートシステムの iDRAC6 IPv4 アドレスまたは IPv6 アドレス（1 行に 1 つの IPv4 または IPv6 アドレス）を入力します。
2 ブータブルなオペレーティングシステム CD または DVD をクライアントのメディアドライブに挿入します。
3 コマンドラインで **vm6deploy** を実行します。

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

```
vm6deploy -r ip.txt -u <iDRAC ユーザー> -p <iDRAC ユーザーのパスワード> -c {<iso9660-img> | <パス>} -f {< フロッピーデバイス > または < フロッピーイメージ >}
```

ここで、

- *<iDRAC6 ユーザー>* は iDRAC ユーザー名です（例：**root**）。
- *<iDRAC ユーザーのパスワード>* は iDRAC 6 ユーザーのパスワードです（**calvin など**）。
- *<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 イメージへのパスです。
- -f {< *フロッピーデバイス*>} は、オペレーティングシステムのインストール CD、DVD、またはフロッピーが挿入されているデバイスへのパスです。
- < *フロッピーイメージ* > は、有効なフロッピーイメージへのパスです。

vm6deploy スクリプトは、コマンドラインオプションを **VMCLI** ユーティリティに渡します。これらのオプションの詳細については、コマンドラインオプション を参照してください。このスクリプトが **-r** オプションを処理する方法は、**vmcli -r** オプションとは若干異なります。**-r** オプションの引数が既存のファイル名である場合、スクリプトは指定したファイルから iDRAC6 IPv4 または IPv6 アドレスを読み取り、各行で **VMCLI** ユーティリティを 1 度実行します。**-r** オプションの引数がファイル名でない場合は、単一の iDRAC6 のアドレスになります。この場合、**-r** は **VMCLI** ユーティリティの説明どおりに機能します。

VMCLI ユーティリティの使用

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

VMCLI ユーティリティには次の機能があります。

メモ : 読み取り専用のイメージファイルを仮想化するとき、複数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
- セキュアソケットレイヤ（SSL）を使用した iDRAC6 へのセキュアな通信

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

警告 : VMCLI コマンドラインユーティリティを起動する場合は、インタラクティブなフラグ「-i」オプションを使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場合にユーザー名とパスワードを表示されるため、ユーザー名とパスワードをプライベートにしておくことにより、セキュリティを強化できます。

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

クライアントシステムの管理者は、ユーザーグループとその権限を制御することで、このユーティリティを実行できるユーザーを制御します。

Windows システムの場合、VMCLI ユーティリティを実行するにはパワーユーザー特権が必要です。

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

VMCLI ユーティリティのインストール

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

『Dell Systems Management Tools and Documentation DVD』には、ストレージ管理、リモートアクセスサービス、IPMItool ユーティリティなど、最新のシステム管理ソフトウェア製品が含まれています。この DVD には、システム管理ソフトウェアに関する最新の製品情報を記載した Readme ファイルも入っています。

『Dell Systems Management Tools and Documentation DVD』には、VMCLI と IPMItool ユーティリティを使ってソフトウェアを複数のリモートシステムに展開する方法を示す **vm6deploy** と呼ばれるサンプルスクリプトも収録されています。

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

コマンドラインオプション

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

VMCLI コマンド形式は次のとおりです。

`VMCLI [ パラメータ ] [ オペレーティングシステムのシェルオプション ]`

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、220 ページの「VMCLI パラメータ <?>」を参照してください。

リモートシステムでコマンドが受け入れられ、iDRAC6 が接続を許可した場合は、次のいずれかが発生するまでコマンドが実行され続けます。

- 何らかの理由で VMCLI の接続が切れた。
- オペレーティングシステムのコントロールを使用して処理を手動で中止した。たとえば、Windows ではタスク マネージャを使用して処理を中止できます。

VMCLI パラメータ

iDRAC6 IP アドレス

`-r <iDRAC の IP アドレス [:iDRAC の SSL ポート]>`

このパラメータは、ユーティリティがターゲット iDRAC6 との仮想メディア接続を確立するために必要な iDRAC6 の IPv4 または IPv6 アドレスと SSL ポートを指定します。無効な IPv4 または IPv6 アドレス、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 IPv4 または IPv6 アドレスまたは iDRAC6 動的ドメインネームシステム（DDNS）名です（サポートされている場合）。*<iDRAC の SSL ポート>* を省くと、デフォルトのポート 443 が使用されます。iDRAC6 のデフォルト SSL ポートを変更する場合を除いて、オプションの SSL ポートは不要です。

iDRAC6 ユーザー名

`-u <iDRAC ユーザー>`

このパラメーターは仮想メディアを実行する iDRAC6 ユーザー名を指定します。

<iDRAC ユーザー> には、次の属性が必要です。

- 有効なユーザー名
- iDRAC6 仮想メディアユーザー権限

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

iDRAC6 ユーザーパスワード

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

フロッピー / ディスクデバイスまたはイメージファイル

`-f {<フロッピーデバイス> または <フロッピーイメージ>}` あるいは

`-c {<CD-DVD デバイス> または <CD-DVD イメージ>}`

ここで、**<フロッピーデバイス>** または `<CD-DVD デバイス>` は、有効なドライブ文字（Windows システムの場合）または有効なデバイスのファイル名（Linux システムの場合）を表し、`<フロッピーイメージ>` または `<CD-DVD イメージ>` は、有効なイメージファイルのファイル名とパスを表します。

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

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

たとえば、イメージファイルは次のように指定します。

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

`-f /tmp/myfloppy.img`（Linux システム）

イメージファイルが書き込み保護されていない場合は、仮想メディアがそのファイルに書き込むことができます。上書きしてはならないフロッピーイメージファイルへの書き込みを禁止するように、オペレーティングシステムを設定してください。

たとえば、デバイスは次のように指定します。

`-f a:\`（Windows システム）

`-f /dev/sdb4 # デバイス上の 4 番目のパーティション /dev/sdb`（Linux システム）

メモ： Red Hat Enterprise Linux バージョン 4 では、複数の LUN はサポートされていませんが、カーネルではこの機能がサポートされています。Red Hat Enterprise Linux バージョン 4 で複数の LUN を持つ SCSI デバイスを認識できるようにするには、次の手順を行います。

1. **/etc/modprobe.conf** を編集して、次の行を追加します。
   `options scsi_mod max_luns=8`
   （LUN の数は 8 のほかにも、2 以上の任意の数を指定できます。）
2. コマンドラインで次のコマンドを入力して、カーネルイメージの名前を取得します。
   `uname -r`
3. **/boot** ディレクトリに移動し、手順 2 で決定した名前のカーネルイメージファイルを削除します。
   `mkinitrd /boot/initrd-Åfuname -rÅf.img Åeuname -rÅf`
4. サーバーを再起動します。
5. 次のコマンドを実行して、手順 1 で指定した 数の LUN のサポートが追加されたことを確認します。
   `cat /sys/modules/scsi_mod/max_luns`

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

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

CD/DVD デバイスまたはイメージファイル

`-c {<` *デバイス名* `> | <` *イメージファイル* `>}`

この場合、< *デバイス名* > は有効な CD/DVD ドライブ文字（Windows システム）または有効な CD/DVD デバイスファイル名 （Linux システム）で、< *イメージファイル* > は有効な ISO-9660 イメージファイルのファイル名とパスです。

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

たとえば、イメージファイルは次のように指定します。

`-c c:\temp\mydvd.img`（Windows システム）

`-c /tmp/mydvd.img`（Linux システム）

たとえば、デバイスは次のように指定します。

`-c d:\`（Microsoft Windows システム）

`-c /dev/cdrom`（Linux システム）

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

スイッチオプションしかない場合を除いて、このコマンドで少なくとも 1 つメディアタイプ（フロッピーまたは CD/DVD ドライブ）を指定します。指定しないと、エラーメッセージが表示されてコマンドが終了し、エラーが生成されます。

バージョン表示

`-v`

このパラメータは、VMCLI ユーティリティのバージョンを表示するために使用します。その他の非スイッチオプションが指定されていない場合、コマンドはエラーメッセージなしで終了します。

ヘルプの表示

`-h`

このパラメータは、VMCLI ユーティリティパラメータの概要を示します。スイッチ以外のオプションがほかに提供されていない場合、コマンドはエラーなしで終了します。

暗号化データ

`-e`

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

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

VMCLI オペレーティングシステムシェルオプション

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

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

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

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

- バックグラウンドでの実行 — デフォルトで VMCLI ユーティリティはフォアグラウンドで実行されます。オペレーティングシステムのコマンドシェル機能を使用すると、ユーティリティをバックグラウンドで実行できます。たとえば、Linux オペレーティングシステムの場合、コマンドの直後にアンパーサンド（&）を指定すると、プログラムが新しいバックグラウンドプロセスとして起動します。

後者の方法はスクリプトプログラムの場合に便利です。VMCLI コマンドの新しいプロセスが開始した後、スクリプトを継続できます（そうでない場合は、VMCLI プログラムが終了するまでスクリプトがブロックされます）。VMCLI の複数のインスタンスがこの方法で開始し、1 つまたは複数のコマンドインスタンス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機能を使用して、プロセスを一覧表示し、終了できます。

VMCLI 戻りコード

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

13

Intelligent Platform Management Interface の設定

本項では、iDRAC6 IPMI インタフェースの設定と使用について説明します。インタフェースには次が含まれます。

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

iDRAC6 は完全に IPMI 2.0 対応です。iDRAC6 IPMI は、次を使用して設定できます。

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

IPMI シェルの ipmish の使用法の詳細については、**support.dell.com\manuals** にある『Dell OpenManage 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』を参照してください。

RACADM の使い方の詳細については、100 ページの「RACADM のリモート使用」を参照してください。

ウェブベースインタフェースを使った IPMI の設定

詳細については、56 ページの「ウェブインタフェースを使った IPMI の設定」を参照してください。

RACADM CLI を使った IPMI の設定

1 RACADM インタフェースを使ってリモートシステムにログインします。
100 ページの「RACADM のリモート使用」を参照してください。

2 IPMI オーバー LAN を設定します。

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

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

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

a IPMI チャネル権限を更新します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

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

< *レベル* > は次のいずれかです。

- 2（ユーザー）
- 3（オペレータ）
- 4（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、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。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey
< キー >
```

< *キー* > は有効な 16 進数形式の 20 文字からなる暗号キーです。

3 IPMI シリアルオーバー LAN （SOL）を設定します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a IPMI SOL の最小権限レベルを更新します。

メモ : IPMI SOL 最小権限レベルは、IPMI SOL をアクティブにするために最低限必要な権限を決定します。詳細については、IPMI 2.0 規格を参照してください。

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

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

< *レベル* > は次のいずれかです。

- 2（ユーザー）
- 3（オペレータ）
- 4（システム管理者）

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

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

b IPMI SOL ボーレートを更新します。

メモ : シリアルコンソールを LAN 経由でリダイレクトするには、SOL ボーレートが管理下システムのボーレートと同じであることを確認してください。

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

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

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

たとえば、次のとおりです。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate
57600
```

c 個々のユーザーに対して SOL 有効にします。

メモ : SOL は個々のユーザーに対して有効または無効にできます。

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

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable -i <ID> 2
```

<ID> はユーザーの一意な ID です。

4 IPMI シリアルを設定します。

a IPMI シリアル接続モードを適切な設定に変更します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

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

b IPMI シリアルボーレートを設定します。

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

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

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

たとえば、次のとおりです。

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate 57600
```

c IPMI シリアルハードウェアフロー制御を有効にします。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialFlowControl 1
```

d IPMI シリアルチャネルの最小権限レベルを設定します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

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

<*レベル*> は次のいずれかです。

- 2（ユーザー）
- 3（オペレータ）
- 4（システム管理者）

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

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

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

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

IPMI の設定が完了しました。

IPMI シリアルがターミナルモードの場合は、**racadm config cfgIpmiSerial** コマンドを使って次の設定を追加できます。

- 削除制御
- エコー制御
- 行編集
- 改行シーケンス
- 改行シーケンスの入力

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

IPMI リモートアクセスシリアルインタフェースの使用

IPMI シリアルインタフェースでは、次のモードを使用できます。

- **IPMI ターミナルモード** — シリアル端末から送信された ASCII コマンドをサポートします。コマンドセット内のコマンド（電源制御を含む）の数は限られていますが、16 進数の ASCII 文字で入力された生の IPMI コマンドをサポートしています。
- **IPMI 基本モード** — プログラムへのアクセス用に、ベースボード管理ユーティリティ（BMU）に含まれている IPMI シェル（IPMISH）など、バイナリインタフェースをサポートしています。

RACADM を使用して IPMI モードを設定するには、次の手順に従います。

1 RAC シリアルインタフェースを無効にします。

コマンドプロンプトで、次のコマンドを入力します。

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

2 適切な IPMI モードを有効にします。

たとえば、コマンドプロンプトで次のように入力します。

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

詳細については、デルサポートサイト **dell.com/support/manuals** で利用できる『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』で「iDRAC6 プロパティデータベースグループとオブジェクトの定義」を参照してください。

ウェブベースインタフェースを使用したシリアルオーバー LAN の設定

詳細については、56 ページの「ウェブインタフェースを使った IPMI の設定」を参照してください。

メモ : シリアルオーバー LAN は、Dell OpenManage ツール SOLProxy および IPMItool で使用できます。詳細については、**support.dell.com\manuals** にある『Dell OpenManage Baseboard Management Controller Utilities ユーザーズガイド』を参照してください。

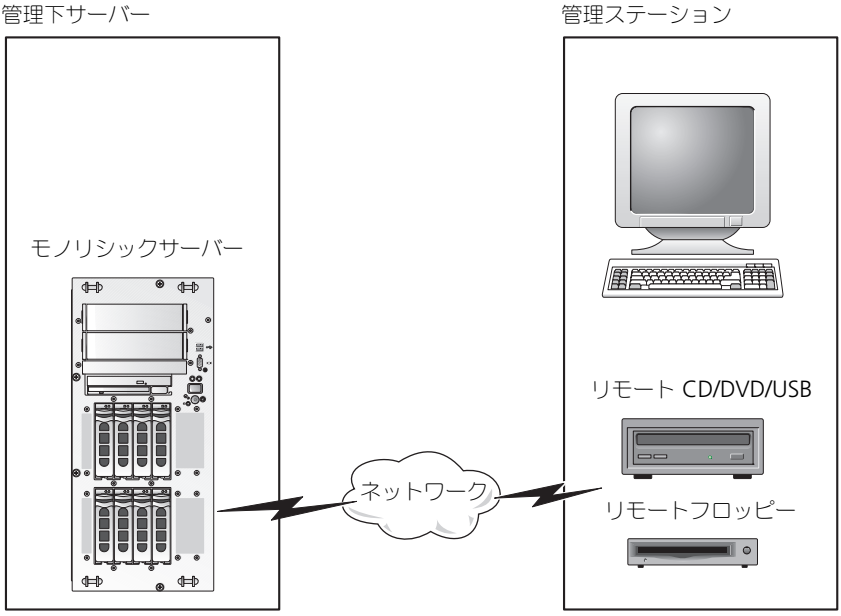
14

仮想メディアの設定と使用

概要

仮想コンソールビューアからアクセスする **仮想メディア** 機能は、ネットワーク上のリモートシステムに接続しているメディアへのアクセスを管理下サーバーに提供します。図 14-1 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 14-1. 仮想メディアの全体的なアーキテクチャ



仮想メディア を使用すると、システム管理者は、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で実行できます。

メモ : 仮想メディア は 128 Kbps 以上のネットワーク帯域幅を必要とします。

仮想メディア は、管理下サーバーのオペレーティングシステムと BIOS 用に、フロッピーディスクデバイスと光ディスクデバイスの 2 つの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** が連結または自動連結している場合、管理下サーバーからのすべての仮想 CD / フロッピードライブのアクセス要求がネットワーク経由で管理ステーションに転送されます。**仮想メディア** の接続は、メディアを管理下システム上の物理デバイスに挿入することと同じです。**仮想メディア** が連結状態にある場合、管理下システム上の仮想デバイスはドライブ内にメディアがインストールされていない 2 つのドライブとして表示されます。

表 14-1 に、仮想フロッピーと仮想光学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、システムの起動シーケンスが停止する可能性があります。

表 14-1. サポートされているドライブ接続

サポートされている仮想フロッピードライブ接続	サポートされている仮想光学ドライブ接続
レガシー 1.44 フロッピードライブ（1.44 フロッピーディスケット）	CD-ROM、DVD、CDRW、CD-ROM メディアとのコンボドライブ
USB フロッピードライブ（1.44 フロッピーディスケット）	ISO9660 フォーマットの CD-ROM/DVD イメージファイル
1.44 フロッピーイメージ	CD-ROM メディアのある USB CD-ROM ドライブ
USB リムーバブルディスク	

Windows ベースの管理ステーション

Microsoft Windows オペレーティングシステムが稼動する管理ステーションで **仮想メディア** 機能を実行するには、対応バージョンの Internet Explorer または Firefox と Java ランタイム環境（JRE）をインストールします。

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が稼動する管理ステーションで仮想メディア機能を実行するには、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、32 ビットの 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。

△ **警告：仮想メディアを正常に起動するためには、32 ビットまたは 64 ビット JRE バージョンが 64 ビットオペレーティングシステムまたは 32 ビット JRE バージョンが 32 ビットオペレーティングシステムにインストールされていることを確認してください。iDRAC6 は 64 ビットの ActiveX バージョンはサポートしていません。また、Linux を使用して仮想メディアを起動する場合は、"compat-libstdc++-33-3.2.3-61" の関連パッケージのインストールが必要です。Windows では、このパッケージが .NET フレームワークパッケージに含まれている場合があります。**

仮想メディアの設定

1. iDRAC6 ウェブインタフェースにログインします。
2. **システム** → **コンソール / メディア** タブ → **設定** → **仮想メディア** の順に選択して、仮想メディアを設定します。

   表 14-2 では、**仮想メディア** の設定値が説明されています。
3. 設定が終了したら、**適用** をクリックします。

表 14-2. 仮想メディアの設定プロパティ

属性	値
状態	**連結** - **仮想メディア** を即時サーバーに連結します。 **分離** - **仮想メディア** から即時サーバーを分離します。 **自動連結** - 仮想メディアセッションが開始している場合のみ、**仮想メディア** をサーバーに連結します。
最大セッション数	許可される最大 **仮想メディア** セッション数が表示されます。これは、常に 1 です。
アクティブセッション数	仮想メディアの現在のセッション数を表示します。
仮想メディア暗号化を有効にする	チェックボックスを選択または選択解除して、**仮想メディア** 接続の暗号化を有効または無効にします。選択すると暗号化は有効になり、選択解除すると暗号化は無効になります。
フロッピーのエミュレーション	**仮想メディア** がサーバーにフロッピードライブとして表示されるか USB キーとして表示されるかを示します。**フロッピーのエミュレーション** のチェックボックスがオンの場合、**仮想メディア** デバイスはサーバーでフロッピーデバイスとして表示されます。選択が解除されている場合は、USB キードライブとして表示されます。 **メモ：**一部の Windows Vista および Red Hat 環境では、**フロッピーエミュレーション** を有効にした状態では USB を仮想化できない場合があります。

表 14-2. 仮想メディアの設定プロパティ （続き）

属性	値
接続状態	**接続** - 仮想メディアセッションが現在進行中です。 **非接続** - 仮想メディアセッションは進行中でありません。
一回限りの起動を有効にする	**一回限りの起動** オプションを有効にするには、このボックスをオンにします。仮想メディアから起動するには、この属性を使用します。次回の起動時に、BIOS 起動メニューから起動デバイスを選択します。このオプションは、サーバーが 1 度起動した後、**仮想メディア** デバイスを自動的に切断します。

仮想メディアの実行

警告：仮想メディア セッションの実行中は、racreset コマンドを使用しないでください。使用すると、データ損失などの望ましくない結果が生じます。

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

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

1 **/ect/modprobe** に次の行を追加します。

```
options scsi_mod max_luns=256

cd /boot

mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
```

2 サーバーを再起動します。

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

```
cat /proc/scsi/scsi
```

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

サポートされている仮想メディア設定

フロッピードライブと光学ドライブ 1 台ずつの仮想メディアを有効にできます。一度に仮想化できるのは各メディアタイプのドライブ 1 台のみです。

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

仮想メディアの接続

仮想メディアを実行するには、次の手順に従います。

1. 管理ステーションで対応ウェブブラウザを開きます。
2. iDRAC6 ウェブインタフェースを起動します。詳細については、43 ページの「ウェブインタフェースへのアクセス」を参照してください。
3. **システム** → **コンソール / メディア** → **仮想コンソールと仮想メディア** の順に選択します。
4. **仮想コンソール**および**仮想メディア** ページが表示されます。表示されている属性値を変更する場合は、233 ページの「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）。光学ドライブ 1 台とフロッピー /USB フラッシュドライブ 1 台の仮想化を同時に選択できます。

   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。
5. **仮想コンソールの起動** をクリックします。

   メモ : Linux では、ファイル **jviewer.jnlp** がデスクトップにダウンロードされ、ファイルの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。

   iDRAC6 コンソールリダイレクト アプリケーションが別のウィンドウで起動します。
6. **仮想メディア** → **仮想メディアの起動** をクリックします。

   仮想メディアセッション ウィザードが表示されます。

   メモ : 仮想メディアセッションを終了する場合以外は、このウィザードを閉じないでください。
7. メディアが接続されている場合は、別のメディアソースを接続する前に切断してください。切断するメディアの左にあるチェックボックスを解除します。

8 接続するメディアのタイプを選択します。

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

メディアが接続され、**状態** ウィンドウが更新されます。

仮想メディアの切断

1 **ツール** → **仮想メディアの起動** の順にクリックします。

2 切断する**メ**ディアの横にあるチェックボックスを解除します。

メディアが切断され、**状態** ウィンドウが更新されます。

3 **仮想メディアセッション** ウィザードを終了するには、**終了** をクリックします。

メモ：仮想メディアセッションを開始したり、vFlash に接続したりすると、「LCDRIVE」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。このドライブは vFlash または仮想メディアセッションが切断されると表示されなくなります。

仮想メディアからの起動

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

BIOS 設定を変更するには、次の手順を実行してください。

1 管理下サーバーを起動します。

2 <F2> キーを押して BIOS 設定ウィンドウを開きます。

3 起動順序をスクロールして、<Enter> キーを押します。

ポップアップウィンドウに、仮想光デバイス 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

本項では、管理ステーションに手動でインタラクティブにオペレーティングシステムをインストールする方法について説明します。完了までに数時間かかる場合があります。**仮想メディア** を使用し、スクリプトでオペレーティングシステムをインストールする手順では 15 分以内で完了します。詳細については、217 ページの「オペレーティングシステムの導入」を参照してください。

1. 次の点を確認します。
   - 管理ステーションの CD ドライブにオペレーティングシステムのインストール CD が挿入されている。
   - ローカル 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. 236 ページの「仮想メディアからの起動」の仮想メディアからの起動手順に従って、BIOS がインストール元の CD ドライブから起動するように設定されていることを確認してください。
3. 画面の指示に従って、インストール作業を完了します。

複数ディスクのインストールの場合は、必ず次の手順に従ってください。

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

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

一回限りの起動機能

一回限りの起動機能は、リモート仮想メディアデバイスから起動できるように、一時的な起動順序の変更を可能にします。この機能は、一般的にオペレーティングシステムのインストール時に仮想メディアで使用されます。

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

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

一回限りの起動機能を使用するには、次の手順に従います。

1. ウェブインタフェースを介して iDRAC6 にログインし、**システム** → **コンソール / メディア** → **設定** の順にクリックします。
2. **仮想メディアの下の 一回限りの起動を有効にする** オプションを選択します。
3. サーバーに電源を入れて、BIOS 起動マネージャを起動します。
4. リモート仮想メディアデバイスから起動するように、起動順序を変更します。
5. サーバーの電源をオフにしてから、再びオンにします。

   サーバーは、リモート仮想メディアデバイスから起動します。次回にサーバーを起動するときには、リモートの仮想メディア接続は切断されます。

   メモ : 起動順序に仮想ドライブが表示されるためには、仮想メディアが **連結** 状態であることが必要です。**一回限りの起動** を有効にする場合は、仮想化されたドライブ内に起動メディアがあることを確認します。

サーバーのオペレーティングシステムが実行しているときの仮想メディアの使用

Windows ベースシステム

Windows システムでは、仮想メディアドライブが連結し、ドライブ文字で設定されていると、それらは自動的にマウントされます。

Windows 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する場合は、ドライブをクリックしてその内容を参照することで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

システムのソフトウェア構成によっては、仮想メディアドライブが自動的にマウントされない場合があります。ドライブが自動的にマウントされない場合は、Linux の **mount** コマンドを使ってドライブを手動でマウントします。

仮想メディアについてよくあるお問い合わせ (FAQ)

表 14-3 は、よくあるお問い合わせとその回答です。

表 14-3. 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した場合、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。 仮想メディアの設定を iDRAC6 ウェブインタフェースまたはローカル RACADM コマンドで変更した場合、設定の変更が適用されると、接続しているすべてのメディアが切断されます。 仮想ドライブに再接続するには、仮想メディアウィザードを使用します。
どのオペレーティングシステムが iDRAC6 に対応していますか。	対応オペレーティングシステムについては、24 ページの「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 に対応していますか。	対応ウェブブラウザについては、24 ページの「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、その前の操作を続けることができます。 • ネットワークのタイムアウトが発生した場合、iDRAC6 ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。また、他のユーザー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もあります。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。

表 14-3. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）（続き）

質問	回答
仮想メディアからの Windows オペレーティングシステムのインストールに時間がかかりすぎるようです。どうしてでしょうか。	『Dell Systems Management Tools and Documentation DVD』を使用して Windows オペレーティングシステムをインストールするときにネットワーク接続が低速な場合は、ネットワークの遅延により iDRAC6 ウェブベースインタフェースへのアクセスに時間がかかることがあります。インストールウィンドウにインストールの進行状況が表示されませんが、インストールプロセスは進行しています。
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。	管理下サーバーで、BIOS セットアップ にアクセスして起動メニューをクリックします。仮想 CD、仮想フロッピー、または 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。また、CMOS 設定の起動順序でスペースキーを押すと、仮想デバイスを起動デバイスにできます。たとえば、CD ドライブから起動するには、その CD ドライブを起動順序の最初のドライブとして設定してください。
どのタイプのメディアから起動できますか。	iDRAC6 では、次の起動メディアから起動できます。 • CDROM/DVD データメディア • ISO 9660 イメージ • 1.44 フロッピーディスクまたはフロッピーイメージ • オペレーティングシステムがリムーバブルディスクとして認識した USB キー • USB キーイメージ
USB キーをブータブルにするには、どうしますか。	**support.dell.com** で、Dell USB キーを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。

表 14-3. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）（続き）

質問	回答
Red Hat Enterprise Linux または SUSE Linux オペレーティングシステムが稼動するシステム上で仮想フロッピー / 仮想 CD デバイスが見つかりません。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見つけます。正しい仮想フロッピードライブを見つけてマウントするには、次の手順に従ってください。 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。

表 14-3. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）（続き）

質問	回答
Red Hat Enterprise Linux または SUSE Linux オペレーティングシステムが稼動するシステム上で仮想フロッピー / 仮想 CD デバイスが見つかりません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。	*（回答の続き）* 仮想 CD ドライブをマウントするには、Linux が仮想 CD ドライブに割り当てるデバイスノードを見つけます。仮想 CD ドライブを見つけ、マウントするには、次の手順に従います。 1 Linux コマンドプロンプトウィンドウを開き、次のコマンドを入力します。 `grep "Virtual CD" /var/log/messages` 2 そのメッセージの最後のエントリを探し、その時刻を書きとめます。 3 Linux のプロンプトで次のコマンドを実行します。 `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込んで、『Dell Virtual CD』に与えられたデバイス名を見つけます。 5 仮想 CD 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/CD` 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。
iDRAC6 ウェブインタフェースを使用してファームウェアのアップデートをリモート実行すると、サーバーで仮想ドライブが削除されました。どうしてでしょうか。	ファームウェアのアップデートによって iDRAC6 がリセットされ、リモート接続が切断して仮想ドライブがアンマウントされます。

表 14-3. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）（続き）

質問	回答
USB デバイスを 1 台接続すると、すべての USB デバイスが分離されるのはなぜですか。	仮想メディアデバイスおよび仮想フラッシュデバイスは、複合 USB デバイスとしてホスト USB バスに接続しているため、共通の USB ポートを共有しています。仮想メディアまたは vFlash USB デバイスがホスト USB バスに接続したり切断されたりすると、すべての仮想メディアと vFlash デバイスが一時的にホスト USB バスから切断されてから、再接続します。仮想メディアデバイスがホストオペレーティングシステムで使用されている場合は、仮想メディアデバイスや vFlash デバイスの連結や分離を避ける必要があります。使用する前に、必要な USB デバイスをすべて接続することをお勧めします。
USB リセット ボタンの機能は何ですか。	サーバーに接続されているリモートおよびローカル USB デバイスをリセットします。
どうすれば仮想メディアの最高性能を得ることができますか。	仮想メディアの最高性能を得るには、仮想コンソールを無効にして仮想メディアを起動するか、次のいずれかを行います。 • 仮想コンソール画面のビデオ解像度と色数を最低限に設定します。 • 仮想メディアと仮想コンソール両方の暗号化を無効にします。 **メモ：**この場合、管理下サーバーと iDRAC 間のデータ転送はセキュリティ保護されません。 • Windows サーバーオペレーティングシステムを使用している場合は、Windows Event Collector という名前の Windows サーバーを停止します。これには、**スタート > 管理ツール > サービス** の順に選択します。**Windows Event Collector** を右クリックして、**停止** をクリックします。

15

vFlash SD カードの設定と vFlash パーティションの管理

vFlash SD カードは、セキュアデジタル（SD）カードの一種で、システム背面にあるオプションの iDRAC6 Enterprise カードスロットに差し込みます。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、USB デバイスとしてシステムが認識するユーザー定義パーティションとして設定することも、起動 USB デバイスを作成するために使用することもできる保存場所です。選択したエミューレーションモードによっては、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 ドライブとしてシステムに認識されます。これらはいずれもブータブルデバイスとして設定できます。

カードの挿入および取り外し方法については、**dell.com/support/manuals** で、お使いのシステムの『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。

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、新しい拡張 vFlash 機能をサポートするカードを指します。標準 SD カードとは、一部の vFlash 機能しかサポートしていない市販の普通の SD カードを指します。

vFlash SD カードを使うと、16 パーティションまで作成できます。パーティションを作成するときには、ラベル名を作成したり、そのパーティションを管理、使用するための一連の操作を行ったりできます。vFlash SD カードは、8GB までの任意のサイズにできます。各パーティションサイズは最大 4GB です。

標準 SD カードは任意のサイズにできますが、1 つのパーティションしかサポートできません。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 SD カードまたは標準 SD カード以外は挿入しないでください。マルチメディアカード（MMC）など、その他のフォーマットのカードを挿入すると、カードを初期化するときに「SD カードの初期化時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 パーティションですべての操作を実行できます。システム管理者以外のユーザーがパーティションの内容を作成、削除、フォーマット、連結、分離、コピーするためには、仮想メディアアクセス権限が必要です。

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、カードを初期化することができます。パーティションの管理には、vFlash 機能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場合は、プロパティしか表示できません。初期化すると、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 の有効と無効を切り替えたり、カードを初期化したりするには、iDRAC 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 カードが検出されませんでした。256 MB 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、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 15-1 に SD カードのプロパティが表示されます。

表 15-1. SD カードのプロパティ

属性	説明
名前	サーバーの iDRAC6 Enterprise カードスロットに挿入されたカードの名前が表示されます。新しい拡張 vFlash 機能をサポートするカードは *vFlash SD カード* と表示されます。vFlash 機能の一部しかサポートしないカードは *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）単位で表示します。
空き容量	vFlash SD カードの空き容量をメガバイト（MB）単位で表示します。この容量は、追加のパーティションを作成するために使用できます。 挿入された vFlash SD カードが初期化されていない場合、空き容量の表示にはカードが初期化されていないと表示されます。 標準 SD カードでは、空き容量は表示されません。
書き込み禁止	カードが書き込み禁止かどうかが表示されます。

表 15-1. SD カードのプロパティ （続き）

属性	説明
状態	vFlash SD カードの正常性が表示されます。これは次のいずれかの状態として表示されます。 • OK • 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、カードを取り付け直してから再初期化してください。 標準 SD カードでは、正常性は表示されません。
vFlash 有効	vFlash パーティション管理を行うには、このチェックボックスを選択します。vFlash 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選択解除します。

4 カード上の vFlash パーティションの管理を有効または無効にするには **適用** をクリックします。

いずれかの vFlash パーティションが連結されている場合、vFlash を無効にできないため、エラーメッセージが表示されます。

メモ : vFlash を無効にすると、**SD カードのプロパティ** サブタブだけが表示されます。

5 **初期化** をクリックします。既存のパーティションはすべて削除され、カードはリセットされます。確認メッセージが表示されます。

6 **OK** をクリックします。初期化が完了したら、その成功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ときにのみ有効になります。

いずれかの vFlash パーティションが連結されている場合、初期化は失敗し、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 を使用中に、vFlash ページのいずれかのオプションをクリックするか、または GUI の別ページに移動すると、DRAC6 は「

`vFlash` は現在、他のプロセスが使用中です。しばらくしてからお試しください。」のメッセージを表示します。

RACADM を使用した vFlash または標準 SD カードの設定

ローカル、リモート、または Telnet/SSH コンソールから RACADM コマンドを使って vFlash または標準 SD カードを表示、設定できます。

メモ : vFlash の有効と無効を切り替えたり、カードを初期化したりするには、iDRAC 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、次のコマンドを入力します。

```
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、次のコマンドを入力します。

- vFlash または標準 SD カードを有効にするには :

  ```
  racadm config -g cfgvFlashsd -o
  cfgvflashSDEnable 1
  ```

- vFlash または標準 SD カードを無効にするには :

  ```
  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、「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、次のコマンドを入力して、カードを初期化します。

```
racadm vflashsd  initialize
```

既存のパーティションはすべて削除され、カードはリセットされます。

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、vFlash または標準 SD カードに最後に送信された初期化コマンドを取得します。

```
racadm vFlashsd status
```

メモ : このコマンドは、SD カードに送信されたコマンドの状態を表示するだけです。SD カード上の個々のパーティションに送信されたコマンドの状態を取得するには、次のコマンドを使用します。
`racadm vflashpartition status`

vFlash または標準 SD カードのリセット

サーバーの Telnet/SSH テキストコンソールを開いてログイン後、次のように入力します。

```
racadm  vflashsd  initialize
```

`vflashsd` の詳細については、デルサポートサイト **dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドライン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 リリース以降ではサポートから外れます。このコマンドの機能は `vflashsd initialize` に含まれます。`vmkey reset` コマンドは当面は実行できますが、`vflashsd initialize` コマンドを使用することを推奨します。詳細については、248 ページの「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用した vFlash パーティションの管理

次を実行できます。

- 空のパーティションの作成
- イメージファイルを使っ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
- パーティションからの起動

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。パーティションの種類として、*フロッピー* または *ハードディスク* を選択できます。空のパーティションの作成用には CD 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、次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になっていない。
- カード上で初期化がすでに実行中でない。

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** サブタブを選択します。**空のパーティションの作成** ページが表示されます。
2. 表 15-2 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。進行状況をパーセントで示すページが表示されます。

   次の場合には、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になっている。
   - ラベル名が既存のパーティションのラベルに一致する。
   - パーティションサイズとして整数以外の値が入力されたか、入力値がカード上で利用可能な容量を超えているか、4GB を超えている。
   - カード上で初期化がすでに実行中である。

   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（RAW）。

表 15-2. 空のパーティションの作成 ページのオプション

フィールド	説明
索引	パーティションインデックスを選択します。ドロップダウンリストには、未使用のインデックスのみが表示されます。利用可能な最小値のインデックスがデフォルトで選択されます。ドロップダウンリストにある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。

表 15-2. 空のパーティションの作成 ページのオプション （続き）

フィールド	説明
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。ラベル名は、6 文字以内の英数字で指定します。空白文字は含めないでください。入力した文字は大文字で表示されます。 **メモ :** 標準 SD カードでは、ラベル名はデフォルトで VFLASH であり、変更できません。
エミュレーションタイプ	ドロップダウンリストからパーティションのエミュレーションタイプを選択します。利用可能なオプションは **フロッピー** と **ハードディスク** です。
サイズ	パーティションサイズをメガバイト（MB）単位で入力します。最大パーティションサイズは 4GB または vFlash SD カード上で利用可能な容量です。 **メモ :** 標準 SD カードでは、パーティションサイズは 256MB であり、変更できません。

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** フォーマットで利用可能）を使って、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のタイプは フロッピー、ハードディスク、または CD 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。

.iso イメージファイル（CD 用）を使う場合は、読み取り専用パーティションしか作成できません。**.img** イメージファイル（フロッピーとハードディスク用）を使う場合は、読み取り書き込みパーティションが作成されます。

新しく作成し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は次の要件を満たす必要があります。

- 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う場合、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 ビットと 64 ビットの両ブラウザ（Internet Explorer と FireFox）で最大 2GB に制限されています。

RACADM や WSMAN インタフェースを使う場合、vFlash SD カードにアップロードできるイメージのサイズは最大 4GB です。

標準 SD カードでは、イメージサイズは 256MB 以下である必要があります。

イメージファイルからパーティションを作成する前に、次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になっていない。
- カード上で初期化がすでに実行中でない。

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ーレーションタイプが一致していることを確認してください。iDRAC はイメージを指定されたイメージタイプとして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タイプが一致しないと問題が起きることがあります。たとえば、ISO イメージを使ってパーティションを作成したときにエミュレーションタイプをハードディスクとして指定すると、このイメージから BIOS を起動できません。

イメージファイルを使って 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 ? **イメージから作成** サブタブを選択します。**イメージからパーティションを作成** ページが開きます。
2. 表 15-3 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。新しいパーティションが作成されます。

   次の場合には、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になっている。
   - ラベル名が既存のパーティションのラベルに一致する。
   - イメージファイルのサイズが 4GB を超えるか、カード上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** または **.iso** でない。
   - カード上で初期化がすでに実行中である。

表 15-3. イメージファイルページのオプションを使ったパーティションの作成

フィールド	説明
索引	パーティションインデックスを選択します。ドロップダウンリストには、未使用のインデックスのみが表示されます。利用可能な最小値のインデックスがデフォルトで選択されます。ドロップダウンリストにある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。6 文字以内の英数字で指定します。空白文字は含めないでください。入力した文字は大文字で表示されます。 **メモ :** 標準 SD カードでは、ラベル名は VFLASH であり、変更できません。
エミュレーションタイプ	ドロップダウンリストからパーティションのエミュレーションタイプを選択します。利用可能なオプションは **フロッピー**、**ハードディスク**、および **CD** 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** と **.iso** ファイルタイプしかサポートされていません。

パーティションのフォーマット

ファイルシステムのタイプに基づいて vFlash SD カード上に既存のパーティションをフォーマットできます。サポートされている ファイルシステムタイプは、EXT2、EXT3、FAT16、および FAT32 です。vFlash 機能が限定されている標準 SD カードは、FAT32 フォーマットしかサポートしていません。

ハードディスクまたはフロップーのパーティションしかフォーマットできません。CD タイプ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、次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になっていない。
- カード上で初期化がすでに実行中でない。

vFlash パーティションをフォーマットするには、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 → **フォーマット** サブタブを選択します。**パーティションのフォーマット** ページが表示されます。

2 表 15-4 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。そのパーティション上のすべてのデータが消去されることを警告する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にフォーマットされます。

次の場合には、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になっている。
- カード上で初期化がすでに実行中である。

表 15-4. 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	フォーマットしたいパーティションのラベルを選択します。最初に利用できるパーティションがデフォルトで選択されます。 フロッピーまたはハードディスクタイプの既存のパーティションがすべてドロップダウンリストに表示されます。連結された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。
フォーマットタイプ	パーティションをフォーマットしたい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、および FAT32 です。

使用可能なパーティションの表示

使用可能なパーティションのリストを表示する場合、vFlash または標準 SD カードが有効になっていることを確認してください。

カード上で使用可能なパーティションを表示するには、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**→ **管理** サブタブを選択します。**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一覧表示されます。

2 各パーティションに付き、表 15-5 で説明されている情報を表示できます。

表 15-5. 使用可能なパーティションの表示

フィールド	説明
索引	パーティションは 1 ～ 16 のインデックスが付けられています。パーティションのインデックスはそのパーティションに一意です。これは、パーティションの作成時に指定されます。
Label	パーティションを識別します。これは、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）単位で指定します。
読み取り専用	パーティションの読み取り書き込み状態 • チェックマーク付き = 読み取り専用パーティション • チェックマークなし = 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可能であるため、この列は表示されません。
連結	パーティションが USB デバイスとしてオペレーティングシステムに認識されるかを示します。パーティションの連結と分離については、256 ページの「パーティションの連結と分離」の項を参照してください。
タイプ	パーティションタイプがフロッピー、ハードディスク、または CD かを表示します。
状態	パーティション上で実行中、または最後に実行された操作の状態が進行状況を示すパーセントと共に表示されます。状態値は次のとおりです。 • アイドル - 操作は行われていません。 • フォーマット中 - パーティションのフォーマット中です。 • 作成中 - パーティションの作成中です。

パーティションの変更

パーティションを変更する場合は、カードが有効になっていることを確認してください。

読み取り専用パーティションを読み取り書き込みに変更したり、反対に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したりできます。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** サブタブを選択します。**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、読み取り専用にしたいパーティションのチェックボックスを選択するか、読み取り書き込みにしたいパーティションのチェックボックスを選択解除します。

メモ : CD タイプのパーティションの状態は読み取り専用で、デフォルトでチェックボックスが選択されています。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。
連結されているパーティション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可能であるため、**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。選択内容に応じて、パーティションは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。複数パーティションを同時に連結すると、インデックスの昇順にホストオペレーティングシステムに認識されます。デバイス文字の割り当てはオペレーティングシステムで行われます。

パーティションを分離すると、そのパーティションはホスト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は認識されなくなり、BIOS ブートオーダー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すると、システムの USB バスはリセットされます。これによって、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）に影響が及び、iDRAC 仮想メディアセッションは切断されます。

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、次を確認してください。

- カードが有効になっている。
- カード上で初期化がすでに実行中でない。

パーティションを連結または分離するには、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** サブタブを選択します。**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、連結したいパーティションのチェックボックスを選択するか、分離したいパーティションのチェックボックスを選択解除します。

メモ : 分離され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。パーティションは選択に基づいて連結または分離されます。

連結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、ホストオペレーティングシステムが Windows であれば、連結パーティションのドライブ文字はオペレーティングシステムによって割り当てられます。

パーティションが読み取り専用であれば、それはホストオペレーティングシステムで読み取り専用となります。

ホストオペレーティングシステムが連結パーティションのファイルシステムをサポートしていないと、ホストオペレーティングシステムからそのパーティションの内容を読み取ったり変更することはできません。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ることはできません。

連結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 で保存されているラベル名には影響ありません。

既存のパーティションの削除

メモ : vFlash または標準 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、次の点を確認してください。

- カードが有効になっている。
- カードが書き込み禁止になっていない。
- パーティションが連結されていない。
- カード上で初期化がすでに実行中でない。

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** サブタブを選択します。**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て、**適用** をクリックします。パーティションが削除されます。

パーティション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場所に **.img** または **.iso** フォーマット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する管理システムです。リモート場所は、管理ステーションにマップされているネットワーク場所です。

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。

パーティションの内容をローカルまたはリモート場所にダウンロードする前に、次を確認してください。

- カードが有効になっている。
- カード上で初期化がすでに実行中でない。
- 読み取り書き込みパーティションは連結されていない。

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、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 → **ダウンロード** サブタブを選択します。**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で、ダウンロードするパーティションを選択します。連結パーティション以外の既存のパーティションはすべてリストに表示されます。最初のパーティションがデフォルトで選択されます。
3. **ダウンロード** をクリックします。
4. ファイルの保存場所を指定します。

   フォルダ場所だけを指定すると、パーティション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ファイル拡張子 **.iso** が、フロッピーとハードディスクタイプのパーティションには **.img** 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。vFlash パーティションを起動デバイスとして設定するためには、ブータブルイメージ（**.img** または **.iso** フォーマット）が必要です。パーティションを起動デバイスとして設定し、起動操作をする場合は、カードが有効になっていることを確認してください。

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。手順は、72 ページの「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 vFlash を最初の起動デバイスとしてサポートしていない場合は、連結 vFlash パーティションは **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する設定をサポートする最新バージョンに必ず 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 が最初の起動デバイスとして vFlash をサポートすることを iDRAC に知らせ、iDRAC はその 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 または標準 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。このサブコマンドのフォーマットは次の通りです。

```
racadm vflashpartition < 作成 | 削除 | 状態 | 一覧表示 >
< オプション >
```

メモ：vFlash パーティション管理を行うには、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 >	このコマンドを適用するパーティションのインデックス < インデックス > は 1 ～ 16 の整数で指定します。 **メモ：**標準 SD カードでは、サイズ 256MB のパーティション 1 つしかサポートされていないため、インデックス値は 1 だけです。

作成操作にのみ有効なオプション：

-o < ラベル >	パーティションをオペレーティングシステムにマウントしたときに表示されるラベル < ラベル > は、6 文字までの英数字の文字列で、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、cddvd、または HDD です。

-t < タイプ >　　< タイプ > のタイプのパーティションを作成します。< タイプ > は次のいずれかとします。

- 空 - 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タイプ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、または EXT3 です。
- イメージ - iDRAC からのイメージを使ってパーティションを作成します。次のオプションは、イメージタイプに有効です。
  - -l < パス > - iDRAC からのリモートパスを指定します。このパスはマウントされているデバイスのものでも構いません。
    SMB パス : //<IP またはドメイン >/< 共有名 > /< イメージへのパス >
    NFS パス : <IP アドレス >:/< イメージへのパス >
  - -u < ユーザー > - リモートイメージにアクセスするためのユーザー名
  - -p < パスワード > - リモートイメージにアクセスするためのパスワード

状態操作にのみ有効なオプション：

-a　　すべての既存パーティション上の操作状態を表示します。

パーティションの作成

- 20MB の空のパーティションを作成するには：

```
racadm vflashpartition create -i 1 -o drive1 -t empty -
e HDD -f fat16 -s 20
```

- リモートシステム上のイメージファイルを使ってパーティションを作成するには：

```
racadm vflashpartition create –i 1 –o drive1 –e HDD –t
image –l //myserver/sharedfolder/foo.iso –u root –p
mypassword
```

メモ : イメージファイル名の拡張子には、大文字と小文字が区別されます。ファイル名の拡張子が大文字になっていると（たとえば、FOO.iso ではなく FOO. ISO になっている）、コマンドが構文エラーを返します。

メモ : イメージファイルを使っ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：

  ```
  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、248 ページの「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 上での動作状態を取得するには：

  ```
  racadm vflashpartition delete -i 1
  ```

- すべての既存パーティションの状態を取得するには：

  ```
  racadm vflashpartition status -a
  ```

パーティション情報の表示

すべての既存パーティションを一覧表示するには：

```
racadm vflashpartition list
```

パーティションからの起動

- 起動リストに使用可能なデバイスを一覧表示するには：

  ```
  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 パーティションを起動デバイスとして設定するには：

  ```
  racadm  config -g cfgServerInfo -o
  cfgServerFirstBootDevice “<vFlash パーティション名 >”
  ```

  ここで、<vFlash パーティション名 > は vFlash SD カードではラベル名で、標準 SD カードでは VFLASH です。

  メモ : このコマンドを実行すると、vFlash パーティションラベルは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。ブートワンスは、パーティションからデバイスを一度だけ起動し、それを起動順序の最初に保つことはしません。

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：

```
racadm config -g cfgvflashpartition  -i 1 -o
cfgvflashPartitionAttachState 1
```

- パーティションを分離するには：

```
racadm config -g cfgvflashpartition  -i 0 -o
cfgvflashPartitionAttachState 1
```

パーティションの変更

- 読み取り専用パーティションを読み取り書き込みに変更するには：

```
racadm config -g cfgvflashpartition  -i 1 -o
cfgvflashPartitionAccessType 1
```

- 読み込み書き出しパーティションを読み取り専用に変更するには：

```
racadm config -g cfgvflashpartition  -i 0 -o
cfgvflashPartitionAccessType 1
```

RACADM サブコマンド、iDRAC6 プロパティデータベースグループおよびオブジェクト定義の詳細については、デルサポートサイト **dell.com/support/manuals** で『iDRAC6 および CMC 向け RACADM コマンドライン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 または標準 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、それが行う動作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。例：初期化動作中

16

電源の監視と管理

Dell PowerEdge システムには、電源管理の新機能と拡張機能が数多く組み込まれています。ハードウェアからファームウェア、さらにシステム管理ソフトウェアへと、プラットフォーム全体が電源効率、電源監視、電源管理に焦点を当てた設計となっています。

基本的なハードウェア設計が電源の観点から最適化されました。

- 高効率電源装置と電圧レギュレータが組み込まれました。
- 該当する場合は、最低電力のコンポーネントが選択されました。
- ファンの電力消費量を最小化するため、シャーシ設計のシステムのエアフローが最適化されました。

PowerEdge システムは電源を制御、管理する多数の機能を提供します。

- **電力インベントリとバジェット：**起動時に、システムインベントリによって、現在の設定のシステム電力バジェットが算出されます。
- **電力制限：**指定した電力制限を維持するように、システムを制御できます。
- **電源監視：**iDRAC6 は電源装置をポーリングして電力測定値を収集します。iDRAC6 は電力測定の履歴を収集して、移動平均とピーク値を計算します。iDRAC6 のウェブベースのインタフェースを使用して、**電源監視** ページでこれら情報を確認できます。

電力インベントリ、電力バジェット、電力制限

使用上、ラックレベルでの冷却量が制限されることがあります。ユーザー定義の電力制限を使用して、パフォーマンスの要件を満たすために必要に応じて電力を割り当てることができます。

iDRAC6 は電力消費量を監視し、指定された電力制限レベルに合わせて動的にプロセッサを減速することで、電源要件に適合しながらパフォーマンスを最大化できます。

電源監視

iDRAC6 は、PowerEdge サーバーの消費電力を継続的に監視します。iDRAC6 は次の電力値を計算し、ウェブインタフェースまたは RACADM CLI で情報を提供します。

- 累積電力

- 平均、最小、最大電力
- 電力ヘッドルーム値
- 電力消費量（ウェブインタフェースでグラフとしても表示）

電源の設定と管理

iDRAC6 ウェブインタフェースと RACADM コマンドラインインタフェース（CLI）を使用して、PowerEdge システムの電源制御の管理と設定ができます。具体的には、次が可能です。

- サーバーの電源状態を表示できます。
- サーバーの電源制御操作（例：電源オン、電源オフ、システムリセット、パワーサイクル）を実行できます。
- サーバーとインストールされている電源装置の電力バジェット情報（設定可能な最大および最小電力消費量）を表示します。
- サーバーの電力バジェットのしきい値を表示、設定できます。

電源装置の正常性状態の表示

電源装置 ページに、サーバーに搭載されている電源装置の状態と定格が表示されます。

ウェブインタフェースの使用

ファン装置の正常性状態を表示するには、次の手順を実行します。

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. システムツリーで **電源装置** を選択します。**電源装置** ページには、次の情報が表示されます。
   - **電源装置冗長性の状態**：次のような値があります。
     - **完全**：システムに設置されている電源装置が同じタイプで、正常に機能しています。
     - **喪失**：電源装置が 2 台あるシステムで、それらの電源装置が異なるタイプか、またはそのうちの 1 台が故障しているか取り外されています。電源装置が 4 台あるシステムで、それらの電源装置が異なるタイプか、またはそのうちの 2 ～ 3 台が故障しているか取り外されています。
     - **無効**：設置されている電源装置のうち 1 台しか使用できません。冗長性なし。
     - **劣化**（電源装置が 4 台あるシステムのみ）：システムに電源装置が 4 台ありますが、そのうちの 1 台が故障しているか取り外されています。
   - **個々の電源装置**：次のような値があります。

- **状態** には次が表示されます。
  - **OK：**電源装置ユニットがあり、サーバーと通信していることを示します。
  - **警告**：警告アラートのみが発行され、システム管理者が 対応処置を取る必要があることを示します。システム管理者が対応処置を取らなかった場合は、サーバーの保全性に影響するような重要または重大な電源エラーを引き起こす可能性があります。
  - **重大**：少なくとも 1 つのエラーアラートが発行されたことを示します。エラーステータスは、シャーシの電源エラーを示し、直ちに対応処置を取る必要があります。
- **場所：**電源装置ユニットの名前 PS-n を表示します。n は電源装置番号です。
- **タイプ**：AD、DC など電源装置のタイプを表示します（AC-DC または DC-DC 電圧変換）。
- **入力ワット数**：電源装置の入力ワット数。これは、システムがデータセンターにかけることのできる最大 AC 電力負荷です。
- **最大ワット数**：電源装置の最大ワット数。これは、システムで使用できる DC 電力です。この値は、システム構成に対して十分な電源容量があることを示すために使用されます。
- **オンライン状態**：電源装置の電源状況（存在し OK、入力の喪失、不在、予測エラー）を示します。
- **ファームウェアバージョン**：電源装置のファームウェアバージョンを表示します。

メモ：電源装置の効率性が関わるため、**最大ワット数**は**入力ワット**数とは異なります。たとえば、電源装置の効率が 89% の場合に**最大ワット数**が 717W であれば、**入力ワット数**は 797W と推定されます。

RACADM の使用

iDRAC への Telnet/SSH テキストコンソールを開いて、ログイン後、次を入力します。

```
racadm getconfig -g cfgServerPower
```

電力バジェットの表示

サーバーで、**電力バジェット情報** ページに電源サブシステムの電力バジェット状態の概要が表示されます。

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** 特権が必要となります。

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. **電源** タブをクリックします。
3. **電力バジェット** オプションを選択します。
4. **電力バジェット情報** ページが表示されます。

最初の表には、現在のシステム構成でのユーザー指定の最大と最小の電源制限しきい値が表示されます。これらは、システム制限として設定できる AC 電力消費量の範囲を表します。選択されたシステム制限は、システムがデータセンターにかけることのできる最大 AC 電力負荷となります。

システム最小電力消費量 は、デフォルトの電力下限値を表示します。

システム最大電力消費量 は、デフォルトの電力上限値を表示します。この値は、現在のシステム設定の絶対的な最大電力消費量でもあります。

RACADM の使用

iDRAC への Telnet/SSH テキストコンソールを開いて、ログイン後、次を入力します。

```
racadm getconfig -g cfgServerPower
```

メモ : 出力の詳細を含む cfgServerPower の詳しい情報については、デルサポートサイト **support.dell.com/manuals** にある、『iDRAC6 および CMC 向け RACADM コマンドラインレファレンスガイド』の cfgServerPower を参照してください。

電力バジェットのしきい値

電力バジェットのしきい値を有効にすると、システムの電力制限の範囲を設定できます。指定したしきい値近く消費電力を維持するために、システムパフォーマンスが動的に調整されます。低負荷環境においては、実際の電力消費量は少なくなり、パフォーマンスの調整が完了するまで、一時的にしきい値を下回る場合もあります。

電力バジェットのしきい値を**有効**にする を選択すると、システムはユーザー指定のしきい値を強制的に適用します。電力バジェットのしきい値**の選択を解除すると**、電力制限は適用されません。たとえば、あるシステム構成での設定可能な最大電力消費量が 700W で、設定可能な最小電力消費量が 500W であるとします。電力バジェットのしきい値を現在の 650W から 525W に下げて有効にすることができます。以降、システムのパフォーマンスはユーザー指定のしきい値 525W を超えないように電力消費量を維持すべく動的に調整されます。

ウェブインタフェースの使用

1. iDRAC6 のウェブベースのインタフェースにログインします。
2. **電源** タブをクリックします。
3. **電力バジェット** オプションを選択します。**電力バジェット情報** ページが表示されます。
4. **電力バジェット** テーブルに値をワット、BTU/ 時、またはパーセント単位で入力します。ワットまたは BTU/ 時 単位は、電力バジェットのしきい値の上限値の入力に使用します。パーセント単位は、設定可能な最大と最小電力消費量範囲内のパーセントで指定する場合に使用します。たとえば、100% しきい値は設定可能な最大電力消費量を示し、0% は最小電力消費量を示します。

   メモ : 電力バジェットのしきい値は設定可能な最大電力消費量を上回ったり、設定可能な最小電力消費量を下回ることはできません。
5. **有効化** を選択して、しきい値を有効化します。システムはユーザー指定のしきい値を強制的に適用します。クリアすると、システムは電力制限されません。
6. **変更の適用** をクリックします。

RACADM の使用

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapWatts < ワット単位の電力制限値 >

racadm getconfig -g cfgServerPower -o
cfgServerPowerCapBTUhr <BTU/ 時単位の電力制限値 >

racadm getconfig -g cfgServerPower -o
cfgServerPowerCapPercent < 電力制限値のパーセント >

racadm config -g cfgServerPower -o cfgServerPowerCapEnable <
有効にする場合は 1、無効にする場合は 0>
```

メモ：電力バジェットのしきい値を BTU/ 時で設定するときは、ワットに変換すると、近似の整数値に丸められます。電力バジェットのしきい値をワットから BTU/ 時に読み戻すときにも、同様に近似の整数値に丸められます。このため、書き込まれた値が読み取り値と若干異なる場合があります。たとえば、600 BTU/ 時に設定されたしきい値は 601 BTU/ 時として読み込まれます。

電源監視の表示

ウェブインタフェースの使用

電源監視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 **電源監視** を選択します。**電源監視** ページが表示されます。

次の項では、**電源監視** ページに表示される情報を説明します。

電源監視

- **状態**：**OK** は、電源装置ユニットがあり、現在サーバーと通信していることを示し、**警告** は警告が発行されたこと、**重大** はエラーアラートが発行されたことを示します。
- **プローブ名：**システム基板のシステムレベル この説明は、システムにおける場所に基づいて、プローブが監視されていることを示します。
- **読み取り値**：ワットまたは BTU/ 時単位の現在の消費電力量。
- **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**：電源装置ユニットの名前 PS-n を表示します。n は電源装置番号です。
- **読み取り値**：現在の消費電力量（アンペア）。

電源 トラッキング統計

- **エネルギー消費量：**電源装置の入力側から測定したサーバーの現在の累積エネルギー消費量を示します。　値は KWh で表示される累積値で、システムによって使用された総エネルギー量です。この値は、**リセット** ボタンを使ってリセットできます。

- **システムピーク電力** は、測定開始後の 1 分間の平均電力の最大値を指定します。この値は、**リセット** ボタンを使ってリセットできます。
- **システムピークアンペア数**：開始時間とピーク時間で指定された間隔内のピークの現在の値を指定します。この値は、**リセット** ボタンを使ってリセットできます。
- **測定開始時間：**統計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。**エネルギー消費量** の場合、この値は **リセット** ボタンを使ってリセットできますが、システムリセットまたはフェールオーバー時まで持続します。**システムピークアンペア数** と **システムピークワット数** では、**リセット** ボタンを使って値をリセットできますが、システムリセットまたはフェールオーバー時まで値は持続します。
- **測定終了時刻**：システムエネルギー消費量が算出された現在の日時を表示します。**ピーク時間** はピークが発生した時間を表示します。

メモ：電力追跡統計はシステムのリセット全体にわたって保持されるため、指定された測定開始から終了までのすべてのアクティビティを反映します。**リセット** ボタンは、個々のフィールドをゼロにリセットします。次の表の電力消費量のデータは、システムのリセット後に失われるため、ゼロにリセットされます。表示される電力値は、特定の時間間隔（過去 1 分、1 時間、1 日 および 1 週間）にわたって測定された累積平均値です。開始から終了までの間隔が電源追跡統計値と異なる場合もあるため、ピーク電力値（最大ピークワット数 対 最大電力消費量）も異なる可能性があります。

Power Consumption（電力消費）

- 過去 1 分、1 時間、1 日、1 週間の平均、最大、および最小電力消費量が表示されます。
- 平均電力消費量：過去 1 分、過去 1 時間、過去 1 日、および過去 1 週間の平均値。
- 最大 および 最小の電力消費量：特定の時間間隔で測定された最大および最小電力消費量。
- 最大および最小の電力時間：電力消費量が最大であった時間と最小であった時間。

ヘッドルーム

- **システムの即時ヘッドルーム**：電源装置ユニットで使用可能な電力とシステムの現在の電力消費量間の差が表示されます。
- **システムのピークヘッドルーム**：電源装置ユニットで使用可能な電力とシステムのピーク電力消費量間の差が表示されます。

グラフの表示

グラフの表示 ボタンをクリックすると、過去 1 時間の iDRAC6 の電力消費量と電流消費量がそれぞれワットとアンペア単位で表示されます。これらの統計値は、グラフの上方にあるドロップダウンメニューを使って 1 週間前まで表示できます。

メモ : グラフに描かれた各データポイントは、読み取り値の 5 分間平均を表します。このため、電力消費量や電流消費量の短時間の変動がグラフに反映されない場合もあります。

RACADM の使用

iDRAC への Telnet/SSH テキストコンソールを開いて、ログイン後、次を入力します。

```
racadm getconfig -g cfgServerPower
```

出力の詳細を含む **cfgServerPower** の詳しい情報については、デルサポートサイト **dell.com/support/manuals** にある、『iDRAC6 および CMC 向け RACADM コマンドラインレファレンスガイド』の **cfgServerPower** を参照してください。

サーバーに対する電源制御操作の実行

メモ : 電源管理の操作を行うには、**シャーシ制御システム管理者** 権限が必要です。

iDRAC6 では、正常なシャットダウンなど、複数の電源管理処置をリモートで実行できます。

ウェブインタフェースの使用

1. iDRAC6 ウェブインタフェースにログインします。
2. **電源** タブをクリックします。**電力制御** ページが表示されます。
3. ラジオボタンをクリックして、**電源制御操作** のいずれかを選択します。
   - **システムの電源を入れる**：サーバーの電源をオンにします（サーバーの電源がオフのときに電源ボタンを押す操作と同じ）。サーバーの電源がすでにオンの場合は、このオプションが無効になっています。
   - **システムの電源を切る**：サーバーの電源をオフにします。サーバーの電源がすでにオフの場合、このオプションは無効になっています。
   - **NMI（マスク不能な割り込み）：** NMI を生成し、システム動作を一時停止させます。
   - **正常なシャットダウン：** システムをシャットダウンします。

メモ : このオプションを使って正常なシャットダウンを行う前に、そのオペレーティングシステムのシャットダウンオプションが有効になっていることを確認してください。シャットダウンオプションを設定せずにオペレーティングシステムでこのオプションを使用すると、シャットダウン操作を実行せずに、管理下システムを再起動します。

- **システムをリセットする（ウォームブート）**：電源をオフにすることなく、システムをリセットします。サーバーの電源が既にオフの場合、このオプションは無効になっています。
- **システムのパワーサイクル（コールドブート）**：電源を切ってからシステムを再起動します。サーバーの電源がすでにオフの場合、このオプションは無効になっています。

4 **適用** をクリックします。確認ダイアログボックスが表示されます。

5 **OK** をクリックして、電力管理の操作（システムのリセットなど）を行います。

RACADM の使用

サーバーへの Telnet/SSH テキストコンソールを開いて、ログイン後、次を入力します。

```
racadm serveraction < 処置 >
```

ここで、< 処置 > は、powerup（電源投入）、powerdown（電源切断）、powercycle（電源サイクル）、hardreset（ハードリセット）または powerstatus（電源状態）を指します。

17

iDRAC6 設定ユーティリティの使用

概要

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

- iDRAC6 および一次バックプレーンのファームウェアリビジョン番号を表示する
- iDRAC6 ローカルエリアネットワークを有効または無効にする
- IPMI オーバー LAN を有効または無効にする
- LAN パラメータを設定する
- 自動検出機能を有効または無効にし、プロビジョニングサーバーを設定する
- 仮想メディアを設定する
- スマートカードを設定する
- システム管理者のユーザー名とパスワードを変更する
- iDRAC6 設定を出荷時のデフォルトに戻す
- システムイベントログ（SEL）からメッセージを表示またはクリアする。
- LCD を設定する
- システムデバイスを設定する

iDRAC6 設定ユーティリティを使用して実行できるタスクはまた、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を使用して実行することも可能です。

iDRAC6 設定ユーティリティの起動

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

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

iDRAC6 設定ユーティリティ ウィンドウが表示されます。最初の 2 行に、iDRAC6 ファームウェアと一次バックプレーンファームウェアのリビジョンに関する情報が表示されます。リビジョンレベルは、ファームウェアアップグレードが必要かどうかの決定に役立ちます。

iDRAC6 ファームウェアは、ウェブベースのインタフェース、SM-CLP、ウェブインタフェースなど、外部インタフェースに関連する情報の一部です。一次バックプレーンファームのファームウェアは、サーバーのハードウェア環境とインタフェースし、それを監視するファームウェアの一部です。

iDRAC6 設定ユーティリティの使用

ファームウェアのリビジョンメッセージの下の iDRAC6 設定ユーティリティの残りの部分は、上下方向キーを使用してアクセスできるメニューアイテムです。

- メニュー項目からサブメニューまたは編集可能なテキストフィールドが表示されたら、<Enter> キーを押してその項目にアクセスし、設定が終了したら <Esc> キーを押します。
- 項目に [はい / いいえ]、[有効 / 無効] など選択可能な値がある場合は、左方向キー、右方向キー、またはスペース キーを押して値を選択します。
- 編集不可の項目は青色で表示されます。項目によっては、他の選択内容によって編集可能になる場合があります。
- 画面の下部に、現在の項目の操作手順が表示されます。F1 キーを押すと、現在の項目のヘルプを表示できます。
- iDRAC6 設定ユーティリティの使用を終えたら、<Esc> キーを押します。終了 メニューが表示され、変更の保存または無視を選択できるほか、ユーティリティに戻ることもできます。

次の項では、iDRAC6 設定ユーティリティのメニュー項目について説明します。

iDRAC6 LAN

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

iDRAC6 LAN は、デフォルト設定では有効になっています。ウェブインタフェース、Telnet/SSH、仮想コンソール、仮想メディアなどの iDRAC6 機能を使用できるようにするには、LAN を有効にする必要があります。

LAN を無効にすると、次の警告が表示されます。

```
LAN チャネルがオフの場合、iDRAC6 帯域外インタフェースは無効になります。
```

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。

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

IPMI Over LAN

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

オフ を選択すると、次の警告が表示されます。

IPMI オーバー LAN がオフの場合、iDRAC6 帯域外 IPMI インタフェースは無効になります。

任意のキーを押してメッセージをクリアし、続行してください。メッセージの説明に関しては、274 ページの「iDRAC6 LAN」を参照してください。

LAN Parameters

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

表 17-1. LAN Parameters

項目	説明
共通設定	
NIC 選択	< 右方向 >、< 左方向 >、およびスペースキーを押して、モードを切り替えます。 **専用、共有、フェールオーバー付きで共有（LOM2）、フェールオーバー付きで共有（すべての LOM）** のモードがあります。 これらのモードは、iDRAC が対応するインタフェースを外部との通信に使用できるようにします。
MAC アドレス	これは、iDRAC6 ネットワークインタフェースの編集不可能な MAC アドレスです。
VLAN の有効化	iDRAC6 の仮想 LAN フィルタを有効にするには、**オン** を選択します。
VLAN ID	**VLAN を有効にする** を **オン** に設定する場合は、VLAN ID を 1 ～ 4094 の範囲で入力します。

表 17-1. LAN Parameters（続き）

項目	説明
VLAN 優先度	**VLAN を有効にする** を **オン** に設定する場合は、VLAN の優先度を 0 ～ 7 の範囲で選択します。
iDRAC6 名の登録	**オン** を選択すると、DNS サービスに iDRAC6 名を登録できます。DNS でユーザーが iDRAC6 の名前を検索できないようにするには、**オフ** を選択します。
iDRAC6 名	**iDRAC 名の登録** を **オン** に設定すると、<Enter> キーを押して **現在の DNS iDRAC 名** テキストフィールドを編集できます。iDRAC6 名の編集が終了したら <Enter> キーを押します。前のメニューに戻るには、<Esc> キーを押します。iDRAC6 名は有効な DNS ホスト名である必要があります。
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）である必要があります。
ホスト名文字列	<Enter> キーを押して編集します。プラットフォームイベントトラップ（PET）アラートを有効にするホスト名を入力します。
LAN アラートを有効にする	PET LAN アラートを有効にするには、**オン** を選択します。
アラートポリシーエントリ 1	**有効** または **無効** を選択すると、最初のアラート送信先がアクティブになります。
アラート送信先 1	**LAN アラートを有効にする** を **オン** に設定する場合は、PET LAN アラートの転送先となる 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。
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。

表 17-1. LAN Parameters（続き）

項目	説明
IP アドレスソース	**DHCP** または **静的** を選択します。DHCP を選択すると、DHCP サーバーから **Ethernet IP アドレス**、**サブネットマスク**、**デフォルトゲートウェイ** フィールドが取得されます。ネットワーク上に DHCP が見つからない場合、フィールドはゼロに設定されます。 **静的** を選択すると、**Ethernet IP アドレス**、**サブネットマスク**、**デフォルトゲートウェイ** アイテムが編集可能になります。
Ethernet IP Address	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得された IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合、iDRAC6 に割り当てる IP アドレスを入力します。 デフォルトは **192.168.0.120** です。
サブネットマスク	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得したサブネットマスクアドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合は、iDRAC6 のサブネットマスクを入力します。デフォルトは **255.255.255.0** です。
デフォルトゲートウェイ	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイの IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。デフォルトは **192.168.0.1** です。
DHCP からの DNS サーバー	ネットワーク上の DHCP サービスから DNS サーバーアドレスを取得するには、**オン** を選択します。下記の DNS サーバーアドレスを指定するには、**オフ** を選択します。
DNS サーバー 1	**DHCP からの DNS サーバー** が **オフ** の場合、最初の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	**DHCP からの DNS サーバー** が **オフ** の場合、2 番目の DNS サーバーの IP アドレスを入力します。
IPv6 の設定	IPv6 接続に対するサポートを有効または無効にします。
IP アドレスソース	**自動設定** または **静的** を選択します。**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。

表 17-1. LAN Parameters（続き）

項目	説明
IPv6 アドレス 1	**IP アドレスソース** を **自動設定** に設定すると、このフィールドには DHCP から取得された IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合、iDRAC6 に割り当てる IP アドレスを入力します。
プレフィックス長	IPv6 アドレスのプレフィックス長を設定します。この値は、1 ～ 128 です。
デフォルトゲートウェイ	**IP アドレスソース** を **自動設定** に設定すると、このフィールドには DHCP から取得した デフォルトゲートウェイの IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。
IPv6 リンクローカルアドレス	これは、iDRAC6 ネットワークインタフェースの編集不可の **IPv6 リンクローカルアドレス** です。
IPv6 アドレス 2	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** 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、最初の DNS サーバーの IP アドレスを入力します。
LAN 詳細設定	
オートネゴシエート	**NIC の選択** を **専用** に設定する場合は、**有効** か **無効** かを選択します。 **有効** を選択した場合は、**LAN 速度設定** と **LAN 二重設定** が自動的に設定されます。
LAN 速度設定	**オートネゴシエート** を **無効** に設定する場合は、10Mbps または 100Mbps を選択します。
LAN 二重設定	**オートネゴシエート** を **無効** に設定する場合は、**半二重 または 全二重** を選択します。

仮想メディアの設定

仮想メディア

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

分離 を選択すると、ユーザーは **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。

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

vFlash

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

- **有効** - vFlash をパーティション管理の対象にできます。
- **無効** - vFlash をパーティション管理の対象にできません。

警告 : 1 つまたは複数のパーティションが使用中か連結されている場合には、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場合に、このオプションを選択します。初期化操作によって、SD カード上にあるデータが消去され、すべてのパーティションが削除されます。1 つまたは複数のパーティションが使用中か連結されている場合には、初期化操作はできません。このオプションは、容量 256 MB を超えるカードが 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利用できます。

<Enter> を押して vFlash SD カードを初期化します。

次の理由で初期化操作に失敗する場合があります。

- 現在 SD カードが存在しない。
- vFlash は現在、他のプロセスが使用中です。
- 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。
- 1 つまたは複数のパーティションが現在使用中。
- 1 つまたは複数のパーティションが現在連結されている。

vFlash のプロパティ

<Enter> を押すと、vFlash SD カードの次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。Dell SD カードであれば、vFlash SD カード と表示されます。Dell SD カード以外であれば、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）単位で表示します。
- **空き容量** - vFlash SD カードの空き容量をメガバイト（MB）単位で表示します。この容量は、追加のパーティションを作成するために使用できます。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が表示されます。
- **正常性** - vFlash SD カード全体の正常性状態を表示します。これは次のいずれかの状態として表示されます。
  - OK
  - 警告
  - 重要

<Esc> を押して終了します。

スマートカードのログオン

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

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

システムサービス設定

System Services

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

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

メモ : 出荷時デフォルト設定に戻しても、システムサービスの設定は変更されません。

システムサービスのキャンセル

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

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

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 **dell.com/support/manuals** にある『*Dell Lifecycle Controller ユーザーズガイド*』を参照してください。

メモ : このオプションを変更すると、設定を保存し iDRAC6 設定ユーティリティを終了した後でサーバーが再起動します。

メモ : 工場出荷時のデフォルトに戻しても、システム情報の収集インベントリの設定は再起動時に変化しません。

LCD の設定

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

表 17-2. LCD ユーザー設定

LCD ライン 1	< 右方向 >、< 左方向 >、およびスペースキーを押して、オプションを切り替えます。 この機能は、LCD の **ホーム** 表示を次のいずれかのオプションに設定します。 **周辺温度、管理タグ、ホスト名、iDRAC6 IPv4 アドレス、iDRAC6 IPv6 アドレス、iDRAC6 MAC アドレス、モデル番号、なし、サービスタグ、システム電源、ユーザー定義の文字列**
LCD ユーザー定義の文字列	LCD に表示される文字列を表示したり入力したりします。文字列は最大 62 文字まで入力できます。
LCD システム電力単位	LCD に表示される単位を指定するために **ワット** または **BTU/時** を選択します。
LCD 周辺温度単位	LCD に表示される単位を指定するために **摂氏** または **華氏** を選択します。
LCD エラー表示	**簡易** または **SEL**（システムイベントログ）を選択します。 この機能を使用すると、次のいずれかの形式で LCD にエラーメッセージを表示できます。 簡易フォーマットは、イベントの説明を英語で表示します。 SEL フォーマットは、システムイベントログのテキスト文字列を表示します。

LCD リモート仮想コンソール表示	装置で仮想コンソールがアクティブの間、テキスト*仮想コンソール* を表示するには、**有効** を選択します。
LCD フロントパネルアクセス	< 右方向 >、< 左方向 >、およびスペースバーを押して、**無効**、**表示 / 変更**、**表示のみ** のオプション間を切り替えます。 この設定は、LCD に対するユーザーのアクセスレベルを決定します。

LAN ユーザー設定

LAN ユーザーは iDRAC6 の システム管理者アカウント（デフォルトで **root**）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。

デフォルトに戻す

デフォルトに戻す メニュー項目を使用すると、iDRAC6 設定項目がすべて出荷時のデフォルトに戻されます。これは、システム管理者のユーザーパスワードを忘れた場合や、iDRAC6 をデフォルト設定から再設定する場合に必要になる可能性があります。

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

出荷時のデフォルト設定に戻すと、リモートの非揮発性ユーザー設定が復元されます。続行しますか？

< いいえ（キャンセル）...>

< はい（続行）>

はい を選択し、<Enter> キーを押すと iDRAC6 はデフォルト設定に戻ります。

操作に失敗すると、次のいずれかのエラーメッセージが表示されます。

- Reset コマンドに成功しませんでした 後でもう一度お試しください - iDRAC は使用中です
- 設定をデフォルト値に戻せませんでした - タイムアウト
- Reset コマンドを送信できません 後でもう一度お試しください - iDRAC は使用中です

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 のメッセージを保持します。

表 17-3. LAN ユーザー設定

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の検出を有効にします。さらに、最初の資格情報を *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認証を実行します。リモートプロビジョニングサーバーはユーザーの資格情報を送信して、iDRAC6 にユーザーアカウントを作成させ ます。ユーザーアカウントが作成されると、リモートコンソールは検出プロセスで指定された資格情報を使用して、iDRAC6 と WS-MAN 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できるように iDRAC6 にセキュアな指示を送信します。 リモートオペレーティングシステム導入の詳細については、デルのサポートウェブサイト **dell.com/support/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、次の必要条件を満たしてください。 • NIC を有効にする • IPv4 を有効にする • DHCP 有効 • 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 サーバーの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は **無効** になっています。自動検出機能を **有効** にしたデルシステムを注文した場合、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に 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、次を確認してください。 • 動的ホスト構成プロトコル（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。

表 17-3. LAN ユーザー設定（続き）

項目	説明
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で **255** 文字以内で指定してください。各アドレスはカンマで区切ります。 自動検出機能が有効な場合に、このプロセスが正常に完了すると、ユーザーの資格情報が設定したプロビジョニングサーバーから取得され、それ以上のプロビジョニングをリモートで行うことができます。 詳細については、デルサポートサイト **dell.com/support/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。システム管理者アカウントを無効にしたり、自動検出機能が有効な場合は、**無効** を選択します。
アカウント権限	**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 **root** です。
パスワードの入力	システム管理者アカウントの新しいパスワードを入力します。入力時に文字は表示されません。
パスワードの確認	システム管理者アカウントの新しいパスワードを再入力します。入力した文字が **パスワードの入力** フィールドに入力した文字と一致しない場合は、メッセージが表示され、パスワードの再入力が必要になります。

SEL メッセージを表示するには、**システムイベントログの表示** を選択して <Enter> キーを押します。左方向キーを使用すると、前の（古い）メッセージに移動し、右方向キー を押すと次の（新しい）メッセージに移動します。レコード番号を入力すると、そのレコードに移動します。SEL メッセージの表示を終了するには、Esc キーを押します。

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

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

iDRAC6 設定ユーティリティの終了

iDRAC6 設定の変更を完了したら、<Esc> キーを押します。これによって [終了] メニューが表示されます。

- **変更 を保存して終了** を選択して <Enter> キーを押すと、変更が維持されます。この操作に失敗した場合には、次のいずれかのメッセージが表示されます。
  - iDRAC6 通信エラー — dDRAC にアクセスできない場合に表示。
  - 一部の設定を適用できません — いくつかの設定が適用できない場合に表示。
- **変更を保存せずに終了** を選択して <Enter> キーを押すと、変更は保存されません。
- **セットアップに戻る** を選択して <Enter> キーを押すと iDRAC6 設定ユーティリティに戻ります。

18

監視とアラート管理

本項では、iDRAC6 の監視方法と、システムと iDRAC6 がアラートを受け取るように設定する手順を説明します。

管理下システムに前回クラッシュ画面のキャプチャを設定する方法

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、次の手順で管理下システムの必須項目を設定する必要があります。

1. 管理下システムソフトウェアをインストールします。管理下システムソフトウェアのインストールについては、『Server Administrator ユーザーズガイド』を参照してください。
2. Windows の 自動再起動 機能を **Windows 起動と回復設定** でオフにしてから、対応する Microsoft Windows オペレーティングシステムを実行します。
3. 前回クラッシュ画面を有効にします（デフォルトでは無効）。

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

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

4. 自動回復タイマーを有効にして、**自動回復** 処置を **リセット**、**電源オフ**、または **パワーサイクル** に設定します。**自動回復** タイマーを設定するには、Server Administrator または IT Assistant を使用する必要があります。

   自動リカバリ の設定手順の詳細については、『Server Administrator ユーザーズガイド』を参照してください。前回のクラッシュ画面をキャプチャできるように、**自動回復** タイマーを 60 秒以上に設定してください。デフォルト設定は 480 秒です。

   自動回復 処置が **シャットダウン** または **パワーサイクル** に設定されている場合は、管理下システムがクラッシュしたときに前回のクラッシュ画面は使用できません。

Windows の自動再起動オプションを無効にする

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

Windows 2008 Server の自動再起動オプションを無効にする

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

Windows Server 2003 の自動再起動オプションを無効にする

1. Windows **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. **詳細** タブをクリックします。
3. **起動と回復** で **設定** をクリックします。
4. **自動再起動** チェックボックスを選択解除します。
5. **OK** を 2 度クリックします。

プラットフォームイベントの設定

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

フィルタ可能なプラットフォームイベントには、次のようなイベントがあります。

1. ファン重要アサートフィルタ
2. バッテリ警告アサートフィルタ
3. バッテリ重要アサートフィルタ
4. 電圧重要アサートフィルタ
5. 温度警告アサートフィルタ
6. 温度重要アサートフィルタ

7 イントルージョン重要アサートフィルタ
8 冗長性低下フィルタ
9 冗長性喪失フィルタ
10 プロセッサ警告アサートフィルタ
11 プロセッサ重要アサートフィルタ
12 プロセッサ不在重要アサートフィルタ
13 電源供給警告アサートフィルタ
14 電源供給重要アサートフィルタ
15 電源供給不在重要アサートフィルタ
16 イベントログ重要アサートフィルタ
17 ウォッチドッグ重要アサートフィルタ
18 システム電源警告アサートフィルタ
19 システム電源重要アサートフィルタ
20 リムーバブルフラッシュメディア不在情報アサートフィルタ
21 リムーバブルフラッシュメディア重要アサートフィルタ
22 リムーバブルフラッシュメディア警告アサートフィルタ

プラットフォームイベント（ファンプローブエラーなど）が発生すると、システムイベントが生成されてシステムイベントログ（SEL）に記録されます。このイベントがプラットフォームイベントフィルタリストにあるプラットフォームイベントフィルタ（PEF）と一致し、このフィルタがアラート（PET または E- メール）を生成するように設定されていると、PET または E- メールアラートが 1 つまたは複数の宛先に送信されます。

同じプラットフォームイベントフィルタで別の処置（システムの再起動など）を実行するように設定すると、その処置が実行されます。

プラットフォームイベントフィルタ（PEF）の設定

プラットフォームイベントトラップまたは E- メールアラートを設定する前に、プラットフォームのイベントフィルタを設定します。

ウェブベースインタフェースを使用した PEF の設定

詳細については、53 ページの「プラットフォームイベントフィルタ（PEF）の設定」を参照してください。

RACADM CLI を使った PEF の設定

1 PEF を有効にします。

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

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

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

PEF インデックス値は 1 ～ 22 です。有効 / 無効の選択は、1（有効）または 0（無効）です。

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

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

2 PEF の処置を設定します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

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

<処置> の値ビットは次のとおりです。

- 0 = アラート処置なし
- 1 = サーバーの電源オフ
- 2 = サーバーの再起動
- 3 = サーバーのパワーサイクル

たとえば、PEF でサーバーを再起動するには次のコマンドを入力します。

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

1 は PEF インデックス、2 は PEF 処置を再起動に設定します。

PET の設定

ウェブインタフェースを使用した PET の設定

詳細については、54 ページの「プラットフォームイベントトラップ（PET）の設定」を参照してください。

RACADM CLI を使用した PET の設定

1 グローバルアラートを有効にします。

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

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

2 PET を有効にします。

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

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

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

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

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

たとえば、PET をインデックス 4 で有効にするには、次のコマンドを入力します。

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

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

3 PET ポリシーを設定します。

コマンドプロンプトで次のコマンドを入力して <Enter> を押します。

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i 1 <IPv4_アドレス>
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6_アドレス>
```

1 は PET の送信先インデックスで、*<IPv4_ アドレス>* と *<IPv6_ アドレス>* はプラットフォームイベントアラートの送信先 IP アドレスです。

4 コミュニティ名の文字列を設定します。

コマンドプロンプトで、次のコマンドを入力します。

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <名前>
```

E- メールアラートの設定

ウェブインタフェースを使用した E- メールアラートの設定

詳細については、55 ページの「E- メールアラートの設定」を参照してください。

RACADM CLI を使用した E- メールアラートの設定

1 グローバルアラートを有効にします。

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

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

2 E- メールアラートを有効にします。

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

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

1 と 1 は、それぞれ E- 送信先のインデックスと、有効 / 無効の選択です。

E- メールの送信先インデックスは 1 ～ 4 の値が可能です。有効 / 無効の選択は、1（有効）または 0（無効）を設定できます。

たとえば、PET をインデックス 4 で有効にするには、次のコマンドを入力します。

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 4 1
```

3 E- メール設定を指定します。

コマンドプロンプトで次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress -i 1 <E- メールアドレス>
```

1 は E- メール送信先のインデックスで、<*E- メールアドレス*> はプラットフォームイベントアラートの送信先の E- メールアドレスです。

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

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

1 は E- メール送信先のインデックスで、<*カスタムメッセージ*> は E- メールアラートに表示されるメッセージです。

E- メールアラートのテスト

RAC E- メールアラート機能を使用すると、ユーザーは管理下システムで重大なイベントが発生したときに E- メールアラートを受信できます。次の例は、RAC がネットワークで正しく E- メールアラートを送信できるかどうかを確認するために、E- メールアラート機能をテストする方法を示しています。

```
racadm testemail -i 2
```

メモ : E- メールアラート機能のテストを行う前に、**SMTP** と **E- メールアラート** 設定が指定されていることを確認してください。詳細については、291 ページの「E- メールアラートの設定」を参照してください。

RAC SNMP トラップアラート機能のテスト

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

次の例で、ユーザーが RAC の トラップアラート機能をテストする例を示します。

```
racadm testtrap -i 2
```

RAC SNMP トラップアラート機能をテストする前に、SNMP とトラップの設定が正しく設定されていることを確認してください。これらを設定するには、デルサポートサイト **dell.com/support/manuals** で利用できる『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』で testtrap および testemail サブコマンドの説明を参照してください。

SNMP 認証についてよくあるお問い合わせ（FAQ）

どうして次のメッセージが表示されるのでしょうか？

リモートアクセス：SNMP 認証エラー

検出作業の一部として、IT Assistant はデバイスの get と set コミュニティ名の確認を試みます。IT Assistant には、**コミュニティ名 = public** 取得と **コミュニティ名 = private** の設定があります。iDRAC6 エージェントのデフォルトコミュニティ名は **public** です。IT Assistant が設定要求を送信すると、iDRAC6 エージェントは **community = public** からの要求しか受け入れないため、SNMP 認証エラーが生成されます。

メモ : これは SNMP エージェントコミュニティ名です。

RACADM を使用して、iDRAC6 のコミュニティ名を変更できます。

iDRAC6 コミュニティ名を表示するには、次のコマンドを使用します。

```
racadm getconfig -g cfgOobSnmp
```

iDRAC6 コミュニティ名を設定するには、次のコマンドを使用します。

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

ウェブベースのインタフェースを使って iDRAC6 SNMP エージェントコミュニティ名にアクセス / 設定するには、**iDRAC の設定** → **ネットワーク / セキュリティ** → **サービス** と進み、**SNMP エージェント** をクリックします。

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

19

管理下システムのリカバリとトラブルシューティング

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

- 295 ページの「リモートシステムのトラブルシューティングの第一歩」を参照してください。
- 296 ページの「リモートシステムの電源管理」を参照してください。
- 304 ページの「POST 起動ログの使用」を参照してください。
- 305 ページの「前回システムクラッシュ画面の表示」を参照してください。

リモートシステムのトラブルシューティングの第一歩

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

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

システムがクラッシュした場合は、前回のクラッシュ画面を確認し（305 ページの「前回システムクラッシュ画面の表示」を参照）、仮想コンソールとリモート電源管理（296 ページの「リモートシステムの電源管理」を参照）を使用してシステムを再起動し、その過程を見てください。

リモートシステムの電源管理

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

iDRAC6 ウェブインタフェースからの電源制御処置の選択

ウェブインタフェースを使用して電源管理処置を実施するには、270 ページの「サーバーに対する電源制御操作の実行」を参照してください。

iDRAC6 CLI からの電源制御処置の選択

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

`racadm serveraction <` *処置* `>`

< *処置* > の文字列のオプションは次のとおりです。

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

システム情報の表示

システム概要 ページでは、システムの正常性と他の基本的な iDRAC6 情報を一目で確認でき、システムの正常性と情報ページにアクセスするためのリンクがあります。また、このページから共通のタスクをすばやく起動し、システムイベントログ（SEL）にログインされた最新のイベントを表示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**？**システム概要** タブ の順にクリックします。詳細は、iDRAC6 のオンラインヘルプ を参照してください。

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。

- メインシステムシャーシ
- Remote Access Controller

システム詳細 ページにアクセスするには、**システム** ツリーを展開し、**プロパティ** → **システム詳細** タブをクリックします。

メインシステムシャーシ

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

表 19-1. システム情報

フィールド	説明
説明	システムの説明。
BIOS バージョン	システム BIOS のバージョン。
サービスタグ	システムのサービスタグナンバー。
エクスプレスサービスコード	システムのサービスコード。
ホスト名	ホストシステムの名前。
OS 名	システムで実行されているオペレーティングシステム。
オペレーティングシステムバージョン	システムで実行されているオペレーティングシステムのバージョン。
システムリビジョン	システムリビジョン番号。
Lifecycle Controller ファームウェア	Lifecycle Controller ファームウェアのバージョン。

表 19-2. 自動回復

フィールド	説明
回復処置	システムハング が検知されたときに、iDRAC6 で 処置なし、ハードリセット、電源を切る、またはパワーサイクル処置を行うように設定できます。
初期カウントダウン	システムハング が検知されてから iDRAC6 が回復処置を実行するまでの秒数。
現在のカウントダウン	カウントダウンタイマーの現在の値（秒）。

表 19-3. 組み込み NIC MAC アドレス

フィールド	説明
仮想 MAC	仮想メディアアクセスコントロール（MAC）アドレスを表示。 仮想 MAC データはハードウェアインベントリから取得されるので、vMAC データを表示する前にハードウェアインベントリを一度収集する必要があります。 **システムインベントリ** をクリックします。インベントリデータがアップデートされ、**システムインベントリ** ページに表示されます。再度 **システムインベントリ** をクリックします。各内蔵 LAN ポートの仮想 MAC が **システム詳細** ページに表示されます。 **メモ：**vMAC 機能は、将来のリリースで Dell Advanced Infrastructure Manager（AIM）によって使用されるようになります。Dell AIM が現在サーバーを管理していない場合、イーサネット MAC アドレスおよび仮想 MAC アドレスは同一です。
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 Ethernet、Internet Small Computer System Interface（iSCSI）、および仮想 MAC アドレスを表示します。 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。 iSCSI NIC は、ホストコンピュータで iSCSI スタックが実行されているネットワークインタフェースコントローラです。 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。
NIC 2	内蔵ネットワークインタフェースコントローラ（NIC）2 をネットワーク上で固有に識別する Ethernet、iSCSI および仮想 MAC アドレスを表示します。
NIC 3	内蔵ネットワークインタフェースコントローラ（NIC）3 をネットワーク上で固有に識別する Ethernet、iSCSI および仮想 MAC アドレスを表示します。
NIC 4	内蔵ネットワークインタフェースコントローラ（NIC）4 をネットワーク上で固有に識別する Ethernet、iSCSI および仮想 MAC アドレスを表示します。

Remote Access Controller

表 19-4. RAC 情報

フィールド	説明
名前	iDRAC6
製品情報	Integrated Dell Remote Access Controller 6 - Enterprise

表 19-4. RAC 情報_（続き）

フィールド	説明
日時	現在の時刻（次の形式で表記）： 曜日 月 日 時間 : 分 : 秒 : 年 例：Fri Jan 28 16:27:29 2011
Firmware Version（ファームウェアバージョン）	iDRAC6 ファームウェアバージョン
ファームウェアアップデート	ファームウェアが最後にフラッシュされた日付（次の形式で表記）： 曜日 月 日 時間 : 分 : 秒 : 年 例：Sat Jan 29 2011 13:31:50
ハードウェアバージョン	Remote Access Controller のバージョン
MAC アドレス	ネットワークの各ノードを固有に識別するメディアアクセスコントロール（MAC）アドレス

表 19-5. IPv4 情報

フィールド	説明
IPv4 有効	**はい** または **いいえ**
IP アドレス	ホストへのネットワークインタフェースカード（NIC）を識別する 32 ビットアドレス。値は、143.166.154.127 のようなドット区切りの形式で表示されます。
サブネットマスク	サブネットマスクは、IP アドレスを構成する拡張ネットワークプレフィックスとホスト番号の部分を示します。値は、255.255.0.0 のようなドット区切りの形式で表示されます。
ゲートウェイ	ルーターまたはスイッチのアドレス。値は、143.166.154.1 のようなドット区切りの形式で表示されます。
DHCP の有効	**はい** または **いいえ** 動的ホスト構成プロトコル（DHCP）を有効にするかどうかを示します。
DHCP を使用して DNS サーバーアドレスを取得する	**はい** または **いいえ** DHCP を使って DNS サーバーアドレスを取得するかどうかを示します。
優先 DNS サーバー	優先 DNS サーバーの静的 IPv4 アドレスを示します。
代替 DNS サーバー	代替 DNS サーバーの静的 IPv4 アドレスを示します。

表 19-6. IPv6 の情報フィールド

フィールド	説明
IPv6 有効	Ipv6 スタックを有効にするかを示します。
IP アドレス 1	iDRAC6 NIC の IPv6 アドレス / プレフィックス長を指定します。*プレフィックス長* は IP アドレス 1 と組み合せて使用します。IPv6 アドレスのプレフィックス長を指定する整数。この値は 1 ～ 128 です。
IP ゲートウェイ	iDRAC6 NIC のゲートウェイを指定します。
リンクのローカルアドレス	iDRAC6 NIC リンクのローカル IPv6 アドレスを指定します。
IP アドレス 2 ～ 15	iDRAC6 NIC の IPv6 アドレスが別にあればそれを指定します。
自動設定の有効化	**はい** または **いいえ**。自動設定は、サーバー管理者が動的ホスト構成プロトコル（DHCPv6）サーバーから iDRAC NIC の IPv6 アドレスを取得できるようにします。
DHCPv6 を使用して DNS サーバーアドレスを取得する	**はい** または **いいえ** DHCPv6 を使って DNS サーバーアドレスを取得するかどうかを示します。
優先 DNS サーバー	優先 DNS サーバーの静的 IPv6 アドレスを示します。
代替 DNS サーバー	代替 DNS サーバーの静的 IPv6 アドレスを示します。

システムインベントリ

システムインベントリ ページは、システムに取り付けられた（またはインストールされた）ハードウェアおよびファームウェアコンポーネントに関する情報を表示します。

システムインベントリ ページにアクセスするには、**システム** ツリーを展開し、**プロパティ** ? **システムインベントリ** とクリックします。

ハードウェアインベントリ

このセクションでは、システムに現在取り付けられているハードウェアに関する情報を表示します。**システムインベントリ** タブをクリックした時にハードウェアインベントリデータがない場合は、次のメッセージが表示されます。

ハードウェアインベントリは利用できません。

ページを更新して詳細を確認してください。

ファームウェアインベントリ

このセクションでは、取り付けられている Dell コンポーネントのファームウェアバージョンを表示します。**システムインベントリ** タブをクリックした時にファームウェアインベントリデータがない場合は、次のメッセージが表示されます。

ハードウェアインベントリは利用できません。

ページを更新して詳細を確認してください。

メモ : CSIOR（再起動時にシステムインベントリを収集）が有効でない場合、データの収集にいくらか時間がかかることから、まず CSIOR を実行して起動時にシステムインベントリを収集し、それから **システムインベントリ** タブをクリックすることをお勧めします。

新しいハードウェアをシステムに追加、またはシステムからハードウェアを取り外した後は、**システムインベントリ** ページでその変更が自動的にアップデートされない場合があります。これは製造プロセスで収集されたインベントリデータが新しい変更でアップデートされない場合があることが原因です。

これを解決するには、BIOS POST 中に **Cntl+E** オプションを選択し、再起動時の **システムインベントリの収集** を有効化します。保存して **Cntl+E** オプションを終了します。

システムが再起動し、新しいシステムインベントリを収集します。インベントリ収集の完了後、**システムインベントリ** ページで正しいハードウェアとソフトウェアインベントリデータが表示されます。

詳細は、iDRAC6 のオンラインヘルプ を参照してください。

システムイベントログ（SEL）の使用

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

システムイベントログを表示するには、次の手順を実行してください。

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

   システムイベントログ ページには、イベントの重大度と、表 19-7 に示すようなその他の情報が表示されます。
3. 適切な **システムイベントログ** ページボタンをクリックして続行します。詳細は、iDRAC6 のオンラインヘルプ を参照してください。
4. **ログのクリア** をクリックして 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。
5. **名前を付けて保存** をクリックして、SEL を希望するディレクトリに保存します。

表 19-7. 状態インジケータのアイコン

アイコン / カテゴリ	説明
	緑のチェックマークは、正常（通常）ステータスを示します。
	感嘆符の入った黄色の三角形は、警告（非重要）ステータスを示します。
	赤い X は、重要（エラー）ステータスを示します。
	疑問符のアイコンは、不明なステータスを示します。
日時	イベントが発生した日時。日付が空白の場合は、システム起動時にイベントが実行されます。フォーマットは、24 時間制に基づいて < 日 > < 月 > dd yyyy hh:mm:ss となります。
説明	イベントの簡単な説明

OEM イベントログの有効化 / 無効化

OEM イベントログは **システムイベントログ** ページに自動的に表示されます。**システム** ? **ログ** タブにある **詳細設定** ボタンは、管理下システムからの OEM イベントメッセージが **システムイベントログ** ページに表示されるのを有効化 / 無効化します。

OEM イベントログが **システムイベントログ** ページに表示されるのを無効化するには、**OEM SEL イベントフィルタ有効** オプションを選択します。

メモ : OEM SEL イベントフィルタ有効 オプションはデフォルトでは選択されていません。

コマンドラインを使ってシステムログを表示する

```
racadm getsel -i
```

getsel -i コマンドは SEL 内のエントリ数を表示します。

```
racadm getsel <オプション>
```

メモ : 引数を何も指定しないと、ログ全体が表示されます。

メモ : 利用できるオプションの詳細については、デルサポートサイト **dell.com/support/manuals** にある『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』で、getsel サブコマンドを参照してください。

clrsel コマンドは SEL から既存のレコードをすべて削除します。

```
racadm clrsel
```

作業メモの使用

作業メモは、ユーザーが追加できるメモやコメントです。iDRAC ユーザーならだれでも作業メモを追加できます。作業メモは削除できません。一度に 1000 もの作業メモを表示できます。素早く参照できるように、最新の 10 の作業メモは iDRAC ホームページに表示されます。

メモ : 追加された作業メモが 800 を超える場合は、GUI ページのロード時間が数秒長くなることがあります。これは、GUI と iDRAC6 間で比較的大型のデータが処理されることが理由です。ページのロード後、新しく追加された作業メモが表示されない場合があります。この問題を解決するには、**更新** をクリックします。

作業メモ ページから、Lifecycle ログへの作業メモの入力が可能です。メモのタイムスタンプは、自動的に記録されます。

作業メモ ページにアクセスするには、**システム** ツリーを展開し、**システム** → **ログ** → **作業メモ** とクリックします。

作業メモページの表示により、作業メモの入力が可能になり、表 19-8 に示されるように、その他の情報も提供されます。

作業メモを入力するには、次の手順を実行します。

1. **作業メモ** ページの **作業メモの追加** セクションに表示されるフィールドに作業メモを入力します。

   メモ : 作業メモでは、最大 50 の英数文字がサポートされます。

2. **保存** をクリックします。

   新しい作業メモが **作業メモの追加** セクションの下にある作業メモ表に表示されます。

表 19-8. 作業メモ

フィールド	説明
日時	作業メモエントリごとに記録されたタイムスタンプを表示します。 フォーマットは、24 時間制の yyyy-mm-ddThh:mm:ssZ で、 yyyy：年 mm：月 dd：日 T：時刻 hh：時間 mm：分 ss：秒 Z：タイムゾーン指示子、となります。 **メモ :** 時刻が UTC の場合は、時刻の後、スペース無しで **Z** を追加します。**Z** は、UTC オフセット値がゼロのゾーン指示子です。したがって、**09:30** UTC は、**09:30Z** または **0930Z** と表され、**14:45:15** UTC は、**14:45:15Z** または **144515Z** となります。
メモ	作業メモエントリの内容を表示します。

POST 起動ログの使用

メモ : ログは iDRAC6 の再起動後にすべてクリアされます。

起動キャプチャ ページでは、使用できる最後の 3 つまでの起動サイクルの記録にアクセスできます。これらの記録は、最新の記録から順に並べられます。サーバーに起動サイクルがない場合は、**記録を使用できません** というメッセージが表示されます。使用できる起動サイクルを新しいウィンドウに表示するには、選択してから **再生** をクリックします。

メモ : 起動キャプチャの表示は Java でのみサポートされています。Active-X では使用できません。

起動キャプチャログを表示するには、次の手順を実行します。

1. **システム** ツリーの **システム** をクリックします。
2. **ログ** タブをクリックしてから、**起動キャプチャ** タブをクリックします。
3. 起動サイクルを選択し、**再生** をクリックします。

   新しい画面にログのビデオが再生されます。

   メモ : 他のビデオを再生するには、開いている起動キャプチャログのビデオを閉じる必要があります。2 つのログを同時に再生することはできません。
4. 起動キャプチャログのビデオを再生するには、**再生** → **再生** の順にクリックします。
5. ビデオを停止するには、**再生** → **メディア制御** の順にクリックします。

メモ : ビューアを開く代わりに **data.jnlp** ファイルを保存するように求めるメッセージが表示される場合があります。この問題を解決するには、Internet Explorer で次の処置を行います。**ツール** → **インターネットオプション** → **詳細設定** タブの順にクリックし、暗号化されたページをディスクに保存しないのオプションを選択解除します。

メモ : ビデオは RAM に保存されており iDRAC のリセットによって削除されるため、iDARC をリセットすると起動キャプチャビデオが利用できなくなります。

iDRAC6 Express Card は、起動中に **F10** を押して USC（Unified Server Configurator）アプリケーションを開始する時に、iDRAC6 にボンディングされます。ボンディングに成功すると、SEL と LCD に「iDRAC6 のアップグレードに成功しました」というメッセージが記録されます。ボンディングに失敗すると、SEL と LCD に「iDRAC6 のアップグレードに失敗しました」というメッセージが記録されます。さらに、そのプラットフォームをサポートしていない古いファームウェア iDRAC6 ファームウェアが含まれている iDRAC6 Express Card をマザーボードに挿入してシステムを起動すると、「iDRAC ファームウェアが最新ものではありません」というログが POST 画面に生成されます。最新のファームウェアにアップデートしてください。指定のプラットフォームに対しては最新の iDRAC6 ファームウェアで iDRAC6 Express Card をアップデートします。詳細については、『Dell Lifecycle Controller ユーザーガイド』を参照してください。

前回システムクラッシュ画面の表示

メモ : 前回クラッシュ画面の機能を使用するには、管理下システムの Server Administrator に **自動回復** 機能が設定されている必要があります。また、iDRAC6 を使用した **自動システム修復** 機能が有効になっていることを確認します。この機能を有効にするは、**iDRAC の設定** セクションの **ネットワーク / セキュリティ** タブにある **サービス** ページに移動します。

前回のクラッシュ画面 ページを表示するには、次の手順を実行してください。

1. **システム** ツリーの **システム** をクリックします。
2. **ログ** タブをクリックして、**前回のクラッシュ 画面**を クリックします。

   前回クラッシュ画面 ページには最新のクラッシュ画面が表示されます。前回システムクラッシュ情報は、iDRAC6 メモリに保存され、リモートからアクセスが可能です。

   前回のクラッシュ画面 ページに表示されるボタンの詳細については、『iDRAC6 オンラインヘルプ』を参照してください。

メモ : 自動回復タイマーの変動により、システムリセットタイマーの値が 30 秒未満に設定されている場合は、**前回のクラッシュ画面** をキャプチャできないことがあります。Server Administrator と IT Assistant でシステムリセットタイマーを 30 秒以上に設定して、**前回クラッシュ画面** が正しく機能することを確認します。詳細については、287 ページの「管理下システムに前回クラッシュ画面のキャプチャを設定する方法」を参照してください。

20

iDRAC6 の修復とトラブルシューティング

本項では、クラッシュした iDRAC6 の修復とトラブルシューティングに関連するタスクの実行方法を説明します。

iDRAC6 のトラブルシューティングには、次のいずれかのツールを使用できます。

- RAC ログ
- 診断コンソール
- サーバーの識別
- トレースログ
- racdump
- coredump

RAC ログの使用

RAC ログ は iDRAC6 ファームウェアに保持される持続的なログです。このログにはユーザーの操作（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 が発行したアラートのリストが保存されています。ログが一杯になると、最も古いエントリから上書きされます。

iDRAC6 ユーザーインタフェース（UI）から RAC ログにアクセスするには、次の手順に従います。

1. **システム** ツリーで、**iDRAC の設定** をクリックします。
2. **ログ** タブをクリックして、**iDRAC ログ** をクリックします。

iDRAC ログ ページに、表 20-1 にリストされる情報が表示されます。

表 20-1. iDRAC ログページ情報

フィールド	説明
日付 / 時刻	日付と時刻（12 月 19 日 16:55:47 など）。 iDRAC6 を最初に起動したときにまだ管理下システムと通信できない間は、時刻に システムの起動 と表示されます。
ソース	イベントを引き起こしたインタフェース
説明	イベントの概要と iDRAC6 にログインしたユーザーの名前。

メモ : iDRAC ログページ ボタンの使用についての詳細は、『iDRAC6 オンラインヘルプ』を参照してください。

コマンドラインの使用

iDRAC6 ログのエントリを表示するには、getraclog コマンドを使用します。

```
racadm getraclog [ オプション ]
racadm getraclog -i
```

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

メモ : 詳細については、デルサポートサイト **dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』の getraclog を参照してください。

iDRAC ログからすべてのエントリをクリアするには、clrraclog コマンドを使用します。

```
racadm clrraclog
```

診断コンソールの使用

iDRAC6 には、Microsoft Windows や Linux システム提供のものと同様なネットワーク診断ツールが標準装備されています（表 20-2 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 で通常の起動操作が実行されます。

診断コンソール ページにアクセスするには、次の手順に従います。

1. **システム** ツリーで、**iDRAC の設定** → **トラブルシューティング** タブ → **診断コンソール** とクリックします。
2. コマンドを入力して **送信** をクリックします。表 20-2 に、使用できるコマンドについて説明しています。デバッグの結果が **診断コンソール** ページに表示されます。
3. **診断コンソール** ページを更新するには、**更新** をクリックします。別のコマンドを実行するには、**診断ページに戻る** をクリックします。

表 20-2. 診断コマンド

コマンド	説明
arp	ARP（Address Resolution Protocol）テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を印刷します。**netstat** オプションの右側のテキストフィールドにインタフェース番号をオプションで入力すると、インタフェースを通るトラフィック、バッファの使用率、その他のネットワークインタフェースに関する情報が印刷されます。

表 20-2. 診断コマンド（続き）

コマンド	説明
ping <IP アドレス>	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC6 から到達可能かどうかを確認します。送信先の IP アドレスをこのオプションの右側のフィールドに入力してください。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）のエコーパケットが宛先 IP アドレスに送信されます。
gettracelog	iDRAC6 トレースログ を表示します。詳細については、デルサポートサイト **dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』の gettracelog を参照してください。

サーバーの識別機能の使用

識別 ページでは、システムの識別機能を有効にできます。

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** → **iDRAC の設定** → **トラブルシューティング** → **識別** とクリックします。
2. **識別** 画面で **サーバーの識別** チェックボックスを選択して、LCD と背面のサーバー識別 LED の点滅を有効にします。
3. **サーバーのタイムアウトの識別** フィールドに、LCD が点滅する秒数が表示されます。LCD を点滅させる秒数を入力します。タイムアウト範囲は 1 ～ 255 秒です。タイムアウトを 0 秒に設定すると、LCD は連続的に点滅します。
4. **適用** をクリックします。

0 秒を入力した場合は、次の手順に従って点滅を無効にします。

1. **システム** → **iDRAC の設定** → **トラブルシューティング** → **識別** とクリックします。
2. **識別** 画面で、**サーバーの識別** オプションを選択解除し、**適用** をクリックします。

トレースログの使用

iDRAC6 の内部トレースログは、システム管理者が iDRAC6 のアラートおよびネットワークに関する問題をデバッグするために使用します。

iDRAC6 のウェブインタフェースからトレースログにアクセスするには、次の手順に従ってください。

1. **システム** ツリーで、**iDRAC の設定** をクリックします。

2 **診断** タブをクリックします。

3 **gettracelog** コマンドまたは **racadm gettracelog** コマンドを **コマンド** フィールドに入力します。

メモ : このコマンドはコマンドラインインタフェースからも使用できます。詳細については、デルサポートサイト **dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』の gettracelog を参照してください。

トレースログは次の情報を追跡します。

- DHCP — DHCP サーバーから送受信したパケットを追跡します。
- IP — 送受信した IP パケットを追跡します。

トレースログには、管理下システムのオペレーティングシステムではなく、iDRAC6 の内部ファームウェアに関連する iDRAC6 ファームウェア固有のエラーコードが含まれている場合もあります。

メモ : iDRAC6 は、1500 バイトより大きいパケットサイズの ICMP（Ping）にはエコーしません。

racdump の使用

`racadm racdump` コマンドは、ダンプ、状態、iDRAC6 ボードの一般情報を取得する単一コマンドです。

メモ : このコマンドは、Telnet、SSH およびリモート racadm インタフェースのみで使用できます。詳細については、デルサポートサイト **dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』の racdump コマンドを参照してください。

coredump の使用

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

使用可能な場合、coredump 情報は RAC の電源を切った後も、次のどちらかの状態が発生するまで保持されます。

- `coredumpdelete` サブコマンドを使用して coredump 情報がクリアされた
- RAC で別の重要な問題が発生した この場合、coredump の内容は最後に発生した重大エラーに関するものとなります。

`racadm coredumpdelete` コマンドを使用すると、現在 RAC に保存されている **coredump** データを消去できます。詳細については、デルサポートサイト **dell.com/support/manuals** の『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』の `coredump` および `coredumpdelete` サブコマンドを参照してください。

21

センサー

ハードウェアセンサーまたはプローブを使用すると、不安定なシステムや損傷などの障害に対して適切な処置を講じることができるため、ネットワーク上のシステムをさらに効率的に監視できます。

iDRAC6 を使用すると、ハードウェアセンサーのバッテリ、ファンプローブ、シャーシイントルージョン、電源装置、消費電力、温度、電圧などを監視できます。

バッテリプローブ

バッテリプローブは、システム基板 CMOS とストレージ ROMB（RAM on Motherboard）のバッテリに関する情報を提供します。

メモ : ストレージ ROMB のバッテリ設定は、システムに ROMB がある場合にのみ表示されます。

ファンプローブ

ファンプローブセンサーは次についての情報を提供します。

- ファンの冗長性 — プライマリファンが事前に設定された速度で熱を放散しなくなると、セカンダリファンが取って代わる機能。
- ファンプローブリスト — システムのすべてのファンの速度についての情報を提供します。

シャーシイントルージョンプローブ

シャーシイントルージョンプローブは、シャーシが開いているか閉じているかというシャーシの状態を表示します。

電源装置プローブ

電源装置プローブは次についての情報を提供します。

- 電源装置の状態
- 電源装置の冗長性（主 電源に障害が発生した場合に、冗長 電源が取って代わる機能）。

  メモ : システムに電源装置が 1 つしかない場合、電源の冗長性は **無効** に設定されます。

リムーバブルフラッシュメディアプローブ

リムーバブルフラッシュメディアセンサーは、vFlash SD カードの状態（アクティブか不在か）を表示します。SD の使い方の詳細については、245 ページの「vFlash SD カードの設定と vFlash パーティションの管理」を参照してください。

電力監視プローブ

電力監視プローブは、*リアルタイム*の消費電力に関する情報をワットとアンペア単位で表示します。

iDRAC6 で設定した現在の日時から数えて最後の 1 分、1 時間、1 日、または 1 週間の消費電力をグラフで表示することもできます。

温度プローブ

温度センサーは、システム基板の周辺温度についての情報を提供します。温度プローブは、プローブの状態が事前に設定された警告値および重要なしきい値の範囲内にあるかどうかを示します。

電圧プローブ

次は一般的な電圧プローブです。ご使用のシステムには、これら以外のものが使用されている可能性があります。

- CPU [n] VCORE
- システム基板 0.9V PG
- システム基板 1.5V ESB2 PG
- システム基板 1.5V PG
- システム基板 1.8V PG
- システム基板 3.3V PG
- システム基板 5V PG
- システム基板バックプレーン PG
- システム基板 CPU VTT
- システム基板リニア PG

電圧プローブは、プローブの状態が事前に設定された警告値および重要なしきい値の範囲内にあるかどうかを示します。

22

セキュリティ機能の設定

iDRAC6 には次のセキュリティ機能があります。

- iDRAC6 管理者用の高度なセキュリティオプション
  - 仮想コンソールリダイレクト無効 オプションをオンにすると、ローカルシステムユーザーが iDRAC6 仮想コンソール機能を使用して仮想コンソールを無効にできます。
  - ローカル設定の無効オプションをオンにすると、*リモート* iDRAC6 管理者が iDRAC6 の設定機能を以下から選択的に無効にできます。
    - BIOS POST オプション ROM
    - ローカル RACADM と Dell OpenManage Server Administrator ユーティリティを使用したオペレーティングシステム
- 128 ビット SSL 暗号化と 40 ビット SSL 暗号化（128 ビットが許可されていない国）をサポートする RACADM CLI とウェブインタフェース

  メモ : Telnet は SSL 暗号化をサポートしていません。
- ウェブインタフェースまたは RACADM CLI を使用したセッションタイムアウトの設定（分単位）
- 設定可能な IP ポート（該当する場合）
- 暗号化トランスポート層を使用してセキュリティを強化するセキュアシェル（SSH）
- IP アドレスごとのログイン失敗回数の制限によって、失敗回数が制限を超えた 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 アドレス範囲を制限

iDRAC6 システム管理者用のセキュリティオプション

iDRAC6 ローカル設定を無効にする

システム管理者は、**i DRAC の設定** ? **ネットワーク / セキュリティ** ? **サービス** を選択して、iDRAC6 グラフィカルユーザーインタフェース（GUI）からローカル設定を無効にできます。オプションの **ROM を使用した iDRAC のローカル設定を無効にする** チェックボックスをオンにすると、iDRAC6 ローカル設定ユーティリティ（システム起動時に **<Ctrl+E>** を押してアクセス）は読み取り専用モードで起動し、ローカルユーザーがデバイスを設定できなくなります。システム管理者が **RACADM を使用した iDRAC のローカル設定を無効にする** チェックボックスをオンにすると、ローカルユーザーは iDRAC6 の設定を読み取ることはできますが、RACADM ユーティリティや Dell OpenManage Server Administrator を使用して設定することができません。

システム管理者はウェブベースのインタフェースを使用して、これらのオプションのいずれか一方、または両方を同時に有効にできます。

システム再起動中のローカル設定を無効にする

この機能は、システムの再起動中に管理下システムのユーザーが iDRAC6 を設定できなくします。

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

メモ : このオプションは、iDRAC6 設定ユーティリティでのみサポートされています。このバージョンにアップグレードするには、BIOS をアップグレードする必要があります。デルサポートサイト **support.dell.com** からの BIOS アップデートパッケージを使用して BIOS をアップグレードしてください。

ローカル RACADM からローカル設定を無効にする

この機能は、管理下システムのユーザーがローカル RACADM または Dell OpenManage Server 管理ユーティリティを使って iDRAC6 を設定する機能を無効にします。

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

警告 : これらの機能は、ローカルユーザーがローカルシステムから iDRAC6 を設定する機能（デフォルト設定に戻す機能も含む）を著しく制限します。これらの機能は注意して使用することをお勧めします。インタフェースを一度に 1 つだけ無効にすると、ログイン権限も一緒に失わないようにできます。

メモ : 詳細については、デルサポートサイト **support.dell.com** にあるホワイトペーパー「DRAC 上のローカル設定とリモート仮想 KVM を無効にする」をお読みください。

システム管理者はローカル RACADM コマンドを使ってローカル設定オプションを設定できますが、セキュリティ上の理由から、リセットは帯域外の iDRAC6 ウェブインタフェース またはコマンドラインインタフェースからしかできません。システムの電源投入時自己診断テストが完了し、オペレーティングシステムが起動したら、cfgRacTuneLocalConfigDisable オプションが適用されます。オペレーティングシステムとしては、ローカル RACADM コマンドを実行できる Microsoft Windows Server または Enterprise Linux、あるいは Dell OpenManage Deployment Toolkit のローカル RACADM コマンド を実行するために限定的に使用される Microsoft Windows Preinstallation Environment や vmlinux などが挙げられます。

次のような場合には、システム管理者がローカル設定を無効にする必要があります。たとえば、サーバーやリモートアクセスデバイスの管理者が複数人いるデータセンターでは、サーバーのソフトウェアスタックの保守担当者はリモートアクセスデバイスへの管理者権限を必要としない場合があります。同様に、技術者はシステムの定期保守作業中、サーバーへの物理的なアクセス権限を持ち、この間、システムを再起動し、パスワード保護されている BIOS にもアクセスできますが、リモートアクセスデバイスの設定はできないようにする必要があります。このような状況では、リモートアクセスデバイスの管理者がローカル設定を無効にすることができます。

ただし、ローカル設定を無効にすると、iDRAC6 をデフォルト設定に戻す能力を含め、ローカル設定権限が著しく制限されるため、これらのオプションは必要なときのみ使用し、通常は一度に 1 つだけのインタフェースを無効にし、ログイン権限を完全に失わないように注意してください。たとえば、システム管理者がローカル iDRAC6 ユーザー全員を無効にし、Microsoft Active Directory ディレクトリサービスのユーザーだけが iDRAC6 にログインできるようにした後、Active Directory の認証インフラストラクチャにエラーが発生すると、システム管理者がログインできなくなる可能性があります。同様に、システム管理者がすべてのローカル設定を無効にし、動的ホスト構成プロトコル（DHCP）サーバーを含むネットワークに静的 IP アドレスを使って iDRAC6 を配置した後、DHCP サーバーが iDRAC6 の IP アドレスをネットワーク上の別のデバイスに割り当てた場合、その競合によって DRAC の帯域外の接続が無効になり、システム管理者がシリアル接続を通してファームウェアをデフォルト設定に戻すことが必要になります。

iDRAC6 仮想コンソールを無効にする

システム管理者は iDRAC6 リモート仮想コンソールを選択的に無効にすることで、仮想コンソールを通して他のユーザーから見られることなくローカルユーザーがシステムを操作するための柔軟でセキュアなメカニズムを提供できます。この機能を使用するには、サーバーに iDRAC 管理下ノードソフトウェアをインストールする必要があります。システム管理者は次のコマンドを使用して、仮想コンソール を無効にできます。

```
racadm LocalConRedirDisable 1
```

LocalConRedirDisable コマンドは、引数 1 を使って実行すると既存のリモート仮想コンソール セッションウィンドウを無効にします。

リモートユーザーがローカルユーザーの設定を上書きするのを防ぐために、このコマンドはローカル RACADM でのみ使用可能です。システム管理者は、Microsoft Windows Server 2003 や SUSE Linux Enterprise Server 10 など、ローカル RACADM 対応のオペレーティングシステムでこのコマンドを使用できます。このコマンドはシステム再起動後も有効であるため、仮想コンソールを再度有効にするには、システム管理者がこのコマンドを無効にする必要があります。これには、次のように引数 0 を使用します。

```
racadm LocalConRedirDisable 0
```

状況によっては、iDRAC6 仮想コンソール を無効にする必要が生じます。たとえば、システム管理者は自分が設定した BIOS 設定をリモート iDRAC6 ユーザーに見られたくない場合、`LocalConRedirDisable` コマンドを使ってシステム POST 中に仮想コンソール を無効にできます。また、システム管理者がシステムにログインするたびに仮想コンソール を自動的に無効にすることでセキュリティを強化できます。これには、ユーザーログオンスクリプトから `LocalConRedirDisable` コマンドを実行します。

メモ : 詳細については、デルサポートサイト **support.dell.com** にあるホワイトペーパー「DRAC 上のローカル設定とリモート仮想 KVM を無効にする」をお読みください。

ログオンスクリプトの詳細については、**technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx** を参照してください。

SSL とデジタル証明書を使用した iDRAC6 通信のセキュリティ確保

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

- 316 ページの「SSL（セキュアソケットレイヤー）」
- 317 ページの「証明書署名要求（CSR）」
- 317 ページの「SSL メインメニューへのアクセス」
- 318 ページの「証明書署名要求の生成」

SSL（セキュアソケットレイヤー）

iDRAC6 には、業界標準の SSL セキュリティプロトコルを使用してインターネットで暗号化データを送信するように構成されたウェブサーバーが含まれています。公開キーと秘密キーの暗号技術に基づく SSL は、クライアントとサーバー間で認証済みの暗号化通信を使用して、ネットワーク上の盗聴を防止するために広く受け入れられているセキュリティ方式です。

SSL に対応したシステムの特徴

- SSL 対応のクライアントに対して自己認証する
- クライアントがサーバーに対して認証できるようにする
- 両方のシステムが暗号化された接続を確立できる

この暗号処理は高度なデータ保護を提供します。iDRAC6 では、北米のインターネットブラウザで一般的に使用されている最も安全な暗号化方式である 128 ビットの SSL 暗号化標準を採用しています。

iDRAC6 ウェブサーバーには、デルが署名をした SSL デジタル証明書（サーバー ID）が含まれています。インターネットにおける高度なセキュリティを確実にするには、次の手順を実行します。

1. デフォルトのウェブサーバー SSL 証明書を、認証局（CA）からの有効な証明書に置き換えます。
2. iDRAC6 に要求を送信することにより、証明書署名要求（CSR）を生成します。
3. 認証局（CA）に CSR を提供して、有効な証明書を取得します。

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は、リモートシステムの身元を保護して、リモートシステムとやり取りする情報を他のユーザーが表示したり変更したりできないようにします。DRAC のセキュリティを確保するため、CSR を生成して CSR を CA に送信し、CA から返された証明書をアップロードすることをお勧めします。

CA は、信頼性の高いスクリーニング、身分証明、その他の重要なセキュリティ条件を満たすことが IT 業界で認められている事業体です。CA には、Thawte や VeriSign などがあります。CA は CSR を受け取ると、CSR に含まれている情報を確認します。応募者が CA のセキュリティ標準を満たしていると、CA はネットワークおよびインターネットを介したトランザクションに対して、応募者を一意に識別する証明書を発行します。

CA が CSR を承認して証明書を送信したら、証明書を iDRAC6 ファームウェアにアップロードする必要があります。iDRAC6 ファームウェアに保管されている CSR 情報は、証明書に記載されている情報と一致する必要があります。

SSL メインメニューへのアクセス

1. **システム** ツリーを展開して、**iDRAC の設定** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **SSL** をクリックします。

CSR を生成、既存サーバー証明書をアップロード、または既存サーバー証明書を表示するには、**SSL メインメニュー**（表 22-1 を参照）を使用します。CSR の情報は iDRAC6 ファームウェアに保存されています。**SSL** ページで使用できるボタンについての情報は、『iDRAC6 オンラインヘルプ』を参照してください。

表 22-1. SSL メインメニュー

フィールド	説明
証明書署名要求（CSR）の生成	**次へ** をクリックしてページを開くと、CA に送信する CSR を生成して、セキュアなウェブ証明書を申請できます。
サーバー証明書のアップロード	**次へ** をクリックし、iDRAC6 へのアクセス制御に使用する会社の既存の証明書をアップロードします。 **メモ：**iDRAC6 で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER によって符号化された証明書は受け入れられません。新しい証明書をアップロードすると、iDRAC6 て受信したデフォルトの証明書が置き換えられます。
サーバー証明書の表示	**次へ** をクリックして、既存のサーバー証明書を表示します。

証明書署名要求の生成

メモ：新しい CSR は、ファームウェアにある古い CSR を上書きします。iDRAC が署名済み CSR を受け入れる前に、ファームウェア内の CSR が CA から返される証明書と一致する必要があります。

1. **SSL メインメニュー** ページで、**証明書署名要求（CSR）の生成** を選択して、**次へ** をクリックします。
2. **証明書署名要求（CSR）の生成** ページで、各 CSR 属性の値を入力します。

   表 22-2 に、**証明書署名要求（CSR）の生成** ページのオプションを示します。
3. CSR を開くまたは保存するには、**生成** をクリックします。
4. **証明書署名要求（CSR）の生成** ページで適切なボタンをクリックして続行します。**証明書署名要求（CSR）の生成** ページで使用できるボタンの詳細については、『iDRAC6 オンラインヘルプ』を参照してください。

表 22-2. 証明書署名要求（CSR）の生成 ページのオプション

フィールド	説明
共通名	証明される名前（通常は、**xyzcompany.com** のようなウェブサーバーのドメイン名）。英数字、ハイフン、ピリオドが有効です。
組織名	この組織に関連付けられた名前（たとえば「XYZ Corporation」）。英数字、ハイフン、ピリオドが有効です。

表 22-2. 証明書署名要求（CSR）の生成 ページのオプション （続き）

フィールド	説明
組織単位	部門など組織単位に関連付けられた名前（たとえば「エンタープライズグループ」）。英数字、ハイフン、ピリオドが有効です。
地域	証明する会社が所在する都市や地域（たとえば「神戸」）。英数字、ハイフン、ピリオドが有効です。
状態名	証明書を申請している組織の所在地（たとえば「東京」）。英数字、ハイフン、ピリオドが有効です。
国番号	証明書を申請している組織が所在する国の名前。国を選択するには、ドロップダウンメニューを使用します。
E- メール	CSR に関連付けられている E- メールアドレス。会社の E- メールアドレスや、CSR に関連付けたいその他の E- メールアドレスを入力できます。このフィールドは省略可能です。

サーバー証明書の表示

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

   表 22-3 に、**証明書** ウィンドウに表示されるフィールドと説明を示します。

2. **サーバー証明書の表示** ページの適切なボタンを押して続行します。

表 22-3. 証明書情報

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	対象者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

セキュアシェル（SSH）の使用

SSH の使い方の詳細については、82 ページの「セキュアシェル（SSH）の使用」を参照してください。

サービスの設定

メモ : これらの設定を変更するには、**iDRAC の設定** 権限が必要です。また、リモート RACADM コマンドラインユーティリティは、ユーザーが **root** としてログインしているときにのみ有効にできます。

1. システム ツリーを展開して、**iDRAC の設定** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **サービス** をクリックします。
3. 必要に応じて次のサービスを設定します。
   - ローカル設定（表 22-4）
   - ウェブサーバー（表 22-5）
   - SSH（表 22-6）
   - Telnet（表 22-7）
   - リモート RACADM（表 22-8）
   - SNMP エージェント（表 22-9）
   - 自動システムリカバリエージェント（表 22-10）

   自動システムリカバリエージェント を使用して、iDRAC6 の **前回のクラッシュ画面** 機能を有効にします。

   メモ : iDRAC6 で **前回クラッシュ画面** が機能するためには、**Server Administrator** をインストールするときに **処置** を **システムの再起動**、**システムの電源を切る**、または **システムの電源を入れなおす** に設定して**自動回復** 機能をアクティブにする必要があります。
4. **変更を適用** をクリックしてサービスページの設定を適用します。

表 22-4. ローカル設定

設定	説明
オプション ROM を使って iDRAC ローカル設定を無効にする	オプション ROM を使って iDRAC のローカル設定を無効にします。システム再起動中に <Ctrl+E> を押してセットアップモジュールを開始するようにプロンプトが表示されます。
RACADM を使って iDRAC ローカル設定を無効にする	ローカル RACADM を使って iDRAC のローカル設定を無効にします。

表 22-5. ウェブサーバーの設定

設定	説明
有効	ウェブサーバーを有効または無効にします。オン = 有効、オフ = 無効
最大セッション数	システムで許可される同時セッションの最大数。
アクティブセッション数	システムの現在のセッション数（**最大セッション数** 以下）。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更はすぐに適用され、現在のウェブインタフェースセッションが終了します。ウェブサーバーもリセットされます。新しいウェブインタフェースセッションが始まるまで数分お待ちください。タイムアウト範囲は 60 ～ 10800 秒です。デフォルト値は 1800 秒です。
HTTP ポート番号	iDRAC がサーバー接続に使用するポート。デフォルト設定は **80** 秒です。
HTTPS ポート番号	iDRAC がサーバー接続に使用するポート。デフォルト設定は **443** 秒です。

表 22-6. SSH の設定

設定	説明
有効	SSH を有効または無効にします。選択されている場合、SSH が有効になります。
タイムアウト	セキュアシェルのアイドルタイムアウト（秒）。タイムアウト範囲は 60 ～ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **300** です。
ポート番号	SSH 接続で iDRAC6 が通信するポート。デフォルトは **22** です。

表 22-7. Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。チェックボックスがオンの場合は、Telnet が有効になります。
タイムアウト	Telnet のアイドルタイムアウト（秒）。タイムアウト時間の範囲は 60 ～ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **300** です。
ポート番号	iDRAC6 が Telnet 接続を待ち受けるポート。デフォルトは **23** です。

表 22-8. リモート RACADM の設定

設定	説明
有効	リモート RACADM を有効または無効にします。チェックボックスをオンにすると、リモート RACADM が有効になります。
アクティブセッション数	システムの現在のセッション数。

表 22-9. SNMP エージェントの設定

設定	説明
有効	SNMP エージェントを有効または無効にします。オン = 有効、オフ = 無効
コミュニティ名	使用される SNMP コミュニティ文字列を定義します。コミュニティ名は、空白文字を含まずに最大 31 文字まで使用できます。デフォルト設定は **public** です。

表 22-10. 自動システムリカバリエージェントの設定

設定	説明
有効	自動システムリカバリエージェントを有効にします。

iDRAC6 の追加のセキュリティオプションを有効にする

リモートシステムへの不正アクセスを防ぐため、iDRAC6 では次の機能を提供しています。

- IP アドレスフィルタ（IPRange）— iDRAC6 にアクセスできる特定の IP アドレス範囲を定義します。
- IP アドレスブロック — 特定の IP アドレスからのログイン試行の失敗回数を制限します。

これらの機能は iDRAC6 のデフォルト設定では無効になっています。次のサブコマンドまたはウェブインタフェースを使用して、これらの機能を有効にしてください。

`racadm config -g cfgRacTuning -o <`*オブジェクト名*`> <`*値*`>`

これらの機能はまた、セッションのアイドルタイムアウト値や、ネットワークに定義済みのセキュリティプランと一緒にも使用できます。

以下の項で、これらの 機能について詳しく説明します。

IP フィルタ（IpRange）

IP アドレスフィルタ（または IP 範囲チェック）を使用すると、ユーザーが特定した範囲内にある IP アドレスの クライアントワークステーションや管理ワークステーションからのみ iDRAC6 へのアクセスを許可します。その他のログインはすべて拒否されます。

IP フィルタは受信ログインの IP アドレスを、次の **cfgRacTuning** プロパティで指定する IP アドレス範囲と比較します。

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

cfgRacTuneIpRangeMask プロパティは着信 IP アドレスと **cfgRacTuneIpRangeAddr** プロパティの両方に適用されます。両方のプロパティの結果が同じであれば、受信ログイン要求の iDRAC6 へのアクセスが許可されます。この範囲外の IP アドレスからのログイン要求にはエラーが返されます。

次の式の値がゼロに等しい場合は、ログインに進みます。

```
cfgRacTuneIpRangeMask &(< 着信 IP アドレス > ^
cfgRacTuneIpRangeAddr)
```

& は数量のビットワイズ AND で ^ はビットワイズ XOR です。

cfgRacTuning プロパティの完全リストは、デルサポートサイト **dell.com/support/manuals** にある『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

表 22-11. 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。 許可する IP アドレスの上位部分を決定するため、このプロパティは **cfgRacTuneIpRangeMask** とビット単位で AND されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0 ～ 192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
cfgRacTuneIpRangeMask	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。

IP フィルタを有効にする

IP フィルタの設定には、次のコマンド例を参照してください。

RACADM と RACADM コマンドの詳細については、100 ページの「RACADM のリモート使用」を参照してください。

メモ : 次の RACADM コマンドは 192.168.0.57 以外のすべての IP アドレスをブロックします。

ログインを 1 つの IP アドレスに限定するには（たとえば 192.168.0.57）、次の項に示すようなフルマスクを使用してください。

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.57
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.255
```

連続する 4 つの IP アドレスにログインを限定するには（たとえば、192.168.0.212 ～ 192.168.0.215）、次の項に示されるように、マスクの最下位の 2 ビットを除くすべてを選択します。

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr
192.168.0.212
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask
255.255.255.252
```

IP フィルタのガイドライン

IP フィルタを有効にする場合は、次のガイドラインに従ってください。

- **cfgRacTuneIpRangeMask** は必ずネットマスク形式で設定します。最上位ビットがすべて 1 で（これがマスクのサブネットを定義）、下位ビットはすべてゼロにします。
- 必要な範囲の基底アドレスを **cfgRacTuneIpRangeAddr** の値として使用します。このアドレスの 32 ビットのバイナリ値は、マスクにゼロがある下位ビットがすべてゼロになります。

IP ブロック

IP ブロックは、事前に選択した時間枠で、特定の IP アドレスからの過剰なログイン失敗を動的に検知し、そのアドレスが iDRAC6 にログインできないようにブロックします。

IP ブロックのパラメータは、次のような **cfgRacTuning** グループ機能を使用します。

- 許可するログイン失敗回数
- これらの失敗を数える時間枠（秒）
- ログイン失敗回数が所定の合計数を超えた IP アドレスからのセッション確立を防止する時間（秒）

特定の IP アドレスからのログイン失敗が累積すると、それらは内部カウンタによって*計数*されます。ユーザーがログインに成功すると、失敗履歴がクリアされて、内部カウンタがリセットされます。

メモ : クライアント IP アドレスからのログイン試行が拒否されると、SSH クライアントに「`SSH ID: リモートホストが接続を閉じました`」というメッセージが表示される場合があります。

cfgRacTuning プロパティの完全リストは、デルサポートサイト **dell.com/support/manuals** にある『*iDRAC6* および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

表 22-12 に、ユーザー定義のパラメータを示します。

表 22-12. ログイン再試行制限のプロパティ

プロパティ	定義
cfgRacTuneIpBlkEnable	IP ブロック機能を有効にします。 一定時間内に（**cfgRacTuneIpBlkFailCount**）1 つの IP アドレスからの失敗が連続すると（**cfgRacTuneIpBlkFailWindow**）、以降そのアドレスからのセッション確立試行が一定の時間（**cfgRacTuneIpBlkPenaltyTime**）拒否されます。
cfgRacTuneIpBlkFailCount	ログイン試行を拒否するまでの IP アドレスのログイン失敗回数を設定します。
cfgRacTuneIpBlkFailWindow	失敗回数を数える時間枠を秒で指定します。失敗回数がこの制限値を超えると、カウンタはリセットされます。
cfgRacTuneIpBlkPenaltyTime	失敗回数が制限値を超えた IP アドレスからのセッションをすべて拒否する時間枠を秒で定義します。

IP ブロックを有効にする

次の例では、クライアントが 1 分間に 5 回ログイン試行に失敗した場合に、5 分間このクライアント IP アドレスのセッション確立を防止します。

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 300
```

次の例は、1 分以内に失敗が 3 回を超えた場合に、1 時間ログイン試行を阻止します。

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

iDRAC6 GUI を使ったネットワークセキュリティの設定

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

1. **システム** ツリーで、**iDRAC の設定** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **ネットワーク** をクリックします。
3. **ネットワークの設定** ページで **詳細設定** をクリックします。
4. **ネットワークセキュリティ** ページで属性値を設定してから **変更の適用** をクリックします。

   表 22-13 に、**ネットワークセキュリティ** ページの設定を示します。
5. **ネットワークセキュリティ** ページの適切なボタンをクリックして続行します。**ネットワークセキュリティ** ページのボタンの使用についての詳細は、『iDRAC6 オンラインヘルプ』を参照してください。

表 22-13. ネットワークセキュリティページの設定

設定	説明
IP 範囲有効	IP 範囲のチェック機能を有効にします。この設定により、iDRAC6 にアクセスできる IP アドレスの範囲を定義できます。
IP 範囲のアドレス	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンが決まります。可能な IP アドレスの上位部分を決定するため、この値は IP 範囲サブネットマスクとビット単位で AND されます。上位部分にこのビットパターンを含んでいる IP アドレスは、iDRAC6 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0 ～ 192.168.1.255 から iDRAC6 セッションが確立できるように設定されています。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。 例：**255.255.255.0**
IP ブロック有効	事前に選択した時間枠で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。
IP ブロックエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。
IP ブロックのエラーウィンドウ	ここで指定した時間枠（秒）内に IP ブロックエラーカウントが制限値を超えると、IP ブロックペナルティ時間がトリガされます。
IP ブロックのペナルティ時間	ログイン失敗回数が制限値を超えた IP アドレスからのセッションをすべて拒否する時間を秒で指定します。

索引

記号

2 要素認証
TFA, 174

A

Active Directory
iDRAC6 での使用 , 129
iDRAC6 へのアクセス設定 , 137
iDRAC6 ユーザーの追加 , 144
オブジェクト , 134
スキーマ拡張 , 134
拡張スキーマでの使用 , 134
証明書の管理 , 62
設定 , 29
標準スキーマでの使用 , 151

Active Directory の設定 , 29

ASR
ウェブインタフェースからの設定 , 66

C

CSR
証明書署名要求 , 58
生成 , 60
説明 , 59

D

Dell 拡張のインストール
Active Directory ユーザーと
コンピュータスナップイン ,
143

E

E- メールアラート
RACADM CLI を使用した設定 , 292
ウェブインタフェースを使用した
設定 , 291
設定 , 291

E- メール警告
ウェブインタフェースからの設定 , 55

I

iDRAC
ダイレクト接続基本モードと
ダイレクト接続ターミナル
モード , 90

iDRAC KVM
コンソールリダイレクトを
使用した有効または
無効の設定 , 196

iDRAC6
ウェブインタフェースの設定 , 43
セットアップ , 29
トラブルシューティング , 307
ネットワークの設定 , 98
ネットワーク経由でのアクセス , 99
ファームウェアのアップデート , 37
ファームウェアのダウンロード , 37
ユーザーの追加と設定 , 115
拡張スキーマを使用した Active
Directory の設定 , 146
詳細設定 , 79
設定 , 34
標準スキーマ Active Directory の
設定 , 153

iDRAC6 CLI, 88

iDRAC6 Enterprise, 21
iDRAC6 Enterprise プロパティ , 298
iDRAC6 IPMI の設定 , 29
iDRAC6 LAN, 274
iDRAC6 NIC の設定 , 46
iDRAC6 ウェブベースの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 , 16
iDRAC6 サービス
設定 , 66
iDRAC6 サービスの設定 , 66
ASR, 66
SSH, 66
telnet, 66
ウェブサーバー , 66
リモート RACADM, 66
リモート SNMP エージェント , 66
ローカル設定 , 66
iDRAC6 シリアル
設定 , 96
iDRAC6 設定ユーティリティ
開始 , 273
説明 , 273
iDRAC6 ソフトウェアのインストールと設定 , 34
idrac6 の設定
シリアル接続 , 88
iDRAC6 のポート , 25
iDRAC6 ファームウェアのアップデート / システムサービスリカバリイメージ , 69
アップデート / ロールバック , 69
設定の保存 , 70
iDRAC6 ファームウェアロールバック , 70
設定の保存 , 71
iDRAC6 プロパティ、ネットワークとユーザーの設定 , 29
iDRAC6 ユーザー
権限を有効にする , 127
iDRAC6 用 VFlash メディアカードの設定 , 245
IP のブロック
説明 , 324
有効にする , 326
IP フィルタ
説明 , 323
有効にする , 324
IP フィルタリングおよびブロック , 51
IP ブロック
ウェブインタフェースからの設定 , 51
IPMI
LAN の設定 , 46
RACADM CLI からの設定 , 226
ウェブインタフェースからの設定 , 56, 225
IPMI Over LAN, 275
IPMI 設定 , 50
IPMI 対応 , 20
IPMI の設定 , 225
IPMI の匿名ユーザー
ユーザー 1, 115
IpRange 確認
説明 , 323
IPv6 の設定 , 49
iVMCLI ユーティリティ
オペレーティングシステムの導入 , 217

L

LAN Parameters, 275

LAN ユーザーの設定 , 282
Linux
シリアルコンソールリダイレクト用の設定 , 84

N

NIC モード
フェールオーバー付きで共有（LOM2）, 32
フェールオーバー付きで共有（すべての LOM）, 33
共用 , 32
専用 , 32

P

PEF
RACACM CLI を使用した設定 , 290
ウェブインタフェースを使用した設定 , 289
設定 , 289
PET
RACADM CLI を使用した設定 , 290
ウェブインタフェースを使用した設定 , 290
フィルタ可能なプラットフォームイベントテーブル , 52
設定 , 290
POST ログ
使用 , 304

R

RACADM
iDRAC6 ユーザーの削除 , 127
iDRAC6 ユーザーの追加 , 126
インストールと削除 , 36
RACADM サブコマンド
getconfig, 200
RACADM を使用した iDRAC6 の設定 , 122-123
RACADM を使用した汎用 LDAP ディレクトリサービスの設定 , 163
racadm ユーティリティ
構文解析規則 , 108

S

SD カードのプロパティ , 246
Secure Shell（SSH）
使用 , 82, 319
Secure Sockets Layer（SSL）
ファームウェア証明書のインポート , 132
SEL
iDRAC6 設定ユーティリティを使用した管理 , 282
Server Management Command Line Protocol（SM-CLP）
サポート , 207
説明 , 207-208
SSL へのアクセス
ウェブインタフェースの使用 , 58

T

telnet
iDRAC サービスの設定 , 66

U

Unified Server Configurator, 26, 280-281

システムサービス , 26, 280-281
USB フラッシュキー , 245
USB フラッシュドライブの
エミュレーション
タイプ , 279

V

vFlash SD カード , 245
vFlash SD カードのプロパティ , 248
vFlash パーティション , 245
VLAN の設定 , 51
vm6deploy スクリプト , 217
VMCLI ユーティリティ , 215
vm6deploy スクリプトを含む , 217
インストール , 219
オペレーティングシステムシェル
のオプション , 223
パラメータ , 220
構文 , 219
使用 , 218
説明 , 215
戻りコード , 223

W

WS-MAN プロトコル , 20

あ

アラートの設定 , 29
イメージファイル , 251
ウェブインタフェース
iDRAC6 設定用 , 43
アクセス , 43
ログアウト , 45
ログイン , 44
ウェブインタフェースからの PEF
設定 , 53
ウェブインタフェースからの PET
設定 , 54
ウェブインタフェースからの SOL
設定 , 230
ウェブブラウザ
サポート , 24
設定 , 39
オペレーティングシステム
インストール（手動方式）, 237
オペレーティングシステムの導入
VMCLI ユーティリティ , 215
温度センサー , 312

か

拡張スキーマ
Active Directory の概要 , 134
仮想メディア
iDRAC6 設定ユーティリティを
使用した設定 , 279
ウェブインタフェースからの設定 , 233
オペレーティングシステムの
インストール , 237
起動 , 236
実行 , 234
説明 , 231
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 , 215
空のパーティション , 250
管理下システム , 29
ソフトウェアのインストール , 35
管理ステーション , 29
コンソールリダイレクトの設定 , 184
ソフトウェアのインストール , 35

端末エミュレーションの設定 , 93
画面解像度、サポート , 187
起動イメージファイル
作成 , 215
コンソールリダイレクト
セッションを開く , 189
使用 , 183
設定 , 188
コンソールリダイレクトと仮想
メディアの設定 , 29

さ

サーバー証明書
アップロード , 61
表示 , 61, 319
サーバーの識別 , 309
サービス
ウェブインタフェースからの設定 , 66
設定 , 320
再起動オプション
無効にする , 288
サポートされている CIM
プロファイル , 203
システム
iDRAC6 を使用する設定 , 32
システムサービス設定
Unified Server
Configurator, 280
システム情報の表示 , 296
シャーシイントルージョン
プローブ , 311
証明書
SSL とデジタル , 58, 316
ルート CA 証明書のエクスポート , 131
証明書署名要求 CSR, 58
証明書署名要求（CSR）
新しい証明書の生成 , 318
説明 , 317
シリアルオーバー LAN（SOL）
設定 , 230
シリアルコンソール
DB-9 ケーブルへの接続 , 93
シリアルモード
設定 , 96
シングルサインオン , 172
自動検出 , 283
スマートカード証明書の
エクスポート , 175
スマートカード認証 , 29, 178
スマートカードのログオン , 174
セキュアソケットレイヤ（SSL）, 58
説明 , 316
セキュリティオプションを
有効にする , 322
セキュリティの設定 , 29
設定
シリアルオーバー LAN, 230
設定のテスト , 159
設定ファイルの作成 , 107
セットアップ
iDRAC6, 29
前回クラッシュ画面
管理下サーバーでのキャプチャ , 28

た

ターミナルモード
設定 , 96-97
ダイレクト接続基本モード , 88
ダイレクト接続ターミナルモード , 88

ダイレクト接続ターミナルモード
とシリアルコンソール
リダイレクト間の
切り替え , 91
データ複製（dd）ユーティリティ , 216
電圧プローブ , 312
電源インベントリとバジェット , 263
電源装置プローブ , 311
電源の監視 , 263, 312
電源の設定と管理 , 264
電力キャップ , 263
トラブルシューティングツール , 307

な

内蔵システムオンチップマイクロ
プロセッサ , 19
認証
スマートカード , 29
ネットワークインタフェース
カードの設定 , 47
ネットワークセキュリティページ
の設定 , 51
ネットワークプロパティ
手動設定 , 110
設定 , 110

は

ハードウェア
インストール , 31
バッテリープローブ , 311
パーティションの起動 , 258
パーティションの削除 , 257
パーティションのフォーマット , 25
パーティションの連結または分離 , 256
パスワードレベルのセキュリティ
管理 , 20
必要なドキュメント , 26
標準スキーマ
Active Directory の概要 , 151
ビデオビューア
使用 , 192
ファームウェア
ウェブインタフェースによる
リカバリ , 69
ダウンロード , 37
ファームウェア / システムサービス
リカバリイメージ
ウェブインタフェースによる
アップデート , 69
ファームウェアのアップデート
iDRAC6, 37
ファイルシステムタイプ , 253
ファンプローブ , 311
ブートワンス
有効にする , 234
プラットフォーム
サポート , 24
プラットフォームイベント
設定 , 288
プラットフォームイベントトラップ
PET, 52
プラットフォームイベントの設定 , 52

ま

メディアリダイレクトウィザード , 235

や

役割ベースの権限 , 20, 115

ユーザー
ウェブインタフェースからの追加と設定 , 58, 115

ユーザー設定 , 115
iDRAC グループ権限 , 116
IPMI ユーザー特権 , 116
一般ユーザー設定 , 115

ユーティリティ
dd, 216

よくあるお問い合わせ
Active Directory での iDRAC6 の使用 , 164
コンソールリダイレクトの使用 , 199
仮想メディアの使用 , 239

よくあるお問い合わせ（FAQ）, 112

ら

リモートアクセス接続
サポート , 25

リモートシステム
トラブルシューティング , 295
電源の管理 , 296

リモートシステムのトラブルシューティング , 295

ローカル iDRAC6 ユーザーへのスマートカードログオンの設定 , 174