

Dell Chassis Management  
Controller ファームウェア  
バージョン 4.0  
ユーザースガイド



# 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:** 手順に従わないと、ハードウェアの損傷やデータの損失につながる可能性があることを示しています。

---

本書の内容は予告なく変更されることがあります。

© 2012 すべての著作権は **Dell Inc.** にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。本書で使用されている商標: Dell™、DELL のロゴ、FlexAddress™、OpenManage™、PowerEdge™、および PowerConnect™ は、Dell Inc. の商標です。Microsoft®、Active Directory®、Internet Explorer®、Windows®、Windows Server®、および Windows Vista® は、米国およびその他の国における Microsoft Corporation の商標または登録商標です。Red Hat® および Red Hat Enterprise Linux® は、米国およびその他の国における Red Hat, Inc. の登録商標です。Novell® は、米国およびその他の国における Novell Inc. の登録商標です。SUSE™ は、米国およびその他の国における Novell Inc. の商標です。Intel® は、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。Avocent® は、Avocent Corporation の商標です。OSCAR® は、Avocent Corporation またはその関連会社の登録商標です。

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. ソースおよびバイナリ形式での再配布と使用は、変更の有無を問わず、OpenLDAP の公開ライセンスで承認されている範囲内でのみ許可されます。このライセンスのコピーは、配布パッケージ内の最上位レベルのディレクトリに入っている LICENSE ファイル、または <http://www.OpenLDAP.org/license.html> でご覧いただけます。OpenLDAP は OpenLDAP Foundation の登録商標です。個々のファイルや提供パッケージは、他社が著作権を所有している場合があり、その他の制約を受ける可能性があります。この製品はミシガン大学 LDAP v3.3 ディストリビューションから派生しています。この製品には、公共ソースから派生した材料も含まれています。OpenLDAP に関する情報は <http://www.openldap.org/> から入手できます。Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. ソースおよびバイナリ形式での再配布と使用は、変更の有無を問わず、OpenLDAP の公開ライセンスで承認されている範囲内でのみ許可されます。Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Hallvard B.Furuseth. All rights reserved. ソースおよびバイナリ形式での再配布と使用は、変更の有無を問わず、この著作権表示を含めた形式でのみ許可されます。著作権所有者の名前を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示的または黙示的を問わず、保証なしに「現状有姿」で提供されます。Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. ソースおよびバイナリ形式での再配布と使用は、この著作権表示を含め、米国アン・アーバーのミシガン大学への謝辞を記載した場合にのみ許可されます。この大学名を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示的または黙示的を問わず、保証なしに「現状有姿」で提供されます。

商標または製品の権利を主張する事業体を表すために、その他の商標および社名が使用されていることがあります。それらの商標や会社名は、一切 Dell Inc. に帰属するものではありません。

**2012 - 03**

# 目次

1	概要	17
	このリリースの新機能	18
	CMC 管理機能	19
	セキュリティ 機能	20
	シャーシの概要	21
	ハードウェア仕様	22
	TCP/IP ポート	22
	対応リモートアクセス接続	23
	対応プラットフォーム	23
	対応ウェブブラウザ	24
	対応管理コンソールアプリケーション	24
	WS-Management のサポート	24
	その他の必要マニュアル	26
2	CMC のインストールと設定	29
	作業を開始する前に	29
	CMC ハードウェアの取り付け	29
	シャーシの統合チェックリスト	29
	CMC の基本的なネットワーク接続	30
	デジチェーン CMC ネットワーク接続	31
	管理ステーションへのリモートアクセスソフトウェアのインストール	35

<b>RACADM の Linux 管理ステーションへのインストール</b>	35
<b>Linux 管理ステーションから RACADM のアンインストール</b>	36
<b>ウェブブラウザの設定</b>	36
プロキシサーバー	37
フィッシングフィルタ	37
証明書失効リスト (CRL) のフェッチ	38
Internet Explorer で CMC からファイルのダウンロード	38
Internet Explorer でアニメーションの再生	38
<b>CMC への初期アクセスの設定</b>	39
CMC ネットワークの設定	40
LCD 設定ウィザードを使用したネットワーク設定	40
<b>ネットワーク経路による CMC へのアクセス</b>	46
<b>CMC ファームウェアのインストールまたはアップデート</b>	47
CMC ファームウェアのダウンロード	47
ウェブインタフェースを使用した CMC ファームウェアのアップデート	48
RACADM を使用した CMC ファームウェアのアップデート	48
<b>CMC プロパティの設定</b>	49
電力バジェットの設定	49
CMC ネットワークの設定	49
ユーザーの追加と設定	50
SNMP と E-メールアラートの追加	50
リモートシスログの設定	50
<b>冗長 CMC 環境について</b>	51
スタンバイ CMC について	51
CMC フェイルセーフモード	52
アクティブ CMC の選択プロセス	53
冗長 CMC の正常性ステータスの取得	53
<b>3 CMC にコマンドラインコンソールの使用を設定する方法</b>	55
<b>CMC 上のコマンドラインコンソール機能</b>	55



シリアル、Telnet、SSH コンソールの使用 . . . . .	56
CMC での Telnet コンソールの使用 . . . . .	56
CMC での SSH の使用 . . . . .	57
CMC で SSH を有効にする方法 . . . . .	57
SSH ポートの変更 . . . . .	58
フロントパネルから iKVM への接続を有効にする方法 . . . . .	58
ターミナルエミュレーションソフトウェアの設定 . . . . .	59
Linux Minicom の設定 . . . . .	59
接続コマンドでサーバーまたは I/O モジュールに接続する . . . . .	61
シリアルコンソールリダイレクト用に管理されたサーバー BIOS の設定 . . . . .	63
シリアルコンソールリダイレクト用 Windows の設定 . . . . .	63
起動中に Linux をシリアルコンソールリダイレクト用に設定する . . . . .	63
起動後に Linux をサーバーシリアルコンソールリダイレクト用に設定する . . . . .	65
<b>4 RACADM コマンドラインインタフェースの使用 . . . . .</b>	<b>69</b>
シリアル、Telnet、SSH コンソールの使用 . . . . .	69
CMC へのログイン . . . . .	70
テキストコンソールの起動 . . . . .	70
RACADM の使用 . . . . .	70
RACADM サブコマンド . . . . .	70
RACADM へのリモートアクセス . . . . .	74
racadm リモート機能の有効 / 無効化 . . . . .	75
RACADM のリモート使用 . . . . .	75
RACADM エラーメッセージ . . . . .	76
RACADM を使用した CMC の設定 . . . . .	76
CMC ネットワークプロパティの設定 . . . . .	77
CMC への初期アクセスの設定 . . . . .	77
現在のネットワーク設定の表示 . . . . .	78
ネットワーク LAN の設定 . . . . .	78

<b>RACADM を使用したユーザーの設定</b> . . . . .	84
<b>CMC ユーザーの追加</b> . . . . .	85
<b>RACADM による SSH 経由の公開キー認証の設定</b> . . . . .	86
<b>Windows 用の公開キーの生成</b> . . . . .	86
<b>Linux 用の公開キーの生成</b> . . . . .	87
<b>CMC の RACADM 構文メモ</b> . . . . .	87
<b>公開キーの表示</b> . . . . .	88
<b>公開キーの追加</b> . . . . .	88
<b>公開キーの削除</b> . . . . .	88
<b>公開キー認証を使用したログイン</b> . . . . .	89
<b>CMC ユーザーの権限を有効にする方法</b> . . . . .	89
<b>CMC ユーザーの無効化</b> . . . . .	90
<b>SNMP と E-メールアラートの設定</b> . . . . .	90
<b>複数シャーシ内の複数 CMC の設定</b> . . . . .	90
<b>CMC 設定ファイルの作成</b> . . . . .	91
<b>構文解析規則</b> . . . . .	93
<b>CMC IP アドレスの変更</b> . . . . .	95
<b>RACADM を使用して iDRAC でプロパティを設定する方法</b> 96	
<b>トラブルシューティング</b> . . . . .	97
<b>5 CMC ウェブインタフェースの使用</b> . . . . .	99
<b>CMC ウェブインタフェースへのアクセス</b> . . . . .	99
<b>ログイン</b> . . . . .	100
<b>ログアウト</b> . . . . .	101
<b>CMC の基本設定</b> . . . . .	101
<b>シャーシの物理的な場所とシャーシ名の設定</b> . . . . .	101
<b>CMC の日付と時刻の設定</b> . . . . .	102
<b>リムーバブルフラッシュメディアの有効化</b> . . . . .	102
<b>シャーシの正常性ページ</b> . . . . .	103
<b>シャーシグループの使用</b> . . . . .	104

シャーシグループの機能 . . . . .	104
シャーシグループのセットアップ . . . . .	104
リーダーからのメンバーの削除 . . . . .	105
シャーシグループの無効化 . . . . .	106
メンバーシャーシでの個別のメンバーの無効化 . . . . .	106
メンバーシャーシまたはサーバーのウェブページの起動 . . . . .	107
新しいメンバーとリーダーシャーシのプロパティの同期 . . . . .	107
MCM グループのブレードインベントリ . . . . .	108
ブレードインベントリレポートの保存 . . . . .	108
シャーシコンポーネントの概要 . . . . .	110
シャーシの図解 . . . . .	110
シャーシの正常性 . . . . .	112
選択したコンポーネントの情報 . . . . .	113
システム正常性ステータスの監視 . . . . .	119
シャーシとコンポーネント概要の表示 . . . . .	119
電力バジェット状態の表示 . . . . .	119
サーバー モデル名とサービス タグの表示 . . . . .	120
すべてのサーバーの正常性ステータスの表示 . . . . .	120
スロット名の編集 . . . . .	123
サーバーのホスト名をスロット名として使用 . . . . .	124
サーバーの第 1 起動デバイスの設定 . . . . .	124
個別のサーバーの正常性ステータスの表示 . . . . .	126
IOM の正常性ステータスの表示 . . . . .	131
ファンの正常性ステータスの表示 . . . . .	132
iKVM ステータスの表示 . . . . .	134
PSU の正常性ステータスの表示 . . . . .	135
温度センサのステータスの表示 . . . . .	137
LCD ステータスの表示 . . . . .	138
ワールドワイドネーム/メディアアクセスコントロール (WWN/MAC) ID の表示 . . . . .	138
ファブリック構成 . . . . .	138
WWN/MAC アドレス . . . . .	139
CMC ネットワークプロパティの設定 . . . . .	139
CMC への初期アクセスのセットアップ . . . . .	139
ネットワーク LAN の設定 . . . . .	140

<b>CMC ネットワークセキュリティの設定</b> . . . . .	146
<b>VLAN の設定</b> . . . . .	148
<b>CMC ユーザーの追加と設定</b> . . . . .	149
ユーザータイプ . . . . .	149
ユーザーの追加と管理 . . . . .	155
<b>Microsoft Active Directory 証明書の設定と管理</b> . . . . .	157
共通設定 . . . . .	158
標準スキーマ設定 . . . . .	160
拡張スキーマの設定 . . . . .	161
<b>Active Directory 証明書の管理</b> . . . . .	161
<b>Kerberos Keytab</b> . . . . .	162
<b>汎用 Lightweight Directory Access Protocol Services の設定と管理</b> 163	
<b>LDAP サーバーの選択</b> . . . . .	165
<b>LDAP グループ設定の管理</b> . . . . .	166
<b>LDAP セキュリティ証明書の管理</b> . . . . .	166
<b>SSL とデジタル証明書を使用した CMC 通信のセキュリティ確保</b> 167	
<b>SSL (セキュアソケットレイヤー)</b> . . . . .	167
<b>証明書署名要求 (CSR)</b> . . . . .	167
<b>SSL メインメニューへのアクセス</b> . . . . .	168
<b>新しい証明書署名要求の生成</b> . . . . .	168
<b>サーバー証明書のアップロード</b> . . . . .	171
<b>ウェブサーバーキーと証明書のアップロード</b> . . . . .	171
<b>サーバー証明書の表示</b> . . . . .	172
<b>セッションの管理</b> . . . . .	172
<b>サービスの設定</b> . . . . .	173
<b>電力バジェットの設定</b> . . . . .	180
<b>ファームウェアアップデートの管理</b> . . . . .	181
<b>現在のファームウェアバージョンの表示</b> . . . . .	182

ファームウェアのアップデート . . . . .	183
CMC での iDRAC ファームウェアのリカバリ . . . . .	188
Lifecycle Controller を使用したサーバーコンポーネントファームウェアのアップデート . . . . .	189
<b>iDRAC の管理 . . . . .</b>	<b>199</b>
iDRAC QuickDeploy . . . . .	199
iDRAC ネットワーク設定 . . . . .	202
CMC GUI からリモートコンソールを起動 . . . . .	205
シングルサインオンを使って iDRAC を起動する . . . . .	206
<b>サーバークローニング . . . . .</b>	<b>208</b>
プロファイルの取得 . . . . .	208
プロファイルの適用 . . . . .	208
サーバーの BIOS 設定の表示 . . . . .	209
保存プロファイルの管理 . . . . .	209
最近のプロファイルログ . . . . .	209
完了ステータスとトラブルシューティング . . . . .	209
<b>FlexAddress . . . . .</b>	<b>210</b>
FlexAddress ステータスの表示 . . . . .	210
FlexAddress の設定 . . . . .	214
ファブリックおよびスロットのシャーシレベルの FlexAddress 設定 . . . . .	215
スロットのサーバーレベルの FlexAddress 設定 . . . . .	216
リモートファイル共有 . . . . .	216
よくあるお問い合わせ (FAQ) . . . . .	219
CMC のトラブルシューティング . . . . .	221
<b>6 FlexAddress の使用 . . . . .</b>	<b>223</b>
FlexAddress の有効化 . . . . .	224
FlexAddress 有効化の検証 . . . . .	225
FlexAddress の無効化 . . . . .	227
FlexAddress の無効化 . . . . .	227
CLI を使用した FlexAddress の設定 . . . . .	228

	Linux 向け FlexAddress の追加設定 . . . . .	229
	CLI を使用した FlexAddress ステータスの表示 . . . . .	229
	GUI を使用した FlexAddress の設定 . . . . .	230
	FlexAddress を利用した Wake-On-LAN の使用 . . . . .	230
	FlexAddress のトラブルシューティング . . . . .	230
	コマンドメッセージ . . . . .	233
	FlexAddress DELL ソフトウェア製品ライセンス契約 . . . . .	235
	よくあるお問い合わせ (FAQ) . . . . .	239
<b>7</b>	<b>FlexAddress Plus の使用 . . . . .</b>	<b>241</b>
	FlexAddress Plus の有効化 . . . . .	241
	FlexAddress と FlexAddress Plus . . . . .	242
<b>8</b>	<b>CMC ディレクトリサービスの 使用 . . . . .</b>	<b>243</b>
	CMC と Microsoft Active Directory との併用 . . . . .	243
	Active Directory スキーマ拡張 . . . . .	243
	標準スキーマと拡張スキーマ . . . . .	243
	標準スキーマの Active Directory の概要 . . . . .	244
	CMC にアクセスするための標準スキーマ Active Directory の設 定 . . . . .	246
	標準スキーマ Active Directory と Web インタフェースを使用し た CMC の設定 . . . . .	246
	標準スキーマ Active Directory と RACADM を使用した CMC の設 定 . . . . .	248
	拡張スキーマの概要 . . . . .	249
	Active Directory スキーマ拡張 . . . . .	249
	RAC スキーマ拡張の概要 . . . . .	250
	Active Directory オブジェクトの概要 . . . . .	250

CMC にアクセスするための拡張スキーマ Active Directory の設定 . . . . .	254
Active Directory スキーマの拡張 . . . . .	254
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 . . . . .	260
Active Directory への CMC ユーザーと特権の追加 . . . . .	261
拡張スキーマ Active Directory と Web インタフェースを使用した CMC の設定 . . . . .	263
拡張スキーマ Active Directory と RACADM を使用した CMC の設定 . . . . .	266
よくあるお問い合わせ (FAQ) . . . . .	267
<b>シングルサインオンの設定 . . . . .</b>	<b>270</b>
システム要件 . . . . .	270
設定の実行 . . . . .	271
Active Directory の設定 . . . . .	271
CMC の設定 . . . . .	272
Kerberos Keytab ファイルのアップロード . . . . .	272
シングルサインオンの有効化 . . . . .	273
シングルサインオンのログインに使用するブラウザの設定 . . . . .	273
シングルサインオンを使用した CMC へのログイン . . . . .	274
<b>スマートカードによる二要素認証の設定 . . . . .</b>	<b>275</b>
システム要件 . . . . .	275
設定の実行 . . . . .	275
Active Directory の設定 . . . . .	275
CMC の設定 . . . . .	276
Kerberos Keytab ファイルのアップロード . . . . .	276
スマートカード認証の有効化 . . . . .	276
スマートカードのログインに使用するブラウザの設定 . . . . .	277
スマートカードを使用した CMC へのログイン . . . . .	277
スマートカードログイン時のトラブルシューティング . . . . .	278
<b>汎用 LDAP と CMC の併用 . . . . .</b>	<b>279</b>
汎用 LDAP ディレクトリを設定して CMC にアクセス . . . . .	279
CMC ウェブインタフェースを使用した汎用 LDAP ディレクトリサービスの設定 . . . . .	280
LDAP サーバーの選択 . . . . .	282
LDAP グループ設定の管理 . . . . .	282
LDAP セキュリティ証明書の管理 . . . . .	283

	<b>RACADM を使用した汎用 LDAP ディレクトリサービスの設定</b>	
	283	
	使用状況 . . . . .	284
	困ったときは . . . . .	284
<b>9</b>	<b>電力管理 . . . . .</b>	<b>285</b>
	AC 冗長性モード . . . . .	286
	電源装置冗長モード . . . . .	287
	冗長性なしモード . . . . .	288
	ハードウェアモジュールの電力バジェット . . . . .	289
	サーバースロットの電力優先度の設定 . . . . .	292
	電源装置の動的制御 . . . . .	293
	<b>冗長性ポリシー . . . . .</b>	<b>294</b>
	AC 冗長性 . . . . .	295
	電源装置冗長性 . . . . .	295
	冗長性なし . . . . .	295
	節電と電力バジェットの変更 . . . . .	295
	システム イベント ログの電源供給および冗長性ポリシーの変更	
	302	
	冗長性状態と全体的な電源状態 . . . . .	303
	<b>電源の設定と管理 . . . . .</b>	<b>303</b>
	PSU の正常性ステータスの表示 . . . . .	303
	消費電力ステータスの表示 . . . . .	306
	電力バジェット状態の表示 . . . . .	309
	電力バジェットと冗長性の設定 . . . . .	314
	サーバに優先度を割り当てる方法 . . . . .	318
	電力バジェットの設定 . . . . .	319
	電源バジェットを維持するためのサーバ電力の低減	320
	シャーシに対する電力制御操作の実行 . . . . .	320
	IOM 上で電源制御操作の実行 . . . . .	322
	サーバに対する電力制御操作の実行 . . . . .	323
	外部電力管理 . . . . .	325
	<b>RACADM の使用 . . . . .</b>	<b>326</b>
	トラブルシューティング . . . . .	326



<b>10 iKVM モジュールの使用</b> . . . . .	<b>327</b>
<b>概要</b> . . . . .	<b>327</b>
iKVM ユーザーインターフェース . . . . .	327
セキュリティ . . . . .	327
スキャン . . . . .	327
サーバーの識別 . . . . .	327
ビデオ . . . . .	328
プラグアンドプレイ . . . . .	328
FLASH アップグレード可能 . . . . .	328
<b>物理的な接続インターフェース</b> . . . . .	<b>328</b>
iKVM の 接続手順 . . . . .	328
ACI 接続の層 . . . . .	329
<b>OSCAR の使用</b> . . . . .	<b>329</b>
ナビゲーションの基本 . . . . .	329
OSCAR の設定 . . . . .	331
<b>iKVM によるサーバーの管理</b> . . . . .	<b>333</b>
周辺機器の互換性とサポート . . . . .	333
サーバーの表示と選択 . . . . .	334
コンソールのセキュリティの設定 . . . . .	337
システムのスキャン . . . . .	342
サーバーへのブロードキャスト . . . . .	343
<b>CMC からの iKVM の管理</b> . . . . .	<b>344</b>
フロントパネルの有効または無効 . . . . .	344
iKVM を介した Dell CMC コンソールの有効化 . . . . .	345
iKVM のステータスとプロパティの表示 . . . . .	345
iKVM ファームウェアのアップデート . . . . .	347
<b>トラブルシューティング</b> . . . . .	<b>349</b>
<b>11 I/O ファブリック管理</b> . . . . .	<b>353</b>
<b>ファブリック管理</b> . . . . .	<b>354</b>
<b>無効な構成</b> . . . . .	<b>355</b>
無効なメザニンカード (MC) 構成 . . . . .	355

無効な IOM- メザニカード (MC) 構成 . . . . .	356
無効な IOM-IOM 構成 . . . . .	356
初期電源投入シナリオ . . . . .	356
IOM 状態の監視 . . . . .	356
個別の IOM の状態ステータスの表示 . . . . .	359
個別 IOM のネットワーク設定 . . . . .	361
IOM ネットワーク設定のトラブルシューティング . . . . .	363
<b>12 トラブルシューティングとリカバリ . . . . .</b>	<b>365</b>
概要 . . . . .	365
シャーシ監視ツール . . . . .	366
設定情報、シャーシステータス、ログの収集 . . . . .	366
使用状況 . . . . .	366
対応インタフェース . . . . .	366
CLI RACDUMP . . . . .	367
リモート RACDUMP . . . . .	368
リモート RACDUMP の使用 . . . . .	368
Telnet RACDUMP . . . . .	369
シャーシ上のコンポーネントを識別するための LED の設定 . . . . .	369
SNMP アラートの設定 . . . . .	370
SNMP Management Information Base (MIB) ファイルのダウンロード . . . . .	375
E- メール警告の設定 . . . . .	375
リモートシステムのトラブルシューティングの最初のステップ . . . . .	378
シャーシ上の電源監視と電源制御コマンドの実行 . . . . .	379
電力バジェット状態の表示 . . . . .	379
電源制御操作の実行 . . . . .	379
電源のトラブルシューティング . . . . .	379
リモートシステムの Lifecycle Controller ジョブの管理 . . . . .	382
シャーシサマリの表示 . . . . .	383
シャーシとコンポーネントの正常性状態の表示 . . . . .	387

イベントログの表示 . . . . .	388
ハードウェアログの表示 . . . . .	388
CMC ログの表示 . . . . .	391
診断コンソールの使用 . . . . .	392
コンポーネントのリセット . . . . .	393
ネットワークタイムプロトコル (NTP) 問題のトラブルシューティング . . . . .	396
LED の色と点滅パターンの解釈 . . . . .	397
無応答 CMC のトラブルシューティング . . . . .	400
LED を観察して問題を特定する . . . . .	400
リカバリ情報は DB-9 シリアルポートから入手します。 . . . .	401
ファームウェアイメージのリカバリ . . . . .	402
ネットワーク問題のトラブルシューティング . . . . .	402
忘れたシステム管理者パスワードのリセット . . . . .	403
シャシ構成設定および資格情報の保存と復元 . . . . .	406
アラートのトラブルシューティング . . . . .	407
13 診断 . . . . .	409
LCD パネルインターフェースの使用 . . . . .	409
LCD のナビゲーション . . . . .	409
Main Menu (メインメニュー) . . . . .	410
LCD セットアップメニュー . . . . .	411
言語設定画面 . . . . .	411
デフォルト画面 . . . . .	411
グラフィカルサーバステータス画面 . . . . .	412
グラフィカルモジュールステータス画面 . . . . .	412
エンクロージャメニュー画面 . . . . .	413
モジュールステータス画面 . . . . .	413
エンクロージャステータス画面 . . . . .	413
IP サマリ画面 . . . . .	414

診断	414
LCD ハードウェアのトラブルシューティング	414
前面パネル LCD メッセージ	417
LCD エラーメッセージ	417
LCD モジュールとサーバーステータス情報	424

索引	429
----	-----

## 概要

Dell Chassis Management Controller (CMC) は、ホットプラグ対応のシステム管理ハードウェアとソフトウェアのソリューションで、Dell PowerEdge M1000e シャーシシステムに以下の機能を提供するように設計されています。

- リモート管理機能
- 電源制御
- 冷却コントロール

CMC は自身のマイクロプロセッサとメモリを持っており、差し込んだモジュールシャーシから電源が供給されます。CMC の利用を開始するには、29 ページの「CMC のインストールと設定」を参照してください。

CMC は、ブレードサーバーに複数のシステム管理機能を提供します。電源と温度の管理は、CMC の基本的な機能です。

- エンクロージャレベルのリアルタイム自動電力 / 温度管理。
  - CMC は、システム電源要件を監視し、オプションの電源装置の動的制御モードをサポートします。これにより、CMC は、電源の効率を改善するため、負荷と冗長性の要件に応じて電源装置を動的に有効にしたりスタンバイに設定したりすることができます。
  - CMC はリアルタイムの消費電力を報告します（タイムスタンプ付きの高低ポイントも記録されます）。
  - CMC は、オプションでエンクロージャの最大電力限度の設定をサポートしています。これを設定すると、設定された最大電力限度値以下に保つために、サーバーモジュールの調整や新しいブレードの電源オンの防止など、アラートが生成されたり処置が実行されたりします。
  - CMC は、実際の周囲温度と内部温度を測定して、ファンの冷却を監視し、自動制御します。
  - CMC は総合的なエンクロージャのインベントリを提供し、ステータス / エラーを報告します。
- CMC には、以下の設定を集中的に行うメカニズムが備わっています。
  - M1000e エンクロージャのネットワークおよびセキュリティの設定
  - 電源の冗長性とパワーシーリングの設定
  - I/O スイッチと iDRAC ネットワークの設定
  - サーバードライブ上の最初の起動デバイス

- I/O モジュールとブレードの間の I/O ファブリックの一貫性をチェックし、システムのハードウェアを保護するために、必要に応じてコンポーネントを無効にする
- ユーザーアクセスセキュリティ

温度、ハードウェアの誤った構成、電源障害、ファン速度に関する警告やエラーの E-メールアラートまたは SNMP トラップアラートを送信するように、CMC を設定できます。

1 つの CMC または冗長 CMC を持つ M1000e シャーシを設定できます。冗長 CMC 設定では、プライマリ CMC が M1000e シャーシまたは管理ネットワークとの通信から切断されると、スタンバイ CMC がシャーシ管理を引き継ぎます。

## このリリースの新機能

このリリースの CMC では、次の機能がサポートされています。

- シャーシ設定の保存と復元。
- 改善された SEL ログ。
- Broadcom 57810-k デュアルポート 10GB ブレードネットワークドーターカード。
- Broadcom 57810-k デュアルポート 10GB ブレードメザニンカード。
- Intel I350 Quad Port 1Gb ブレードメザニンカード。
- Intel x520-k デュアルポート 10Gb ブレードネットワークドーターカード。
- Intel x520-k デュアルポート 10Gb ブレードメザニンカード。
- Qlogic QMD8262-k デュアルポート 10Gb ブレードネットワークドーターカード。
- Mellanox M4001Q QDR/DDR InfiniBand スイッチ。
- Mellanox M4001F FDR InfiniBand スイッチ。
- Mellanox ConnectX-3 QDR/DDR InfiniBand ブレードメザニンカード。
- Mellanox ConnectX-3 FDR InfiniBand ブレードメザニンカード。
- シャーシの物理的な場所を示す OID を含むように拡張された CMC MIB。
- ブレードサーバーサービスタグとスロット名を示す OID を含むように拡張された CMC MIB。
- **Open Manage Power Connect (OMPC)** により、外部電源管理に対応。
- iDRAC6 サーバーと iDRAC7 サーバー（サーバークローニング）の 1 対多の BIOS サーバー設定の複製。
- 新しいメンバーのプロパティをリーダーのプロパティに同期するための機能をマルチシャーシ管理機能に追加。
- 初期 iDRAC7 PowerEdge M620 サーバーのサポート。
- **Lifecycle Controller (LC)** をサポートするサーバーについて、GUI から CPU とメモリの情報を入手可能。
- サーバーと IOM のインベントリのサポートと、MCM（マルチシャーシ管理）グループの世代報告。

## CMC 管理機能

CMC は次の管理機能を提供します。

- 冗長性を備えた CMC 環境。
- IPv4 および IPv6 のダイナミック DNS (DDNS) 登録。
- SNMP、Web インタフェース、iKVM、Telnet または SSH 接続を利用してリモートシステム管理と監視。
- 監視 — 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を提供。
- システムイベントログへのアクセス — ハードウェアログと CMC ログへのアクセスを提供。
- 各種シャーシコンポーネントのファームウェアアップデート — CMC、サーバー、iKVM、I/O モジュールインフラデバイスのファームウェアアップデートが可能。
- シャーシ内の複数サーバーで、BIOS、ネットワークコントローラ、ストレージコントローラなどのサーバーコンポーネントを、Lifecycle Controller を使用してファームウェアアップデート可能。
- Dell OpenManage ソフトウェア統合 — **Dell OpenManage Server Administrator** または **IT Assistant** から CMC ウェブインタフェースを起動。
- CMC アラート — E-メールメッセージまたは SNMP トラップを使って管理対象ノードに関する潜在的な問題を通知。
- リモート電源管理 — シャーシコンポーネント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を管理コンソールから提供。
- 電源使用率の報告。
- セキュアソケットレイヤー (SSL) 暗号化 — Web インタフェースからセキュアリモートシステム管理を提供。
- **Integrated Dell Remote Access Controller (iDRAC)** ウェブインタフェースの起動ポイント。
- WS-Management のサポート。
- FlexAddress 機能 — 特定のスロットに対して、工場で割り当てられたワールドワイドネーム / メディアアクセスコントロール (WWN/MAC) ID のシャーシに割り当てられた WWN/MAC ID への置き換え 詳細については、223 ページの「FlexAddress の使用」参照してください。
- シャーシのコンポーネントステータスおよび状態のグラフィック表示。
- 単一およびマルチスロットサーバーのサポート。
- LCD iDRAC 設定ウィザードによる iDRAC ネットワーク構成のサポート。
- iDRAC シングルサインオン。
- ネットワークタイムプロトコル (NTP) 対応。
- サーバーサマリ、電力レポート、電力制御ページの強化。
- 強制 CMC フェイルオーバー、サーバーの仮想 再装着。
- 最大 8 つまでのシャーシをリードシャーシから監視できるマルチシャーシ管理。

## セキュリティ 機能

CMC は次のセキュリティ機能を提供しています。

- パスワードレベルのセキュリティ管理 — リモートシステムへの無許可のアクセスを防止。
- **Active Directory** (オプション) またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証。
- 役割ベースの権限 — システム管理者が各ユーザーに特定の権限を設定可能。
- ウェブインタフェースを介してのユーザー ID とパスワードの設定。
- ウェブインタフェースは **128 ビット SSL 3.0 暗号化**と **40 ビット SSL 3.0 暗号化** (128 ビットが使用できない国向け) をサポート。



**メモ:** Telnet は SSL 暗号化をサポートしていません。

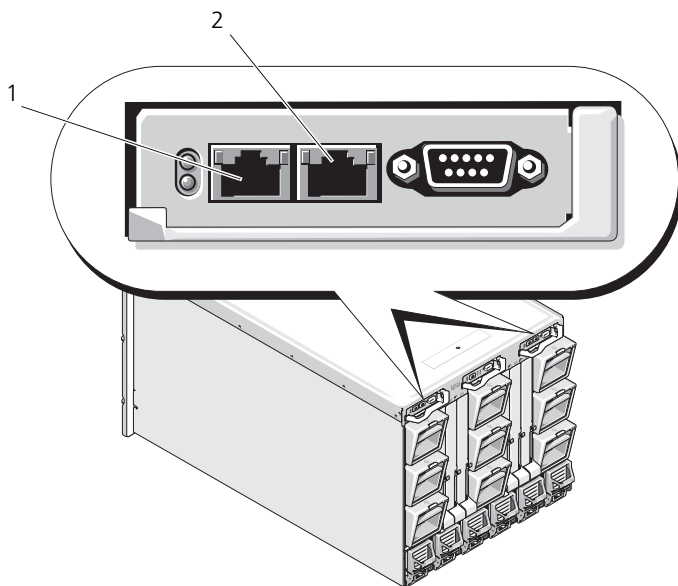
- 設定可能な IP ポート (該当する場合)。
- IP アドレスごとのログイン失敗数の制限による、制限を超えた IP アドレスのログインの阻止。
- 設定可能なセッション自動タイムアウトおよび複数の同時セッション数。
- CMC に接続するクライアントの IP アドレス範囲を限定。
- 暗号化層を使用してセキュリティを強化するセキュアシェル (SSH)。
- シングルサインオン、二要素認証、公開キー認証。



## シャーシの概要

図 1-1 は、CMC（差し込み）の前面図とシャーシ内の CMC スロット位置を表示しています。

図 1-1. Dell M1000e シャーシと CMC



1 GB ポート      2 STK ポート

# ハードウェア仕様

以下の項で、CMC のハードウェア仕様についての情報を示します。

## TCP/IP ポート

CMC のリモートアクセス用にファイアウォールを開くときにポート情報を提供する必要があります。

表 1-1. CMC 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
161	SNMP エージェント
443*	HTTPS

\* 設定可能なポート

表 1-2. CMC クライアントポート

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

\* 設定可能なポート

# 対応リモートアクセス接続

表 1-3 には、サポートされているリモートアクセスコントローラを示します。

表 1-3. 対応リモートアクセス接続

接続	機能
CMC ネットワークインタフェースサポート	<ul style="list-style-type: none"><li>• GB ポート：CMC ウェブインタフェース専用のネットワークインタフェース。2 つの 10/100/1000 Mbps ポート。一方は管理用、他方はシャーシ対シャーシのケーブル統合用</li><li>• STK: シャーシ対シャーシ管理ネットワークケーブル統合用のアップリンクポート</li><li>• CMC GbE ポート経由での 10Mbps/100Mbps/1Gbps Ethernet 接続</li><li>• DHCP のサポート</li><li>• SNMP トラップと E-メールによるイベント通知</li><li>• iDRAC と I/O モジュール (IOM) 用ネットワークインタフェース</li><li>• 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 Telnet/SSH コマンドコンソールおよび RACADM CLI コマンドに対応</li></ul>
シリアルポート	<ul style="list-style-type: none"><li>• システムブート、リセット、電源投入、およびシャットダウンコマンドなどのシリアルコンソールおよび racadm CLI コマンドに対応</li><li>• 特定タイプの IOM へのバイナリプロトコルによる通信を行うために特別に設計されたアプリケーション用バイナリ交換をサポート</li><li>• シリアルポートは、connect (または racadm connect) コマンドを使ってサーバーのシリアルコンソールまたは I/O モジュールに内部的に接続できます。</li></ul>
その他の接続	<ul style="list-style-type: none"><li>• Avocent 内蔵 KVM スイッチモジュール (iKVM) 経由での Dell CMC コンソールへのアクセス</li></ul>

# 対応プラットフォーム

CMC は、M1000e プラットフォーム用に設計されたモジュラシステムをサポートします。CMC との互換性の詳細については、ご利用デバイスのマニュアルを参照してください。

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

## 対応ウェブブラウザ

次のウェブブラウザが CMC 4.0 用にサポートされています。

- Microsoft Internet Explorer 8.0 for Windows 7、Windows Vista、Windows XP、および Windows Server 2003 シリーズ。
- Microsoft Internet Explorer 7.0 for Windows 7、Windows Vista、Windows XP、および Windows Server 2003 シリーズ。
- Mozilla Firefox 1.5 (32 ビット) – 機能制限。

CMC 4.0 向けの対応ウェブブラウザの最新情報については、デルのサポートサイト [support.dell.com/manuals](http://support.dell.com/manuals) の『Dell システムソフトウェアサポートマトリックス』を参照してください。

CMC 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：

- 1 Windows の **コントロールパネル** を開きます。
- 2 **地域のオプション** アイコンをダブルクリックします。
- 3 **ロケーション** ドロップダウン メニューで対象となる場所を選択します。

## 対応管理コンソールアプリケーション

CMC は、Dell OpenManage IT Assistant と統合できます。詳しくは、Dell サポートサイト [support.dell.com](http://support.dell.com) から入手可能な IT Assistant の説明書を参照してください。

## WS-Management のサポート

Web Services for Management (WS-MAN) は、システム管理に使用する SOAP (Simple Object Access Protocol、シンプルオブジェクトアクセスプロトコル) ベースのプロトコルです。WS-MAN は、ネットワーク上でデータを共有および管理するための相互運用可能なプロトコルです。CMC は、WS-MAN を使用して、分散型管理タスクフォース (DMTF) のコモンインフォメーションモデル (CIM) ベースの管理情報を伝達します。CIM 情報は、管理化システムにで使用できるセマンティックや情報の種類を定義します。Dell の組み込み型サーバープラットフォーム管理インタフェースは、複数のプロファイルに編成されます。各プロファイルは、特定の管理ドメインや機能領域のための固有のインタフェースを定義します。さらに、追加機能用のインタフェースを提供する多数のモデルやプロファイル拡張機能も定義されています。

WS-Management にアクセスするには、ポート 443 からセキュアソケットレイヤ (SSL) プロトコル経由で基本認証を使用して、ローカルユーザー権限でログインする必要があります。ユーザーアカウント設定の詳細については、『[RACADM Command Line Reference Guide for iDRAC6 and CMC](#)』のセッション管理データベースプロパティの項を参照してください。

WS-Management で使用できるデータは、次の DMTF プロファイルバージョン 1.0.0 にマップされている CMC 計装インタフェースによって提供されるデータのサブセットです。

- 割り当て機能プロファイル
- ベースメトリックプロファイル
- ベースサーバープロファイル
- コンピュータシステムプロファイル
- モジュラシステムプロファイル
- 物理アセットプロファイル
- Dell 電源割り当てプロファイル
- Dell 電源プロファイル
- Dell 電源トポジプロファイル
- 電源状況管理プロファイル
- プロファイル登録プロファイル
- レコードログプロファイル
- リソース割り当てプロファイル
- ロールベース認証プロファイル
- センサープロファイル
- サービスプロセスプロファイル
- 簡易 ID 管理プロファイル
- Dell Active Directory クライアントプロファイル
- 起動制御プロファイル
- Dell 簡易 NIC プロファイル

CMC WS-MAN の実装は、トランスポートセキュリティに対してポート 443 の SSL を使用し、基本認証をサポートしています。ユーザーアカウント設定の情報は、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（DRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の `cfgSessionManagement` データベースプロパティの項を参照してください。ウェブサービスインタフェースは、Windows WinRM や Powershell CLI、WSMANCLI などのオープンソースユーティリティ、Microsoft .NET などのアプリケーションプログラミング環境といったクライアントインフラストラクチャを活用することで、使用できます。

Microsoft WinRM を使用してクライアント接続を行うには、最低バージョン 2.0 が必要です。詳細については、Microsoft の記事 <http://support.microsoft.com/kb/968929> を参照してください。

このほか、デルテクニカルセンター [www.delltechcenter.com](http://www.delltechcenter.com) には、実装ガイド、ホワイトペーパー、プロファイル、コードサンプルに関する資料が揃っています。詳細については、次を参照してください。

- DMTF ウェブサイト：[www.dmtf.org/standards/profiles/](http://www.dmtf.org/standards/profiles/)
- WS-MAN リリースノートまたは Read Me ファイル。
- [www.wbemsolutions.com/ws\\_management.html](http://www.wbemsolutions.com/ws_management.html)

- DMTF WS-Management 仕様：  
[www.dmtf.org/standards/wbem/wsman](http://www.dmtf.org/standards/wbem/wsman)

## その他の必要マニュアル

このガイド以外にも、デルサポートサイト [support.dell.com/manuals](http://support.dell.com/manuals) から次のガイドを入手できます。マニュアル ページで、**ソフトウェア** → **Systems Managements** をクリックします。右側の適切な製品リンクをクリックして、ドキュメントにアクセスします。

- 『CMC オンラインヘルプ』では、ウェブインタフェースの使用方法について説明しています。
- 『Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification』（シャーシ管理コントローラ SD カード技術仕様）は、BIOS およびファームウェアの最小バージョン、インストール方法および使用方法についての情報を提供します。
- 『Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers ユーザーガイド』には、管理下システムでの iDRAC のインストール、設定、およびメンテナンスに関する情報が記載されています。
- 『Dell OpenManage IT Assistant ユーザーズ ガイド』は、IT Assistant についての情報を提供しています。
- サードパーティ製管理コンソールアプリケーションのマニュアル
- 『Dell OpenManage Server Administrator ユーザーズガイド』には、Server Administrator のインストールと使用方法について記載されています。
- 『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 の入手と使用方法について説明しています。

また、次のシステムマニュアルには、CMC のインストール先のシステムに関する詳細が含まれています。

- システムに同梱の「安全にお使いいただくために」には、安全および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、[www.dell.com/regulatory\\_compliance](http://www.dell.com/regulatory_compliance) にある法規制の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。
- 『ラック取り付けガイド』および『ラック取り付け手順』では、システムをラックに取り付ける方法を説明しています。
- 『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。
- 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。
- 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。
- IOM ネットワーク設定の詳細については、『**Dell PowerConnect M6220 Switch Important Information 文書**』および『**Dell PowerConnect 6220 Series Port Aggregator ホワイトペーパー**』を参照してください。

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。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。





# CMC のインストールと設定

本項では、CMC ハードウェアの取り付け、CMC へのアクセス確立、CMC を使うための管理環境の設定、および CMC の設定の各種方法について説明します。

- CMC への初期アクセスの設定。
- ネットワーク経由による CMC へのアクセス。
- CMC ユーザーの追加と設定。
- CMC ファームウェアのアップデート。

冗長 CMC 環境の取り付けと設定の詳細については、52 ページの「冗長 CMC 環境について」を参照してください。

## 作業を開始する前に

CMC 環境を設定する前に、デルサポートサイト [support.dell.com](https://support.dell.com) から CMC ファームウェアの最新バージョンをダウンロードしてください。

また、システム付属の『Dell Systems Management Tools and Documentation DVD』（Dell システム管理ツールおよびマニュアル DVD）があることを確認してください。

## CMC ハードウェアの取り付け

CMC はシャーシに事前に取り付けられているため、取り付けは必要ありません。2 台目の CMC を取り付け、アクティブ CMC のスタンバイとして使用できます。スタンバイ CMC の詳細については、52 ページの「冗長 CMC 環境について」を参照してください。

### シャーシの統合チェックリスト



次の手順を参照して、シャーシを正確に設定してください。

- 1 CMC とブラウザを使用する管理ステーションは同じネットワーク上にあることが必要です。このネットワークを管理ネットワークと呼びます。Ethernet ネットワークケーブルを、**GB** とラベル付けされた CMC ポートから管理ネットワークに接続します。



**メモ** : STK とラベル付けされた CMC Ethernet にはケーブルを接続しないでください。STK ポートのケーブル接続の詳細については、52 ページの「冗長 CMC 環境について」を参照してください。


- 2 シャーシに IO モジュールを取り付けてからケーブルで接続します。

- 3 シャーシにサーバーを挿入します。
- 4 シャーシを電源に接続します。
- 5 手順 7 を完了したら、シャーシの左下隅にある電源ボタンを押すか、CMC GUI からシャーシの電源を入れます。  
 **メモ:**サーバーの電源は入れないでください。
- 6 システムの全部にある LCD パネルを使用して、CMC に静的 IP アドレスを指定するか、DHCP の設定を行います。
- 7 デフォルトのユーザー名 (root) とパスワード (calvin) を使用して、ウェブブラウザから CMC IP アドレスに接続します。
- 8 CMC GUI で各 iDRAC に IP アドレスを指定し、LAN と IPMI インタフェースを有効にします。  
 **メモ:**デフォルトでは、一部のサーバーの iDRAC LAN インタフェースは無効になっています。
- 9 CMC GUI で各 IO モジュールに IP アドレスを指定します。
- 10 ウェブブラウザから各 iDRAC に接続し、iDRAC の最終設定を行います。デフォルトのユーザー名は root、パスワードは calvin です。
- 11 ウェブブラウザから各 IO モジュールに接続し、IO モジュールの最終設定を行います。
- 12 サーバーの電源を入れ、オペレーティングシステムをインストールします。

## CMC の基本的なネットワーク接続

最大限の冗長性を得るためには、使用可能な各 CMC を管理ネットワークに接続してください。

各 CMC には、**GB1** (アップリンクポート) および **STK** (スタッキングポートまたはケーブル統合ポート) の 2 つの RJ-45 Ethernet ポートがあります。基本的なケーブル接続では、GB1 ポートを管理ネットワークに接続し、STK ポートは使用しません。

 **注意:** STK ポートを管理ネットワークに接続すると、予期しない結果が発生する可能性があります。GB と STK を同一ネットワーク (ブロードキャストドメイン) にケーブル接続すると、ブロードキャストストームの原因となることがあります。

## デージーチェーン CMC ネットワーク接続

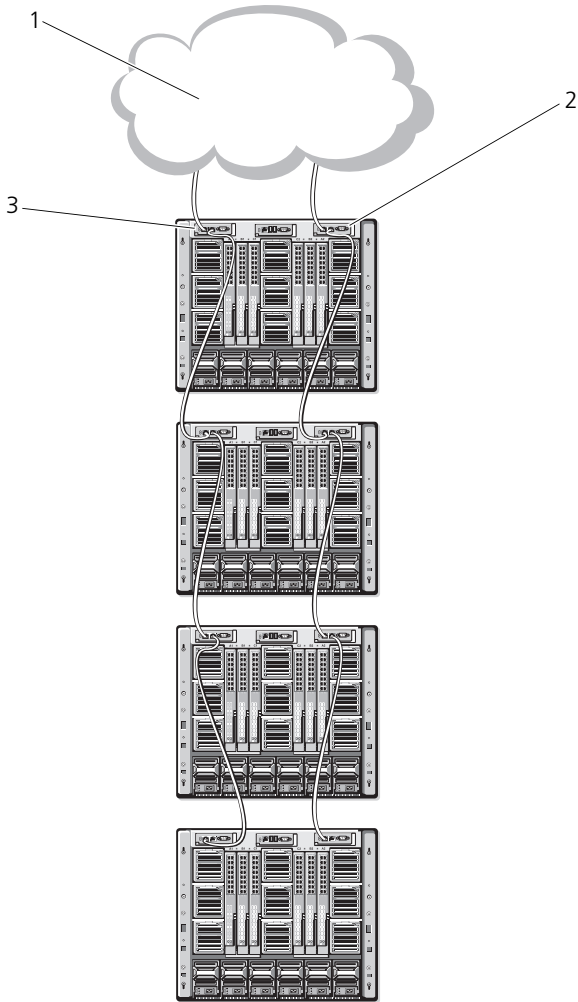
ラックに複数のシャーシがある場合は、4 つまでのシャーシをデージーチェーン接続することで管理ネットワークへの接続数を削減できます。4 つのシャーシのそれぞれが 1 つずつ冗長 CMC を持つ場合は、デージーチェーン接続によって管理ネットワークへの接続数を 8 つから 2 つに減らすことができます。各シャーシが 1 つずつしか CMC を持たない場合には、接続数は 4 つから 1 つに減らせます。

シャーシをデージーチェーン接続する場合、GB がアップリンクポート、STK がスタッキング（ケーブル統合）ポートとなります。ネットワークに近いシャーシにある CMC の GB ポートを管理ネットワークまたは STK ポートに接続します。STK ポートは、チェインまたはネットワークから遠い GB ポートのみ接続してください。

アクティブ CMC スロットにある CMC とセカンダリ CMC スロットにある CMC は、別々にデージーチェーン接続します。

図 2-1 では、デージーチェーン接続された 4 つのシャーシのケーブルの配線を示しています。それぞれシャーシに、アクティブとスタンバイ CMC があります。

図 2-1. デイジーチェーン CMC ネットワーク接続



- 1 管理ネットワーク
- 2 スタンバイ CMC
- 3 アクティブ CMC

図 2-2、図 2-3、および 図 2-4 では、CMC の正しくないケーブル接続の例を示します。

図 2-2. CMC ネットワーク接続の正しくないケーブル接続 – CMC が 2 つ

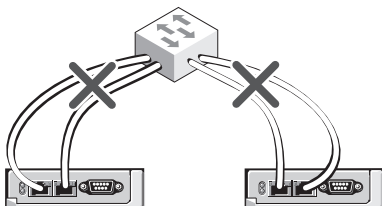


図 2-3. CMC ネットワーク接続の正しくないケーブル接続 – CMC が 1 つ

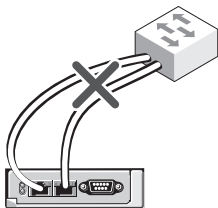
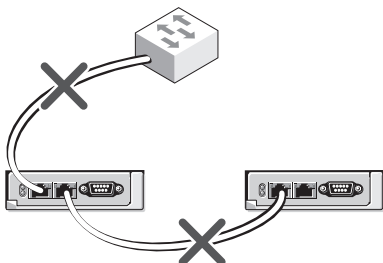


図 2-4. CMC ネットワーク接続の正しくないケーブル接続 – CMC が 2 つ



- 4 台までのシャーシをダイジーチェーンで接続するには、次の手順を実行します。
- 1 最初のシャーシのアクティブ CMC の GB ポートを管理ネットワークに接続します。
  - 2 2 つ目のシャーシのアクティブ CMC の GB ポートを最初のシャーシのアクティブ CMC の STK ポートに接続します。
  - 3 3 つ目のシャーシがある場合は、そのシャーシのアクティブ CMC の GB ポートを 2 つ目のシャーシのアクティブ CMC の STK ポートに接続します。
  - 4 4 つ目のシャーシがある場合は、そのシャーシのアクティブ CMC の GB ポートを 3 つ目のシャーシの STK ポートに接続します。
  - 5 シャーシ内に冗長 CMC がある場合は、上記と同じように、それぞれ相互に接続します。

**注意**：CMC 上の STK ポートは管理ネットワークに接続してはいけません。STK ポートは、別のシャーシ上の GB ポートにしか接続できません。STK ポートを管理ネットワークに接続すると、ネットワークに支障をきたし、データの損失を招く恐れがあります。GB と STK を同一ネットワーク（ブロードキャストドメイン）にケーブル接続すると、ブロードキャストストームの原因となることがあります。



**メモ**：アクティブ CMC をスタンバイ CMC に接続しないでください。



**メモ**：STK ポートが別の CMC にチェーン接続されている CMC をリセットすると、チェーン後方の CMC のネットワークに支障をきたす可能性があります。チェーン後方の CMC は、ネットワーク接続が失われたことをログ記録し、冗長 CMC にフェールオーバーする場合があります。

CMC の利用を開始するには、35 ページの「管理ステーションへのリモートアクセスソフトウェアのインストール」を参照してください。

# 管理ステーションへのリモートアクセスソフトウェアのインストール

Telnet、セキュアシェル (SSH)、またはオペレーティングシステム付属のシリアルコンソールユーティリティなどのリモートアクセスソフトウェア、またはウェブインタフェースを使用して、管理ステーションから CMC にアクセスできます。

管理ステーションからリモート RACADM を使用するには、システムに付随する『Dell Systems Management Tools and Documentation DVD』（Dell システム管理ツールおよびマニュアル DVD）を使用してリモート RACADM をインストールします。この DVD には、次の Dell OpenManage コンポーネントが含まれます。

- DVD ルート - Dell システムビルドおよびアップデートユーティリティが含まれます。
- SYSMGMT - Dell OpenManage Server Administrator を含むシステム管理ソフトウェアの製品が含まれます。
- Docs: このディレクトリには、システム、システム管理ソフトウェア製品、周辺機器および RAID コントローラのマニュアルが入っています。
- SERVICE - システムを設定するために必要なツールやシステムの最新の診断および Dell 最適化ドライバが含まれます。

Dell OpenManage ソフトウェアコンポーネントのインストールの詳細については、DVD または [support.dell.com](http://support.dell.com) にある『Dell OpenManage のインストールとセキュリティユーザーガイド』を参照してください。Dell DRAC Tools の最新バージョンは、デルのサポートサイト [support.dell.com](http://support.dell.com) からダウンロードできます。

## RACADM の Linux 管理ステーションへのインストール

- 1 管理下システムコンポーネントを取り付けようとしている、サポートされた Red Hat Enterprise Linux または SUSE Linux Enterprise Server オペレーティングシステムを実行するシステムに、root 権限でログインします。
- 2 DVD ドライブに『Dell Systems Management Tools and Documentation DVD』（Dell システム管理ツールおよびマニュアル DVD）を挿入します。
- 3 DVD を必要なロケーションにマウントするには、mount コマンドまたは類似のコマンドを使用します。



**メモ:** Red Hat Enterprise Linux 5 オペレーティングシステムでは、DVD は `-noexec mount` オプションで自動マウントされています。このオプションでは、DVD から実行可能ファイルを実行することはできません。手動で DVD-ROM をマウントしてから実行ファイルを実行する必要があります。

- 4 **SYSMGMT/ManagementStation/linux/rac** ディレクトリに移動します。RAC ソフトウェアをインストールするには、次のコマンドを入力します。

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

- 5 RACADM コマンドのヘルプを表示するには、前のコマンドを入力した後「racadm help」と入力します。RACADM の詳細については、69 ページの「RACADM コマンドラインインタフェースの使用」を参照してください。



**メモ:** RACADM リモート機能を使うとき、ファイル操作を含む RACADM サブコマンドを使用する対象となるフォルダへの書き込み権限が必要です。

例:

```
racadm getconfig -f <file name>
```

リモート racadm の詳細については、74 ページの「RACADM へのリモートアクセス」およびそれに続く項を参照してください。

## Linux 管理ステーションから RACADM のアンインストール

- 1 管理ステーション機能をアンインストールするシステムに、root でログインします。
- 2 次の rpm クエリコマンドを使用して、インストールされている DRAC ツールのバージョンを確認します。

```
rpm -qa | grep mgmtst-racadm
```

- 3 アンインストールするパッケージバージョンを確認してから、rpm -e `rpm -qa | grep mgmtst-racadm` コマンドを使って機能をアンインストールします。

## ウェブブラウザの設定

シャーシに取り付けられている CMC、サーバー、モジュールはウェブブラウザを使って設定、管理することができます。デルサポートサイト

[support.dell.com/manuals](http://support.dell.com/manuals) の『Dell Dell Systems Software Support Matrix』（システムソフトウェアサポートマトリックス）の対応ブラウザの項を参照してください。

CMC とブラウザを使用する管理ステーションは同じネットワーク上にあることが必要です。このネットワークを管理ネットワークと呼びます。セキュリティ要件によっては、管理ネットワークをセキュリティ上、安全な分離されたネットワークにすることができます。



**メモ:** ファイアウォールやプロキシサーバーなどの管理ネットワークのセキュリティ対策によって、ウェブブラウザから CMC へのアクセスが妨げられることがないことを確認してください。



また、ブラウザの一部の機能が接続性や性能に支障をきたすことがあります。特に管理ネットワークがインターネットへの経路を持たない場合はご注意ください。管理ステーションで Windows オペレーティングシステムが稼動している場合は、コマンドラインインターフェースを使って管理ネットワークにアクセスする場合でも Internet Explorer の設定により接続が妨げられることがあります。

## プロキシサーバー

管理ネットワークにアクセスしていないプロキシサーバーからブラウズするには、管理ネットワークアドレスをブラウザの例外リストに追加します。これにより、管理ネットワークにアクセスする際、ブラウザはプロキシサーバーを迂回することができます。

### Internet Explorer

Internet Explorer の例外リストを編集するには、次の手順を実行します。

- 1 Internet Explorer を起動します。
- 2 ツール → インターネットオプション → 接続 をクリックします。
- 3 ローカル エリア ネットワーク (LAN) 設定 セクションで、LAN の設定 をクリックします。
- 4 プロキシ サーバー セクションで 詳細設定 をクリックします。
- 5 例外 セクションのリストに管理ネットワーク上の CMC と iDRAC のアドレスをセミコロンで区切って追加します。エントリに DNS 名やワイルドカードを使用できます。

### Mozilla FireFox

Mozilla Firefox バージョン 3.0 で例外リストを編集するには：

- 1 Mozilla Firefox を起動します。
- 2 Windows の場合は ツール → オプション、Linux の場合は 編集 → プレファレンス をクリックします。
- 3 詳細、ネットワーク タブの順にクリックします。
- 4 設定 をクリックします。
- 5 手動プロキシ設定を 選択します。
- 6 プロキシなしの接続 フィールドに、管理ネットワーク上の CMC と iDRAC のアドレスをカンマで区切って追加します。エントリに DNS 名やワイルドカードを使用できます。

## フィッシングフィルタ

Microsoft フィッシング詐欺検出機能が管理システムの Internet Explorer で有効になっており、また CMC がインターネットにアクセスできない場合、CMC は数秒遅れる可能性があります。この遅延は、ブラウザやリモート RACADM などの他のインタフェースを使用中に生じる可能性があります。次の手順に従って、フィッシング詐欺検出機能を無効にしてください。

- 1 Internet Explorer を起動します。
- 2 ツール → **フィッシング詐欺検出機能** をクリックしてから、**フィッシング詐欺検出機能の設定** をクリックします。
- 3 **フィッシング詐欺検出機能を無効にする** チェックボックスを選択し、**OK** をクリックします。

## 証明書失効リスト (CRL) のフェッチ

CMC がインターネットへのルートを持たない場合は、Internet Explorer の証明書失効リスト (CRL) のフェッチ機能を無効にしてください。この機能では、CMC ウェブサーバーなどのサーバーが、インターネットから取得する無効な証明書リストにある証明書を使用するかどうかをテストします。インターネットにアクセスできない場合、ブラウザまたはリモート RACADM などのコマンドラインインタフェースを使って CMC にアクセスするときにこの機能は数秒の遅延を引き起こす可能性があります。

CRL フェッチングを無効にするには：

- 1 Internet Explorer を起動します。
- 2 ツール → **インターネットオプション** をクリックしてから、**詳細設定** をクリックします。
- 3 セキュリティセクションにスクロールして、**発行元証明書の取り消しを確認する** のチェックをはずし、**OK** をクリックします。

## Internet Explorer で CMC からファイルのダウンロード

Internet Explorer を使って CMC からファイルをダウンロードするとき、**暗号化されたページをディスクに保存しない** オプションが有効になっていないと問題が発生する場合があります。

**暗号化されたページをディスクに保存しない** オプションを有効にするには：

- 1 Internet Explorer を起動します。
- 2 ツール → **インターネットオプション** をクリックしてから、**接続** をクリックします。
- 3 セキュリティセクションにスクロールして、**暗号化されたページをディスクに保存しない** を選択します。

## Internet Explorer でアニメーションの再生


ウェブインタフェースとの間でファイルが送受信される際、ファイル転送アイコンが回転して転送が行われていることを示します。Internet Explorer では、このためにはブラウザがアニメーションを再生するように設定されていることが必要です（デフォルト設定）。

アニメーションを再生するように Internet Explorer を設定するには：

- 1 Internet Explorer を起動します。
- 2 ツール → **インターネット オプション** をクリックしてから、**接続** をクリックします。
- 3 マルチメディア セクションにスクロールして、**Web ページのアニメーションを再生する** を選択します。

## CMC への初期アクセスの設定


CMC をリモートで管理するには、CMC を管理ネットワークに接続してから CMC ネットワーク設定を行います。

 **メモ** : M1000e ソリューションを管理するには、管理ネットワークに接続している必要があります。

CMC のネットワーク設定の詳細については、41 ページの「CMC ネットワークの設定」を参照してください。この初期設定によって、CMC へのアクセスを可能にするための TCP/IP ネットワークパラメータが割り当てられます。

各サーバーとすべてのスイッチ I/O モジュールのネットワーク管理ポートにある CMC と iDRAC は、M1000e シャーシ内の共通の内部ネットワークに接続されます。これにより、管理ネットワークは、サーバーデータネットワークから分離できます。シャーシ管理に中断せずにアクセスするには、このトラフィックを分離することが重要です。

CMC は管理ネットワークに接続されます。CMC と iDRAC への外部アクセスはすべて CMC 介して達成できます。一方、管理サーバーへのアクセスは I/O モジュール (IOM) へのネットワーク接続を介して行われます。これによって、アプリケーションネットワークを管理ネットワークから分離できます。

 **メモ** : シャーシ管理とデータネットワークを分離することを推奨します。Dell は、ユーザー環境に不適切に統合されたシャーシのアップタイムのサポートまたは保証はできません。データネットワーク上の潜在的なトラフィックのため、内部管理ネットワーク上の管理インタフェースはサーバー向けのトラフィックにより飽和状態になる可能性があります。このため、CMC と iDRAC 間の通信に遅延が発生します。遅延が起これると、iDRAC が稼動中であっても CMC が iDRAC をオフライン状態と見なしたりするなどの予期しないシャーシ動作が発生し、他の不要な動作が発生する原因になります。管理ネットワークを物理的に分離することができない場合は、CMC および iDRAC トラフィックをそれぞれ異なる VLAN に分離するというオプションもあります。CMC と個々の iDRAC ネットワークインタフェースは、`racadm setniccfg` コマンドを用いて VLAN を使用するよう設定することもできます。詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』(iDRAC6 および CMC 用 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。

シャーシが 1 つの場合は、CMC およびスタンバイ CMC を管理ネットワークに接続します。冗長 CMC の場合は、別のネットワークケーブルを使用して **GB CMC** ポートを管理ネットワークの 2 番目のポートに接続します。

シャーシが複数存在する場合は、各 CMC を管理ネットワークに接続する基本接続か、シャーシを直列的に接続し、1 つの CMC のみを管理ネットワークに接続するデジチェーン接続のいずれかを選択できます。基本接続タイプは管理ネットワーク上のポートの使用数が多く、冗長性が高いという特徴を持ちます。デジチェーン接続タイプでは管理ネットワーク上のポート数は少なくなりませんが、CMC 間の依存性が生じるため、システムの冗長性が低くなります。

デジチェーン接続の詳細については、31 ページの「デジチェーン CMC ネットワーク接続」を参照してください。



**メモ:** CMC の冗長構成において、適切にケーブル接続しないと、管理ができなくなり、ブロードキャストストームが発生する場合があります。

## CMC ネットワークの設定



**メモ:** CMC 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。

CMC の初期ネットワーク設定は、CMC に IP アドレスが与えられる前でも後でも行うことができます。IP アドレスが与えられる前に CMC の初期ネットワーク設定を行う場合は、次のいずれかのインターフェースを使用できます。

- シャーシの前面にある LCD パネル
- Dell CMC シリアルコンソール

IP アドレスが与えられた後に CMC の初期ネットワーク設定を行う場合は、次のいずれかのインターフェースを使用できます。

- シリアルコンソール、Telnet、SSH などのコマンドラインインターフェース (CLI)、または iKVM 経由の Dell CMC コンソール
- リモート RACADM
- CMC ウェブインターフェース

## LCD 設定ウィザードを使用したネットワーク設定

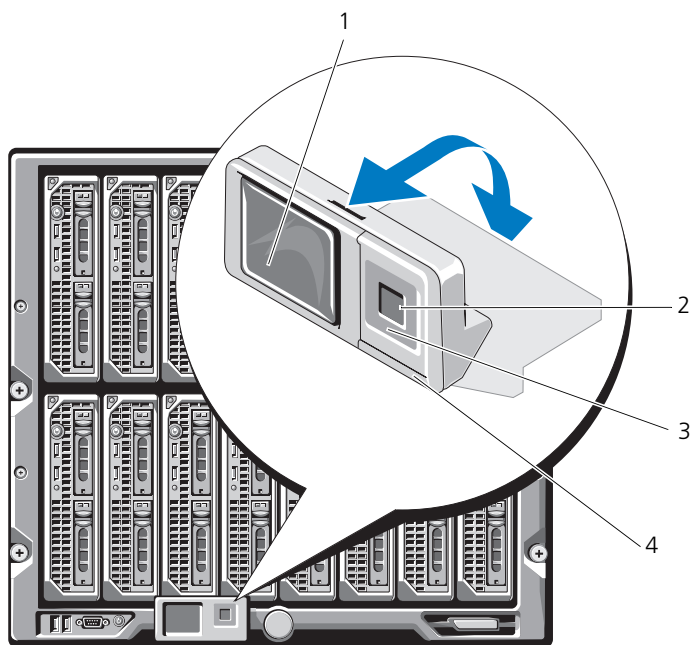


**メモ:** LCD 設定ウィザードを使用してサーバーを設定するオプションは、CMC が導入されるか、またはデフォルトパスワードが変更されるまでに限って利用できません。パスワードが変更されない場合、LCD を引き続き利用して CMC を再設定できるため、セキュリティのリスクが発生します。

LCD はシャーシ前面の左下の角にあります。

図 2-5 は、LCD パネルの図解です。

図 2-5. LCD ディスプレイ



- |   |             |   |                 |
|---|-------------|---|-----------------|
| 1 | LCD 画面      | 2 | 選択（「チェック」）ボタン   |
| 3 | スクロールボタン（4） | 4 | ステータスインジケータ LED |

LCD 画面にはメニュー、アイコン、画像およびメッセージが表示されます。  
LCD パネル上のステータスインジケータ LED は、シャーシとそのコンポーネントの正常性を示します。

- 青色の点灯は、正常であることを示します。
- 橙色の点滅は、少なくとも 1 つのコンポーネントに障害があることを示します。
- 青色の点滅は、シャーシグループ内でシャーシを特定するための ID 信号です。

## LCD 画面上での移動方法

LCD パネルの右側には 5 つのボタン、4 つの矢印ボタン（上下左右）、中央のボタンがあります。

- 別の画面へ移動するには、右（次へ）と左（前の）矢印ボタンを使用します。設定ウィザードの使用中はいつでも前の画面に戻ることができます。
- 画面上のオプション間を移動するには、上下の矢印ボタンを使用します。
- 画面上の項目を選択して保存し、次の画面へ移動するには、中央のボタンを使用します。

LCD パネルの使用法の詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の LCD パネルの項を参照してください。

## LCD 設定ウィザードの使用

LCD 設定ウィザードを使用してネットワークをセットアップするには、次の手順を実行します。

- 1 シャーシの電源ボタンをオンにします。

電源が投入される間、LCD 画面に一連の初期化画面が表示されます。使用準備が整ったら、**言語の設定** 画面が表示されます。


- 2 方向ボタンを使って言語を選択し、中央のボタンを押して **承認する / はい** を選択してから、中央のボタンを再度押します。
- 3 **エンクロージャ** 画面が開き、「**エンクロージャを設定しますか?**」という質問が表示されます。
  - a 中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。手順 4 を参照してください。
  - b **エンクロージャの設定** メニューを終了するには、いいえのアイコンを選択し、中央のボタンを押します。手順 9 を参照してください。
- 4 中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。
- 5 下矢印ボタンを使って、ネットワーク速度（10Mbps、100Mbps、自動（1Gbps））を選択します。




**メモ:** ネットワークのスループットを効果的にするには、ネットワーク速度の設定をネットワーク設定に合わせる必要があります。ネットワーク速度をネットワーク設定の速度より下げると、帯域幅の消費が増えてネットワーク通信が遅くなります。**使用しているネットワークがネットワーク速度を超える速度をサポートしているかどうかを判断し、それに従って設定してください。** ネットワーク設定がこれらの値のどれにも一致しない場合は、オートネゴシエーション（**自動** オプション）を使用するか、ネットワーク装置のメーカーに問い合わせてください。

中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。

- 6 使用しているネットワーク環境に適した二重モード（半二重または全二重）を選択します。

 **メモ**：オートネゴシエーションがオンかまたは 1000MB（1Gbps）が選択されている場合には、ネットワーク速度と二重モードの設定はできません。

 **メモ**：オートネゴシエーションを 1 台のデバイスでオンにし、別の 1 台でオフにすると、オートネゴシエーションはもう一つのデバイスのネットワーク速度を判別できますが、二重モードを判別できません。この場合、二重モードはオートネゴシエーション中にデフォルトで半二重の設定になります。このような二重モードの不一致は、ネットワーク接続が減速する原因となります。

中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。

- 7 CMC に使用するインターネットプロトコル（IPv4、IPv6、または両方）を選択します。

中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。

- 8 CMC の NIC IP アドレスを取得するモードを選択します。

#### 動的ホスト構成 プロトコル (DHCP)

CMC は IP 設定（IP アドレス、マスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。CMC には、ネットワーク上で割り振られた固有の IP アドレスが割り当てられます。DHCP オプションを選択した場合は、中央のボタンを押します。**iDRAC を設定しますか？** の画面が表示されます。手順 10 に進みます。

#### 静的

続く画面に、IP アドレス、ゲートウェイ、サブネットマスクを手動で入力します。

**静的** オプションを選択した場合は、中央のボタンを押して次の **CMC ネットワーク設定** 画面へ進みます。

- 左右の矢印キーを使って位置を移動し、上下の矢印キーを使って各位置の数値を選択することで、**静的 IP アドレス** を設定します。**静的 IP アドレス** の設定を終えたら、中央のボタンを押して先に進みます。
- サブネットマスクを設定してから中央のボタンを押します。
- サブネットマスクを設定してから中央のボタンを押します。**ネットワークの概要** 画面が表示されます。  
**ネットワークの概要** 画面には、入力した **静的 IP アドレス**、**サブネットマスク**、**ゲートウェイ** の設定が表示されます。設定が正確であることを確認してください。設定を修正するには、左矢印キーで移動し、中央のボタンを押して、対象の設定画面に戻ります。修正を終えたら、中央のボタンを押します。
- 入力した設定が正しいことを確認してから、中央のボタンを押します。**DNS を登録しますか？** の画面が表示されます。





**メモ**：CMC IP 構成に DHCP（動的ホスト設定プロトコル）モードを選択すると、デフォルトで DNS 登録も有効になります。

- 9 前の手順で **DHCP** を選択した場合は、手順 **10** に進みます。

DNS サーバーの IP アドレスを登録するには、中央のボタンを押して先に進みます。DNS がない場合は、右矢印キーを押します。

**DNS を登録しますか？** の画面が表示されたら、手順 **10** に進みます。

左右の矢印キーを使って位置を移動し、上下の矢印キーを使って各位置の数値を選択することで、**静的 IP アドレス** を設定します。静的 IP アドレスの設定を終えたら、中央のボタンを押して先に進みます。

- 10 iDRAC を設定するかどうかを指定します。

- **いいえ**：手順 **13** に進みます。
- **はい**：中央のボタンを押して先に進みます。

また、CMC GUI から iDRAC を設定できます。

- 11 サーバーに使用するインターネットプロトコル（IPv4、IPv6、または両方）を選択します。

#### 動的ホスト構成プロトコル (DHCP)

iDRAC は IP 設定（IP アドレス、マスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。iDRAC には、ネットワーク上で割り振られた固有の IP アドレスが割り当てられます。中央のボタンを押してください。

#### 静的

続く画面に、IP アドレス、ゲートウェイ、サブネットマスクを手動で入力します。

**固定** オプションを選択した場合は、中央のボタンを押して次の **iDRAC ネットワーク設定** 画面へ進みます。

- a 左右の矢印キーを使って位置を移動し、上下の矢印キーを使って各位置の数値を選択することで、**静的 IP アドレス** を設定します。このアドレスは、最初のスロットに装着された iDRAC の静的 IP アドレスです。後続の iDRAC の固定 IP アドレスは、この IP アドレスを増分したスロット番号として算出されます。**静的 IP アドレス** の設定を終えたら、中央のボタンを押して先に進みます。
  - b サブネットマスクを設定してから中央のボタンを押します。
  - c サブネットマスクを設定してから中央のボタンを押します。
- a IPMI LAN チャンネルの **有効** または **無効** を選択します。中央のボタンを押して処理を続けます。
- b **iDRAC 構成** 画面で、インストールされているサーバーにすべての iDRAC ネットワーク設定を適用するには、**承諾する / はい** アイコンをハイライト表示して、中央のボタンを押します。インストールされてい

るサーバーに iDRAC ネットワーク設定を適用するには、**いいえ** アイコンを反転表示させてから、センター ボタンを押して手順 c を続けます。

- c 次の **iDRAC 構成** 画面で、新しくインストールされたサーバーにすべての iDRAC ネットワーク設定を適用するには、**承認する / はい** アイコンをハイライト表示してから、中央のボタンを押します。新しいサーバーがシャーシに挿入されると、以前に設定したネットワーク設定 / ポリシーを使ってサーバーを自動展開するかどうかを尋ねるメッセージが、LCD に表示されます。新しくインストールされたサーバーに iDRAC ネットワーク設定を適用しない場合は、**いいえ** アイコンをハイライト表示してから中央のボタンを押します。新しいサーバーがシャーシに挿入されても、iDRAC ネットワーク設定は構成されません。
- 12 エンクロージャ** 画面で、すべてのエンクロージャ設定を適用するには、**承認する / はい** アイコンをハイライト表示させてから中央のボタンを押します。エンクロージャの設定を適用するには、**いいえ** アイコンをハイライト表示させてから中央のボタンを押します。
- 13 IP の概要** 画面では、設定した IP アドレスが正しいことを確認します。設定を修正するには、左矢印キーで移動し、中央のボタンを押して、対象の設定画面に戻ります。修正を終えたら、中央のボタンを押します。必要に応じて、右矢印キーで移動し、中央のボタンを押して、**IP の概要** 画面に戻ります。入力した設定がすべて正しいことを確認したら、中央のボタンを押します。設定ウィザードが閉じて、**メインメニュー** 画面に戻ります。



**メモ** : **はい / 承認する** を選択している場合は、**待機** 画面が表示されてから、**IP の概要** 画面が表示されます。

CMC と iDRAC は、ネットワークでも利用できるようになりました。ウェブインタフェース、シリアルコンソール、Telnet、SSH などの CLI を使用して、割り当てられた IP アドレスの CMC にアクセスできます。



**メモ** : LCD 設定ウィザードを使ってネットワークの設定を終えた後は、ウィザードが使用できなくなります。

# ネットワーク経路による CMC へのアクセス

CMC ネットワーク設定を終えた後、さまざまなインターフェースを使って CMC にリモートアクセスできます。表 2-1 に、リモートで CMC にアクセスするために使用できるインターフェースを示します。



 **メモ** : Telnet は他のインターフェースほどセキュアではないため、デフォルトでは無効です。Telnet は、ウェブ、ssh またはリモート RACADM を使用して有効にします。

表 2-1. CMC 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ーフェースを使って CMC 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 CMC のファームウェアに組み込まれ、管理ステーションで対応ウェブブラウザから NIC インタフェースを介してアクセスします。 対応するウェブブラウザのリストは、デルサポートサイト <a href="http://support.dell.com/manuals">support.dell.com/manuals</a> にある『Dell システムソフトウェアサポートマトリックス』で対応ブラウザの項を参照してください。
リモート RACADM コマンドラインインタフェース	管理ステーションからコマンドラインインタフェース (CLI) を使って CMC にリモートアクセスできます。リモート RACADM は、CMC の IP アドレスと共に <b>racadam -r</b> オプションを使用して、CMC 上でコマンドを実行します。 リモート <b>racadm</b> の詳細については、74 ページの「RACADM へのリモートアクセス」およびそれに続く項を参照してください。
Telnet	ネットワーク経路でコマンドラインによる CMC へのアクセスを提供します。RACADM コマンドライン インタフェースとサーバーまたは IO? モジュールのシリアル コンソールの接続に使われる <b>connect</b> コマンドは、CMC コマンド ラインから実行できます。 <b>メモ</b> : Telnet は、すべてのデータ (パスワードも含めて) を平文で送信するため、セキュアではないプロトコルです。機密情報を送信する場合は、SSH インタフェースを使用してください。
SSH	高度なセキュリティを実現するために暗号化されたトランスポート層を使用して、Telnet コンソールと同じ機能を提供します。

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

CMC と iDRAC ウェブインタフェースは、対応ウェブブラウザを使って CMC ネットワークインターフェースを介してアクセスでき、Dell Server Administrator または Dell OpenManage IT Assistant を使って起動できます。

対応するウェブブラウザのリストは、デルサポートサイト

**support.dell.com/manuals** にある『Dell システムソフトウェアサポートマトリックス』で対応ブラウザの項を参照してください。対応ウェブブラウザを使用して CMC にアクセスする方法については、99 ページの「CMC 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。

Dell Server Administrator を使って CMC インタフェースにアクセスするには、管理ステーションで 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、『Dell Server Administrator ユーザーズガイド』を参照してください。

Telnet または SSH を使って CMC コマンドラインにアクセスする方法については、55 ページの「CMC にコマンドラインコンソールの使用を設定する方法」を参照してください。

RACADM の使い方の詳細については、69 ページの「RACADM コマンドラインインタフェースの使用」を参照してください。

**connect** または **racadm connect** コマンドを使ってサーバーおよび IO モジュールに接続する詳細については、61 ページの「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。

## CMC ファームウェアのインストールまたはアップデート

次の項では、CMC ファームウェアのインストールおよびアップデートの方法について説明します。

### CMC ファームウェアのダウンロード


ファームウェアのアップデートを開始する前に、デルサポートサイト **support.dell.com** から最新のファームウェアバージョンをダウンロードし、ローカルシステムに保存します。


CMC 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 CMC ファームウェアコードとデータ
- ウェブインタフェース、JPEG、および他のユーザーインタフェースデータファイル
- デフォルト設定ファイル



**メモ:** CMC ファームウェアのアップデート中、シャーシ内の冷却ファンの一部または全部が全速回転します。

 **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 CMC 設定を保持します。アップデート処理中に、CMC 構成設定を工場出荷時のデフォルト設定にリセットするオプションがあります。

 **メモ:** シャーシに冗長 CMC がある場合、両方とも同じファームウェアバージョンにアップデートすることが重要です。ファームウェアのバージョンが異なる場合、フェイルオーバーが起きた際、不測の結果が生じます。

**RACADM getsysinfo** コマンド (『iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド』の **getsysinfo** コマンドの項を参照) または **シャーシサマリ** ページ (182 ページの「現在のファームウェアバージョンの表示」を参照) を使って、シャーシに取り付けられている CMC のファームウェアの現在のバージョンを表示します。

スタンバイ CMC がある場合は、1 つの操作で両方の CMC を同時にアップデートすることをお勧めします。スタンバイ CMC をアップデートし終わったら、CMC の役割を交代させて新しくアップデートした CMC をアクティブにし、古いバージョンのファームウェアの CMC がスタンバイになるようにします。(役割の交代についてのヘルプは、『iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド』の **cmchangeover** コマンドの項を参照してください。) これにより、2 番目の CMC のファームウェアをアップデートする前に、アップデートが正常に完了し、新しいファームウェアが正しく機能していることを確認できます。両方の CMC をアップデートしたら、**cmchangeover** コマンドを使用して CMC をそれぞれ元の役割に戻すことができます。CMC Firmware revision 2.x は、**cmchangeover** コマンドを使用せずに、プライマリ CMC と冗長 CMC の両方をアップデートします。

## ウェブインタフェースを使用した CMC ファームウェアのアップデート

ウェブインタフェースを使って CMC ファームウェアをアップデートする手順については、183 ページの「CMC ファームウェアのアップデート」を参照してください。


## RACADM を使用した CMC ファームウェアのアップデート

RACADM **fwupdate** サブコマンドを使用して CMC ファームウェアをアップデートする手順については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』(iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド) の **fwupdate** コマンドの項を参照してください。

## CMC プロパティの設定

ウェブインタフェースまたは RACADM を使って、電力バジェット、ネットワーク設定、ユーザー、SNMP および E-メールアラートなどの CMC プロパティを設定できます。

ウェブインタフェースの使い方の詳細については、99 ページの「CMC 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。RACADM の使い方の詳細については、69 ページの「RACADM コマンドラインインタフェースの使用」を参照してください。

 **注意**：複数の CMC 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。

### 電力バジェットの設定

CMC には、シャーシに電力バジェット、冗長、動的電源機能を提供する電力バジェットサービスがあります。

電源管理サービスは、電力消費量の最適化、および必要に応じて異なるモジュールに電力を再割り当てする機能を持ちます。

CMC 電力管理の詳細については、285 ページの「電力管理」を参照してください。

ウェブインタフェースを使って電力バジェットおよびその他の電源設定を行う手順は、180 ページの「電力バジェットの設定」を参照してください。

### CMC ネットワークの設定



**メモ**：CMC 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。

次のいずれかのツールを使って、CMC ネットワーク設定を行うことができます。

- RACADM — 詳細については、92 ページの「複数シャーシ内の複数 CMC の設定」を参照してください。



**メモ**：Linux 環境で CMC を導入する場合は、35 ページの「RACADM の Linux 管理ステーションへのインストール」を参照してください。

- ウェブインターフェース — 詳細については、139 ページの「CMC ネットワークプロパティの設定」を参照してください。

## ユーザーの追加と設定

RACADM または CMC ウェブインタフェースを使って CMC の追加、設定を行うことができます。また、Microsoft Active Directory を使ってユーザーの管理を行うこともできます。

RACADM を使用して公開キーの追加と設定を行う手順については、88 ページの「RACADM による SSH 経由の公開キー認証の設定」を参照してください。

ウェブインタフェースを使用してユーザーを追加および設定する手順については、149 ページの「CMC ユーザーの追加と設定」を参照してください。

CMC で Active Directory を使用する手順については、243 ページの「CMC ディレクトリサービスの使用」を参照してください。

## SNMP と E-メールアラートの追加

特定のシャシーイベントが発生したときに、SNMP や E-メールアラートを生成するように CMC を設定できます。詳細については、370 ページの「SNMP アラートの設定」および 375 ページの「E-メール警告の設定」を参照してください。

## リモートシスログの設定

リモートシスログ機能は、CMC GUI または **racadm** コマンドを使用してアクティブ化 / 設定されます。設定オプションには、ログエントリを転送する場合に CMC が使用する **syslog** サーバー名（または IP アドレス）と **UDP** ポートが含まれています。設定では、最大 3 つの異なるシスログサーバーを転送先として指定できます。リモートシスログは、追加の CMC ログターゲットです。リモートシスログを設定したら、新しい各ログエントリが CMC によって生成され、送信先に転送されます。



**メモ:** 転送されるログエントリのネットワークトランスポートは UDP であるため、ログエントリが確実に配信されるという保証もなければ、ログエントリが正常に受信されたかどうかを通知するフィードバックが CMC に送られることもありません。

CMC サービスを設定するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 **ネットワーク** タブをクリックします。
- 3 **サービス** サブタブをクリックします。**サービス** ページが表示されます。

リモートシスログの詳細については、表 5-58 を参照してください。

## 冗長 CMC 環境について

アクティブ CMC に障害が発生した場合に、フェイルオーバーするためのスタンバイ CMC を取り付けられます。冗長 CMC は、事前に取り付けすることも、後日追加することもできます。CMC ネットワークを適切にケーブル接続し、完全冗長性またはベストパフォーマンスを確保することが大切です。

フェイルオーバーは、次のような場合に行われます。

- RACADM **cmchangeover** コマンドを実行した場合。（『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **cmchangeover** コマンドの項を参照してください。）
- アクティブ CMC で RACADM **racreset** コマンドを実行した場合。（『iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド』の **racreset** コマンドの項を参照してください。）
- ウェブインタフェースでアクティブ CMC をリセットした場合。（320 ページの「シャーシに対する電力制御操作の実行」に説明される **電力制御操作の CMC のリセット** オプションを参照）
- アクティブ CMC からネットワークケーブルを外した場合。
- シャーシからアクティブ CMC を取り外した場合。
- アクティブ CMC で CMC ファームウェアフラッシュアップデートを行った場合。
- アクティブ CMC が機能していない場合



**メモ**：CMC フェイルオーバーが発生すると、すべての iDRAC 接続およびすべてのアクティブな CMC セッションが失われます。セッションを失ったユーザーは、新しいアクティブ CMC に再接続する必要があります。

## スタンバイ CMC について

スタンバイ CMC はアクティブ CMC と同一で、そのミラーとして維持されています。アクティブ CMC とスタンバイ CMC には共に同じファームウェアリビジョンがインストールされている必要があります。ファームウェアリビジョンが異なる場合、冗長性劣化として報告されます。

スタンバイ CMC はアクティブ CMC と同じ設定とプロパティを引き継ぎます。CMC のファームウェアリビジョンは同じでなければなりません。スタンバイ CMC に設定を複製する必要はありません。



**メモ**：スタンバイ CMC の取り付けに関する詳細は、『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。スタンバイ CMC に CMC ファームウェアをインストールする手順については、48 ページの「CMC ファームウェアのインストールまたはアップデート」を参照してください。



## CMC フェイルセーフモード

フェイルセーフモードでは、冗長 CMC によって提供されるフェイルオーバー保護と同じように、M1000e エンクロージャがフェイルセーフモードを有効にし、ブレードと I/O モジュールを障害から保護します。フェイルセーフモードは、シャーシを制御している CMC がないときに有効になります。CMC フェイルオーバー時、または単一 CMC 管理にロスがある場合は以下の点にご注意ください。

- 新たに取り付けられたブレードの電源を入れることはできません。
- 既存のブレードにリモートでアクセスできません。
- シャーシの冷却ファンは、コンポーネントの温度保護のために 100% で稼働します。
- CMC の管理が復元されるまで、電力消費を制限するためにブレードのパフォーマンスは低減します。

以下のような条件が発生すると、CMC が管理されなくなります。

- CMC の取り外し — CMC を交換したあと、またはフェイルオーバーからスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。
- CMC ネットワークケーブルの取り外し、またはネットワーク接続の切断 — シャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。ネットワークフェイルオーバーは、冗長 CMC モードでのみ有効になります。
- CMC のリセット — CMC が再起動したあと、またはシャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。
- CMC フェイルオーバーコマンドの発行 — シャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとにシャーシ管理が再開します。
- CMC ファームウェアのアップデート — CMC が再起動したあと、またはシャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。フェイルオーバーイベントが 1 つだけになるように、先にスタンバイ CMC をアップデートすることをお勧めします。
- CMC エラー検出と修正 — CMC のリセット後、またはシャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。



**メモ:** 1 つの CMC または冗長 CMC を持つエンクロージャを設定できます。冗長 CMC 設定では、プライマリ CMC がエンクロージャまたは管理ネットワークとの通信から切断されると、スタンバイ CMC がシャーシ管理を引き継ぎます。

## アクティブ CMC の選択プロセス

2 つの CMC スロットには違いはありません。つまり、スロットによってアクティブかスタンバイかが決まるわけではありません。最初に取り付けた、または起動した CMC がアクティブ CMC になります。CMC が 2 つ取り付けられている場合に AC 電源を入れると、CMC シャーシスロット 1 (左側) に取り付けられている CMC がアクティブ CMC になります。アクティブ CMC は青色 LED で示されます。

既に電源が入っているシャーシに 2 台の CMC を挿入した場合、自動アクティブ / スタンバイネゴシエーションに 2 分間までかかることがあります。ネゴシエーションが完了したら、通常のシャーシの動作が再開されます。

## 冗長 CMC の正常性ステータスの取得

ウェブインタフェースでスタンバイ CMC の正常性ステータスを表示できます。ウェブインタフェースで CMC の正常性ステータスにアクセスする詳細については、119 ページの「シャーシとコンポーネント概要の表示」を参照してください。

# CMC にコマンドラインコンソールの使用を設定する方法

本項では、CMC コマンドラインコンソール（またはシリアル/Telnet/SSH コンソール）の機能について、およびコンソールからシステム管理操作を実行できるようにシステムを設定する方法について説明します。コマンドラインコンソールを介して CMC で RACADM コマンドを使用する方法については、69 ページの「RACADM コマンドラインインタフェースの使用」を参照してください。

## CMC 上のコマンドラインコンソール 機能

CMC は、次のシリアル、Telnet、SSH コンソール機能をサポートしています。

- 単一のシリアルクライアント接続と最大 4 つの Telnet クライアントの同時接続。
- 最大 4 つのセキュアシェル（SSH）クライアント同時接続。
- RACADM コマンドに対応。
- サーバーおよび I/O モジュールのシリアルコンソールに接続するビルトイン **connect** コマンド。これは **racadm onnect** としても利用可能です。
- コマンドラインの編集と履歴。
- 全コンソールインタフェースにおけるセッションタイムアウト制御。

# シリアル、Telnet、SSH コンソールの使用

CMC コマンドラインに接続すると、次のコマンドを入力できます。

表 3-1. CMC コマンドラインのコマンド

コマンド	説明
racadm	RACADM コマンドはキーワード <b>racadm</b> で始まり、 <b>getconfig</b> 、 <b>serveraction</b> 、 <b>getsensorinfo</b> のようなサブコマンドが続きます。RACADM の使用に関する詳細は、69 ページの「RACADM コマンドラインインタフェースの使用」を参照してください。
connect	サーバーまたは I/O モジュールのシリアル コンソールに接続します。 <b>connect</b> コマンドの使用に関するヘルプは、61 ページの「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。 <b>メモ</b> : <b>racadm connect</b> コマンドも使えます。
exit、 logout、quit	これらのコマンドはすべて同じ処置を実行します。現在のセッションを終了してログインプロンプトに戻ります。

## CMC での Telnet コンソールの使用

一度に最大 4 台の telnet クライアントシステムと 4 台の SSH クライアントを接続できます。

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、CMC 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](http://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。

## CMC での SSH の使用

SSH は Telnet セッションと同じ機能を備えたコマンドラインセッションですが、セッションのネゴシエーションと暗号化によってセキュリティが強化されています。CMC 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。CMC ではデフォルトで SSH が有効になっています。

 **メモ:** CMC は SSH バージョン 1 をサポートしていません。

ログイン時にエラーが発生した場合は、SSH クライアントからエラーメッセージが発行されます。メッセージのテキストはクライアントによって異なり、CMC で制御することはできません。エラーの原因を特定するには、RACLog メッセージを確認してください。

 **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。また、Putty.exe を使用して OpenSSH を実行できます。Windows のコマンドプロンプトで OpenSSH を実行すると、完全には機能しません（一部のキーが応答せず、グラフィックが表示されません）。Linux の場合は、SSH クライアントサービスを実行して、いずれかのシェルで CMC に接続します。

SSH は一度に 4 セッションがサポートされています。セッションタイムアウトは、`cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）のデータベースプロパティの章、ウェブインタフェースの **サービス管理** ページ、または 173 ページの「サービスの設定」を参照してください。

CMC では、SSH を使った公開キー認証（PKA）もサポートされています。この認証方法を使用すると、ユーザー ID / パスワードの組み込みや入力を行う必要がないため、SSH スクリプトの自動化が向上します。詳細については、88 ページの「RACADM による SSH 経由の公開キー認証の設定」を参照してください。

### CMC で SSH を有効にする方法

SSH はデフォルトで有効になっています。SSH が無効になっている場合は、サポートされている他のインタフェースを使用して有効にできます。

RACADM を使用して CMC の SSH 接続を有効にする手順については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **config** コマンドの項および **cfgSerial** データベースプロパティの項を参照してください。ウェブインタフェースを使用して CMC で SSH 接続を有効にする手順については、173 ページの「サービスの設定」を参照してください。

## SSH ポートの変更

SSH ポートを変更するには、次のコマンドを実行します。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort  
<port number>
```

cfgSerialSshEnable および cfgRacTuneSshPort プロパティの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）のデータベースプロパティの章を参照してください。

CCH SSH の実装では、表 3-2 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 3-2. 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 仕様に準拠）
対称暗号	<ul style="list-style-type: none"><li>• AES256-CBC</li><li>• RIJNDAEL256-CBC</li><li>• AES192-CBC</li><li>• RIJNDAEL192-CBC</li><li>• AES128-CBC</li><li>• RIJNDAEL128-CBC</li><li>• BLOWFISH-128-CBC</li><li>• 3DES-192-CBC</li><li>• ARCFOUR-128</li></ul>
メッセージの整合性	<ul style="list-style-type: none"><li>• HMAC-SHA1-160</li><li>• HMAC-SHA1-96</li><li>• HMAC-MD5-128</li><li>• HMAC-MD5-96</li></ul>
認証	パスワード

## フロントパネルから iKVM への接続を有効にする方法

iKVM 前面パネルポートの詳細および使用手順については、345 ページの「フロントパネルの有効または無効」を参照してください。

# ターミナルエミュレーションソフトウェアの設定

CMC は、次の種類のターミナルエミュレーションソフトウェアを実行している管理ステーションからシリアルテキストコンソールをサポートしています。

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

必要なタイプのターミナルソフトウェアを設定するには、次の副項の手順に従ってください。

## Linux Minicom の設定

Minicom は Linux 用のシリアルポートアクセスユーティリティです。次の手順は、Minicom のバージョン 2.0 の設定に有効です。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、60 ページの「必要な Minicom 設定」を参照してください。

### Minicom バージョン 2.0 の設定



**メモ:** 最適な結果を得るには、`cfgSerialConsoleColumns` プロパティをコンソールの列数に一致するように設定します。プロンプトは 2 列分とることに注意してください。たとえば、80 列のターミナルウィンドウでは、次のように設定します。  
`racadm config -g cfgSerial -o  
cfgSerialConsoleColumns 80`

- 1 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 config file name>` と入力し、手順 13 に進みます。

- 2 Linux コマンドプロンプトで、`minicom -s` と入力します。
- 3 **シリアルポートのセットアップ** を選択し、<Enter> を押します。
- 4 <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`)。
- 5 <e> を押して、**速度 / パリティ / ビット** のオプションを **115200 8N1** に設定します。
- 6 <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。  
**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。
- 7 **モデムとダイヤル** を選択して、<Enter> を押します。
- 8 **モデムダイヤルとパラメータの設定** メニューで、<Backspace> をクリックして **init**、**reset**、**connect** および **hangup** 設定をクリアして空白にし、<Enter> をクリックして各空白値を保存します。

- 9 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。
- 10 **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。
- 11 **Minicom から終了** を選択して、<Enter> を押します。
- 12 コマンドシェルプロンプトで、`minicom <Minicom config file name>` と入力します。
- 13 <Ctrl+a>、<x>、<Enter> を押して、Minicom を終了します。

Minicom ウィンドウがログイン画面を表示するか確認します。ログイン画面が表示されたら、正しく接続されています。これでログインの準備が完了し、CMC コマンドライン インタフェースにアクセスできます。

### 必要な Minicom 設定

表 3-3 を参照して、Minicom のバージョンを設定します。

表 3-3. Minicom 設定

設定の説明	必要な設定
速度 / パリティ / ビット	115200 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。



## 接続コマンドでサーバーまたは I/O モジュールに接続する

CMC は、サーバーのシリアル コンソールまたは I/O モジュールにリダイレクトする接続が確立できます。サーバーの場合は、次の方法でシリアル コンソール リダイレクトを実現できます。

- CMC コマンドライン、**connect** または **racadm connect** コマンドの使用。**connect** の詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）で **racadm connect** コマンドを参照してください。
- iDRAC ウェブインタフェースのシリアルコンソールリダイレクト機能の使用。
- iDRAC シリアルオーバー LAN (SOL) 機能の使用。

シリアル /Telnet/SSH コンソールでは、CMC は、**connect** コマンドをサポートして、サーバーまたは IOM モジュールとのシリアル接続を確立します。サーバーのシリアルコンソールには、オペレーティングシステムのシリアルコンソールの他にも、BIOS 起動およびセットアップ画面が含まれています。I/O モジュールの場合は、スイッチ シリアル コンソールが使えます。



**注意:** CMC シリアルコンソールから実行した場合、**connect -b** オプションは CMC がリセットするまで接続したままになります。この接続は、セキュリティ上の潜在的なリスクとなりえます。



**メモ:** **connect** コマンドは **-b** (バイナリ) オプションを提供します。**-b** オプションは未処理のバイナリデータを渡し、**cfgSerialConsoleQuitKey** は使用されません。また、CMC シリアルコンソールを使用してサーバーに接続すると、DTR 信号の変化（たとえば、デバッグに接続するためにシリアルケーブルが抜かれる）がログアウトを引き起こすことはありません。



**メモ:** IOM がコンソールリダイレクトをサポートしていない場合は、**connect** コマンドは空のコンソールを表示します。その場合、CMC コンソールに戻るには、エスケープシーケンスを入力してください。コンソールのデフォルトのエスケープシーケンスは **<Ctrl>\** です。

管理下システムには最大 6 つの IOM があります。IOM に接続するには、次のように入力します。

```
connect switch-n
```

ここで **n** は IOM ラベルの A1、A2、B1、B2、C1 および C2 です。

(シャーシにおける IOM の配置の図解については、図 11-1 を参照してください。) **connect** コマンドで IOM を参照する際は、表 3-4 で示されるように、IOM はスイッチにマッピングされています。

表 3-4. I/O モジュールからスイッチへのマッピング

I/O モジュールのラベル	スイッチ
A1	switch-a1 または switch-1
A2	switch-a2 または switch-2
B1	switch-b1 または switch-3
B2	switch-b2 または switch-4
C1	switch-c1 または switch-5
C2	switch-c2 または switch-6



**メモ** : 各シャーシで一度に 1 つの IOM 接続のみが可能です。



**メモ** : シリアル コンソールからパススルーに接続することはできません。

管理サーバーのシリアル コンソールに接続するには、**connect server-n** コマンドを使います。このとき、**-n** はサーバーのスロット番号を指定します。**racadm connect server-n** コマンドも使えます。**-b** オプションを指定したサーバー接続は、バイナリ通信が想定され、エスケープ文字が無効になります。iDRAC が使用不可の場合は、ホストへの経路がありませんというエラーメッセージが表示されます。

**connect server-n** コマンドは、ユーザーによるサーバーのシリアル ポートのアクセスを有効にします。この接続が確立された後、ユーザーは、CMC のシリアル ポート経由でサーバーのコンソールリダイレクトを表示できます。これには、BIOS シリアルコンソールとオペレーティングシステムのシリアルコンソールが含まれます。



**メモ** : BIOS 起動画面を表示するには、サーバーの BIOS セットアップで、シリアルリダイレクトを有効にしてください。また、ターミナルエミュレータウィンドウは 80x25 に設定してください。この設定を行わない場合、画面が文字化けします。



**メモ** : BIOS セットアップ画面ではすべてのキーが使えるわけではないため、ユーザーは **CTRL+ALT+DEL** に適切なシーケンスを提供するか、別のエスケープシーケンスを提供しなければなりません。最初のリダイレクト画面には、必要なエスケープシーケンスが表示されます。

## シリアルコンソールリダイレクト用に管理されたサーバー BIOS の設定

KVM を使用して管理下サーバーに接続するか（333 ページの「iKVM によるサーバーの管理」を参照）、iDRAC ウェブ GUI からリモートコンソールセッションを確立します（[support.dell.com/manuals](http://support.dell.com/manuals) にある『iDRAC ユーザーズガイド』を参照）。

BIOS 内のシリアル通信はデフォルトでオフになっています。ホストテキストコンソールデータをシリアルオーバー LAN にリダイレクトするためには、COM1 を介したコンソールのリダイレクトを有効にする必要があります。BIOS 設定を変更するには、次の手順を実行します。

- 1 管理下サーバーを起動します。
- 2 POST 中に <F2> キーを押して BIOS セットアップユーティリティを起動します。
- 3 **シリアル通信** にスクロールダウンして <Enter> キーを押します。ポップアップダイアログボックスのシリアル通信リストには、次のオプションが表示されます。
  - オフ
  - コンソールリダイレクトなしでオン
  - COM1 経由のコンソールリダイレクトでオン方向キーを使用して、オプション間を移動します。
- 4 **COM1 経由のコンソールリダイレクトでオン** が有効になっていることを確認します。
- 5 **起動後のリダイレクト** を有効にします（デフォルトは **無効**）。このオプションは、その後の再起動での BIOS コンソールのリダイレクトを有効にします。
- 6 変更を保存して終了します。
- 7 管理下サーバーが再起動します。

## シリアルコンソールリダイレクト用 Windows の設定

Microsoft Windows Server バージョンが稼動するサーバー（Windows Server 2003 以降）では、設定は必要ありません。Windows は BIOS から情報を取得し、COM 1 の Special Administration Console (SAC) を有効にします。

## 起動中に Linux をシリアルコンソールリダイレクト用に設定する

次は、Linux GRand Unified Bootloader (GRUB) に固有の手順です。別のブートローダーを使用する場合も、同様の変更が必要です。



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

**/etc/grub.conf** ファイルを次のように編集します。

- 1 ファイルの一般設定セクションを見つけ、次の 2 行を新たに追加します。

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

- 2 カーネル行に次の 2 つにオプションを追加します。

```
kernel console=ttyS1,57600
```

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

次の例は、この手順で説明した変更を示しています。

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making
changes
# to this file
# NOTICE: You do not have a /boot partition. This means that
#         all kernel and initrd paths are relative to
/, e.g.
#         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=ttyS1,57600
    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
    initrd /boot/initrd-2.4.9-e.3.img
```

**/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。

- GRUB のグラフィカルインタフェースを無効にし、テキストベースのインタフェースを使用します。そのようにしない場合、コンソールリダイレクトで GRUB 画面が表示されません。グラフィカルインタフェースを無効にするには、`splashimage` で始まる行をコメントアウトします。
- 複数の GRUB オプションを開始してシリアル接続でコンソールセッションを起動するには、すべてのオプションに次の行を追加します。

```
console=ttyS1,57600
```

これは、最初のオプションだけに `console=ttyS1,57600` を追加した例です。

## 起動後に Linux をサーバーシリアルコンソールリダイレクト用に設定する

**/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
```

次の例は、新しい行が追加されたファイルを示しています。

```
#
# inittab This file describes how the INIT process
#         should set up the system in a certain
#         run-level.
#
# Author: Miquel van Smoorenburg
#         Modified for RHS Linux by Marc Ewing and
#         Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you
#    do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

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

# When our UPS tells us power has failed, assume we have a
# few
# minutes of power left. Schedule a shutdown for 2 minutes
# from now.
# This does, of course, assume you have power installed and
# your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System
Shutting Down"
# If power was restored before the shutdown kicked in,
# cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored;
Shutdown Cancelled"

# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon

/etc/securetty ファイルを次のように編集します。
COM2 のシリアル tty の名前を使用して次の新しい行を追加します。
    ttyS1
```

次の例は、新しい行が追加されたサンプルファイルを示しています。

```
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
```





# RACADM コマンドラインインタフェースの使用

RACADM は、テキストベースのインタフェースを通して CMC の設定と管理を行えるコマンド群を提供します。RACADM には、Telnet/SSH またはシリアル接続の使用、iKVM 上で Dell CMC コンソールの使用、あるいは管理ステーションにインストールされた RACADM コマンドラインインタフェースのリモート使用によってアクセスできます。

RACADM インタフェースは、次のように分類されます。



**メモ:** リモート RACADM は、『Dell Systems Management Tools and Documentation DVD』（Dell システム管理ツールおよびマニュアル DVD）に含まれており、管理ステーションにインストールされます。

- リモート RACADM — **-r** オプションと CMC の DNS 名または IP アドレスを使って、管理ステーション上で RACADM コマンドを実行できます。
- ファームウェア RACADM — Telnet、SSH、シリアル接続、または iKVM を使って CMC にログインできます。ファームウェア RACADM では、CMC ファームウェアの一部である RACADM を実行することになります。

リモート RACADM コマンドをスクリプトで使用して、複数 CMC を設定することができます。CMC はスクリプトに対応していないため、スクリプトを直接 CMC で実行することはできません。複数の CMC を設定する方法については、92 ページの「複数シャーシ内の複数 CMC の設定」を参照してください。

## シリアル、Telnet、SSH コンソールの使用

シリアルまたは Telnet/SSH 接続、あるいは iKVM 上の Dell CMC コンソールを使って CMC にログインできます。CMC のシリアルまたはリモートアクセスを設定するには、55 ページの「CMC にコマンドラインコンソールの使用を設定する方法」を参照してください。一般的に使用されるサブコマンドのオプションは、表 4-2 に記載されています。RACADM サブコマンドの完全なリストは、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の RACADM サブコマンドの章に記載されています。

## CMC へのログイン

管理ステーションのターミナルエミュレータソフトウェアおよび管理下ノード BIOS を設定した後、次の手順に従って CMC にログインします。

- 1 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を使って、CMC に接続します。
- 2 CMC ユーザー名とパスワードを入力して、<Enter> を押します。  
これで、CMC にログインできます。

## テキストコンソールの起動

ネットワーク、シリアルポート、または iKVM を通して Dell CMC コンソールから Telnet または SSH を使用して CMC にログインできます。Telnet または SSH セッションを開いて、CMC に接続し、ログインします。

iKVM を介した CMC への接続方法については、327 ページの「iKVM モジュールの使用」を参照してください。

## RACADM の使用

RACADM サブコマンドは、シリアル、Telnet、SSH コンソールのコマンドプロンプト、または通常のコマンドプロンプトから、リモート実行できます。

RACADM サブコマンドを使って、CMC プロパティを設定し、リモート管理タスクを実行します。RACADM サブコマンドのリストを表示するには、次のように入力します。

```
racadm help
```

オプションやサブコマンドなしで実行する場合、RACADM は構文情報、およびサブコマンドとヘルプへのアクセス方法を表示します。個々のサブコマンドの構文とコマンドラインオプションを表示するには、次のように入力します。

```
racadm help <subcommand>
```

## RACADM サブコマンド

表 4-1 に、RACADM の一般的なサブコマンドを簡単に示します。構文および有効な入力値などを含む RACADM サブコマンドの完全なリストについては、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の RACADM サブコマンドの章を参照してください。



**メモ** : **connect** コマンドは RACADM コマンドとビルトインの CMC コマンドの両方で使用できます。connect、**exit**、**quit**、および **logout** コマンドは CMC のビルトインコマンドで、RACADM コマンドではありません。これらのコマンドはリモート RACADM で使用することはできません。これらコマンドの使用に関する詳細は、61 ページの「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。

表 4-1. RACADM サブコマンド

コマンド	説明
help	CMC サブコマンドの説明を一覧表示します。
help <サブコマンド>	指定したサブコマンドの使用方法の概要を一覧表示します。
?	CMC サブコマンドの説明を一覧表示します。
?<サブコマンド>	指定したサブコマンドの使用方法の概要を一覧表示します。
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。
chassisaction	シャーシ、スイッチ、KVM の電源投入、電源切断、リセット、パワーサイクルを実行します。
closessn	セッションを閉じます。
clrraclog	CMC ログをクリアして、ログをクリアしたユーザーと時刻を示すエントリを 1 つ作成します。
clrsel	システムイベントログのエントリをクリアします。
cmchangeover	冗長 CMC 環境で CMC のステータスをアクティブとスタンバイの間で切り替えます。
config	CMC の設定を行います。
connect	サーバーまたは I/O モジュールのシリアル コンソールに接続します。 <b>connect</b> サブコマンドの使用に関するヘルプは、61 ページの「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。
deploy	必要なプロパティを指定することでサーバーを導入します。
feature	アクティブな機能および無効になっている機能を表示します。
featurecard	機能カードのステータス情報を表示します。
fwupdate	システムコンポーネントのファームウェアアップデートを実施し、ファームウェアのアップデートステータスを表示します。
getassettag	シャーシの管理タグを表示します。
getchassisname	シャーシの名前を表示します。
getconfig	現在の CMC 設定のプロパティを表示します。

表 4-1. RACADM サブコマンド (続き)

コマンド	説明
getdcinfo	一般的な I/O モジュールとドーターカードの誤設定情報を表示します。
getfanreqinfo	サーバーおよびスイッチに関するファン要求を % 単位で表示します。
getflexaddr	スロット / ファブリックごとに、FlexAddress の有効 / 無効化ステータスを表示します。-i オプションを付けてこのコマンドを使用すると、特定スロットの WWN および MAC アドレスを表示します。
getioinfo	一般 I/O モジュール情報を表示します。
getkvminfo	iKVM についての情報を表示します。
getled	モジュールの LED 設定を表示します。
getmacaddress	サーバーの MAC アドレスを表示します。
getmodinfo	モジュールの構成とステータス情報を表示します。
getniccfg	コントローラの現在の IP 設定を表示します。
getpbinfo	電力バジェット状態の情報を表示します。
getpminfo	電力バジェット状態の情報を表示します。
getraclog	CMC ログを表示します。
getractime	CMC 時間を表示します。
getredundancymode	CMC の冗長性モードを表示します。
getsel	システムイベントログ (ハードウェアログ) を表示します。
getsensorinfo	システムセンサーについての情報を表示します。
getslotname	シャーシ内のスロットの名前を表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsvctag	サービスタグを表示します。
getsysinfo	CMC とシステムの一般情報を表示します。
gettracelog	CMCtrace ログを表示します。-i オプションを付けてこのコマンドを使用すると、CMC トレースログ内のエントリ数を表示します。
getversion	現在使用するソフトウェアのバージョン、モデル情報、更新可能なデバイスかどうかなどの情報を表示します。
ifconfig	現在の CMC の IP 設定を表示します。

表 4-1. RACADM サブコマンド (続き)

コマンド	説明
krbkeytabupload	Kerberos Keytab を CMC にアップロードします。
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 IPv4 アドレスが現在のルーティングテーブルの内容で CMC から到達可能かどうかを確認します。
ping6	送信先の IPv6 アドレスが現在のルーティングテーブルの内容で CMC から到達可能かどうかを確認します。
racdump	包括的なシャーシステータスおよび構成状況の情報と共に、イベントログの履歴を表示します。導入後の構成検証およびデバッグ時に使用します。
racreset	CMC をリセットします。
racresetcfg	CMC をデフォルト設定にリセットします。
remoteimage	リモートサーバー上のメディアファイルを接続、切断、または導入します。
serveraction	管理下システムの電源管理を行います。
setassettag	シャーシの管理タグを設定します。
setchassisname	シャーシの名前を設定します。
setflexaddr	シャーシ上で FlexAddress が有効になった際に、特定のスロット / ファブリック上で FlexAddress を有効 / 無効にします。
setled	モジュールの LED 設定を設定します。
setniccfg	コントローラの IP 設定を指定します。
setractime	CMC 時間を設定します。
setslotname	シャーシ内のスロットの名前を設定します。
setsysinfo	シャーシの名前と場所を設定します。
sshpkauth	最大 6 個の SSH 公開キーをアップロードし、既存のキーを削除してから、CMC にあるキーを表示します。
sslcertdownload	認証局が署名した証明書をダウンロードします。
sslcertupload	認証局が署名した証明書またはサーバー証明書を CMC にアップロードします。
sslcertview	認証局が署名した証明書またはサーバー証明書を CMC で表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。

表 4-1. RACADM サブコマンド (続き)

コマンド	説明
sslresetcfg	CMC ウェブ GUI で使用される自己署名の証明書を再生成します。
testemail	CMC NIC で CMC に E-メールを送信させます。
testfeature	指定の機能の設定パラメータを確認できます。たとえば、簡易認証 (ユーザー名とパスワード) または認証 (シングルサインオンまたは Smart Card ログイン) によって Active Directory の設定をテストすることができます。
testtrap	CMC のネットワークインタフェース経由で CMC に SNMP を送信させます。
traceroute	IPv4 パケットがコマンドネットワークノードに到達するまでの経路を印刷します。
traceroute6	IPv6 パケットがコマンドネットワークノードに到達するまでの経路を印刷します。


## RACADM へのリモートアクセス

表 4-2. リモート RACADM サブコマンドオプション

オプション	説明
-r <racIpAddr>	コントローラのリモート IP アドレスを指定します。
-r <racIpAddr>:<port>	CMC のポート番号がデフォルトのポート (443) ではない場合は、<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 <usrName>	コマンドのトランザクションの認証に使用するユーザー名を指定します。-u オプションを使用すると、-p オプションも必要になり、-i オプション (インタラクティブ) は使用できなくなります。
-p <password>	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。

RACADM にリモートアクセスするには、次のコマンドを入力します。

```
racadm -r <CMC IP address> -u <username> -p <password>
<subcommand> <subcommand options>
racadm -i -r <CMC IP address> <subcommand> <subcommand
options>
```

 **メモ**：-i オプションは、RACADM にユーザー名とパスワードの入力をインタラクティブにプロンプトするよう指示します。-i オプションを指定しない場合は、-u と -p オプションを使ってコマンド内でユーザー名とパスワードを指定する必要があります。


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
```

CMC の HTTPS ポート番号をデフォルトポート（443）からカスタムポートに変更した場合は、次の構文を使用する必要があります。

```
racadm -r <CMC IP address>:<port> -u <username> -p
<password> <subcommand> <subcommand option>
racadm -i -r <CMC IP address>:<port> <subcommand>
<subcommand option>
```

## racadm リモート機能の有効 / 無効化

 **メモ**：デルでは、これらのコマンドをシャードで実行することを推奨しています。

CMC 上での RACADM リモート機能はデフォルトで有効になっています。次のコマンドでは、-g はオブジェクトが属する設定グループを指定し、-o は設定する設定オブジェクトを指定します。


RACADM リモート機能を無効にするには、次を入力します。

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

RACADM リモート機能を再び有効にするには、次を入力します。

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

## 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、CMC の IP アドレスを設定してください。CMC の設定に関する詳細は、29 ページの「CMC のインストールと設定」を参照してください。

RACADM コンソールのリモートオプション (-r) を使うと、管理下システムに接続してリモートコンソールまたは管理ステーションから RACADM サブコマンドを実行できます。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 CMC IP アドレスが必要です。RACADM へのリモートアクセスを試みる前に、それにアクセスする権限があることを確認してください。ユーザー権限を表示するには、次を入力します。

```
racadm getconfig -g cfguseradmin -i n
```

ここで、*n* はユーザー ID (1 ~ 16) です。

ユーザー ID がわからない場合は、異なる *n* 値を試してください。



**メモ** : RACADM リモート機能は、対応ブラウザを通して管理ステーション上でのみ使用できます。詳細については、デルサポートサイトの [support.dell.com/manuals](http://support.dell.com/manuals) の『Dell システムソフトウェアサポートマトリックス』の対応ブラウザの項を参照してください。



**メモ** : RACADM リモート機能を使用する場合には、次に示すようなファイル操作で RACADM サブコマンドを使っているフォルダへの書き込み権限が必要になります。たとえば、次のとおりです。

```
racadm getconfig -f <file name> -r <IP address>
```

または

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

リモート RACADM を使用して設定グループをファイル内に取り込むときに、グループ内のキープロパティが設定されていない場合、その設定グループは設定ファイルの一部として保存されません。これらの設定グループを別の CMC にクローンする必要がある場合は、キープロパティを設定してから、getconfig -f コマンドを実行する必要があります。あるいは、getconfig -f コマンドを実行した後に、必要なプロパティを設定ファイルに手動で入力することもできます。これは、racadm インデックス化されたすべてのグループに対して適用されます。次は、この動作と対応するキープロパティを示したインデックス化されたグループを一覧にしたものです。

```
cfgUserAdmin - cfgUserAdminUserName
```

```
cfgEmailAlert - cfgEmailAlertAddress
```

```
cfgTraps - cfgTrapsAlertDestIPAddr
```

```
cfgStandardSchema - cfgSSADRoleGroupName
```


```
cfgServerInfo - cfgServerBmcMacAddress
```

## RACADM エラーメッセージ

RACADM CLI エラーメッセージの詳細については、99 ページの「トラブルシューティング」を参照してください。



## RACADM を使用した CMC の設定

 **メモ:** 最初の CMC の設定を行うためには、リモートシステム上での RACADM コマンドの実行に **root** ユーザーとしてログインする必要があります。CMC の設定権限を持つ別のユーザーを作成することもできます。


CMC を最も迅速に設定する方法は、CMC ウェブインタフェースを利用することです (99 ページの「CMC ウェブインタフェースの使用」を参照)。ただし、CLI またはスクリプト設定を使用したり、複数の CMC の設定をする場合は、管理ステーションに CMC と一緒にインストールされる リモート RACADM を使用してください。

## CMC ネットワークプロパティの設定


CMC の設定を始める前に、まず CMC ネットワーク設定を指定し、CMC がリモート管理できるようにする必要があります。この初期設定によって、CMC へのアクセスを可能にするための TCP/IP ネットワークパラメータが割り当てられます。

### CMC への初期アクセスの設定

ここでは、RACADM コマンドを使って CMC ネットワークの初期設定を行う手順を説明します。ここで説明するすべての設定は、フロントパネル LCD を使って行うことができます。41 ページの「LCD 設定ウィザードを使用したネットワーク設定」を参照してください。

 **注意:** CMC ネットワーク設定画面の設定を変更すると、現行のネットワーク接続が遮断されることがあります。

ネットワークのサブコマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』(iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド) の RACADM サブコマンド、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章を参照してください。

 **メモ:** CMC ネットワーク設定を指定するには、**シャーシ設定システム管理者** の権限が必要です。

CMC では、IPv4 と IPv6 の両方のアドレス指定モードがサポートされています。IPv4 と IPv6 の設定は、互いから独立しています。

### 現在の IPv4 ネットワーク設定の表示

NIC、DHCP、ネットワーク速度、デュプレックス設定の概要を表示するには、次を入力します。

```
racadm getniccfg
```

または

```
racadm getconfig -g cfgCurrentLanNetworking
```

### 現在の IPv6 ネットワーク設定の表示

ネットワーク設定の概要を表示するには、次を入力します。

```
racadm getconfig -g cfgIpv6LanNetworking
```

シャードタイプの IPv4 と IPv6 アドレス指定情報を表示するには、次を入力します。

```
racadm getsysinfo
```

CMC はデフォルトで DHCP サーバーから自動的に CMC IP アドレスを要求して取得します。

この機能を無効にして、CMC の静的 IP アドレス、ゲートウェイ、サブネットマスクを指定することもできます。

DHCP を無効にして、CMC の静的 IP アドレス、ゲートウェイ、サブネットマスクを指定するには、次を入力します。

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgNicIpAddress
<static IP address>

racadm config -g cfgLanNetworking -o cfgNicGateway
<static gateway>

racadm config -g cfgLanNetworking -o cfgNicNetmask
<static subnet mask>
```

### 現在のネットワーク設定の表示

NIC、DHCP、ネットワーク速度、デュプレックス設定の概要を表示するには、次を入力します。

```
racadm getniccfg
```

または

```
racadm getconfig -g cfgCurrentLanNetworking
```

シャーシの IP アドレスと DHCP、MAC アドレス、DNS 情報を表示するには、次を入力します。

```
racadm getsysinfo
```

### ネットワーク LAN の設定



**メモ：**次の手順を行うには、**シャーシ設定システム管理者** の権限が必要です。



**メモ：**コミュニティ文字列や SMTP サーバー IP アドレスなどの LAN 設定は、CMC およびシャーシの外部設定に影響します。



**メモ：**シャーシに CMC が 2 つあり（アクティブとスタンバイ）、ネットワークに接続されている場合は、フェイルオーバーが生じた場合、スタンバイ CMC は自動的にアクティブ CMC のネットワーク設定を引き継ぎます。




**メモ：**IPv6 が起動時に有効になると、3 つのルーターの要請が 4 秒ごとに送信されます。外部ネットワークのスイッチがスパニングツリープロトコル（SPT）を実行している場合、外部スイッチポートが 12 秒超ブロックされ、IPv6 の要請が送信されます。このような場合、ルーター広告が IPv6 ルーターによって送信されるまで、接続が制限される期間があります。

## CMC ネットワークインタフェースの有効化

CMC ネットワークインタフェースで IPv4 と IPv6 を有効 / 無効にするには、次を入力します。

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

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

 **メモ**: CMC NIC はデフォルトで有効になっています。

CMC IPv6 アドレス指定を有効 / 無効にするには、次を入力します。

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable 1
```

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable 0
```

 **メモ**: CMC IPv4 アドレス設定 はデフォルトで有効になっています。

CMC IPv6 アドレス指定を有効 / 無効にするには、次を入力します。

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6Enable 1
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6Enable 0
```

 **メモ**: CMC IPv6 アドレス指定はデフォルトで無効になっています。

IPv4 では、CMC はデフォルトで DHCP サーバーから自動的に CMC IP アドレスを要求して取得します。この機能を無効にして、CMC の静的 IP アドレス、ゲートウェイ、サブネットマスクを指定できます。

IPv4 ネットワークで DHCP を無効にして、CMC の静的 IP アドレス、ゲートウェイ、サブネットマスクを指定するには、次を入力します。

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

```
racadm config -g cfgLanNetworking -o cfgNicIpAddress  
<static IP address>
```

```
racadm config -g cfgLanNetworking -o cfgNicGateway  
<static gateway>
```

```
racadm config -g cfgLanNetworking -o cfgNicNetmask  
<static subnet mask>
```

デフォルトで、IPv6 では、CMC は IPv6 自動設定メカニズムを使用して CMC IP アドレスを自動的に要求し取得します。

IPv6 ネットワークにおいて、自動設定機能を無効にし、静的 CMC IPv6 アドレス、ゲートウェイ、プレフィックス長を指定するには、次を入力します。

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6AutoConfig 0
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6Address  
<IPv6 address>
```

```
racadm config -g cfgIPv6LanNetworking -o  
cfgIPv6PrefixLength 64
```

```
racadm config -g cfgIPv6LanNetworking -o  
cfgIPv6Gateway <IPv6 address>
```

## CMC ネットワークインタフェースアドレスの DHCP を有効または無効にする

有効にすると、CMC の DHCP を使って NIC アドレスを取得する機能は、動的ホスト構成プロトコル (DHCP) サーバーから自動的に IP アドレスを要求して取得します。この機能はデフォルトでは有効になっています。

DHCP を使って NIC アドレスを取得する機能を無効にして、静的 IP アドレス、サブネットマスク、ゲートウェイを指定することもできます。詳細については、77 ページの「CMC への初期アクセスの設定」を参照してください。

## DHCP を使用した DNS IP アドレスの取得機能の有効 / 無効化

CMC の DHCP を使って DNS アドレスを取得する機能はデフォルトで無効になっています。この機能を有効にすると、プライマリとセカンダリ DNS サーバーアドレスが DHCP サーバーから取得されます。この機能を使用すると、DNS サーバーの静的 IP アドレスを設定する必要はありません。

DHCP を使用した DNS アドレスの取得機能を無効にして、プライマリとセカンダリ DNS サーバーの静的アドレスを指定するには、次を入力します。

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

IPv6 で DHCP を使用した DNS アドレスの取得機能を無効にして、プライマリとセカンダリ DNS サーバーの静的サーバーアドレスを指定するには、次を入力します。

```
racadm config -g cfgIPv6LanNetworking -o  
cfgIPv6DNSServersFromDHCP6 0
```

## DNS の静的 IP アドレスの設定



**メモ:** 静的 DNS IP アドレス設定は、DNS アドレス機能が無効ではない場合は、有効ではありません。



IPv4 でプライマリとセカンダリ DNS IP サーバーアドレスを設定するには、次を入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServer1  
<IP-address>  
racadm config -g cfgLanNetworking -o cfgDNSServer2  
<IPv4-address>
```

IPv6 でプライマリとセカンダリ DNS IP サーバーアドレスを設定するには、次を入力します。

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer1  
<IPv6-address>  
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer2  
<IPv6-address>
```

## DNS 設定のセットアップ (IPv4 と IPv6)

- **CMC 設定— DNS サーバーで CMC を登録するには、次を入力します。**  
`racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1`  
 **メモ**：一部の DNS サーバーは 31 文字以内の名前しか登録しません。指定する名前が DNS で要求される上限以下であることを確認してください。  
 **メモ**：次の設定は、`cfgDNSRegisterRac` を 1 に設定することで DNS サーバー上に CMC を登録した場合にのみ有効です。
- **CMC 名—デフォルトでは、DNS サーバー上の CMC 名は `cmc-<サービスタグ>` です。DNS サーバー上の CMC の名前を変更するには、次を入力します。**  
`racadm config -g cfgLanNetworking -o cfgDNSRacName <name>`  
ここで、`<name>` は 63 文字以内の英数字とハイフンを使って指定します。  
例：`cmc-1`、`d-345`
- **DNS ドメイン名** デフォルトの DNS ドメイン名は空白文字 1 文字です。DNS ドメイン名を設定するには、次を入力します。  
`racadm config -g cfgLanNetworking -o cfgDNSDomainName <name>`  
ここで、`<name>` は 254 文字以内の英数字とハイフンを使って指定します。例：`p45`、`a-tz-1`、`r-id-001`

## オートネゴシエーション、二重モード、ネットワーク速度の設定 (IPv4 と IPv6)

オートネゴシエーション機能は、有効にした場合、最も近いルーターまたはスイッチと通信することで CMC が自動的に二重モードとネットワーク速度を設定するかどうかを判定します。オートネゴシエーションはデフォルトで有効になっています。

オートネゴシエーションを無効にして、二重モードとネットワーク速度を指定するには、次を入力します。

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <duplex mode>
```

ここで、

`<duplex mode>` は 0 (半二重) または 1 (全二重、デフォルト) です。

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <speed>
```

ここで、

`<speed>` は 10 または 100 (デフォルト) です。

## CMC VLAN の設定 (IPv4 と IPv6)

- 1 外部シャーシ管理ネットワークの VLAN 機能を有効にします。

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

- 2 外部シャーシ管理ネットワークの VLAN ID を指定します。

```
racadm config -g cfgLanNetworking -o cfgNicVlanID  
<VLAN id>
```

<VLAN id> に指定できる値は 1 ~ 4000、および 4021 ~ 4094 の範囲の数値です。デフォルトは 1 です。

たとえば、次のとおりです。

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

- 3 次に、外部シャーシ管理ネットワークの VLAN 優先順位を指定します。

```
racadm config -g cfgLanNetworking -o cfgNicVlanPriority  
<VLAN priority>
```

<VLAN priority> の有効値は 0 ~ 7 です。デフォルトは 0 です。

たとえば、次のとおりです。

```
racadm config -g cfgLanNetworking -o cfgNicVlanPriority 7
```

また、1つのコマンドで VLAN ID と VLAN 優先順位を指定できます。

```
racadm setniccfg -v <VLAN id> <VLAN priority>
```

たとえば、次のとおりです。

```
racadm setniccfg -v 1 7
```

## CMC VLAN の削除

CMC VLAN を削除するには、外部シャーシ管理ネットワークの VLAN 機能を無効にします。

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

次のコマンドを使用しても、CMC VLAN を削除できます。

```
racadm setniccfg -v
```

## VLAN の設定

次のコマンドで、特定のサーバーの VLAN ID と優先順位を指定します。

```
racadm setniccfg -m server-<n> -v <VLAN id> <VLAN priority>
```

<n> の有効値は 1 ~ 16 です。

<VLAN id> に指定できる値は 1 ~ 4000、および 4021 ~ 4094 の範囲の数値です。デフォルトは 1 です。

<VLAN priority> の有効値は 0 ~ 7 です。デフォルトは 0 です。

たとえば、次のとおりです。

```
racadm setniccfg -m server-1 -v 1 7
```

## サーバー VLAN の削除

サーバー VLAN を削除するには、指定したサーバーのネットワークの VLAN 機能を無効にします。

```
racadm setniccfg -m server-<n> -v
```

<n> の有効値は 1 ~ 16 です。

たとえば、次のとおりです。

```
racadm setniccfg -m server-1 -v
```

## 最大転送単位 (MTU) の設定 (IPv4 と IPv6)

MTU プロパティでは、インタフェースを通して渡すことができるパケットの最大サイズを設定できます。MTU を設定するには、次を入力してください。

```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

ここで、<mtu> は 576 ~ 1500 の数値です (デフォルトは 1500)。



**メモ** : IPv6 では最低 1280 の MTU が必要です。IPv6 が有効で、**cfgNetTuningMtu** の値がこれよりも低い値に設定されている場合、CMC は 1280 の MTU を使用します。

## SMTP サーバーの IP アドレスの設定 (IPv4 と IPv6)

CMC を有効にして、シンプルメールトランスファープロトコル (SMTP) を使って指定した IP アドレスに E-メールアラートを送信できます。この機能を有効にするには、次を入力します。

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSmtpServerIpAddr <SMTP IP address>
```

ここで、<SMTP IP address> はネットワーク上の SMTP サーバーの IP アドレスです。





**メモ:** ネットワークに、IP アドレスのリースを定期的に発行および更新する SMTP サーバーがあり、かつそれらのアドレスが異なる場合は、指定した SMTP サーバー IP アドレスが変更されるため、このプロパティ設定が機能しない期間があります。そのような場合は、DNS 名を使用してください。

## ネットワークセキュリティ設定のセットアップ (IPv4 のみ)

次の手順を行うには、**シャーシ設定システム管理者** の権限が必要です。

### IP 範囲チェックの有効化 (IPv4 のみ)

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**

受信 IP アドレスを使ってログインできるのは、次の両方のアドレスが同一である場合に限られます。

- **cfgRacTuneIpRangeMask** (ビットワイズ) および受信 IP アドレス
- **cfgRacTuneIpRangeMask** (ビットワイズ) および **cfgRacTuneIpRangeAddr** で指定された IP アドレス

## RACADM を使用したユーザーの設定

CMC のプロパティデータベースには 16 のユーザーを設定できます。CMC 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確認します。新しい CMC を設定している場合や、RACADM の **racresetcfg** コマンドを実行した場合、現在のユーザーは、パスワードが **calvin** の **root** のみが存在します。**racresetcfg** サブコマンドは、CMC を元のデフォルトにリセットします。



**注意:** **racresetcfg** コマンドを使用すると、すべての設定パラメータが元のデフォルトにリセットされますので、注意してください。それまでに行った変更がすべて失われます。



**メモ:** ユーザーをいつでも有効および無効に切り替えられますが、ユーザーを無効にしてもそのユーザーはデータベースから削除されません。

ユーザーが存在するかどうかを確認するには、CMC への **Telnet/SSH** テキストコンソールを開き、ログインしてから、1-16 のインデックスごとに、次のコマンドを一度入力します。

```
racadm getconfig -g cfgUserAdmin -i <index>
```

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。「=」（等号）の後に名前が表示される場合は、インデックスがそのユーザーによって使用されています。



**メモ:** RACADM `config` サブコマンドを使ってユーザーを手動で追加または削除する場合は、`-i` オプションでインデックスを指定する必要があります。前の例に表示された `cfgUserAdminIndex` オブジェクトに「#」文字があることに注意してください。また、グループ / オブジェクトを書き込むことを指定するために `racadm config -f racadm.cfg` コマンドを使用する場合は、インデックスは指定できません。最初に使用可能な索引に新しいユーザーが追加されます。この動作によって、プライマリ CMC と同じ設定を持つセカンダリ CMC を設定するときの柔軟性が得られます。

## CMC ユーザーの追加

新しいユーザーを CMC 設定に追加する場合は、基本的なコマンドをいくつか使用できます。次の手順を実行します。

- 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 ユーザー権限を設定します。ユーザー権限の詳細については、表 5-42 および表 5-43 を参照してください。
- 4 ユーザーを有効にします。

### 例

次の例は、パスワードが「123456」で CMC へのログイン権限を持つ「John」という新しいユーザーを追加する方法を示しています。



**メモ:** 特定のユーザー権限に対する有効なビットマスク値の一覧については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）のデータベースプロパティの章の表 3-1 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 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 cfgUserAdminEnable 1
```

正しい権限を持つユーザーが追加されたことを確認するには、次のいずれかのコマンドを使用します。

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

## RACADM による SSH 経由の公開キー認証の設定

SSH インタフェース経由のサービスユーザー名には、最大 6 つの公開キーを設定できます。公開キーを追加または削除する前に、表示コマンドを使って設定済みのキーを確認してください。これは、キーを誤って上書きしたり削除したりするのを防ぐためです。サービスユーザー名は、SSH 経由で CMC にアクセスする場合に使用できる特殊なユーザーアカウントです。SSH 経由の PKA が正しく設定された場合、CMC にログインするためにユーザー名やパスワードを入力する必要はなくなります。この機能は、各種機能を実行するために自動化されたスクリプトを設定するときに大変便利です。

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。

- この機能を管理するための GUI サポートは用意されていません。使用できるのは RACADM のみです。
- 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。CMC 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。
- 公開キーの公開キーコメントセクションを使用する場合は、CMC で使用するのは最初の 16 文字のみであることに注意してください。すべての PKA ユーザーはサービスユーザー名を使用してログインします。そのため、RACADM `getssninfo` コマンドを使用する場合は、SSH ユーザーを識別できるように公開キーコメントが使用されます。

たとえば、コメント PC1 およびコメント PC2 を持つ 2 つの公開キーが設定されている場合は、次のようになります。

```
racadm getssninfo
```

タイプ	ユーザー	IP アドレス	ログイン
SSH	PC1	x.x.x.x	06/16/2009 09:00:00
SSH	PC2	x.x.x.x	06/16/2009 09:00:00

sshpkauth の詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 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。

### Windows 用の公開キーの生成

アカウントを追加する前に、SSH 経由で CMC にアクセスするシステムからの公開キーが必要になります。公開 / 秘密キーペアを生成する方法には、Windows を実行しているクライアントの PuTTY キー生成アプリケーションを使用する方法と Linux を実行しているクライアントの ssh-keygen を使用する方法の 2 通りがあります。

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、生成するキーの種類として、SSH-2 RSA または SSH-2 DSA を選択します（SSH-1 はサポートされていません）。
- 2 キーのビット数を入力します。数字は 788 ~ 4096 の間で指定します。



**メモ:** 768 未満、または 4096 を超えるキーを追加しても CMC から何のメッセージも表示されない場合がありますが、ログインしようとするとこれらのキーは失敗します。

- 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 公開キーの使用方法には 2 つのオプションがあります。
  - 公開キーをファイルに保存し、後でアップロードする
  - テキストオプションを使用してアカウントを追加する場合に、**公開キーの貼り付け** ウィンドウからテキストをコピーして貼り付ける

## 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ー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
```

ここで、

-t オプションは、dsa または rsa でなければなりません。

-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。このオプションは任意です。

<passphrase> オプションは任意です。コマンドを完了したら、パブリックファイルを使用してファイルをアップロードするために RACADM に渡します。

## CMC の RACADM 構文メモ

racadm sshpkauth コマンドを使用する場合、次を確認します。

- **-i** オプションを使用する場合は、パラメータが `svcacct` である必要があります。それ以外のパラメータを **-i** で使用すると、CMC で失敗します。`svcacct` は、CMC の SSH で公開キー認証を行うための特殊なアカウントです。
- CMC にログインするには、ユーザーは **サービス** である必要があります。他のカテゴリのユーザーは、`sshpkauth` コマンドを使用して入力した公開キーにアクセスできません。

## 公開キーの表示

CMC に追加した公開キーを表示するには、次を入力します。

```
racadm sshpkauth -i svcacct -k all -v
```

キーを一度に 1 つずつ表示するには、すべてのキーを 1～6 の数字で置き換えます。たとえば、キー 2 を表示するには、次を入力します。

```
racadm sshpkauth -i svcacct -k 2 -v
```

## 公開キーの追加

ファイルのアップロード **-f** オプションを使用して公開キーを CMC に追加するには、次のように入力します。

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -f <public key file>
```



**メモ**: リモート RACADM ではファイルのアップロードオプションのみを使用できます。詳細については、74 ページの「RACADM へのリモートアクセス」とその後の項を参照してください。

公開キーの権限については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）のデータベースプロパティの章の表 3-1 を参照してください。テキストのアップロードオプションを使用して公開キーを追加するには、次を入力します。

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -t "<public key text>"
```

## 公開キーの削除

公開キータイプを削除するには、次を入力します。

```
racadm sshpkauth -i svcacct -k 1 -d
```

公開キータイプをすべて削除するには、次を入力します。

```
racadm sshpkauth -i svcacct -k all -d
```

## 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すると、パスワードを入力せずに、SSH 経由で CMC にログインできるようになります。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 service@<domain>
または
ssh service@<IP_address>
```

ここで、<IP\_address> には CMC の IP アドレスを指定します。

racadm コマンドの送信

```
ssh service@<domain> racadm getversion
ssh service@<domain> racadm getsel
```

サービスアカウントへのログイン時に、パスフレーズが公開 / 秘密キーペアを作成するときに設定された場合は、そのパスフレーズの再入力を求めるメッセージが表示されます場合があります。パスフレーズをキーと一緒に使用している場合は、Windows および Linux の両方のクライアントには、その操作を自動化する方法が用意されています。Windows クライアントでは、Pageant アプリケーションを使用できます。このアプリケーションはバックグラウンドで実行され、パスフレーズの入力操作は透過的に行われます。Linux クライアントでは、ssh-agent を使用できます。これらのいずれかのアプリケーションを設定および使用するには、そのアプリケーションに付属のマニュアルを参照してください。

## CMC ユーザーの権限を有効にする方法

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 29 ページの「作業を開始する前に」の手順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。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i
<index> <user privilege bitmask value>
```



**メモ：**特定のユーザー権限に対する有効なビットマスク値の一覧については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）のデータベースプロパティの章の表 3-1 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。

## CMC ユーザーの無効化

RACADM を使って、CMC ユーザーだけを個別に手動で無効にすることができます。設定ファイルを使ってユーザーを無効にすることはできません。

次の例は、CMC ユーザーを削除するときを使用できるコマンド構文です。

```
racadm config -g cfgUserAdmin -i 2 cfgUserAdminPrivilege 0x0
```

## SNMP と E-メールアラートの設定

シャーシ上で特定のイベントが発生した際に、SNMP イベントトラップ や E-メールアラートを送信するように CMC を設定できます。詳細および手順については、370 ページの「SNMP アラートの設定」および 375 ページの「E-メール警告の設定」を参照してください。

トラップ送信先は適切な形式の数値アドレス (IPv6 または IPv4)、または完全修飾されたドメイン名 (FQDN) で指定できます。お使いのネットワーキング技術 / インフラストラクチャと一貫性のあるフォーマットを選択します。



**メモ:** テストトラップ 機能では、現在のネットワーク設定に不適切な選択項目は検出されません (IPv4 専用の環境で IPv6 送信先を使用する場合など)。

## 複数シャーシ内の複数 CMC 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 CMC 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 CMC をクエリすると、RACADM は取得した情報から **racadm.cfg** 設定ファイルを作成します。ファイルを 1 つまたは複数の CMC にエクスポートして、同じプロパティのコントロールを最短の時間で設定できます。



**メモ:** 一部の設定ファイルには、他の CMC にファイルをエクスポートする前に変更しなければならぬ固有の CMC 情報 (静的 IP アドレスなど) が含まれています。

- 1 適切な設定を含むターゲット CMC に RACADM を使ってクエリします。



**メモ:** 生成される設定ファイルは **myfile.cfg** です。このファイル名は変更できません。




**メモ:** **.cfg** ファイルにはユーザー パスワードは含まれません。新しい CMC に **.cfg** ファイルをにアップロードしたら、必ずすべてのパスワードを再度追加してください。



- 2 CMC 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 -f myfile.cfg
```

 **メモ : getconfig -f** を使用して CMC の設定をファイルにリダイレクトする機能は、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。詳細については、74 ページの「RACADM へのリモートアクセス」を参照してください。

- 3 テキストのみのエディタ（オプション）を使用して設定ファイルを変更します。設定ファイルに特殊なフォーマット文字を使用すると、RACADM データベースが破損する可能性があります。
- 4 新しく作成した設定ファイルを使ってターゲット CMC を変更します。コマンドプロンプトで、次のコマンドを入力します。

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

- 5 設定されたターゲット CMC をリセットします。コマンドプロンプトで、次のコマンドを入力します。

```
racadm reset
```

**getconfig -f myfile.cfg** サブコマンド（手順 1）は、アクティブ CMC の設定を要求し、**myfile.cfg** ファイルを生成します。必要に応じて、ファイル名を変更したり、別の場所に保存することができます。

**getconfig** コマンドを使用して、次の操作を実行できます。

- 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、この情報をその他の CMC にロードします。サーバー管理者は **config** コマンドを使ってユーザーとパスワードのデータベースを同期します。

## CMC 設定ファイルの作成

CMC 設定ファイル **<filename>.cfg** を `racadm config -f <filename>.cfg` コマンドで使用して、テキストファイルを作成します。このコマンドを使うと、（.ini ファイルに類似した）設定ファイルを作成し、このファイルから CMC を設定することができます。

ファイル名は自由に指定できます。ここでは拡張子 **.cfg** を付けて説明していますが、その必要はありません。

 **メモ : getconfig** サブコマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 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。

RACADM は、CMC に初めてロードされたときに **.cfg** をパースして有効なグループとオブジェクト名が存在し、簡単な構文に適合していることを確認します。エラーには、検出された行番号のフラグと、その問題を説明したメッセージが付きます。正確性についてファイル全体がパースされ、すべてのエラーが表示されます。**.cfg** ファイルにエラーが発見された場合は、CMC への書き込みコマンドは送信されません。ユーザーは、設定を行う前に、すべてのエラーを訂正する必要があります。

設定ファイルを作成する前にエラーをチェックするには、**-c** オプションを **config** サブコマンドで使用します。**-c** オプションを使うと、**config** は構文を確認するだけで、CMC 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。

- パーサーがインデックス付けされたグループを見つけた場合、さまざまなインデックスの違いはアンカー付きオブジェクトの値で示されます。

パーサーは、CMC からそのグループのすべてのインデックスを読み取ります。グループ内のオブジェクトは、CMC が設定されたときに修正されたものです。修正されたオブジェクトが新しいインデックスを表す場合、設定中 CMC にそのインデックスが作成されます。

- ユーザーは **.cfg** ファイルの必要なインデックスを指定できません。

インデックスを作成したり、削除することができます。時間と共に、使用済みおよび未使用のインデックスでグループがフラグメント化される可能性があります。インデックスが存在する場合は、変更されます。インデックスが存在しない場合は、最初に使用できるインデックスが使用されます。この方法では、管理しているすべての CMC 間でインデックスの一致をとる必要がないので、インデックス エントリを柔軟に追加できます。新しいユーザーは、最初に使用可能なインデックスに追加されます。1 つの CMC で正しくパースおよび実行される **.cfg** ファイルは、すべてのインデックスが一杯で新しいユーザーを追加しなければならない場合に、別の CMC では正しく実行されない場合があります。

- 同等のプロパティを持つ CMC を両方共に設定するには、**racresetcfg** サブコマンドを使用します。

**racresetcfg** サブコマンドを使って CMC をデフォルトにリセットした後、**racadm config -f <filename>.cfg** コマンドを実行します。

**.cfg** ファイルに、必要なオブジェクト、ユーザー、インデックス、およびその他のパラメータがすべて含まれていることを確認します。オブジェクトとグループの完全なリストについては、『**RACADM Command Line Reference Guide for iDRAC6 and CMC**』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の「データベース プロパティ」の章を参照してください。

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

## 構文解析規則

- ハッシュ文字 (#) で始まる行はコメントとして取り扱われます。コメント行は一列目から記述する必要があります。その他の列の「#」文字は単に # 文字として扱われます。

モデムパラメータでは文字列に # 文字が含まれている場合があります。エスケープ文字は必要ありません。`racadm getconfig -f <filename>.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 <filename>` コマンドを異なる CMC 上で実行します。

例えば、次のようになります。

```
#
# これはコメントです
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Modem init # コメントでは  
ありません>
```

- グループエントリはすべて大カッコ ([ と ]) で囲む必要があります。グループ名を示す右カッコ (]) 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。構成データは、『**RACADM Command Line Reference Guide for iDRAC6 and CMC**』(iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド)のデータベースプロパティの章で定義されているようにグループ化されます。次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。


```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object name}
{object value}
```

- すべてのパラメータは、「オブジェクト」、「=」、または「値」の間に空白を入れずに「オブジェクト = 値」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 つ目の「=」、「#」、「[」、「]」、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。

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object value}
```

- **.cfg** パーサーはインデックスオブジェクトエントリを無視します。ユーザーは、使用するインデックスを指定できません。索引が既に存在する場合は、それが使用されます。索引がない場合は、そのグループで最初に使用可能な索引に新しいエントリが作成されます。

`racadm getconfig -f <filename>.cfg` コマンドは、インデックスオブジェクトの前にコメントを配置するため、ここでコメントを確認できます。


 **メモ:** 次のコマンドを使用すると、インデックスグループを手動で作成できます。

```
racadm config -g <groupName> -o <anchored object>
-i <index 1-16> <unique anchor name>
```

- インデックスグループの行は、**.cfg** ファイルからは削除できません。この行をテキストエディタで削除すると、**RACADM** は設定ファイルをパースするときに停止し、エラー警告を発生します。

次のコマンドを使用して、手動でインデックスオブジェクトを削除する必要があります。

```
racadm config -g <groupName> -o <objectName> -i
<index 1-16> ""
```

 **メモ:** NULL 文字列 (2 つの " 文字で示される) は、指定したグループの索引を削除するように CMC に命令します。

インデックス付きグループの内容を表示するには、次のコマンドを実行します。

```
racadm getconfig -g <groupName> -i <index 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 [ ] の組の後にくる最初のオブジェクトでなければなりません。次は、現在のインデックス付きグループの例です。

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<USER_NAME>
```

`racadm getconfig -f <myexample>.cfg` と入力すると、現在の **CMC** 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。

## CMC IP アドレスの変更

設定ファイルの CMC IP アドレスを変更するには、不要な `<variable>=<value>` のエントリをすべて削除します。IP アドレス変更に関連する 2 つの `<variable>=<value>` エントリを含め、`"[" と "]"` が付いた実際の変数グループのラベルのみが残ります。

例：

```
#
# 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、この行の残りは無視
cfgNicGateway=10.35.9.1
```

`racadm config -f <myfile>.cfg` コマンドは、このファイルをパースし、行番号ごとにエラーを探します。正しいファイルが適切なエントリをアップデートします。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 `racadm getconfig -f <myfile>.cfg` と併用して、全社的な変更をダウンロードしたり、新しいシステムをネットワーク経由で設定することができます。



**メモ：**「アンカー」は予約語のため、`.cfg` ファイルでは使用しないでください。

# RACADM を使用して iDRAC でプロパティを設定する方法

RACADM config/getconfig コマンドでは、次の t 設定グループに対する -m <モジュール> オプションがサポートされています。

- cfgLanNetworking
- cfgIPv6LanNetworking
- cfgRacTuning
- cfgRemoteHosts
- cfgSerial
- cfgSessionManagement



**メモ:** プロパティのデフォルト値と範囲の詳細については、『Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers ユーザーガイド』を参照してください。

ブレードサーバー上のファームウェアによって機能がサポートされていない場合は、その機能に関連するプロパティを設定するとエラーが表示されます。たとえば、RACADM を使用して非対応の iDRAC でリモート syslog を有効にしようとすると、エラーメッセージが表示されます。

同様に、RACADM getconfig コマンドを使用して iDRAC プロパティを表示しようとすると、ブレードサーバーで非対応の機能に対するプロパティ値には該当なしと表示されます。

たとえば、次のとおりです。

```
$ racadm getconfig -g cfgSessionManagement -m server-1
# cfgSsnMgtWebServerMaxSessions= 該当なし
# cfgSsnMgtWebServerActiveSessions= 該当なし
# cfgSsnMgtWebServerTimeout= 該当なし
# cfgSsnMgtSSHMaxSessions= 該当なし
# cfgSsnMgtSSHActiveSessions= 該当なし
# cfgSsnMgtSSTimeout= 該当なし
# cfgSsnMgtTelnetMaxSessions= 該当なし
# cfgSsnMgtTelnetActiveSessions= 該当なし
# cfgSsnMgtTelnetTimeout= 該当なし
```

## トラブルシューティング

表 4-3 は、リモート RACADM に関する一般的な問題を掲載しています。

表 4-3. シリアル/RACADM コマンドの使用：よくあるお問い合わせ (FAQ)

質問	回答
CMC リセットを実行した後 (RACADM <b>racreset</b> サブコマンドを使用)、コマンドを入力すると次のメッセージが表示されます。  racadm <サブコマンド> 転送 : エラー : (RC=-1)  このメッセージは何を意味しますか？	CMC のリセットが完了するまで待ってから、別のコマンドを発行してください。
RACADM サブコマンドを使用するとき、理解できないエラーが発生します。	RACADM 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。 <ul style="list-style-type: none"><li>ローカルエラーメッセージ — 構文、入力ミス、誤った名前などの問題。例： エラー : &lt;メッセージ&gt; <b>RACADM help</b> サブコマンドを使って、正しい構文と使用方法を表示します。</li><li>CMC 関連のエラーメッセージ — CMC が対処できないエラー。「racadm コマンドエラー」と表示されることもあります。 デバッグ情報を取得するには、<b>racadm gettracelog</b> と入力します。</li></ul>
リモート RACADM を使用しているとき、プロンプトが「>」に変わって「\$」に戻りません。	コマンド内で、開始と終了が正しくマッチしない二重引用符 (") または引用符 (') を入力すると、CLI は「>」プロンプトに変化し、すべてのコマンドが待ち状態になります。  「\$」のプロンプトに戻すには、<Ctrl>-d と入力します。
次のコマンドの利用を試みましたが、「見つかりません」のエラーが返されました。  \$ ログアウト  \$ 終了	logout および quit コマンドは、CMC CLI インタフェースでサポートされていません。





## CMC ウェブインタフェースの使用

CMC はウェブインタフェースを提供しており、これを利用して、CMC のプロパティとユーザーの設定、リモート管理タスクの実行、問題が起きた際のリモート（管理対象）システムのトラブルシューティングを行うことができます。日常のシャーシ管理には CMC ウェブインタフェースをご使用ください。本章では、CMC ウェブインタフェースを使って一般的なシャーシ管理タスクを行う方法について説明します。

すべての設定タスクはローカル RACADM コマンドまたはコマンドライン コンソール（シリアル コンソール、Telnet、または SSH）を使って実行することもできます。ローカル RACADM の使い方の詳細については、69 ページの「RACADM コマンドラインインタフェースの使用」を参照してください。コマンドラインコンソールの使い方については、55 ページの「CMC にコマンドラインコンソールの使用を設定する方法」を参照してください。



**メモ：**プロキシ経由の接続で Microsoft Internet Explorer を使用している場合、エラーメッセージ「XML ページを表示できません」が表示されたときは、プロキシを無効にする必要があります。

## CMC ウェブインタフェースへのアクセス

IPv4 経由で CMC ウェブインタフェースにアクセスするには：

- 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。

対応ウェブブラウザの最新情報については、デルのサポートサイト [support.dell.com/manuals](https://support.dell.com/manuals) の『Dell システムソフトウェアサポートマトリックス』を参照してください。

- 2 アドレスフィールドに次の URL を入力し、<Enter> を押します。

```
https://<CMC IP address>
```

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://<CMC IP address>:<port number>
```

<CMC IP address> は CMC の IP アドレス、<port number> は HTTPS のポート番号です。

**CMC のログイン** ページが表示されます。

IPv6 経由で CMC ウェブインタフェースにアクセスするには：

- 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。  
対応ウェブブラウザの最新情報については、デルのサポートサイト **support.dell.com/manuals** の『Dell システムソフトウェアサポートマトリックス』を参照してください。
- 2 アドレスフィールドに次の URL を入力し、<Enter> を押します。  
https://[<CMC IP address>]

 **メモ**：IPv6 を使用する場合は、<CMC IP address> を角かっこ ([ ]) で囲む必要があります。

デフォルト値 (443) をまだ使用している場合は、URL で HTTPS ポート番号を指定しなくてもかまいません。そうでない場合は、ポート番号を指定してください。ポート番号が指定された IPv6 CMC URL の構文は次のとおりです。


https://[<CMC IP address>]:<port number>


<CMC IP address> は CMC の IP アドレス、<port number> は HTTPS のポート番号です。


**CMC のログイン** ページが表示されます。

## ログイン

 **メモ**：CMC にログインするには、**CMC へのログイン** 権限を持つ CMC アカウントが必要です。

 **メモ**：デフォルトの CMC ユーザー名は **root**、パスワードは **calvin** です。ルートアカウントは、CMC 出荷時のデフォルトの管理者アカウントです。セキュリティを強化するために、初期設定時に root アカウントのデフォルトパスワードを変更することを強くお勧めします。

 **メモ**：CMC では、ß、â、é、ü などの拡張 ASCII 文字、および主に英語以外の言語で使用されるその他の文字がサポートされていません。

 **メモ**：1 台のワークステーション上で複数のブラウザウィンドウを開き、異なるユーザー名を利用してウェブインタフェースにログインすることはできません。

CMC ユーザーまたは Microsoft Active Directory ユーザーとしてログインしてください。

ログインするには：

- 1 **ユーザー名** フィールドにユーザー名を入力します。
  - CMC ユーザー名：<ユーザー名>
  - Active Directory ユーザー名：<ドメイン>\<ユーザー名>、<ドメイン>/<ユーザー名> または <ユーザー>@<ドメイン>
  - LDAP ユーザー名：<ユーザー名>

 **メモ**：このフィールドでは大文字と小文字が区別されます。


- 2 **パスワード** フィールドに **CMC ユーザーパスワード** または **Active Directory ユーザーパスワード** を入力します。

 **メモ:** このフィールドは大文字と小文字を区別します。

- 3 オプションとして**セッションタイムアウト**を選択します。これは、自動的にログアウトするまで操作を行わずにログインしたままにできる時間を指します。デフォルト地は、**ウェブサービスアイドルタイムアウト**です。詳細については、「サービスの設定」を参照してください。
- 4 **OK** をクリックするか、<Enter> キーを押します。

## ログアウト

ウェブインタフェースにログインした後、各ページの右上の角にある **ログアウト** をクリックすることでいつでもログアウトできます。

 **メモ:** ページ上で入力した設定や情報は忘れず適用（保存）してください。変更を適用せずにログアウトしたりそのページから移動すると、変更内容は失われます。


## CMC の基本設定

以下の項では、CMC の基本設定を行う方法について説明します。

### シャーシの物理的な場所とシャーシ名の設定

ネットワーク上でシャーシを識別するために、データセンターでのシャーシの物理的な場所とシャーシ名（デフォルト名は「**Dell Rack System**」）を設定できます。たとえば、シャーシでの **SNMP** クエリで、設定した名前が返されます。

シャーシの場所とシャーシ名を設定するには、次の手順を実行してください。

- 1 **CMC** ウェブインタフェースにログインします。  
**シャーシの正常性** ページが表示されます。
- 2 **セットアップ** タブをクリックします。  
**シャーシの一般設定** ページが表示されます。
- 3 **データセンター、通路、ラック、ラックスロット** フィールドに場所のプロパティを入力します。  
 **メモ:** シャーシの場所 フィールドはオプションです。**データセンター、通路、ラック、およびラックスロット** フィールドを使用して、シャーシの物理的な場所を示すことを推奨します。
- 4 **シャーシ名** フィールドに新しい名前を入力して、**適用** をクリックします。

## CMC の日付と時刻の設定

日付や時刻を手動で設定でき、あるいはネットワーク時間プロトコル（NTP）サーバーと日付と時刻を同期させることができます。CMC で日付と時刻を設定するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。  
シャーシの正常性 ページが表示されます。
- 2 セットアップ タブをクリックします。  
シャーシの一般設定 ページが表示されます。
- 3 日付 / 時刻 サブタブをクリックします。  
日付 / 時刻 ページが表示されます。
- 4 日付および時刻をネットワーク時間プロトコル（NTP）サーバーと同期させるには、**NTP を有効にする** をチェックして、最大 3 台まで NTP サーバーを指定します。
- 5 日付や時刻を手動で設定するには、**NTP を有効にする** のチェックを外して、**日付と時刻** フィールドを編集し、ドロップダウンメニューから **タイムゾーン** を選択して **適用** をクリックします。

コマンドラインインタフェースを使って日付と時刻を設定するには、『**RACADM Command Line Reference Guide for iDRAC7 and CMC**』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の config コマンドと `cfgRemoteHosts` データベースプロパティグループの項を参照してください。

## リムーバブルフラッシュメディアの有効化

拡張不揮発性ストレージとして使用するため、オプションのリムーバブルフラッシュメディアの設定を有効化または修復することができます。CMC の機能のなかには、動作が拡張不揮発性ストレージに依存するものもあります。

リムーバブルフラッシュメディアを有効化または修復するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。  
シャーシの正常性 ページが表示されます。
- 2 ツリーリストで **シャーシコントローラ** をクリックします。  
**シャーシコントローラのステータス** ページが表示されます。
- 3 **フラッシュメディア** タブをクリックします。  
**リムーバブルフラッシュメディア** ページが表示されます。

- 4 メディアの使用を開始するには、ドロップダウンリストの **シャーシデータの保存にフラッシュメディアを使用** を選択します。
- 5 CMC 上のメディアに問題がある可能性がある場合には、その CMC をアクティブにして、ドロップダウンで **アクティブなコントローラのメディアの準備または修復** を選択します。


シャーシ内に 2 台の CMC がある場合は、両方の CMC にフラッシュメディアが装着されている必要があります。フラッシュメディアに依存する CMC 機能 (Flexaddress を除く) は、デル承認のメディアをインストールして、このページで有効化するまで、正しく動作しません。




## シャーシの正常性ページ

CMC にログインすると、**シャーシの正常性** ページ (**シャーシの概要** → **プロパティ** → **正常性**) が表示されます。最も頻繁に必要な情報と操作は、このページに表示されます。お使いのシャーシがグループリードとして設定されている場合は、ログイン後に **グループの正常性** ページが表示されます。詳細については、104 ページの「シャーシグループの使用」を参照してください。

**シャーシの正常性** ページでは、シャーシとコンポーネントのグラフィック表示およびコンポーネントの詳細が表示されます。選択されたコンポーネントに応じて、各種の操作や他のページへのリンクが利用できます。さらに、CMC ハードウェアログの最新イベントも表示されます。

**シャーシの正常性** ページに掲載される全情報は、動的に更新されます。このページには、**シャーシのコンポーネントの概要** が上部に、**最新の CMC ハードウェアログイベント** のリストが下部に記載されています。

**シャーシのコンポーネントの概要** の項 (シャーシ全体の情報が表示されるときは、「シャーシの正常性」というタイトルになります) では、 と関連情報が表示されます。この項全体を非表示にするには、**閉じる** アイコンをクリックします。

**シャーシのコンポーネントの概要** の項の左半分には、 とシャーシのクイックリンクが表示されます。この項の右半分には、選択されたコンポーネント関連の情報、リンク、操作が表示されます。コンポーネントを選択するには、 の該当する部分をクリックしてください。選択した後、 が青色に変わります。

**最新の CMC ハードウェアログイベント** リストでは、このログの最新の 10 イベントが表示されます。この項のコンテンツは動的に更新され、リストの上部の最新イベントに表示されます。CMC ハードウェアログ入力の詳細については、388 ページの「イベントログの表示」を参照してください。

## シャーシグループの使用

CMC では、単一のリードシャーシから複数のシャーシを監視することが可能になります。シャーシグループを有効にした場合、リードシャーシの CMC は、リードシャーシおよびそのシャーシグループ内のすべてのメンバーシャーシのステータスのグラフィカル表示を生成します。

### シャーシグループの機能

シャーシグループの機能は以下のとおりです。

- シャーシグループ GUI ページには、リーダーおよび各メンバーシャーシの前面と背面を描写した画像がそれぞれ 1 セットずつ表示されます。
- グループのリーダーおよび各メンバーの正常性に関する懸念がある場合、その症状があるコンポーネントは赤色または黄色で表示され、**X** または **!** のマークで識別されます。詳細情報は、該当のシャーシの画像または **詳細** ボタンをクリックすると、そのシャーシ画像の下に表示されます。
- メンバーシャーシまたはサーバーのウェブページを開くために、クイック起動のリンクを使用できます。
- グループに対する、ブレードと入出力のインベントリが可能です。
- 新しいメンバーがグループに追加されたときに、新しいメンバーのプロパティをリーダーのプロパティと同期させることができるオプションを選択できます。

### シャーシグループのセットアップ

1 つのシャーシグループには、最大 8 つのメンバーを含むことができます。また、リーダーおよび各メンバーは、1 つのグループにのみ参加できます。あるグループに属するシャーシを別のグループに参加させることは（リーダーまたはメンバーのどちらとしても）できません。そのシャーシをグループから削除すれば、後で別のグループに追加することはできます。

GUI でシャーシグループをセットアップするには、次の手順を実行します。

- 1 リーダーに予定しているシャーシに、シャーシ管理者権限でログインします。
- 2 **セットアップ** → **グループ管理** とクリックします。  
シャーシグループ ページが表示されます。
- 3 シャーシグループ ページの **役割** で **リーダー** を選択します。  
グループ名を追加するフィールドが表示されます。
- 4 **グループ名** フィールドにグループの名前を入力して、**適用** をクリックします。



**メモ**：ドメイン名に適用される規則と同じものが、グループ名にも適用されます。

シャーシグループが作成されると、GUI が自動的にそのシャーシグループの GUI ページに切り替わります。システムツリーはグループをグループ名で示し、リードシャーシと未実装のメンバーシャーシがシステムツリーに表示されます。

シャーシグループをセットアップした後、次の手順でそのグループにメンバーを追加することができます。

- 1 リーダーシャーシに、シャーシ管理者権限でログインします。
- 2 システムツリーでリードシャーシを選択します。
- 3 **セットアップ** → **グループ管理** とクリックします。
- 4 **グループ管理** にある **ホスト名 /IP アドレス** フィールドで、メンバーの IP アドレスまたは DNS 名を入力します。
- 5 **ユーザー名** フィールドに、そのメンバーシャーシのシャーシ管理者権限のあるユーザーの名前を入力します。
- 6 **パスワード** フィールドに、該当するパスワードを入力します。
- 7 オプションとして、**新しいメンバーとリーダーのプロパティを同期** 選択して、リーダーのプロパティをメンバーにプッシュします。詳細については、107 ページの「新しいメンバーとリーダーシャーシのプロパティの同期」の項を参照してください。
- 8 **適用** ボタンを選択します。
- 9 手順 4 ~ 手順 8 の手順を繰り返して、最大 8 つのメンバーを追加します。  
新しく追加したメンバーのシャーシ名が、**メンバー** ダイアログボックスに表示されます。

ツリー内のグループを選択すると、新しいメンバーのステータスが表示されます。シャーシの画像または詳細ボタンをクリックすると、詳細情報が表示されます。



**メモ:** メンバーに対して入力された資格情報は、セキュアにメンバーシャーシに受け渡され、そのシャーシとリードシャーシとの間の信頼関係が確立されます。この資格情報は、いずれのシャーシにも存続するものではなく、一度信頼関係が確立された後は、相互にやりとりされることはありません。

## リーダーからのメンバーの削除

グループのメンバーをリードシャーシから削除することができます。メンバーを削除するには、次の手順を実行します。

- 1 リーダーシャーシに、シャーシ管理者権限でログインします。
- 2 システムツリーでリードシャーシを選択します。
- 3 **セットアップ** → **グループ管理** とクリックします。
- 4 **メンバーの削除** リストで、削除対象のメンバーの名前（1 つまたは複数）を選択し、**適用** をクリックします。

その後、リードシャーシは、グループから削除されたメンバー（1 つまたは複数）との通信を行います。ダイアログボックスから、それらのメンバー名が削除されます。ネットワーク上の問題によりリードとメンバー間の通信が妨げられている場合、メンバーシャーシがメッセージを受信しない場合があります。そのような場合には、メンバーシャーシからそのメンバーを無効にして削除を完了させてください。詳細については、106 ページの「メンバーシャーシでの個別のメンバーの無効化」の副項を参照してください。

### シャーシグループの無効化

リードシャーシからグループを解除するには、次の手順を実行します。

- 1 リーダーシャーシに、管理者権限でログインします。
- 2 システムツリーでリードシャーシを選択します。
- 3 **セットアップ** → **グループ管理** とクリックします。
- 4 **シャーシグループ** ページの **役割** で **なし** を選択し、**適用** をクリックします。

その後、リードシャーシはすべてのメンバーに、グループから削除された旨の通信を行います。最後にリードシャーシがそのグループのリードシャーシとしての役割を打ち切ります。この時点で、このシャーシは別のグループのメンバーまたはリーダーとしての役割を割り当てることができます。

ネットワーク上の問題によりリードとメンバー間の通信が妨げられている場合、メンバーシャーシがメッセージを受信しない場合があります。そのような場合には、メンバーシャーシからそのメンバーを無効にして削除を完了させてください。詳細については、106 ページの「メンバーシャーシでの個別のメンバーの無効化」の副項を参照してください。

### メンバーシャーシでの個別のメンバーの無効化

リードシャーシによるグループからのメンバーの削除を実行できない場合があります。このような状況は、メンバーへのネットワーク接続が失われた場合に発生します。メンバーシャーシでグループからメンバーを削除するには、次の手順を実行します。

- 1 メンバーシャーシに、シャーシ管理者権限でログインします。
- 2 **セットアップ** → **グループ管理** とクリックします。
- 3 **なし** を選択して、**適用** をクリックします。



## メンバーシャーシまたはサーバーのウェブページの起動

グループ内のメンバーシャーシのウェブページ、サーバーのリモートコンソール、またはサーバー iDRAC のウェブページへのリンクは、リードシャーシのグループページから利用できます。メンバーデバイスにログインするには、リードシャーシにログインするときに使用したユーザー名とパスワードを使用できます。メンバーデバイスのログイン資格情報が同じ場合には、重ねてログインする必要はありません。同じでない場合は、メンバーデバイスのログインのログインページにリダイレクトされます。メンバーデバイスに移動するには、次の手順を実行します。

- 1 リードシャーシにログインします。
- 2 ツリー内で **グループ：名前** を選択します。
- 3 移動先がメンバーの CMC の場合には、目的のシャーシの **CMC の起動** を選択します。

シャーシ内のサーバーが移動先の場合には、次の手順を実行します。

- a 目的のシャーシの画像を選択します。
- b **正常性とアラート** ペインの下に表示されるシャーシ画像内で、目的のサーバーをクリックします。
- c **クイックリンク** という表題のボックスで、移動先デバイスを選択します。移動先ページ、またはログイン画面を表示する新しいウィンドウが開きます。

## 新しいメンバーとリーダーシャーシのプロパティの同期

リーダーのプロパティを、グループに新しく追加されたメンバーシャーシに適用することができます。新しいメンバーのプロパティとリーダーのプロパティを同期するには、次の手順を実行します。

- 1 リーダーシャーシに、管理者権限でログインします。
- 2 システムツリーでリードシャーシを選択します。
- 3 **セットアップ** → **グループ管理** とクリックします。
- 4 **シャーシグループ** ページで、新しいメンバーをグループに追加するときに、**新しいメンバーとリーダーのプロパティを同期** を選択します。
- 5 **適用** をクリックします。

リーダーのプロパティがメンバーに適用されます。

同期後、シャーシ内の複数のシステムの以下の設定サービスプロパティが影響を受けます。

表 5-1. 設定サービスプロパティ

プロパティ	ナビゲーション
SNMP の設定	詳細については、 <b>シャーシの概要</b> → <b>ネットワーク</b> → <b>サービス</b> → <b>SNMP</b> をクリックしてください。
シャーシのリモートロギング	詳細については、 <b>シャーシの概要</b> → <b>ネットワーク</b> → <b>サービス</b> → <b>Remote Syslog</b> (リモートシスログ) をクリックしてください。
LDAP サービスおよび Active Directory サービスを使用したユーザー認証	詳細については、 <b>シャーシの概要</b> → <b>ユーザー認証</b> → <b>ディレクトリサービス</b> をクリックしてください。
シャーシアラート	詳細については、 <b>シャーシの概要</b> → <b>アラート</b> をクリックしてください。

## MCM グループのブレードインベントリ

**シャーシグループの正常性** ページには、すべてのメンバーシャーシが表示され、標準のブラウザダウンロード機能を使用して、ブレードインベントリレポートをファイルに保存することができます。レポートには以下のデータが含まれています。

- すべてのグループシャーシ（リーダーを含む）に現在あるすべてのブレード。
- 空のスロットおよび拡張スロット（フルハイトおよびダブルワイドのブレードを含む）。

## ブレードインベントリレポートの保存

ブレードインベントリレポートを保存するには、次の手順を実行してください。

- 1 **CMC** ウェブインタフェースにログインして、システムツリーで **グループ** を選択します。  
**シャーシグループの正常性** ページが表示されます。
- 2 **インベントリレポートの保存** ボタンをクリックします。  
ファイルを開くか保存するかを確認する **ファイルのダウンロード** ダイアログボックスが表示されます。
- 3 **保存** をクリックして、ブレードインベントリレポートのパスとファイル名を指定します。



**メモ:** 最も正確なブレードインベントリレポートを取得するには、シャーシグループのリーダー、シャーシグループのメンバーシャーシ、および関連シャーシ内のブレードが **オン** になっている必要があります。

## エクスポートされたデータ

ブレードインベントリレポートには、シャーシグループのリーダーの通常のポーリング（30 秒ごと）で各シャーシグループのメンバーによって最近返されたデータが示されます。

最も正確なブレードインベントリレポートを取得するには、以下の条件を満たしている必要があります。

- シャーシグループのリーダーシャーシとシャーシグループのすべてのメンバーシャーシが **シャーシ電源状態オン** になっている
- 関連シャーシ内のすべてのブレードの電源がオンになっている

関連シャーシとブレードのインベントリデータは、シャーシグループの一部のメンバーシャーシが以下の場合、インベントリレポートに含まれない可能性があります。

- **シャーシ電源状態オフ**
- 電源オフ

表 5-2 は、各ブレードについてレポートされる特定のデータフィールドとフィールドの特定の要件を示しています。

表 5-2. ブレードインベントリフィールドの説明

データフィールド	例
シャーシ名	データセンターのシャーシリーダー
シャーシ IP アドレス	192.168.0.1
スロットの場所	1
スロット名	SLOT-01
ホスト名	企業のウェブサーバー <b>メモ:</b> サーバー上で Server Administrator エージェントが実行されている必要があります。実行されていない場合は、ブランクで表示されます。
オペレーティングシステム	Windows Server 2008 <b>メモ:</b> サーバー上で Server Administrator エージェントが実行されている必要があります。実行されていない場合は、ブランクで表示されます。
モデル	PowerEdgeM610
サービスタグ	1PB8VF1
システムメモリの総量	4.0 GB <b>メモ:</b> メンバー上に CMC 4.0 以上が必要です。これがない場合は、ブランクで表示されます。

表 5-2. ブレードインベントリフィールドの説明（続き）

データフィールド	例
CPU の数	2 <b>メモ</b> ：メンバー上に CMC 4.0 以上が必要です。 これがない場合は、ブランクで表示されます。
CPU 情報	Intel (R) Xeon (R) CPU E5502 @1.87GHz <b>メモ</b> ：メンバー上に CMC 4.0 以上が必要です。 これがない場合は、ブランクで表示されます。

### データフォーマット

インベントリレポートは、Microsoft Excel などのさまざまなツールにインポートできるように、**.CSV** ファイルフォーマットで生成されます。インベントリレポートの **.CSV** ファイルは、MS Excel で **データ** → **テキストファイル** を選択してテンプレートにインポートできます。インベントリレポートを MS Excel にインポートするとき、追加情報を求めるメッセージが表示される場合は、カンマ区切りを選択してファイルを MS Excel にインポートしてください。

## シャーシコンポーネントの概要

次の項では、シャーシコンポーネントの概要について説明します。

### シャーシの図解

シャーシは、正面図と背面図で表示されます（上部と下部のイメージ）。サーバーと LCD は正面図で、残りのコンポーネントは背面図で表示されます。コンポーネントを選択するとブルーで表示され、必要なコンポーネントイメージをクリックするとコントロールできます。シャーシにコンポーネントがある場合、そのコンポーネントのタイプのアイコンが、コンポーネントが設置されている場所（スロット）を示す図に表示されます。空の場所は、背景色がチャコールグレーで表示されます。コンポーネントアイコンは、コンポーネントの状態を視覚的に示します。サーバーのアイコンは、例として表 5-1 で使用されます。その他のコンポーネントでは、物理コンポーネントを視覚的に表すアイコンが表示されます。ダブルサイズのコンポーネントが設置されると、サーバーと IOM のアイコンは、複数のスロットにまたがります。コンポーネント上にカーソルを移動すると、そのコンポーネントに関するツールチップが表示されます。

表 5-3. サーバーアイコンの状況

アイコン	説明
	サーバーの電源が入り、正常に動作しています。
	サーバーの電源がオフです。
	サーバーは非重要なエラーを報告しています。
	サーバーは重要なエラーを報告しています。

表 5-3. サーバーアイコンの状況（続き）


アイコン	説明
	サーバーがありません。

表 5-4 は、シャーシクイックリンクを示しています。

表 5-4. シャーシクイックリンク

フィールド	説明
ユーザーの設定	シャーシの概要 → ユーザー認証 → ローカルユーザー に移動します。
ネットワーク設定	シャーシの概要 → ネットワーク → ネットワーク に移動します。
電源構成	シャーシの概要 → 電源 → 構成 に移動します。
ファームウェアアップデート	シャーシの概要 → アップデート → ファームウェアのアップデート に移動します。

## シャーシの正常性

このページが最初に表示されたときは、ページの右側にシャーシレベルの情報とアラートが表示されます。すべての重要および非重要アラートが表示されます。コンポーネントをクリックすると、シャーシレベルの情報は、選択したコンポーネントの情報に変わります。シャーシレベル情報に戻るには、右上隅の **シャーシの正常性に戻る** をクリックします。

表 5-5. シャーシページの情報

フィールド	説明
モデル	シャーシ LCD パネルのモデルが表示されます。
ファームウェア	アクティブ CMC のファームウェアバージョンが表示されます。
サービスタグ	シャーシのサービスタグを表示します。サービスタグは、サポートとメンテナンスのためにメーカーが提供する一意の識別子です。
資産タグ	シャーシの管理タグを表示します。
入力電源	シャーシが現在消費する電力量。
電力限度	ユーザーが割り当てる最大消費電力量。シャーシがこの限度に達すると、サーバーが必要な入力電源でこれ以上上昇しないように制御を開始します。
電源ポリシー	複数の電源装置を調整するためにユーザーが割り当てる設定。
状態	シャーシ電源サブシステムの全体的な正常性が表示されます。

## 選択したコンポーネントの情報

選択したコンポーネントの情報は、次の 3 つの独立した項で表示されます。

- 正常性、パフォーマンス、プロパティです。  
ハードウェアログで表示されるアクティブな重要および重要ではないイベントは、存在する場合ここに表示されます。時間により推移するパフォーマンスデータもここに表示されます。
- プロパティ  
時間により推移またはほとんど変化しないコンポーネントプロパティは、ここに表示されます。
- クイックリンク  
クイックリンクの項では、最も頻繁にアクセスするページと最も頻繁に実行する操作へ移動する方法が示されます。選択したコンポーネントに適用されるリンクのみが、この項に表示されます。

**表 5-6. 正常性とパフォーマンスの情報－サーバー**

項目	説明
電源状態	サーバーのオン / オフ状況 電源状況の各種タイプについては、表 5-25 を参照してください。
状態	正常性アイコンのテキストが表示されます。
電力消費量	現在サーバーが消費する電力量。
割り当てられた電力	サーバーに割り当てられた電力量。
温度	サーバー温度センサーが示す温度。

**表 5-7. サーバープロパティ**

項目	説明
名前	ユーザーが割り当てたスロット名。
モデル	サーバーモデル。たとえば、「PowerEdge M600」、「PowerEdge M605」
サービスタグ	サーバーのサービスタグ サービスタグは、サポートとメンテナンスのためにメーカーが提供する一意の識別子です。サーバーが不在の場合、このフィールドは空になります。
OS	サーバー上のオペレーティングシステム。
ホスト名	オペレーティングシステムに設定されたサーバー名。
iDRAC	サーバー上の iDRAC ファームウェアのバージョン。
BIOS	サーバー BIOS のバージョン。
CPLD	サーバーの Complex Programmable Logic Device (CPLD) のバージョン番号。
CPU 情報	サーバーに取り付けられている CPU の数とタイプを示します。
システムメモリの総量	サーバーに取り付けられているシステムメモリの総量 (GB) を示します。



表 5-8. クイックリンク-サーバー

項目	説明
サーバーステータス	<b>サーバーの概要</b> → < 選択したサーバー > → <b>プロパティ</b> → <b>ステータス</b> に移動します。
リモートコンソールの起動	サーバーがこの操作をサポートしている場合、キーボード-ビデオマウス (KVM) セッションを起動します。
iDRAC GUI の起動	サーバーの iDRAC 管理コンソールを起動します。
サーバーの電源を入れる	サーバーの電源を「オフ」状況にあるサーバーの電源をオンにします。
サーバーの電源を切る	サーバーの電源を「オン」状況にあるサーバーの電源をオフにします。
リモートファイル共有	<b>サーバーの概要</b> → <b>設定</b> → <b>リモートファイル共有</b> に移動します。
iDRAC ネットワークの導入	<b>サーバーの概要</b> → <b>設定</b> → <b>iDRAC</b> (iDRAC の導入) に移動します。
Lifecycle Controller	<b>シャシの概要</b> → <b>アップデート</b> → <b>ファームウェアのアップデート</b> に移動します。

表 5-9. IOM の正常性とパフォーマンス

項目	説明
電源状態	I/O モジュールの電源ステータスが表示されます：オン、オフ、不明（不在）。
役割	I/O モジュールをリンク付けしているときにモジュールのスタックメンバーシップが表示されます。メンバーは、モジュールがスタック セットの一部であることを示します。マスターは、モジュールがプライマリアクセスポイントであることを示します。

表 5-10. IOM プロパティ

項目	説明
モデル	I/O モジュール製品名が表示されます。
サービスタグ	I/O モジュールのサービスタグが表示されます。サービスタグはサポートおよびメンテナンス用に Dell が提供する固有の識別子です。

表 5-11. クイックリンク - I/O モジュール

項目	説明
IOM ステータス	<b>I/O モジュール</b> → <選択した IOM> → <b>プロパティ</b> → <b>ステータス</b> に移動します。
IOM GUI の起動	特定の I/O モジュール用の <b>IOM GUI</b> の起動リンクが存在する場合は、リンクををクリックすると、新しいブラウザウィンドウまたはタブで その I/O モジュールの <b>IOM 管理コンソール</b> が起動します。

表 5-12. アクティブ CMC の正常性とパフォーマンス

項目	説明
冗長モード	スタンバイ CMC のフェールオーバーの準備状態が表示されます。CMC ファームウェアが一致しない場合、または CMC が管理ネットワークに正しくケーブル接続されていない場合、冗長性が存在しないような表示になります。
MAC アドレス	CMC ネットワークインターフェースカード (NIC) の MAC アドレスが表示されます。MAC アドレスはネットワーク上の CMC の一意の識別子です。
IPv4	CMC ネットワークインターフェースの現在の IPv4 アドレスが表示されます。
IPv6	CMC ネットワークインターフェースカードの最初の IPv6 アドレスが表示されます。

表 5-13. CMC プロパティ

項目	説明
ファームウェア	アクティブ CMC のファームウェアバージョンが表示されます。
スタンバイファームウェア	スタンバイ CMC にインストールされているファームウェアバージョンが表示されます。2 番目の CMC が取り付けられていない場合、このフィールドには <b>NA</b> (該当なし) が表示されます。
最終更新日	ファームウェアが最後に更新された日付を示します。更新されない場合、このフィールドには <b>NA</b> (該当なし) が表示されます。
ハードウェア	アクティブ CMC のハードウェアバージョンが表示されます。

表 5-14. クイックリンク – CMC

項目	説明
CMC ステータス	シャージコントローラ → プロパティ → ステータス に移動します。
ネットワーク	シャージコントローラ → ネットワーク → ネットワーク に移動します。
ファームウェアアップデート	シャージの概要 → アップデート → ファームウェアのアップデート に移動します。

表 5-15. iKVM の正常性とパフォーマンス

項目	説明
OSCAR コンソール	背面パネル VGA コネクタで CMC へのアクセスが有効かどうか（はいまたはいいえ）が表示されます。

表 5-16. iKVM プロパティ

項目	説明
名前	iKVM の名前を表示します。
パーツ番号	iKVM のパーツ番号を示します。パーツ番号は、ベンダーが提供する一意の識別子です。パーツ番号の命名規則はベンダーによって異なります。
ファームウェア	iKVM のファームウェアバージョンを表示します。
ハードウェア	iKVM のハードウェアバージョンを表示します。

表 5-17. クイックリンク – iKVM

項目	説明
iKVM ステータス	iKVM → プロパティ → ステータス に移動します。
ファームウェアアップデート	シャージの概要 → アップデート → ファームウェアのアップデート に移動します。

表 5-18. ファンの正常性とパフォーマンス

項目	説明
速度	ファンの速度を 1 分あたりの回転数（RPM）で示します。

表 5-19. ファンのプロパティ

項目	説明
重要な下限しきい値	この速度を下回ると、ファンが故障したと見なされます。
重要な上限しきい値	この速度を上回ると、ファンが故障したと見なされます。

表 5-20. クイックリンク-ファン

項目	説明
ファンステータス	<b>ファン</b> → <b>プロパティ</b> → <b>ステータス</b> に移動します。

表 5-21. PSU の正常性とパフォーマンス

項目	説明
電源ステータス	電源装置の電源ステータスを示します—初期化中、オンライン、スタンバイ、診断中、故障、アップデート中、オフラインまたは不明。

表 5-22. PSU プロパティ

項目	説明
容量	電源装置の容量（ワット単位）を示します。

表 5-23. クイックリンク- PSU

項目	説明
電源装置のステータス	<b>電源</b> → <b>プロパティ</b> → <b>ステータス</b> に移動します。
電力消費量	<b>シャーシの概要</b> → <b>電力</b> → <b>電力消費</b> に移動します。
システムのバジェット	<b>シャーシの概要</b> → <b>電力</b> → <b>バジェットステータス</b> に移動します。

表 5-24. LCD の正常性とパフォーマンス

項目	説明
LCD の正常性	LCD パネルの存在と正常性を示します。
シャーシの正常性	シャーシの正常性のテキストによる説明を示します。

LCD のクイックリンクはありません。

# システム正常性ステータスの監視

## シャーシとコンポーネント概要の表示

CMC はシャーシのグラフィック表示を **シャーシの正常性** ページに表示し、取り付けられたコンポーネントのステータスの概要を視覚的に提供します。**シャーシの正常性** ページは動的に更新され、現在の状況を反映するようにコンポーネントサブグラフィックの色およびテキストヒントも自動的に変更されます。

図 5-1. ウェブインタフェースにおけるシャーシグラフィックスの例



**シャーシの正常性** ページには、シャーシ、アクティブおよびスタンバイ CMC、サーバーモジュール、IO モジュール (IMO)、ファン、iKVM、電源装置 (PSU)、および LCD アセンブリの全体的な正常性ステータスが表示されます。各コンポーネントの詳細情報は、そのコンポーネントをクリックすると表示されます。シャーシおよびこのコンポーネントの概要を表示する手順については、383 ページの「シャーシサマリの表示」を参照してください。

## 電力バジェット状態の表示

**電力バジェットステータス** ページには、シャーシ、サーバー、およびシャーシ電源装置の電力バジェットのステータスが表示されます。

電力バジェットステータスを表示する手順については、306 ページの「消費電力ステータスの表示」を参照してください。CMC 電力管理の詳細については、285 ページの「電力管理」を参照してください。

## サーバー モデル名とサービス タグの表示

各サーバーのモデル名とサービス タグは、次の手順で簡単に入手することができます。

- システム ツリーで **サーバー** を展開します。展開されたサーバーリストにすべてのサーバー（0～16）が表示されます。サーバーなしのロットは名前がグレー表示されます。
- カーソルをサーバーのロット名またはロット番号の上に重ねると、ツールチップとしてサーバーのモデル名とサービス タグ番号が表示されます（存在する場合）。

## すべてのサーバーの正常性ステータスの表示

**シャーシの正常性** ページまたは **サーバーステータス** ページのシャーシの **シャーシグラフィックス** の項で、全サーバーの状態ステータスを表示できます。

シャーシグラフィックスには、シャーシに取り付けられた全サーバーが図で表示されます。

シャーシグラフィックスを使用してすべてのサーバーの正常性ステータスを表示するには：

- 1 CMC ウェブインタフェースにログインします。

**シャーシの正常性** ページが表示されます。**シャーシグラフィックス** の左のセクションには、シャーシの正面図と全サーバーの正常性ステータスが表示されます。サーバーの正常性ステータスは、サーバーサブグラフィックの色で示されます。

- 色なしサーバーが存在し、電源がオンで CMC と通信中。悪条件の兆候はありません。
- 橙色の警告サインー警告アラートが発せられているため、対応措置を取る必要があります。
- 赤色の X ー最低 1 つエラー条件が存在することを示します。CMC はまだコンポーネントと通信できますが、正常性ステータスに関する深刻な状態が報告されています。
- グレー表示ーコンポーネントが存在していますが、電源がオンではありません。CMC と通信しておらず、悪条件の兆候なし。

**サーバーステータス** ページには、シャーシ内のサーバーの概要が表示されます。サーバーステータスページで全サーバーの正常性ステータスを表示するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **サーバーの概要** を選択します。

**サーバーステータス** ページが表示されます。

表 5-25. すべてのサーバステータス情報


項目	説明		
スロット	サーバの場所を表示します。スロット番号はシャーシ内の場所に基づいてサーバを識別するシリアル番号です。		
名前	サーバ名を示します。サーバ名はデフォルトで <b>スロット名</b> (SLOT-01 ~ SLOT-16) によって識別されます。 <b>メモ:</b> デフォルトのサーバ名を変更できます。手順については、123 ページの「スロット名の編集」を参照してください。		
モデル	サーバのモデル名を表示します。このフィールドが空白の場合は、サーバは存在しません。このフィールドに # の拡張子 (ここで、# の値は 1 ~ 8) が表示された場合は、その番号 # がマルチスロットサーバの主なスロットになります。		
状態		OK	サーバが存在し CMC と通信していることを表示します。CMC とサーバ間で通信障害が発生した場合は、CMC はサーバの正常性ステータスを取得または表示できません。
		情報	正常性ステータス (OK、警告、重要) に変化がない場合に、サーバについての情報が表示されます。
		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。対応措置が取られない場合、サーバの整合性に影響を与える可能性がある深刻なエラーが生じる場合があります。
		重要	少なくとも 1 つの障害警告が発行されたことを示します。重要なステータスはサーバのシステムエラーを示し、直ちに対応処置を取る必要があります。
		値なし	サーバがスロットにない場合は、正常性情報は表示されません。

表 5-25. すべてのサーバステータス情報（続き）

項目	説明
リモートコンソールの起動	<p>クリックして、新しいブラウザまたはタブでサーバーのキーボード-ビデオ-マウス（KVM）セッションを起動します。このアイコンは、サーバーが次のすべての条件を満たした場合に限り表示されます。</p> <ul style="list-style-type: none"> <li>• iDRAC6 と iDRAC7 をサポートしている</li> <li>• シャーシの電源が入っている</li> <li>• サーバーの LAN インタフェースが有効である</li> <li>• iDRAC のバージョンが 2.20 以降</li> </ul> <p>この機能は、次の条件を満たした場合のみ、正常に動作します。</p> <ul style="list-style-type: none"> <li>• ホストシステムに JRE（Java Runtime Environment）6 アップデート 16 以降がインストールされている</li> <li>• ホストシステム上のブラウザで、ポップアップウィンドウが許可されている（ポップアップブロッキングが無効）</li> </ul>
iDRAC GUI の起動	<p>ボタンを左クリックして、新しいブラウザウィンドウまたはタブでサーバー用の iDRAC 管理コンソールを起動します。このアイコンは、サーバーが次のすべての条件を満たした場合に限り表示されます。</p> <ul style="list-style-type: none"> <li>• サーバーが存在する</li> <li>• シャーシの電源が入っている</li> <li>• サーバーの LAN インタフェースが有効である</li> </ul> <p>この機能は、次の条件を満たした場合のみ正常に動作します。</p> <ul style="list-style-type: none"> <li>• ホストシステム上のブラウザで、ポップアップウィンドウが許可されている（ポップアップブロッキングが無効）</li> </ul> <p><b>メモ：</b>サーバーがシャーシから取り外された、iDRAC の IP アドレスが変更された、または iDRAC のネットワーク接続に問題が発生した場合は、<b>iDRAC GUI の起動</b> アイコンをクリックすると、iDRAC LAN インタフェースのエラーページが表示される場合があります。</p>
電源状態	<p>サーバーの電源状態を表示します。</p> <ul style="list-style-type: none"> <li>• <b>該当なし</b> - CMC はサーバーの電源状況を特定していません。</li> <li>• <b>オフ</b> - サーバーまたはシャーシのどちらかの電源がオフです。</li> <li>• <b>オン</b> - シャーシおよびサーバーともに電源がオンです。</li> <li>• <b>電源投入中</b> - 電源オフおよび電源オンの間の一時的な状態です。操作が完了すると、<b>電源状態</b> は <b>オン</b> になります。</li> <li>• <b>電源切断中</b> - 電源オンおよび電源オフの間の一時的な状態です。操作が完了すると、<b>電源状態</b> は <b>オフ</b> になります。</li> </ul>
サーバスタグ	<p>サーバーのサーバスタグを表示します。サーバスタグは、サポートとメンテナンスのためにメーカーが提供する一意の識別子です。サーバーが不在の場合、このフィールドは空になります。</p>

iDRAC 管理コンソールを起動する方法およびシングル サインオンに関する詳細は、206 ページの「シングルサインオンを使って iDRAC を起動する」を参照してください。



## スロット名の編集

**スロット名** ページでは、シャーシのスロット名を更新できます。スロット名は個別のサーバーを識別するために使用します。スロット名を選択するとき、次のルールが適用されます。

- 名前には、非拡張 **ASCII** 文字 (ASCII コード 32 から 126 まで) を **最大 15 文字** 含めることができます。
- スロット名はシャーシ内で一意でなければなりません。複数のスロットに同じ名前を割り当てることはできません。
- スロット名では大文字と小文字は区別されません。Server-1、server-1、SERVER-1 はすべて同じ名前と見なされます。
- スロット名には、次の文字列で始まる名前を付けることはできません。
  - Switch-
  - Fan-
  - PS-
  - KVM
  - DRAC-
  - MC-
  - Chassis
  - Housing-Left
  - Housing-Right
  - Housing-Center
- Server-1 から Server-16 までの文字列を使用することはできますが、対応するスロットに割り当てる必要があります。たとえば、server-3 はスロット 3 では有効ですが、スロット 4 では無効です。ただし、Server-03 は、どのスロットに対しても有効な名前です。



**メモ:** スロット名の変更は、必ず **シャーシ設定管理者** の権限で行ってください。



**メモ:** ウェブインタフェースでのスロット名の設定は、CMC 内でのみ保存されています。サーバーがシャーシから取り外されても、スロット名の設定はスロットに残ります。



**メモ:** スロット名の設定は、オプションの iKVM に対応していません。スロット名の情報は、iKVM FRU から入手可能です。



**メモ:** CMC ウェブインタフェースで設定したスロット名の設定は、iDRAC インタフェースに表示されている名前の変更に常に優先します。

スロット名を編集するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーの **シャーシ** メニューで **サーバーの概要** を選択します。
- 3 **セットアップ** → **スロット名** をクリックします。  
スロット名 ページが表示されます。
- 4 **スロット名** フィールドにスロットの新しい名前を入力します。名前を変更する各スロットについてこの操作を繰り返し、**適用** をクリックします。
- 5 サーバーに対してデフォルトのスロット名（サーバーのスロット位置にに応じて **SLOT-01** ～ **SLOT-16**）に戻すには、**デフォルト値に戻す** を押します。

### サーバーのホスト名をスロット名として使用

**スロット名** ページでは、静的なスロット名をサーバーのホスト名（またはシステム名）で上書きできます。この操作には、サーバーに **OMSA** エージェントをインストールすることが必要です。**OMSA** エージェントの詳細については、『**Dell OpenManage Server Administrator ユーザーズガイド**』を参照してください。

サーバーのホスト名をスロット名として使用するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーの **シャーシ** メニューで、**サーバーの概要** を選択します。
- 3 **セットアップ** → **スロット名** をクリックします。  
スロット名 ページが表示されます。
- 4 **スロット名にホスト名を使用** を選択し、**適用** をクリックします。

### サーバーの第1 起動デバイスの設定

**最初の起動デバイス** ページでは、各サーバーの **CMC** の最初の起動デバイスを指定できます。これはサーバーの実際の最初の起動デバイスでなくてもよく、またそのサーバー上に存在するデバイスでなくてもかまいません。ここで指定するのは、**CMC** によってサーバーに送信されるデバイスであり、このデバイスはそのサーバーに対する最初の起動デバイスとして利用されます。

デフォルト起動デバイスを設定できるほか、**Diagnostics**（診断）の実行や **OS** の再インストールなどのタスクを実行するための特別なイメージから起動できるように、1 回限りの起動デバイスを設定することも可能です。

指定する起動デバイスは存在するもので、ブータブルメディアを含む必要があります。

表 5-26. 起動デバイス

起動デバイス	説明
PXE	ネットワークインタフェースカードの PXE（プレブート実行環境）プロトコルから起動します。
ハードディスクドライブ	サーバーのハードディスクドライブから起動します。
ローカル CD/DVD	サーバー上の CD/DVD ドライブから起動します。
仮想フロッピー	仮想フロッピードライブから起動します。フロッピードライブ（またはフロッピーディスクイメージ）は管理ネットワーク上の別のコンピュータ上にあり、iDRAC GUI コンソールビューアで接続されます。
仮想 CD/DVD	仮想 CD/DVD ドライブまたは CD/DVD ISO イメージから起動します。この光学ドライブまたは ISO イメージファイルは管理ネットワーク上の別のコンピュータまたはディスク上にあり、iDRAC GUI コンソールビューアで接続されます。
iSCSI	インターネット SCSI（小型コンピュータシステムインタフェース）から起動します。
ローカル SD カード	ローカル SD カードから起動します。（iDRAC6 および iDRAC7 システムをサポートするサーバーでのみ可能。）
フロッピー	ローカルのフロッピーディスクドライブにあるフロッピーディスクから起動します。
RFS	リモートファイル共有（RFS）イメージから起動します。イメージファイルは iDRAC GUI コンソールビューアで接続されます。



**メモ：**サーバーの第 1 起動デバイスを設定するには、**サーバー管理者** 特権または **シャーシ設定システム管理者** 特権、および **iDRAC ログイン特権** を持っている必要があります。

シャーシ内の一部またはすべてのサーバーの第 1 起動デバイスを設定するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーの **サーバーの概要** をクリックし、次に **設定** → **最初の起動デバイス** の順にクリックします。  
サーバーのリストが表示されます。
- 3 各サーバーに使用する起動デバイスをリストボックスから選択します。
- 4 選択した同じデバイスから毎回起動するようにサーバーを設定するには、そのサーバーの **ブートワンス** チェックボックスの選択を解除します。  
選択したデバイスから次回のみ起動するようにサーバーを設定するには、そのサーバーの **1 回限りの起動** チェックボックスを選択し、**適用** をクリックします。

## 個別のサーバーの正常性ステータスの表示

個々のサーバーの正常性ステータスは、2つの方法で表示することができます。1つは **シャーシの正常性** ページの **シャーシグラフィックス** セクション、もう1つは **サーバーステータス** ページです。

**シャーシの正常性** ページは、シャーシに取り付けられた個々のサーバーのグラフィック表示を提供します。

シャーシグラフィックスを使用して個々のサーバーの正常性ステータスを表示するには：

### 1 CMC ウェブインタフェースにログインします。

**シャーシの正常性** ページが表示されます。**シャーシグラフィックス** の上部セクションは、シャーシの正面図を表しており、個々のサーバーの正常性ステータスが表示されます。サーバーの正常性ステータスは、サーバーサブグラフィックの色で示されます。

- 色なしサーバーが存在し、電源が入り、CMC と通信していることを示します。悪条件の兆候はありません。
- 橙色の警告サイン—警告アラートが発せられているため、対応措置を取る必要があります。
- 赤色の X—最低1つエラー条件が存在することを示します。CMC は引き続きコンポーネントと通信できますが、正常性ステータスが重要として報告されていることを示します。
- グレー表示—コンポーネントが存在していますが、電源がオンではありません。CMC と通信しておらず、悪条件の兆候なし。

### 2 カーソルをそれぞれのサーバーのサブグラフィックに置きます。

対応するテキストのヒントまたはスクリーンのヒントが表示されます。テキストヒントは、対象サーバーに関する追加情報を提供します。

### 3 サーバーのサブグラフィックをクリックしてそのサーバーの情報を選択すると、シャーシのグラフィックスの右にクイックリンクが表示されます。

**サーバーステータス** ページ (**サーバーステータス** ページとは別) には、サーバーの概要、およびサーバーの管理に使用されるファームウェアである **Integrated Dell Remote Access Controller (iDRAC)** 用のウェブインタフェースの起動ポイントが表示されます。



**メモ** : iDRAC ユーザーインタフェースを使用するには、iDRAC ユーザー名とパスワードが必要です。iDRAC および iDRAC ウェブインタフェースの使い方の詳細は、『Integrated Dell Remote Access Controller ファームウェアのユーザーズガイド』を参照してください。

個々のサーバーの正常性ステータスを表示するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **サーバーの概要** を展開します。  
すべてのサーバー（1～16）が展開された **サーバー** リストに表示されます。
- 3 表示するサーバー（スロット）をクリックします。  
**サーバーステータス** ページが表示されます。

また、サーバーステータスのページは、ページの右側にあるサーバーのクイックリンクでステータスリンクをクリックして表示することができます。

表 5-27. 個別サーバーステータス - プロパティ













項目	説明															
スロット	シャーシでサーバーを装着するスロットを示します。スロット番号は 1～16（シャーシには使用できるスロットが 16 個あります）の連番 ID で、シャーシのサーバーの場所を識別します。															
スロット名	サーバーがあるスロットの名前を示します。															
存在	サーバーがスロットにあるかどうかを示します（ある、またはない）。サーバーが不在の場合、サーバーの正常性、電源状態、サービスタグ情報は不明です（表示されません）。															
状態	<table><tbody><tr><td></td><td>OK</td><td>サーバーが存在し CMC と通信していることを表示します。CMC とサーバー間で通信障害が発生した場合は、CMC はサーバーの正常性ステータスを取得または表示できません。</td></tr><tr><td></td><td>情報</td><td>正常性ステータス（OK、警告、重要）に変化がない場合に、サーバーについての情報が表示されます。</td></tr><tr><td></td><td>警告</td><td>警告アラートが発行されたこと、および対応処置を取る必要があることを示します。対応処置が取られない場合、サーバーの整合性に影響を与える可能性がある深刻なエラーが生じる場合があります。</td></tr><tr><td></td><td>重要</td><td>少なくとも 1 つの障害警告が発行されたことを示します。重要なステータスはサーバーのシステムエラーを示し、直ちに対応処置を取る必要があります。</td></tr><tr><td></td><td>値なし</td><td>サーバーがスロットにない場合は、正常性情報は表示されません。</td></tr></tbody></table>		OK	サーバーが存在し CMC と通信していることを表示します。CMC とサーバー間で通信障害が発生した場合は、CMC はサーバーの正常性ステータスを取得または表示できません。		情報	正常性ステータス（OK、警告、重要）に変化がない場合に、サーバーについての情報が表示されます。		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。対応処置が取られない場合、サーバーの整合性に影響を与える可能性がある深刻なエラーが生じる場合があります。		重要	少なくとも 1 つの障害警告が発行されたことを示します。重要なステータスはサーバーのシステムエラーを示し、直ちに対応処置を取る必要があります。		値なし	サーバーがスロットにない場合は、正常性情報は表示されません。
	OK	サーバーが存在し CMC と通信していることを表示します。CMC とサーバー間で通信障害が発生した場合は、CMC はサーバーの正常性ステータスを取得または表示できません。														
	情報	正常性ステータス（OK、警告、重要）に変化がない場合に、サーバーについての情報が表示されます。														
	警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。対応処置が取られない場合、サーバーの整合性に影響を与える可能性がある深刻なエラーが生じる場合があります。														
	重要	少なくとも 1 つの障害警告が発行されたことを示します。重要なステータスはサーバーのシステムエラーを示し、直ちに対応処置を取る必要があります。														
	値なし	サーバーがスロットにない場合は、正常性情報は表示されません。														
サーバーモデル	シャーシ内のサーバーのモデルを示します。例： <b>PowerEdge M600、PowerEdge M605</b> 。															

表 5-27. 個別サーバステータス - プロパティ (続き)

項目	説明
サービスタグ	サーバのサービスタグを表示します。サービスタグは、サポートとメンテナンス用にデルが提供する一意の識別子です。サーバが不在の場合、このフィールドは空になります。
iDRAC ファームウェア	現在サーバにインストールされている iDRAC のバージョンを表示します。
CPLD バージョン	サーバの Complex Programmable Logic Device (CPLD) のバージョン番号を表示します。
BIOS バージョン	サーバの BIOS バージョン を示します。
オペレーティングシステム	サーバのオペレーティングシステムを示します。
CPU 情報	サーバに取り付けられている CPU のタイプと数を示します。
システムメモリの総量	サーバに取り付けられているシステムメモリの総量 (GB) を示します。

表 5-28. 個別サーバステータス - iDRAC システムイベントログ






項目	説明
重大度	 OK 対応処置を必要としない正常なイベントを示します。
	 情報 重大度のステータスが変化していないイベントに関する情報のエントリを示します。
	 不明 不明 / 未分類のイベントを示します。
	 警告 システムエラーを防ぐために早めに対応処置を講じる必要のある非重要イベントを示します。
	 重要 システムエラーを防ぐために直ちに対応処置を講じる必要のある重要イベントを示します。
日時	イベントが発生した正確な日時を示します (例: Wed May 02 16:26:55 2007)。
説明	イベントの簡単な説明を示します。

表 5-29. 個別サーバステータス - iDRAC ネットワークの設定

項目	説明
LAN 有効	LAN チャンネルが有効（はい）と無効（いいえ）のどちらであることを示します。

表 5-30. 個別サーバステータス - IPv4 iDRAC ネットワークの設定

項目	説明
有効	IPv4 プロトコルが LAN 上で使用されている（はい）かどうかを示します。サーバーで IPv6 がサポートされていない場合、IPv4 プロトコルは常に有効になり、この設定は表示されません。
DHCP の有効	DHCP（動的ホスト設定プロトコル）が有効（はい）または無効（いいえ）のどちらであるかを示します。 このオプションが有効（はい）の場合、サーバーは IP 設定（IP アドレス、サブネットマスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。サーバーには常に、ネットワーク上で割り当てられた固有の IP アドレスがあります。
IPMI オーバー LAN を有効にする	IPMI LAN チャンネルが有効（はい）または無効（いいえ）のいずれかを示します。
IP アドレス	iDRAC ネットワーク インタフェースの IP アドレスを指定します。
サブネットマスク	iDRAC ネットワーク インタフェースのサブネットマスクを指定します。
ゲートウェイ	iDRAC ネットワーク インタフェースのゲートウェイを指定します。

表 5-31. 個別サーバステータス - IPv6 iDRAC ネットワークの設定

項目	説明
有効	IPv6 プロトコルが LAN 上で使用されている（はい）かどうかを示します。
自動設定の有効化	IPv6 の自動設定機能が有効（はい）であるかどうかを示します。 自動設定が有効である場合は、サーバーはネットワーク上の IPv6 ルータから IPv6 設定（IPv6 アドレス、プレフィックス長、IPv6 ゲートウェイ）を自動的に取得します。サーバーには常に、お使いのネットワーク上での固有の IPv6 アドレスがあり、最大 16 個の IPv6 アドレスを割り当てることができます。

表 5-31. 個別サーバステータス - IPv6 iDRAC ネットワークの設定 (続き)

項目	説明
リンクのローカルアドレス	CMC の MAC アドレスに基づいて CMC に割り当てられた IPv6 アドレスです。
ゲートウェイ	iDRAC ネットワークインタフェースの IPv6 ゲートウェイを表示します。
IPv6 アドレス	iDRAC ネットワークインタフェースの IPv6 アドレスを表示します。最大 16 のアドレスを表示できます。プレフィックス長はゼロ以外の場合は、前方スラッシュ (/) の後に指定されます。

表 5-32. 個別サーバ ステータス - WWN/MAC アドレス

項目	説明
スロット	シャーシでサーバが装着されているスロットを表示します。
場所	入出力モジュールが装着されている場所を表示します。グループ名 (A、B、または C) およびスロット番号 (1 または 2) の組み合わせで 6 箇所が識別されます。ロケーション名: A1、A2、B1、B2、C1、または C2
ファブリック	入出力ファブリックの種類を表示します。
サーバ指定	コントローラのハードウェアに埋め込まれたサーバ指定の WWN/MAC アドレスを表示します。「該当なし」と表示される WWN/MAC アドレスは、指定されたファブリックのインタフェースがインストールされていないことを示します。
シャーシ指定	特定のスロットで使用されるシャーシ指定の WWN/MAC アドレスを表示します。「該当なし」と表示される WWN/MAC アドレスは、FlexAddress 機能がインストールされていないことを示します。 <b>メモ:</b> <b>サーバ指定</b> または <b>シャーシ指定</b> のカラムの緑色のチェックマークは、アクティブなアドレスの種類を示します。 <b>メモ:</b> FlexAddress を有効にすると、サーバがインストールされていないスロットに、内蔵型 Ethernet コントローラ (ファブリック A) に対するシャーシ指定 MAC/WWN 割り当てを表示します。ファブリック B および C 用のシャーシ指定アドレスは、使用中のスロットのサーバでこれらのファブリックが使用されている場合を除き、該当なしと表示されます。これは、未使用のスロットに同じタイプのファブリックが導入されることを前提としています。

iDRAC 管理コンソールを起動する方法およびシングル サインオンに関する詳細は、206 ページの「シングルサインオンを使って iDRAC を起動する」を参照してください。



## IOM の正常性ステータスの表示

IOM の正常性ステータスは、2 つの方法で確認することができます。1 つは **シャーシの正常性** ページの **シャーシコンポーネントの概要** セクション、もう 1 つは **I/O モジュールステータス** ページです。**シャーシの正常性** ページには、シャーシに取り付けられた IOM の図の概要が表示されます。

シャーシグラフィックスを使用して IOM の正常性ステータスを閲覧するには：

### 1 CMC ウェブインタフェースにログインします。

**シャーシの正常性** ページが表示されます。**シャーシグラフィックス** の下方のセクションには、シャーシの背面図と IOM の正常性ステータスが表示されます。IOM の正常性ステータスは、IOM のサブグラフィックの色で示されます。

- 色なし – IOM が存在し、電源がオンで CMC と通信中。悪条件の兆候はありません。
- 橙色の警告サイン – 警告アラートが発せられているため、対応措置を取る必要があります。
- 赤色の X – 最低 1 つエラー条件が存在することを示します。CMC は引き続きコンポーネントと通信できますが、正常性ステータスが重要として報告されていることを示します。
- グレー表示 – IOM が存在していますが、電源がオンではありません。CMC と通信しておらず、悪条件の兆候なし。

### 2 カーソルをそれぞれの IOM のサブグラフィックに置きます。

テキストヒントまたはスクリーンのヒントが表示されます。テキストヒントは、IOM に関する追加情報を提供します。

### 3 IOM のサブグラフィックをクリックすると、その IOM の情報とクイックリンクがシャーシのグラフィックスの右側に表示されます。

**I/O モジュールステータス** ページには、シャーシに関連付けられているすべての IOM の概要が表示されます。ウェブインタフェースまたは RACADM を使って IOM の正常性を表示する手順は、356 ページの「IOM 状態の監視」を参照してください。

## ファンの正常性ステータスの表示



**メモ：**サーバーの CMC または iDRAC ファームウェアを更新中に、シャーシ内のファンの一部またはすべてが 100 パーセントの速度で回転します。これは正常な動作です。

ファンのサーバーの正常性ステータスは、2 つの方法で表示することができます。1 つは **シャーシの正常性** ページの **シャーシのコンポーネントの概要** セクション、もう 1 つは **ファンステータス** ページです。**シャーシの正常性** ページには、シャーシに取り付けられたファンの図が表示されます。

**シャーシグラフィックス**を使用してすべてのファンの正常性ステータスを表示するには：

**1** CMC ウェブインタフェースにログインします。

**シャーシの正常性** ページが表示されます。**シャーシグラフィックス** の下方のセクションには、シャーシの背面図とファンの正常性ステータスが表示されます。ファンの正常性ステータスは、ファンのサブグラフィックの色で示されます。

- 色なしファンが存在し、実行しています。悪条件の兆候はありません。
- 橙色の警告サインー警告アラートが発せられているため、対応措置を取る必要があります。
- 赤色の Xー最低 1 つエラー条件が存在することを示します。すなわち、正常性ステータスが重要であることが報告されています。
- グレー表示ファンが存在していますが、電源がオンではありません。悪条件の兆候は報告されていません。

**2** カーソルをそれぞれのファンのサブグラフィックに置きます。

テキストヒントまたはスクリーンのヒントが表示されます。テキストヒントは、対象ファンに関する追加情報を提供します。

- 3 ファンサブグラフィックをクリックして、そのファンの情報とクイックリンクがシャーシのグラフィックスの右側に表示されます。

**ファンステータス** ページには、シャーシ内のファンの状態と速度の測定値 (RPM) が表示されます。ファンは 1 台または複数台です。

ファンの速度を調整する **CMC** は、システム全体のイベントに基づいてファンの速度を自動的に増減します。次のイベントが起きた場合、**CMC** は警告を生成し、ファン速度を上げます。

- **CMC** の周辺温度がしきい値を超えた。
- ファンが故障した。
- シャーシからファンが取り外された。


ファン装置の正常性ステータスを表示するには：

- 1 **CMC** ウェブインタフェースにログインします。
- 2 システムツリーで **ファン** を選択します。

**サーバーステータス** ページが表示されます。

また、ページの右側にあるファン情報のクイックリンクでステータスリンクをクリックしても、**ファンステータス** が表示されます。

**表 5-33. ファンの正常性ステータスの情報**

項目	説明	
名前	ファンの名前を <b>FAN-n</b> 形式で表示します ( <i>n</i> はファンの番号)。	
存在	ファン装置が存在するかどうかを示します ( <b>はい</b> または <b>いいえ</b> )。	
状態	 <b>OK</b>	ファン装置が存在し <b>CMC</b> と通信していることを示します。 <b>CMC</b> とファン装置間で通信障害が発生した場合は、 <b>CMC</b> はサーバーの正常性ステータスを取得または表示できません。
	 <b>重要</b>	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。重要ステータスとは、ファンユニット上のシステムの障害を示し、過熱やシステムのシャットダウンを避けるために直ちに対応処置を取る必要があることを示します。
	 <b>不明</b>	シャーシが最初に電源が入ったときに表示されます。 <b>CMC</b> とファン装置間で通信障害が発生した場合は、 <b>CMC</b> はサーバーの正常性ステータスを取得または表示できません。
速度	ファン内の速度を <b>RPM</b> で表示します。	

## iKVM ステータスの表示

Dell M1000e サーバシャーシのローカルアクセス KVM モジュールは Avocent 内蔵 KVM スイッチモジュールまたは iKVM と呼ばれます。シャーシに関連付けられた iKVM の正常性ステータスは、**シャーシの正常性** ページで閲覧できます。

**シャーシグラフィックス** を使用して iKVM の正常性ステータスを表示するには

- 1 CMC ウェブインタフェースにログインします。

**シャーシの正常性** ページが表示されます。**シャーシグラフィックス** の下方のセクションには、シャーシの背面図と iKVM の正常性ステータスが表示されます。iKVM の正常性ステータスは、iKVM サブグラフィックの色で示されます。

- 色なし - iKVM が存在し、電源がオンで CMC と通信中。悪条件の兆候はありません。
- 橙色の警告サイン - 警告アラートが発せられているため、対応措置を取る必要があります。
- 赤色の X - 最低 1 つエラー条件が存在することを示します。CMC は引き続き iKVM と通信できますが、正常性ステータスが重要として報告されていることを示します。
- グレー表示 - iKVM が存在していますが、電源がオンではありません。CMC と通信しておらず、悪条件の兆候なし。

- 2 カーソルを iKVM のサブグラフィックに置きます。

テキストヒントまたはスクリーンのヒントが表示されます。テキストヒントは、対象の iKVM に関する追加情報を提供します。

- 3 iKVM のサブグラフィックをクリックすると、その iKVM の情報とクイックリンクがシャーシのグラフィックスの右側に表示されます。

また、ページの右側にある iKVM 情報のクイックリンクでステータスリンクをクリックしても、**iKVM ステータス** が表示されます。

iKVM ステータスの表示と iKVM のプロパティの設定手順については、次を参照してください。

- 346 ページの「iKVM のステータスとプロパティの表示」
- 345 ページの「フロントパネルの有効または無効」
- 346 ページの「iKVM を介した Dell CMC コンソールの有効化」
- 348 ページの「iKVM ファームウェアのアップデート」

iKVM の詳細については、327 ページの「iKVM モジュールの使用」を参照してください。

## PSU の正常性ステータスの表示

シャーシに関連付けられた PSU の正常性ステータスは、**シャーシの正常性** ページの **シャーシのコンポーネントの概要** セクションと **電源装置ステータス** ページに表示できます。**シャーシ正常性** ページは、シャーシに取り付けられたすべての PSU のグラフィック表示を提供します。

**シャーシグラフィックス** を使用してすべての PSU の正常性ステータスを表示するには：

- 1 CMC ウェブインタフェースにログインします。

**シャーシの正常性** ページが表示されます。**シャーシグラフィックス** の下側のセクションにはシャーシの背面図が描写され、すべての PSU の正常性ステータスが表示されます。PSU の正常性ステータスは、PSU サブグラフィックの色で示されます。

- 色なし – PSU が存在し、電源がオンで CMC と通信中。悪条件の兆候はありません。
- 橙色の警告サイン – 警告アラートが発せられているため、対応措置を取る必要があります。
- 赤色の X – 最低 1 つエラー条件が存在することを示します。CMC は引き続き PSU と通信できますが、正常性ステータスが重要として報告されていることを示します。
- グレー表示 – PSU が存在してはいますが、電源がオンではありません。CMC と通信しておらず、悪条件の兆候なし。

- 2 それぞれの PSU のサブグラフィックにマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象 PSU に関する追加情報を提供します。

- 3 PSU のサブグラフィックをクリックすると、その PSU の情報とクイックリンクがシャーシのグラフィックスの右側に表示されます

**電源装置ステータス** ページには、シャーシに関連付けられている PSU の状態が表示されます。CMC 電力管理の詳細については、285 ページの「電力管理」を参照してください。

PSU の正常性ステータスを表示するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **電源装置** を選択します。

**電源装置ステータス** ページが表示されます。

また、シャーシグラフィックスの右側の PSU クイックリンクのステータスリンクをクリックすることで、**PSU ステータス** ページを表示できます。

表 5-34. 電源装置の正常性ステータスの情報




項目	説明
名前	PSU の名前 <i>PS-n</i> が表示されます。ここで <i>n</i> は電源装置番号です。
存在	電源装置 が存在するかどうかを示します ( <b>はい</b> または <b>いいえ</b> )。
状態	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  </div> <div> <p><b>OK</b></p> <p>PSU が存在し、CMC と通信を行っていることを示します。PSU の正常性が <b>OK</b> であることを示します。CMC とファン装置間で通信障害が発生した場合は、CMC は PSU の正常性ステータスを取得または表示できません。</p> </div> </div>
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  </div> <div> <p><b>重要</b></p> <p>PSU が故障しており、正常性が深刻な状態にあることを示します。<b>速やかな対応処置が必要です</b>。早急に対応処置を行わないと、電源喪失によりコンポーネントはシャットダウンしてしまう可能性があります。</p> </div> </div>
	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  </div> <div> <p><b>不明</b></p> <p>シャージが最初に電源が入ったときに表示されます。CMC と PSU 間で通信障害が発生した場合は、CMC は PSU の正常性ステータスを取得または表示できません。</p> </div> </div>
電源ステータス	PSU の電源ステータス ( <b>オンライン</b> 、 <b>オフ</b> 、または <b>スロットが空</b> ) が表示されます。
容量	電源容量がワット単位で表示されます。

表 5-35. システム電源の状態

項目	説明
全体的な電源正常性	シャージ全体の電源管理の正常性ステータス ( <b>OK</b> 、 <b>非重要</b> 、 <b>重要</b> 、 <b>回復不可</b> 、 <b>その他</b> 、 <b>不明</b> ) を示します。
システム電源の状態	シャージの電源状態 ( <b>オン</b> 、 <b>オフ</b> 、 <b>電源オン</b> 、 <b>電源オフ</b> ) を示します。
冗長性	<p>電源装置冗長性のステータスを示します。有効値は次のとおりです。</p> <p><b>いいえ</b>：電源装置は非冗長です。</p> <p><b>はい</b>：完全冗長化されています。</p>

## 温度センサのステータスの表示

温度センサーステータス ページでは、シャーシ全体（シャーシとサーバー）の温度プローブのステータスと値が表示されます。















**メモ:** 温度プローブ値は編集できません。しきい値を超える変化にはすべて、ファン速度を変化させる警告が生成されます。たとえば、CMC 周囲温度プローブがしきい値を超えると、シャーシ内のファンの速度が上昇します。

温度プローブの正常性ステータスを表示するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **温度センサー** を選択します。  
**温度センサーのステータス** ページが表示されます。

表 5-36. 温度センサーの正常性ステータスの情報

項目	説明												
ID	温度プローブの場所が表示されます。												
Name (名前)	シャーシとサーバー用の各温度プローブの名前が表示されます。												
存在	モジュールがシャーシ内に存在する (はい) か、存在しない (いいえ) かを示します。												
状態	<table border="0"><tr><td></td><td><b>OK</b></td><td>モジュールが存在し、CMC と通信を行っていることを示します。CMC とサーバー間で通信障害が発生した場合は、CMC はサーバーの正常性ステータスを取得または表示できません。</td></tr><tr><td></td><td><b>警告</b></td><td>警告アラートのみが発行されたこと、および対応処置を取る必要があることを示します。対応処置が取られない場合、サーバーの整合性に影響を与える可能性がある重要または重大なエラーが生じる場合があります。</td></tr><tr><td></td><td><b>重要</b></td><td>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。重要なステータスはモジュールのシステムエラーを示し、直ちに対応処置を取る必要があります。</td></tr><tr><td></td><td><b>不明</b></td><td>モジュールとの通信が確立されていないことを示します。シャーシがオフまたはシャーシが初期化を完了していないため、この状態は普通です。</td></tr></table>		<b>OK</b>	モジュールが存在し、CMC と通信を行っていることを示します。CMC とサーバー間で通信障害が発生した場合は、CMC はサーバーの正常性ステータスを取得または表示できません。		<b>警告</b>	警告アラートのみが発行されたこと、および対応処置を取る必要があることを示します。対応処置が取られない場合、サーバーの整合性に影響を与える可能性がある重要または重大なエラーが生じる場合があります。		<b>重要</b>	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。重要なステータスはモジュールのシステムエラーを示し、直ちに対応処置を取る必要があります。		<b>不明</b>	モジュールとの通信が確立されていないことを示します。シャーシがオフまたはシャーシが初期化を完了していないため、この状態は普通です。
	<b>OK</b>	モジュールが存在し、CMC と通信を行っていることを示します。CMC とサーバー間で通信障害が発生した場合は、CMC はサーバーの正常性ステータスを取得または表示できません。											
	<b>警告</b>	警告アラートのみが発行されたこと、および対応処置を取る必要があることを示します。対応処置が取られない場合、サーバーの整合性に影響を与える可能性がある重要または重大なエラーが生じる場合があります。											
	<b>重要</b>	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。重要なステータスはモジュールのシステムエラーを示し、直ちに対応処置を取る必要があります。											
	<b>不明</b>	モジュールとの通信が確立されていないことを示します。シャーシがオフまたはシャーシが初期化を完了していないため、この状態は普通です。											
読み取り値	現在の温度を摂氏 (°C) および華氏 (°F) で示します。												
最大しきい値	エラーアラートが発行される最高温度を (°C) および華氏 (°F) で示します。												

## LCD ステータスの表示

LCD ステータスは、**シャーシの正常性** ページでシャーシに関連した図を使用して表示できます。

LCD の正常性ステータスを表示するには：

- 1 CMC ウェブインタフェースにログインします。  
**シャーシの正常性** ページが表示されます。シャーシグラフィックの情報のセクションでは、シャーシの正面図が表示されます。LCD の正常性ステータスは、LCD のサブグラフィックの色で示されます。
  - 色なし - LCD が存在し、電源がオンであり、CMC と通信中であることを示します。悪条件の兆候はありません。
  - 橙色の警告サイン - 警告アラートが発せられているため、対応措置を取る必要があります。
  - 赤色の X - 最低 1 つエラー条件が存在することを示します。正常性ステータスは重要です。
  - グレー表示 - LCD が存在していますが、電源がオンではありません。CMC と通信しておらず、悪条件はありません。
- 2 カーソルを LCD のサブグラフィックに移動します。対応するテキストのヒントまたはスクリーンのヒントに、LCD の追加情報が表示されます。
- 3 LCD サブグラフィックをクリックし、LCD 情報を選択すると、シャーシの図の右側に表示されます。

## ワールドワイドネーム / メディアアクセスコントロール (WWN/MAC) ID の表示

**WWN/MAC サマリ** ページは、シャーシ内のスロットの WWN 設定および MAC アドレスを表示します。

### ファブリック構成

**ファブリック構成** セクションでは、ファブリック A、ファブリック B およびファブリック C に取り付けられた入力 / 出力ファイブリックの種類が表示されます。緑色のチェックマークは、ファブリックが **FlexAddress** が有効になっていることを示します。**FlexAddress** 機能は、シャーシ指定およびスロット固定の WWN/MAC アドレスをシャーシ内のさまざまなファイブリックおよびスロットに展開するために使用します。この機能は、ファブリックおよびスロットごとに有効にすることができます。



**メモ** : FlexAddress 機能の詳細については、223 ページの「FlexAddress の使用」を参照してください。



## WWN/MAC アドレス

**WWN/MAC アドレス** の部分は、サーバスロットが現在空の状態の場合でも、全サーバに割当てられた **WWN/MAC** の情報を表示します。**位置** は、I/O モジュールが取り付けられたスロットの位置を表示します。6 つのスロットがグループ名 (A、B または C) およびスロット番号 (1 または 2) の組み合わせで識別され、A1、A2、B1、B2、C1 または C2 のスロット名で示されます。iDRAC はサーバの統合管理コントローラです。**ファブリック** では、I/O ファブリックの種類が表示されます。**サーバ指定** は、コントローラのハードウェアに埋め込まれたサーバ指定の **WWN/MAC** アドレスを表示します。**シャーシ指定** は、特定のスロットで使用されるシャーシ指定の **WWN/MAC** アドレスを表示します。**サーバ指定** または **シャーシ指定** のカラムの緑色のチェックマークは、アクティブなアドレスの種類を示します。シャーシ指定アドレスは、シャーシの FlexAddress が有効でスロット持続アドレスを示す場合に割当てられます。シャーシ指定アドレスが選択されている場合は、サーバが別のサーバと交換された場合でもそのアドレスが使用されます。

## CMC ネットワークプロパティの設定



**メモ** : ネットワーク設定を変更すると、現在のネットワークにログインするときに接続が失われる場合があります。

### CMC への初期アクセスのセットアップ


CMC の設定を始める前に、まず CMC ネットワーク設定を指定し、CMC がリモート管理できるようにする必要があります。この初期設定によって、CMC へのアクセスを可能にする TCP/IP ネットワークパラメータが割り当てられます。





**メモ** : CMC ネットワーク設定を指定するには、**シャーシ設定システム管理者** の権限が必要です。

- 1 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 **シャーシの概要** を選択します。
- 3 **ネットワーク** タブをクリックします。  
**ネットワーク設定** ページが表示されます。
- 4 **DHCP を使用 (CMC ネットワークインタフェース IP アドレス用)** チェックボックスをオンまたはオフにすることで、CMC の DHCP を有効または無効にします。
- 5 DHCP を無効にした場合は、IP アドレス、ゲートウェイ、サブネットマスクを入力します。
- 6 ページの下部の **変更の適用** をクリックします。

## ネットワーク LAN の設定

 **メモ** : CMC ネットワーク設定を指定するには、**シャーシ設定システム管理者** の権限が必要です。

 **メモ** : コミュニティ文字列や SMTP サーバー IP アドレスなどの **ネットワーク設定** ページ上の設定は、シャーシの外部設定と CMC の両方に影響します。

 **メモ** : シャーシに 2 つの CMC (アクティブとスタンバイ) があり、両方ともネットワークに接続していると、アクティブ CMC が故障した場合にスタンバイ CMC が自動的にそのネットワーク設定を引き継ぎます。

ネットワーク LAN の設定には、次の手順を実行します。

- 1 ウェブインタフェースにログインします。
- 2 **ネットワーク** タブをクリックします。
- 3 表 5-37 ~ 表 5-39 で説明されている CMC ネットワーク設定を設定、**変更を適用** をクリックします。

IP 範囲および IP ブロック設定を設定するには、**詳細設定** ボタンをクリックします (146 ページの「**CMC ネットワークセキュリティの設定**」を参照)。

**ネットワーク設定** ページの内容を更新するには、**更新** をクリックします。

**ネットワーク設定** ページの内容を印刷するには、**印刷** をクリックします。

表 5-37. ネットワークの設定

設定	説明
<b>CMC MAC アドレス</b>	シャーシの MAC アドレスを表示します。これはネットワーク上でこのシャーシを識別する一意の ID です。
<b>CMC ネットワーク インタフェースの 有効化</b>	<p>CMC のネットワークインタフェースを有効にします。</p> <p><b>デフォルト:</b> 有効 このオプションがオンの場合</p> <ul style="list-style-type: none"> <li>• CMC はコンピュータネットワークと通信し、ネットワーク経由でアクセスできます。</li> <li>• ウェブインタフェース、CLI (リモート RACADM)、WSMAN、Telnet、および、CMC に関連付けられた SSH が使用可能です。</li> </ul> <p>このオプションがオフの場合</p> <ul style="list-style-type: none"> <li>• CMC ネットワークインタフェースは、ネットワーク経由で通信できません。</li> <li>• CMC からシャーシへの通信はできません。</li> <li>• ウェブインタフェース、CLI (リモート RACADM)、WSMAN、Telnet、および CMC に関連付けられた SSH は使用できません。</li> <li>• サーバー iDRAC ウェブインタフェース、ローカル CLI、I/O モジュール、iKVM は通常どおり使用可能です。</li> <li>• iDRAC6 と CMC のネットワークアドレスを取得できます。この場合は、シャーシの LCD から取得します。</li> </ul> <p><b>メモ:</b> シャーシ内の他のネットワークアクセス可能なコンポーネントへのアクセスは、シャーシ上のネットワークが無効になった(または失われた)場合でも影響はありません。</p>
<b>DNS への CMC の 登録</b>	<p>このプロパティは DNS サーバーに CMC 名を登録します。</p> <p><b>デフォルト:</b> デフォルトでオフ (無効)</p> <p><b>メモ:</b> 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。指定する名前が DNS で要求される上限以下であることを確認してください。</p>
<b>DNS の CMC 名</b>	<p><b>DNS への CMC の登録</b> を選択している場合にのみ CMC 名が表示されます。デフォルトの CMC 名は <code>CMC_service_tag</code> で、<code>service_tag</code> はシャーシのサービスタグ番号です。例: <code>CMC-00002</code>。最大文字数は 63 文字です。最初の文字は英字 (a-z、A-Z) で、英数字 (a-z、A-Z、0-9) またはハイフン (-) が続く必要があります。</p>
<b>DNS ドメイン名に DHCP を使用</b>	<p>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は、<b>DHCP を使用 (NIC IP アドレス用)</b> が選択されている場合にのみ使用できます。</p> <p><b>デフォルト:</b> 有効</p>

表 5-37. ネットワークの設定（続き）

設定	説明
DNS ドメイン名	<p>デフォルトの DNS ドメイン名は空白になっています。このフィールドは、<b>DNS ドメイン名の DHCP を使用</b>のチェックボックスが選択されている場合にのみ編集可能です。</p>
オートネゴシエーション (1 Gb)	<p>CMC が一番近くのルーターまたはスイッチと通信して、二重モードとネットワーク速度を自動設定するか (<b>オン</b>)、手動で二重モードとネットワーク速度を設定できるようにするかを決定します (<b>オフ</b>)。</p> <p><b>デフォルト</b>：オン</p> <p><b>オートネゴシエーションがオンの場合は</b>、CMC が自動的に最も近いルーターと通信するか、または 1 Gb の速度に切り替わり実行されます。</p> <p><b>オートネゴシエーションがオフの場合は</b>、二重モードとネットワーク速度を手動で設定する必要があります。</p>
ネットワーク速度	<p>使用しているネットワーク環境に応じて、ネットワーク速度を 100 Mbps、または 10 Mbps に設定します。</p> <p><b>メモ</b>：ネットワークのスループットを効果的にするには、ネットワーク速度 の設定をネットワーク設定に合わせる必要があります。ネットワーク速度 をネットワーク設定の速度より下げると、帯域幅の消費が増えてネットワーク通信が遅くなります。<b>使用しているネットワークがネットワーク速度を超える速度をサポートしているかどうかを判断し、それに従って設定してください。</b> ネットワーク設定がこれらの値のどれにも一致しない場合は、<b>オートネゴシエーション</b> を使用するか、ネットワーク装置のメーカーに問い合わせてください。</p> <p><b>メモ</b>：1000 Mb または 1 Gb の速度にするには、<b>オートネゴシエーション</b> を選択します。</p>
二重モード	<p>ネットワーク環境に応じて、二重モードを全二重または半二重に設定します。</p> <p><b>意味</b>：<b>オートネゴシエーション</b> が 1 つのデバイスに対してオンになっているが、他のデバイスではオフであるような場合、オートネゴシエーションを使用しているデバイスは他のデバイスのネットワーク速度を判別できませんが、二重モードは判別できません。この場合、オートネゴシエーション時に、二重モードはデフォルトで半二重になります。このような二重モードの不一致は、ネットワーク接続が減速する原因となります。</p> <p><b>メモ</b>：ネットワーク速度と二重モードの設定は、オートネゴシエーション が オン に設定されている場合は使用できません。</p>

表 5-37. ネットワークの設定（続き）

設定	説明
<b>MTU</b>	<p>最大伝送単位（MTU）のサイズまたはインタフェースを通して渡すことのできる最大のパケットサイズを設定します。</p> <p><b>設定範囲</b>：576～1500</p> <p><b>デフォルト</b>：1500</p> <p><b>メモ</b>：IPv6 では最低 1280 の MTU が必要です。IPv6 が有効で、<b>cfgNetTuningMtu</b> の値がこれよりも低い値に設定されている場合、CMC は 1280 の MTU を使用します。</p>

表 5-38. IPv4 設定

設定	説明
<b>IPv4 を有効にする</b>	<p>CMC が IPv4 プロトコルを使ってネットワーク上で通信できるようにします。このボックスをクリアしても、IPv6 ネットワークの導入が阻止されることはありません。</p> <p>デフォルト：オン（有効）</p>
<b>DHCP 有効</b>	<p>CMC が IPv4 動的ホスト構成プロトコル（DHCP）サーバーから自動的に IP アドレスを要求して取得できるようになります。</p> <p>デフォルト：オン（有効）</p> <p>このオプションがオンの場合、CMC は IPv4 設定（IP アドレス、サブネットマスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。CMC には常に、ネットワーク上で割り当てられた固有の IP アドレスがあります。</p> <p><b>メモ</b>：この機能を有効にすると、<b>静的 IP アドレス</b>、<b>静的サブネットマスク</b>、<b>静的ゲートウェイ</b> の各プロパティフィールド（<b>ネットワーク設定</b> ページ上の このオプションに隣接）は無効になり、これらのプロパティに前回入力した値は無視されます。</p> <p>このオプションがオンでない場合は、<b>ネットワーク設定</b> ページ上の このオプションのすぐなりにあるテキストフィールドに <b>静的 IP アドレス</b>、<b>静的サブネットマスク</b>、<b>静的ゲートウェイ</b> を手動で入力する必要があります。</p>
<b>静的 IP アドレス</b>	CMC NIC の IPv4 アドレスを指定します。
<b>静的サブネットマスク</b>	CMC NIC の静的 IPv4 サブネットマスクを指定します。

表 5-38. IPv4 設定 (続き)

設定	説明
静的ゲートウェイ	<p>CMC NIC の IPv4 ゲートウェイを指定します。</p> <p><b>メモ:</b> 静的 IP アドレス、静的サブネットマスク、静的ゲートウェイ の各フィールドは、DHCP 有効 (これらのフィールドの前にあるプロパティフィールド) が無効 (オフ) である場合にのみアクティブです。この場合、ネットワーク上で使用するには CMC の静的 IP アドレス、静的サブネットマスク、静的ゲートウェイを手動で入力する必要があります。</p> <p><b>メモ:</b> 静的 IP アドレス、静的サブネットマスク、静的ゲートウェイ の各フィールドは、シャーシデバイスのみに適応されます。これらのフィールドは、サーバーネットワーク、ローカルアクセス、I/O モジュール、iKVM など、シャーシソリューション内の他のネットワークアクセス可能なコンポーネントには影響しません。</p>
DHCP を使用して DNS サーバーアドレスを取得する	<p>静的設定ではなく、DHCP サーバーから一次と二次の DNS サーバーアドレスを取得します。</p> <p><b>デフォルト:</b> デフォルトでオン (有効)</p> <p><b>メモ:</b> DHCP を使用 (NIC IP アドレス用) が有効になっている場合は、DHCP を使用して DNS サーバーアドレスを取得する プロパティを有効にします。</p> <p>このオプションがオンの場合、CMC はネットワーク上の DHCP サーバーから自動的にその DNS IP アドレスを取得します。</p> <p><b>メモ:</b> このプロパティを有効にすると、静的優先 DNS サーバーと静的代替 DNS サーバーのプロパティフィールド (ネットワーク設定 ページ上のこのオプションの直後にある) は非アクティブになり、これらのプロパティに対してそれまでに入力された値はすべて無視されます。</p> <p>このオプションが <b>選択されていない場合</b>、CMC は静的優先 DNS サーバーと静的代替 DNS サーバーから DNS の IP アドレスを取得します。これらのサーバーのアドレスは、ネットワーク設定 ページ上のこのオプションの直後にあるテキストフィールドで指定します。</p>
静的優先 DNS サーバー	<p>優先 DNS サーバーの静的 IP アドレスを指定します。静的優先 DNS サーバーは、DHCP を使用して DNS サーバーアドレスを取得する が無効になっているときのみ組み込まれます。</p>
静的代替 DNS サーバー	<p>代替 DNS サーバーの静的 IP アドレスを指定します。静的代替 DNS サーバーは、DHCP を使用して DNS サーバーアドレスを取得する が無効になっているときのみ組み込まれます。代替 DNS サーバーがない場合は、0.0.0.0 の IP アドレスを入力してください。</p>


表 5-39. IPv6 の設定

設定	説明
<b>IPv6 を有効にする</b>	CMC が IPv6 プロトコルを使ってネットワーク上で通信できるようにします。このボックスをクリアしても、IPv4 ネットワークの導入が阻止されることはありません。デフォルト：チェック済み（有効）
<b>自動設定の有効化</b>	CMC が IPv6 関連のアドレスとゲートウェイ設定に関する情報を提供するように設定された IPv6 プロトコルを使用して、これらの情報を取得できるようにします。こうすることで、CMC はネットワーク上で一意の IPv6 アドレスを持ちます。 <b>デフォルト：</b> オン（有効） <b>メモ：</b> この機能を有効にすると、 <b>静的 IPv6 アドレス</b> 、 <b>静的プレフィックス長</b> 、 <b>静的ゲートウェイ</b> の各プロパティフィールド（ネットワーク設定ページ上のこのオプションに隣接）は無効になり、これらのプロパティに前回入力した値は無視されます。このオプションがオンでない場合は、ネットワーク設定ページ上のこのオプションに隣接するテキストフィールドに <b>静的 IPv6 アドレス</b> 、 <b>静的プレフィックス長</b> 、 <b>静的ゲートウェイ</b> を手動で入力する必要があります。
<b>静的 IPv6 アドレス</b>	自動設定が有効でない場合に、CMC NIC の IPv6 アドレスを指定します。
<b>静的プレフィックス長</b>	自動設定が有効でない場合に、CMC NIC の IPv6 プレフィックス長を指定します。
<b>静的ゲートウェイ</b>	自動設定が有効でない場合に、CMC NIC の静的 IPv6 ゲートウェイを指定します。 <b>メモ：</b> <b>静的 IPv6 アドレス</b> 、 <b>静的プレフィックス長</b> 、 <b>静的ゲートウェイ</b> の各フィールドは、 <b>自動設定の有効化</b> （これらのフィールドの前にあるプロパティフィールド）が無効（オフ）である場合にのみアクティブです。この場合、IPv6 で使用するには CMC の <b>静的 IPv6 アドレス</b> 、 <b>静的プレフィックス長</b> 、 <b>静的ゲートウェイ</b> を手動で入力する必要があります。 <b>メモ：</b> <b>静的 IPv6 アドレス</b> 、 <b>静的プレフィックス長</b> 、 <b>静的ゲートウェイ</b> の各フィールドは、シャーシデバイスだけに適用されます。これらのフィールドは、サーバーネットワーク、ローカルアクセス、I/O モジュール、iKVM など、シャーシソリューション内の他のネットワークアクセス可能なコンポーネントには影響しません。
<b>静的優先 DNS サーバー</b>	優先 DNS サーバーの静的 IPv6 アドレスを指定します。静的優先 DNS サーバーの項目を使用するのは、 <b>DHCP を使用して DNS サーバーアドレスを取得する</b> が無効またはオフになっている場合のみです。IPv4 および IPv6 設定エリアには、このサーバーの項目があります。

表 5-39. IPv6 の設定（続き）

設定	説明
静的代替 DNS サーバー	代替 DNS サーバーの静的 IPv6 アドレスを指定します。代替 DNS サーバーがない場合は、「::」の IPv6 アドレスを入力します。静的代替 DNS サーバーの項目を使用するのは、 <b>DHCP を使用して DNS サーバーアドレスを取得する</b> が無効またはオフになっている場合のみです。IPv4 および IPv6 設定エリアには、このサーバーの項目があります。

## CMC ネットワークセキュリティの設定

 **メモ**：次の手順を行うには、**シャーシ設定システム管理者** の権限が必要です。

CMC ネットワークセキュリティ設定を設定するには：

- 1 ウェブインタフェースにログインします。
- 2 **ネットワーク** タブをクリックします。  
**ネットワーク設定** ページが表示されます。
- 3 **詳細設定** ボタンをクリックします。  
**ネットワークセキュリティ** ページが表示されます。
- 4 CMC ネットワークセキュリティの設定  
表 5-40 に、**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。

 **メモ**：IP 範囲と IP ブロック設定は、IPv4 のみに適用可能です。



表 5-40. ネットワークセキュリティページの設定

設定	説明
<b>IP 範囲有効</b>	IP 範囲のチェック機能を有効にします。この設定により、CMC にアクセスできる IP アドレスの範囲を定義できます。
<b>IP 範囲のアドレス</b>	範囲チェック用のベース IP アドレスを指定します。
<b>IP 範囲のマスク</b>	<p>CMC にアクセスできる IP アドレス範囲を定義します。このプロセスは IP 範囲チェックと呼ばれます。</p> <p>IP 範囲チェックをでは、ユーザーが指定した範囲内の IP アドレスを持つクライアントまたは管理ステーションからのみ CMC にアクセスできるようになります。その他のログインはすべて拒否されます。</p> <p>たとえば、次のとおりです。</p> <p>IP 範囲マスク：255.255.255.0 (11111111.11111111.11111111.00000000)</p> <p>IP 範囲のアドレス：192.168.0.255 (11000000.10101000.00000000.11111111)</p> <p>上記により、IP アドレス範囲は、192.168.0 を含む任意のアドレス、つまり 192.168.0.0 ~ 192.168.0.255 の任意のアドレスになります。</p>
<b>IP ブロック有効</b>	IP アドレスのブロック機能を有効にします。これにより、あらかじめ選択された時間帯に特定の IP アドレスからのログイン失敗回数を制限します。
<b>IP ブロックエラーカウント</b>	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。
<b>IP ブロックのエラーウィンドウ</b>	IP ブロックのペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間枠を秒で指定します。
<b>IP ブロックのペナルティ時間</b>	<p>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。</p> <p><b>メモ：</b> IP ブロックのエラーカウント、IP ブロックのエラーウィンドウ、IP ブロックのペナルティ時間 フィールドは、IP ブロック有効 チェックボックス（これらのフィールドの前にあるプロパティフィールド）がオン（有効）の場合にのみアクティブです。この場合、IP ブロックのエラーカウント、IP ブロックのエラーウィンドウ、IP ブロックのペナルティ時間 プロパティを手動で入力する必要があります。</p>

5 適用 をクリックして設定を保存します。

ネットワークセキュリティ ページの内容を更新するには、**更新** をクリックします。ネットワークセキュリティ ページの内容を印刷するには、**印刷** をクリックします。

# VLAN の設定

VLAN を使用すると、複数の仮想 LAN が同じ物理ネットワーク上で共存でき、セキュリティやロード管理の目的でネットワークトラフィックを分離できます。VLAN 機能を有効にすると、各ネットワークパケットに VLAN タグが割り当てられます。VLAN を設定するには、次の手順を実行します。

- 1 ウェブインタフェースにログインします。
- 2 **ネットワーク** タブ → **VLAN** サブタブをクリックします。  
**VLAN タグ設定** ページが表示されます。VLAN タグはシャーシプロパティです。このタグは、コンポーネントを削除した後もシャーシに残ります。
- 3 CMC/iDRAC VLAN 設定を行います。

表 5-41 に、**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。

表 5-41. VLAN タグ設定

設定	説明
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1 ~ 16 (シャーシには使用できるスロットが 16 個あります) の連番 ID で、シャーシのサーバーの場所を識別します。
名前	各スロットのサーバー名を表示します。
有効	チェックボックスが選択されている場合は、VLAN を有効にします。VLAN はデフォルトで無効になっています。
優先度	フレームの優先順位レベルを示します。このレベルは、異なるタイプのトラフィック (音声、ビデオ、データ) の優先順位を決定するのに使用できます。有効な優先順位は 0 ~ 7 です。0 (デフォルト) は最も低い優先順位を示し、7 は最も高い優先順位です。
ID	VLAN ID を表示します。有効な VLAN ID は 1 ~ 4000 および 4021 ~ 4094 です。デフォルトの VLAN ID は 1 です。

- 4 **適用** をクリックして設定を保存します。

シャーシの概要 → **サーバー** → **設定** タブ → **VLAN** サブタブから、このページにアクセスすることもできます。

# CMC ユーザーの追加と設定

CMC を装備したシステムを管理し、そのセキュリティを維持するため、特定の管理者権限（または役割ベースの権限）を持つ固有のユーザーを作成します。セキュリティを強化するために、特定のシステムイベントが発生したときに特定のユーザーに電子メールで警告を送るように設定することもできます。

## ユーザータイプ

CMC ユーザーと iDRAC ユーザーの 2 つのユーザータイプがあります。CMC ユーザーは「シャールシユーザー」とも呼ばれます。また、iDRAC がサーバー上に介在するため、iDRAC ユーザーは「サーバーユーザー」とも呼ばれます。

CMC ユーザーは、ローカルユーザーまたはディレクトリサービスユーザーにすることができます。また、iDRAC ユーザーも、ローカルユーザーまたはディレクトリサービスユーザーにすることができます。

サーバーユーザーは CMC ユーザーとは独立して作成されるため、CMC ユーザーが **サーバー管理者権限** を持つ場合を除き、CMC ユーザーに与えられる権限はサーバー上の同じユーザーに自動的に転送されるわけではありません。つまり、CMC Active Directory ユーザーと iDRAC Active Directory ユーザーは、Active Directory ツリーの異なるブランチに位置することになります。ローカルサーバーユーザーを作成するには、ユーザー設定システム管理者は直接サーバーにログインする必要があります。ユーザー設定システム管理者は、CMC からサーバーユーザーまたはその逆を作成できません。このルールにより、サーバーのセキュリティと整合性は保護されます。

表 5-42. ユーザータイプ

権限	説明
<b>CMC ログインユーザー</b>	ユーザーは CMC にログインし、全 CMC データを表示できますが、データの追加や修正、またはコマンドの実行はできません。 ユーザーは、CMC ログインユーザー権限を持たずに他の権限を持つこともできます。この機能は、ユーザーが一時的にログインを禁止されている場合に便利です。そのユーザーの CMC ログインユーザー権限が復元した場合にも、その前に与えられていたその他のすべての権限を保持できます。

表 5-42. ユーザータイプ (続き)

権限	説明
シャーシ設定システム管理者	<p>ユーザーは、次のデータの追加や変更ができます。</p> <ul style="list-style-type: none"> <li>シャーシを識別する (シャーシ名やシャーシの位置など)</li> <li>シャーシに特別に割り当てられている (静的または DHCP IP モード、静的 IP アドレス、静的ゲートウェイ、静的サブネットマスクなど)</li> <li>シャーシにサービスを提供する (日時、ファームウェアアップデート、CMC リセットなど)</li> <li>シャーシに関連している (スロット名やスロットの優先順位など) これらのプロパティはサーバーに適用されますが、正確にはサーバーそのものではなくスロットに関連付けられるシャーシプロパティです。このため、スロット名とスロットの優先順位は、サーバーがスロットにあるなしに関係なく、追加または変更することができます。</li> </ul> <p>サーバーが別のシャーシに移動されると、サーバーは新しいシャーシのそのスロットに割り当てられているスロット名と優先順位を継承します。前のスロット名と優先順位はそのまま前のシャーシに残ります。</p> <p><b>メモ:</b> シャーシ設定システム管理者 権限を持つ CMC ユーザーが電源設定を行うことができます。ただし、シャーシの電源オン、電源オフ、パワーサイクルなどのシャーシ電源操作を行うには、<b>シャーシ制御システム管理者</b> 権限が必要です。</p>
ユーザー設定システム管理者	<p>ユーザーは次の操作ができます。</p> <ul style="list-style-type: none"> <li>新規ユーザーの追加。</li> <li>既存のユーザーの削除。</li> <li>ユーザーのパスワードの変更。</li> <li>ユーザー権限の変更。</li> <li>ユーザーのログイン権限を有効または無効にしますが、ユーザーの名前やデータベース内のその他の権限は保持されます。</li> </ul>
ログのクリアシステム管理者	<p>ユーザーはハードウェアログと CMC ログをクリアできます。</p>
シャーシ制御システム管理者 (電源コマンド)	<p><b>シャーシ電源システム管理者</b> の権限を持つ CMC ユーザーは、電源関連の操作をすべて行うことができます。電源オン、電源オフ、パワーサイクルなどのシャーシ電力操作を制御できます。</p> <p><b>メモ:</b> 電源設定を行うには、<b>シャーシ設定システム管理者</b> 権限が必要です。</p>

表 5-42. ユーザタイプ (続き)

権限	説明
<b>Server Administrator</b>	<p>これは、CMC ユーザーにシャース内に存在する任意のサーバー上の任意の操作を実行する全権利を与える包括的な権限です。</p> <p><b>CMC サーバー管理者</b> の権限を持つユーザーがサーバー上で実行するアクションを発行すると、CMC ファームウェアはサーバー上のユーザーの権限を確認せずに、コマンドを対象のサーバーに送信します。つまり、<b>CMC サーバー管理者</b> はサーバーにシステム管理者権限がない場合でも、それを無視してコマンドを送信できます。</p> <p><b>サーバー管理者</b> 権限がない場合、シャースで作成されたユーザーは次のすべての条件が満たされた場合にのみ、サーバー上でコマンドを実行することができます。</p> <ul style="list-style-type: none"> <li>• 同じユーザー名がサーバー上に存在する。</li> <li>• サーバー上の同じユーザー名は同じパスワードが所有する必要がある。</li> <li>• そのユーザーがコマンドを実行する権限を持っている。</li> </ul> <p><b>サーバー管理者</b> 権限のないユーザーがサーバー上で実行されるアクションを発行した場合、CMC は、対象となるサーバーに対してユーザーのログイン名とパスワードを伴うコマンドを送信します。ユーザーがサーバー上に存在しない、またはパスワードが一致しない場合は、ユーザーは操作を実行することができません。</p> <p>ユーザーが対象のサーバーに存在し、パスワードが一致する場合は、サーバーはサーバー上でユーザーに与えられた権限で応答します。CMC ファームウェアはサーバーから返された権限に基づいてユーザーが操作を実行する権利があるかどうかを判断します。</p>
	<p>次のリストに、<b>サーバー管理者</b>が持つサーバー上の権限と実行できる操作を示します。これらの権限は、シャースユーザーがシャース上のサーバーシステム管理者権限を持っていない場合にのみ適用されます。</p>

表 5-42. ユーザータイプ (続き)

権限	説明
サーバー管理者 (続き)	<p>サーバー設定システム管理者：</p> <ul style="list-style-type: none"> <li>• IP アドレスの設定</li> <li>• ゲートウェイの設定</li> <li>• サブネットマスクの設定</li> <li>• 最初の起動デバイスの設定</li> </ul> <p>ユーザーの設定</p> <ul style="list-style-type: none"> <li>• iDRAC ルートパスワードの設定</li> <li>• iDRAC のリセット</li> </ul> <p>サーバー制御システム管理者：</p> <ul style="list-style-type: none"> <li>• 電源オン</li> <li>• 電源オフ</li> <li>• パワーサイクル</li> <li>• 正常なシャットダウン</li> <li>• サーバーの再起動</li> </ul>
テストアラート ユーザー	ユーザーはテストアラートメッセージを送信できます。
コマンドのデバ ッグシステム管理者	ユーザーはシステム診断コマンドを実行できます。
ファブリック A システム管理者	ユーザーは、I/O スロットのスロット A1 またはスロット A2 に存在するファブリック A IOM を設定できます。
ファブリック B システム管理者	ユーザーは、I/O スロットのスロット B1 またはスロット B2 に存在するファブリック B IOM を設定できます。
ファブリック C システム管理者	ユーザーは、I/O スロットのスロット C1 またはスロット C2 に存在するファブリック C IOM を設定できます。
スーパーユーザー	ユーザーは CMC に対するルートアクセス権を持ち、 <b>ユーザー設定システム管理者</b> と <b>CMC ユーザーへのログイン</b> 権限を持っています。 <b>スーパーユーザー</b> 権限を持つユーザーのみが、新規または既存ユーザーの <b>デバッグコマンド管理者</b> と <b>スーパーユーザー</b> の権限を与えられます。

CMC ユーザーグループは、あらかじめ割り当てられたユーザー権限を持つ一連のユーザーグループを提供します。



**メモ**：システム管理者、パワーユーザー、またはゲストユーザーを選択してから、事前定義されている権限に新しい権限を追加したりいずれかの権限を削除したりすると、CMC グループは自動的に **カスタム** に変更されます。

表 5-43. CMC グループ権限

ユーザーグループ	与えられる権限
管理者	<ul style="list-style-type: none"> <li>• CMC ログインユーザー</li> <li>• シャーシ設定システム管理者</li> <li>• ユーザー設定システム管理者</li> <li>• ログのクリアシステム管理者</li> <li>• Server Administrator</li> <li>• テストアラートユーザー</li> <li>• コマンドのデバッグシステム管理者</li> <li>• ファブリック A システム管理者</li> <li>• ファブリック B システム管理者</li> <li>• ファブリック C システム管理者</li> </ul>
パワーユーザー	<ul style="list-style-type: none"> <li>• ログイン</li> <li>• ログのクリアシステム管理者</li> <li>• シャーシ制御システム管理者</li> <li>• Server Administrator</li> <li>• テストアラートユーザー</li> <li>• ファブリック A システム管理者</li> <li>• ファブリック B システム管理者</li> <li>• ファブリック C システム管理者</li> </ul>
ゲストユーザー	ログイン
カスタム	<p>次の権限を任意の組み合わせで選択します。</p> <ul style="list-style-type: none"> <li>• CMC ログインユーザー</li> <li>• シャーシ設定システム管理者</li> <li>• ユーザー設定システム管理者</li> <li>• ログのクリアシステム管理者</li> <li>• シャーシ制御システム管理者</li> <li>• スーパーユーザー</li> <li>• Server Administrator</li> <li>• テストアラートユーザー</li> <li>• コマンドのデバッグシステム管理者</li> <li>• ファブリック A システム管理者</li> <li>• ファブリック B システム管理者</li> <li>• ファブリック C システム管理者</li> </ul>
なし	権限の割り当てなし

表 5-44. CMC システム管理者、パワーユーザー、ゲストユーザー間の権限の比較

権限セット	システム管理者 のアクセス権	パワーユーザー アクセス権	ゲストユーザー アクセス権
CMC ログインユーザー	✓	✓	✓
シャーシ設定システム管理者	✓	✗	✗
ユーザー設定システム管理者	✓	✗	✗
ログのクリアシステム管理者	✓	✓	✗
シャーシ制御システム管理者	✓	✓	✗
スーパーユーザー	✓	✗	✗
Server Administrator	✓	✓	✗
テストアラートユーザー	✓	✓	✗
コマンドのデバッグシステム管理者	✓	✗	✗
ファブリック A システム管理者	✓	✓	✗
ファブリック B システム管理者	✓	✓	✗
ファブリック C システム管理者	✓	✓	✗



## ユーザーの追加と管理

ウェブインタフェースの **ユーザー** と **ユーザー設定** ページで、CMC ユーザーについての情報の表示、新しいユーザーの追加、既存のユーザーの設定の変更を行うことができます。

16 人までのローカルユーザーを設定できます。ユーザーを追加する必要があり、かつ Microsoft Active Directory または汎用 Lightweight Directory Access Protocol (LDAP) サービスを使用している場合、このアプリケーションを設定して CMC へのアクセスを提供します。このように Active Directory を設定することによって、16 のローカルユーザーに加えて、Active Directory ソフトウェアの既存のユーザーに CMC ユーザー権限を追加して制御できます。詳細については、243 ページの「CMC ディレクトリサービスの使用」を参照してください。LDAP の詳細については、「Lightweight Directory Access Protocol Services での CMC を使用」セクションを参照してください。

ユーザーは、ウェブインタフェース、Telnet シリアル、SSH、iKVM セッションからログインできます。最大 22 のアクティブセッション（ウェブインタフェース、Telnet シリアル、SSH、iKVM などの任意の組み合わせ）をユーザー間で分割できます。



**メモ:** セキュリティを強化するために、ルート（ユーザー 1）アカウントのデフォルトパスワードを変更することを強くお勧めします。ルートアカウントは、CMC 出荷時のデフォルトの管理者アカウントです。root アカウントのデフォルトパスワードを変更するには、**ユーザー ID 1** をクリックして **ユーザー設定** ページを開きます。そのページのヘルプには、ページの右上にある ヘルプ リンクからアクセスできます。

### CMC ユーザーの追加と設定



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

- 1 ウェブインタフェースにログインします。
- 2 **ユーザー認証** タブをクリックします。**ローカルユーザー** ページが開いて、ルートユーザーを含む各ユーザーのユーザー ID、ユーザー名、CMC 権限、ログイン状況が表示されます。設定に使用できるユーザー ID には、ユーザー情報が一切表示されません。
- 3 使用可能なユーザー ID 番号をクリックします。**ユーザー設定** ページが表示されます。  
**ユーザー** ページの内容を更新するには、**更新** をクリックします。**ユーザー** ページの内容を印刷するには、**印刷** をクリックします。
- 4 そのユーザーの一般設定を選択します。

表 5-45. では、新規または既存の CMC ユーザー名とパスワードを設定するための一般ユーザー設定について説明します

プロパティ	説明
<b>ユーザー ID</b> (読み取り専用)	CLI のスクリプト用に使用される 16 の事前設定された連番でユーザーを識別します。ユーザー ID は、CLI ツール (RACADM) を使用してユーザーを設定する際、特定のユーザーを識別するために使用します。ユーザー ID は編集できません。  ユーザールート情報を編集する場合、このフィールドは静的です。ルートのユーザー名は編集できません。
<b>ユーザーを有効にする</b>	CMC に対するユーザーのアクセスを有効または無効にします。
<b>ユーザー名</b>	ユーザーに関連付けられている一意の CMC ユーザー名の設定または表示を行います。ユーザー名には 16 文字まで使用できます。CMC ユーザー名には、前方スラッシュ (/) やピリオド (.) を含むことはできません。 <b>メモ:</b> ユーザー名を変更した場合、新しい名前は次のログインまでユーザーインターフェースに表示されません。新しいユーザー名を適用した後でログインするすべてのユーザーは、その変更をその場で確認できます。
<b>パスワードの変更</b>	既存のユーザーパスワードを変更できるようにします。 <b>新しいパスワード</b> フィールドで新しいパスワードを設定します。  新しいユーザーを設定している場合は、 <b>パスワードの変更</b> チェックボックスは選択できません。既存のユーザーの設定を変更する場合にはのみ選択できます。
<b>パスワード</b>	既存のユーザーの新しいパスワードを設定します。パスワードを変更する場合は、 <b>パスワードの変更</b> チェックボックスも選択する必要があります。パスワードは 20 文字まで指定でき、入力する際は各文字がドットで表示されます。
<b>パスワードの確認</b>	<b>新しいパスワード</b> フィールドに入力したパスワードを確認します。 <b>メモ:</b> <b>新しいパスワード</b> と <b>新しいパスワードの確認</b> フィールドは、(1) 新しいユーザーを設定するとき、または (2) 既存のユーザーの設定の編集を行うために <b>パスワードの変更</b> チェックボックスを選択したときにのみ編集可能です。

- 5 ユーザーを CMC ユーザーグループに割り当てます。表 5-42 は、CMC ユーザー権限について説明します。


CMC グループ ドロップダウンメニューからユーザー特権の設定を選択すると、そのグループについてあらかじめ定義された設定に従って、有効に設定された特権（リスト内のチェックボックスにチェックが入った状態）が表示されます。


各ユーザーの特権の設定は、チェックボックスのチェックを入れたり解除したりしてカスタマイズします。CMC グループを選択したり、またはカスタムユーザー特権の選択を行った後で、設定を保存するには **変更の適用** をクリックします。

**ユーザー設定** ページの内容を更新するには、**更新** をクリックします。

**ユーザー設定** ページの内容を印刷するには、**印刷** をクリックします。

## Microsoft Active Directory 証明書の設定と管理

 **メモ** : CMC に Active Directory を設定するには、**シャージ設定システム管理者** 権限が必要です。

 **メモ** : Active Directory 設定および、Active Directory を標準スキーマまたは拡張スキーマで設定する方法の詳細に関しては、243 ページの「CMC ディレクトリサービスの使用」を参照してください。

Microsoft Active Directory サービスを使用して、お使いのソフトウェアが CMC へのアクセスを提供するように設定できます。Active Directory サービスを使用すると、既存ユーザーの CMC ユーザー権限を追加したり管理することができます。

**Active Directory メインメニュー** ページにアクセスするには：

- 1 ウェブインタフェースにログインします。
- 2 **ユーザー認証** タブをクリックしてから、**ディレクトリサービス** サブタブをクリックします。
- 3 **Microsoft Active Directory の標準スキーマ** または **拡張スキーマ** のラジオボタンを選択します。**Active Directory** の表が表示されます。

## 共通設定

この項では、CMC 向けの Active Directory の共通設定を設定および表示することが可能です。

表 5-46. 共通設定

フィールド	説明
Active Directory を有効にする	CMC で Active Directory ログインを有効にします。同じ認証局が署名した Active Directory サーバーの SSL 証明書をインストールした後、それを CMC にアップロードする必要があります。
スマートカードログインの有効化	Dell が供給する自動インストールされたブラウザプラグインとスマートカードの使用により、Kerberos 認証に基づく Active Directory 相互使用を有効にします。スマートカードを有効にするには、チェックボックスを選択します。スマートカードを無効にするには、チェックボックスを選択解除します。スマートカードを有効にするには、Microsoft Windows Client Workstation を設定してスマートカードリーダーが正しく動作する必要があります。これには、使用中のスマートカードリーダーの適切なドライバと、実際に使用されるスマートカードの適切なドライバのインストールが含まれます。スマートカードドライバは、ベンダーごとに異なります。スマートカードは、適切な Active Directory Server により提供されるスマートカード登録サービスを使用して、必要な資格情報でプログラムする必要があります。 <b>メモ</b> ：スマートカードログインとシングルサインオンの選択は、相互に排他的です。一度に選択できるのは 1 つだけです。
シングルサインオンを有効にする	CMC が <b>Active Directory</b> を活用できるようにします。 <b>シングルサインオン</b> を有効にするには、チェックボックスを選択します。 <b>シングルサインオン</b> を無効にするには、チェックボックスを選択解除します。 <b>シングルサインオン</b> を有効にする場合、 <b>Active Directory</b> プロパティを設定し、使用するスキーマを選択する必要があります。 <b>メモ</b> ：スマートカードログインとシングルサインオンの選択は、相互に排他的です。一度に選択できるのは 1 つだけです。

表 5-46. 共通設定 (続き)

フィールド	説明
SSL 証明書検証を有効にする	<p>CMC の Active Directory SSL 接続のための SSL 証明書検証を有効にします。SSL 証明書検証を無効にするには、チェックボックスを選択解除します。</p> <p><b>注意：この機能を無効にすると、認証情報が中間者攻撃の危険に晒される可能性があります。</b></p> <p>ブラウザ操作では、CMC の完全修飾ドメインアドレスを含む HTTP URL (すなわち、<b>http://cmc-6g2wxf1.dom.net</b>) 経由で CMC にアクセスする必要があります。そのままの CMC の IP アドレスでは、適切なシングルサインオン操作ができません。完全修飾ドメインアドレスをサポートするには、Active Directory Server のドメイン名サービスで CMC を登録する必要があります。</p> <p>シングルサインオンのブラウザ認証ができない場合、通常のローカルまたは Active Directory のユーザー名 / パスワードによるブラウザ認証方式が自動的に表示されます。同様に、シングルサインオンした後のログアウト操作には、ユーザー名 / パスワード方式が表示されます。シングルサインオンの使用は、便宜上のみで制限するためではありません。</p> <p><b>メモ：</b>スマートカードベースのブラウザ認証は、Microsoft Windows Clients と Internet Explorer ブラウザのみをサポートしています。</p> <p>Dell が供給する自動ロードするブラウザログイン (ActiveX コントロール) は、ランタイムコンポーネント Microsoft Visual C++ 2005 再配布可能パッケージ (x86) があらかじめインストールされた Microsoft Windows Client オペレーティングシステムに依存します。コンポーネントを検索するには、次のリンクが役立ちます。</p> <p><b>microsoft.com/downloads/details.aspx?FamilyID=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&amp;displaylang=en</b>。Windows クライアントでは、ActiveX コントロールを正常にインストールするために <b>権限の昇格</b> が必要です。同様に、ブラウザでも「署名なし」の ActiveX コントロールのインストールを受け入れる設定が必要です。</p> <hr/> <p>スマートカードを有効にすると、ブラウザ認証を行うためにスマートカード専用ポリシーが実施されます。ブラウザ認証の他の方法、たとえば、ローカルまたは Active Directory のユーザー名 / パスワード認証は、禁止されています。スマートカードのみの使用ポリシーを採用する場合は、CMC に対する他のアクセス法を無効にする前に、スマートカードの操作の有効性を十分に確認することが重要です。確認を怠ると、CMC へのすべてのアクセスを誤ってロックしてしまう可能性があります。</p>

表 5-46. 共通設定 (続き)

フィールド	説明
ルートドメイン名	<p>Active Directory が使用するドメイン名を指定します。ルートドメイン名はフォレストの完全修飾ルートドメイン名です。</p> <p><b>メモ</b>：ルートドメイン名は x.y という命名規則に従った有効なドメイン名でなければなりません。この x は文字間に空白文字が入っていない 1 ~ 256 文字 ASCII 文字列、y は com、edu、gov、int、mil、net、org などの有効なドメインタイプで指定します。</p>
AD タイムアウト	<p>時間を秒単位で設定すると、Active Directory セッションが自動的に閉じます。</p> <p>有効値：15-300 秒</p> <p>デフォルト：90 秒</p>
検索する AD サーバーの指定 (オプション)	<p>(選択した場合、)ドメインコントローラとグローバルカタログ上の指示呼び出しを有効にします。このオプションを有効にする場合は、次の設定でドメインコントローラとグローバルカタログの場所も指定する必要があります。</p> <p><b>メモ</b>：Active Directory の CA 発行の証明書に記載された名前は、指定された Active Directory サーバーまたはグローバルカタログサーバーと照合されません。</p>
ドメインコントローラ	<p>Active Directory サービスのインストール先のサーバーを指定します。このオプションは、検索する AD サーバーの指定 (オプション) が有効である場合にのみ使用できます。</p>
グローバルカタログ	<p>Active Directory ドメインコントローラにおけるグローバルカタログの場所を指定します。グローバルカタログは Active Directory フォレストを検索するためのリソースを提供します。このオプションは、検索する AD サーバーの指定 (オプション) が有効である場合にのみ使用できます。</p>

## 標準スキーマ設定

Microsoft Active Directory (標準スキーマ) を選択した場合、標準スキーマの設定が表示されます。このセクションには、すでに設定されている役割グループと、それに関連する名前、ドメイン、および権限が表示されます。

役割グループの設定を変更するには、**役割グループ** リスト内の該当する役割グループのボタンをクリックします。



**メモ**：指定した新しい設定を適用する前に役割グループリンクをクリックすると、設定の内容が失われます。新しい設定を失うことのないように、役割グループリンクをクリックする前に **適用** をクリックしてください。

役割グループの設定 ページが表示されます。

- グループ名 - CMC カード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。
- グループのドメイン - グループが置かれているドメイン。
- グループ権限 - グループの権限レベル。

**適用** をクリックして設定を保存します。

**設定ページに戻る** をクリックすると、**ディレクトリサービス** ページに戻ります。

**ディレクトリサービス** ページの内容を更新するには、**更新** をクリックします。

**ディレクトリサービス** ページの内容を印刷するには、**印刷** をクリックします。

## 拡張スキーマの設定

**Microsoft Active Directory (拡張スキーマ)** を選択した場合、拡張スキーマ設定に次のプロパティが表示されます。

- **CMC デバイス名** - CMC に対して作成した RAC デバイスオブジェクト名が表示されます。CMC デバイス名は Active Directory で CMC カードを一意に識別します。CMC デバイス名は、ドメインコントローラで作成した新しい CMC オブジェクトのコモンネーム (CN) と同じでなければなりません。名前には空白を含まない 1 ~ 256 文字の ASCII 文字列を使用します。
- **CMC ドメイン名** - Active Directory の RAC デバイスオブジェクトが存在するドメインの DNS 名 (文字列) を表示します。名前は x.y からなる有効なドメイン名とします。ここで、x は空白を含まない 1 ~ 256 文字の ASCII 文字列で、y は com、edu、gov、int、mil、net、org などの有効なドメインタイプです。

## Active Directory 証明書の管理

この項では、最近 CMC にアップロードされた Active Directory 証明書のプロパティが表示されます。証明書をアップロードした場合、この情報を使用して証明書が有効で、期限が切れていないことを確認します。



**メモ:** デフォルトでは、認証局が発行した Active Directory 用のサーバー証明書は CMC にありません。認証局が署名した最新のサーバー証明書をアップロードする必要があります。

証明書の次のプロパティが表示されます。

- シリアル番号 - 証明書のシリアル番号。
- 対象者情報 - 証明書の対象者 (証明対象の個人名または会社名)。
- 発行者情報 - 証明書の発行者 (証明機関名)。
- 有効期限開始日 - 証明書の開始日。
- 有効期限終了日 - 証明書の失効日。

次のコントロールを使用すると、この証明書のアップロードおよびダウンロードが可能になります。

- アップロード - 証明書のアップロードプロセスを初期化します。Active Directory から取得するこの証明書によって CMC へのアクセスが許可されます。
- ダウンロード - ダウンロードプロセスを初期化します。ファイルを保存する場所を問われます。このオプションを選択して **次へ** をクリックすると、**ファイルのダウンロード** ダイアログボックスが表示されます。このダイアログボックスで、管理ステーションまたは共有ネットワークにサーバー証明書を保存する場所を指定します。



**メモ** : デフォルトでは、認証局が発行した Active Directory 用のサーバー証明書は CMC にありません。認証局が署名した最新のサーバー証明書をアップロードする必要があります。

## Kerberos Keytab

Active Directory Server 関連で生成される Kerberos Keytab をアップロードできます。**ktpass.exe** ユーティリティを実行すると、Active Directory Server から Kerberos Keytab を生成できます。この keytab は、Active Directory Server と CMC の間の信頼関係を確立します。



**メモ** : CMC には、Active Directory 用の Kerberos Keytab はありません。現在生成された Kerberos Keytab をアップロードする必要があります。詳細については、270 ページの「シングルサインオンの設定」を参照してください。


次のアクションが可能です。

- 参照 - **参照** ダイアログボックスを開き、アップロードするサーバー証明書を選択します。
- アップロード - 指定するファイルパスを使用して、証明書のアップロードプロセスを初期化します。



# 汎用 Lightweight Directory Access Protocol Services の設定と管理

汎用 Lightweight Directory Access Protocol (LDAP) サービスを使用して、お使いのソフトウェアが CMC へのアクセスを提供するように設定できます。LDAP を使用すると、既存ユーザーの CMC ユーザー権限を追加したり管理することができます。

 **メモ:** LDAP を CMC 用に設定するには、**シャーン設定システム管理者** の権限が必要です。

LDAP の表示と設定を行うには、

- 1 ウェブインタフェースにログインします。
- 2 **ユーザー認証** タブをクリックしてから、**ディレクトリサービス** サブタブをクリックします。**ディレクトリサービス** ページが表示されます。
- 3 汎用 LDAP に関連付けられるラジオボタンをクリックします。
- 4 表示されているオプションを設定してから、**適用** をクリックします。

表 5-47 では、使用可能な設定オプションがリストされています。

表 5-47. 共通設定

設定	説明
汎用 LDAP を有効にする	CMC で汎用 LDAP サービスを有効にします。
識別名を使用してグループメンバーシップを検索	メンバーがデバイスにアクセスを許可されている LDAP グループの識別名 (DN) を指定します。
SSL 証明書検証を有効にする	チェックした場合、CMC は CA 証明書を使用して、SSL ハンドシェイク中に LDAP サーバー証明書を検証します。
バインド DN	ログインユーザーの DN の検索時に、サーバーにバインドするユーザーの識別名を指定します。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。
パスワード	バインド DN と併用するバインドパスワード。 <b>メモ:</b> バインドパスワードは機密データで、適切にセキュリティ保護されている必要があります。
検索するベース DN	すべての検索を開始するディレクトリの分岐の DN。

表 5-47. 共通設定（続き）

設定	説明
ユーザーログイン属性	検索対象の属性を指定します。設定されていない場合は、デフォルトで <b>uid</b> を使用します。選択したベース DN 内では一意であることを薦めます。そうでない場合、ログインユーザーの一意性を確保するために、検索フィルタを設定する必要があります。ユーザー DN が属性と検索フィルタの組み合わせを検索するときに一意に識別できない場合、ログインに失敗し、エラーが表示されます。
グループメンバーシップ属性	グループメンバーシップのチェックに使用される 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、 <b>member</b> 属性と <b>uniquemember</b> 属性が使用されます。
検索フィルタ	有効な LDAP 検索フィルタを指定します。ユーザー属性によって、選択した <b>baseDN</b> 内でログインユーザーを一意に識別できない場合に使用します。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 <b>objectClass=*</b> に設定されます。このプロパティの最大長は <b>1024</b> 文字です。
ネットワークタイムアウト（秒）	時間を秒単位で設定すると、アイドルの LDAP セッションが自動的に閉じます。
検索タイムアウト（秒）	時間を秒単位で設定すると、検索が自動的に閉じます。

## LDAP サーバーの選択

サーバーを設定して汎用 LDAP を使用するには、2 つの方法があります。静的サーバーでは、システム管理者がフィールド内に FQDN または IP アドレスを設定できます。代わりに、DN 内で SRV を検索して、LDAP サーバーリストを取得できます。次に挙げるのは、LDAP サーバーセクションのプロパティです。

- 静的 LDAP サーバーの使用 - このオプションを使用すると、LDAP サービスは、指定したサーバーとポート番号を使用します（詳細は次を参照してください）。



**メモ:** 静的 または DNS を選択します。

- LDAP サーバーアドレス - LDAP サーバーの FQDN または IP を指定します。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。CMC 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 - SSL オーバー LDAP のポート。設定されていない場合、デフォルトの 636 が使用されます。CMC バージョン 3.0 では、SSL なしでパスワードを転送することができないため、非 SSL ポートはサポートされていません。
- DNS を使用して LDAP サーバーを検索 - このオプションを選択すると、LDAP が DNS 経由で検索ドメインとサービス名を使用します。静的 または DNS を選択します。

次の DNS クエリが SRV レコードに対して実行されます。

```
_[Service Name]._tcp.[Search Domain]
```

ここで、<Search Domain> は、クエリ内で使用するルートレベルドメインで、

<Service Name> はクエリ内で使用するサービス名です。たとえば、次のとおりです。

```
_ldap._tcp.dell.com
```

ここで、ldap はサービス名、dell.com は検索ドメインです。

## LDAP グループ設定の管理

グループ管理セクションの表は、役割グループ、関連名、ドメイン、既に設定されている役割グループの権限を表示します。

- 新しい役割グループを設定するには、名前、ドメイン、権限がリストアップされていない役割グループ名をクリックします。
- 既存の役割グループの設定を変更するには、役割グループ名をクリックします。

役割グループ名をクリックすると、**役割グループの設定** ページが表示されます。そのページのヘルプには、ページの右上にある **ヘルプ** リンクからアクセスできます。

## LDAP セキュリティ証明書の管理

この項では、最近 CMC にアップロードされた LDAP 証明書のプロパティを表示します。証明書をアップロードした場合、この情報を使用して証明書が有効で、期限が切れていないことを確認します。



**メモ**: デフォルトでは、認証局が発行した Active Directory 用のサーバー証明書は CMC にありません。認証局が署名した最新のサーバー証明書をアップロードする必要があります。

証明書の次のプロパティが表示されます。

- シリアル番号 - 証明書のシリアル番号。
- 対象者情報 - 証明書の対象者（証明対象の個人名または会社名）。
- 発行者情報 - 証明書の発行者（証明機関名）。
- 有効期限開始日 - 証明書の開始日。
- 有効期限終了日 - 証明書の失効日。

次のコントロールを使用すると、この証明書のアップロードおよびダウンロードが可能になります。

- アップロード - 証明書のアップロードプロセスを初期化します。LDAP サーバー から取得するこの証明書によって CMC へのアクセスが許可されます。
- ダウンロード - ダウンロードプロセスを初期化します。ファイルを保存する場所を問われます。このオプションを選択して **次へ** をクリックすると、**ファイルのダウンロード** ダイアログボックスが表示されます。このダイアログボックスで、管理ステーションまたは共有ネットワークにサーバー証明書を保存する場所を指定します。

# SSL とデジタル証明書を使用した CMC 通信のセキュリティ確保

ここでは、CMC 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。

- 167 ページの「SSL (セキュアソケットレイヤー)」。
- 167 ページの「証明書署名要求 (CSR)」。
- 168 ページの「SSL メインメニューへのアクセス」。
- 168 ページの「新しい証明書署名要求の生成」。
- 171 ページの「サーバー証明書のアップロード」。
- 171 ページの「ウェブサーバーキーと証明書のアップロード」。
- 172 ページの「サーバー証明書の表示」。

## SSL (セキュアソケットレイヤー)

CMC には、インターネットで暗号化データを送信するための業界標準 SSL セキュリティプロトコルを使用する Web サーバーが備わっています。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に認証と暗号化を備えた通信を提供してネットワーク上の盗聴を防止するセキュリティ方式として広く受け入れられています。

SSL は、SSL を有効にしたシステムで次のタスクを実行します。

- 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。

この暗号処理は高度なデータ保護を提供します。CMC は、128 ビットの SSL 暗号化標準を採用しています。これは、北米のインターネットブラウザで一般的に利用可能な最も安全な暗号化方式です。

CMC Web 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保するため、新しい証明書署名要求 (CSR) の生成要求を CMC に送信して、Web サーバーの SSL 証明書を置き換えてください。

## 証明書署名要求 (CSR)

CSR はセキュアサーバー証明書の認証局 (ウェブインタフェースでは CA という) へのデジタル要求です。セキュアサーバー証明書は、リモートシステムの身元を確認して、リモートシステムとやり取りする情報を他の人が閲覧または変更できないようにします。CMC のセキュリティを確保するため、CSR を生成して認証局に提出し、認証局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。

認証局（CA）は、IT 業界で認知されたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を提供しています。CA には、Thawte や VeriSign などがあります。認証局は CSR を受け取ると、CSR に含まれている情報を審査、検証します。申請者が認証局のセキュリティ標準を満たしていれば、ネットワークとインターネット上でトランザクションを行う申請者を一意に識別する証明書を発行します。

認証局が CSR を承認して証明書を送信したら、それを CMC ファームウェアにアップロードする必要があります。CMC 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



**メモ** : SSL を CMC 用に設定するには、**シャーシ設定システム管理者** の権限が必要です。



**メモ** : アップロードするサーバー証明書は最新で（期限が切れていない）、認証局が署名したものでなければなりません。

SSL メインメニューにアクセスするには、次の手順を実行してください。

- 1 ウェブインタフェースにログインします。
- 2 **ネットワーク** タブをクリックしてから、**SSL** タブをクリックします。**SSL メインメニュー** ページが表示されます。

**SSL メインメニュー** ページオプションを使って、認証局に送信する CSR を生成します。CSR 情報は CMC ファームウェアに保存されています。

## 新しい証明書署名要求の生成

セキュリティ確保のため、セキュアサーバー証明書を取得して CMC にアップロードすることを強くお勧めします。セキュアサーバー証明書は、リモートシステムの ID を確認し、リモートシステムとやり取りする情報を他者が表示したり変更したりできないようにします。セキュアサーバー証明書なしでは、非認証ユーザーによる CMC へのアクセスに対して脆弱になります。

表 5-48. SSL メインメニューオプション

フィールド	説明
新規証明書署名要求 (CSR) の生成	<p>このオプションを選択し、<b>次へ</b> をクリックして証明書署名要求 (CSR) の生成 ページを表示されます。そこで安全なウェブ証明書を要求する CSR 要求を生成して認証局に送信できます。</p> <p><b>メモ</b> : 新しい CSR はそれぞれ、CMC の古い CSR を上書きします。認証局が CSR を受け入れるには、CMC の CSR が、認証局から返される証明書と一致する必要があります。</p>

表 5-48. SSL メインメニューオプション (続き)

フィールド	説明
生成された CSR に基づいたサーバー証明書のアップロード	<p>このオプションを選択し、<b>次へ</b> をクリックして <b>証明書のアップロード</b> ページを表示します。そこで会社が権利を所有し、CMC へのアクセス制御に使用している既存の証明書をアップロードできます。</p> <p><b>メモ</b> : CMC が受け入れるのは、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、CMC で受け取ったデフォルトの証明書が置き換えられます。</p>
ウェブサーバーキーと証明書のアップロード	<p>このオプションを選択し、<b>次へ</b> をクリックして <b>ウェブサーバーキーと証明書のアップロード</b> ページを表示します。そこで会社が権利を所有し、CMC へのアクセス制御に使用している既存のウェブサーバーキーとサーバー証明書をアップロードできます。</p> <p><b>メモ</b> : CMC が受け入れるのは、X509、Base 64 エンコードの証明書のみです。バイナリの 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、CMC で受け取ったデフォルトの証明書が置き換えられます。</p>
サーバー証明書の表示	<p>このオプションを選択し、<b>次へ</b> ボタンをクリックして <b>サーバー証明書の表示</b> ページを表示されます。そこで現在のサーバー証明書を表示できます。</p>

CMC のセキュアサーバー証明書を取得するには、希望の認証局に証明書署名要求 (CSR) を送信する必要があります。CSR とは、組織に関する情報と一意の識別キーが含まれた署名入りのセキュアサーバー証明書を申請するデジタル要求です。

**証明書署名要求の生成 (CSR)** ページで CSR が作成されると、管理ステーションまたは共有ネットワークにコピーを保存するように指示するメッセージが表示され、CSR の生成に使用した一意の情報が CMC に保存されます。この情報は、後で認証局から受け取るサーバー証明書の認証に使用されます。認証局からサーバー証明書を受け取った後、それを CMC にアップロードする必要があります。



**メモ** : 認証局から返されたサーバー証明書を CMC が受け入れるためには、新しい証明書の認証情報が、CSR 生成時に CMC に保存された情報と一致する必要があります。



**注意** : 新しい CSR が生成されると、CMC に保管されている古い CSR はすべて上書きされます。認証局からサーバー証明書が付与される前に保留中の CSR が上書きされた場合、証明書の認証に使用する情報が失われるため、CMC がサーバー証明書を受け入れなくなります。CSR を生成するとき、保留中の CSR を上書きしないように注意してください。

CSR を生成するには：

- 1 **SSL メインメニュー** ページで、**新しい証明書署名要求 (CSR) の生成** を選択して、**次へ** をクリックします。**証明書署名要求 (CSR) の生成** ページが表示されます。
- 2 各 CSR 属性値の値を入力します。
- 3 **生成** をクリックします。**ファイルのダウンロード** ダイアログボックスが表示されます。
- 4 **csr.txt** ファイルを管理ステーションまたは共有ネットワークに保存します。(このままファイルを開いて、後で保存することも可能です。) このファイルを後で CA に提出する必要があります。

表 5-49. 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	認証する名前 (通常は <b>www.xyzcompany.com/</b> のようなウェブサーバーのドメイン名)。 <b>有効</b> ：英数字 (A ~ Z、a ~ z、0 ~ 9)、ハイフン、下線、ピリオド。 <b>無効</b> ：上記の英数字以外の文字 (@ # \$ % & * など)、主に英語以外の言語で使用される文字 (ß、ã、é、ü など)。
組織名	自分の組織に関連付けられた名前 (例： <b>XYZ Corporation</b> )。 <b>有効</b> ：英数字 (A ~ Z、a ~ z、0 ~ 9)、ハイフン、下線、ピリオド、空白文字。 <b>無効</b> ：上記の英数字以外の文字 (@ # \$ % & * など)。
組織単位	部署など事業体に関連する名前 (例： <b>Kikakubu</b> )。 <b>有効</b> ：英数字 (A ~ Z、a ~ z、0 ~ 9)、ハイフン、下線、ピリオド、空白文字。 <b>無効</b> ：上記の英数字以外の文字 (@ # \$ % & * など)。
地域	組織が存在する都市その他の場所 (例： <b>Kawasaki、Shibuya</b> )。 <b>有効</b> ：英数字 (A ~ Z、a ~ z、0 ~ 9) と空白文字。 <b>無効</b> ：上記の英数字以外の文字 (@ # \$ % & * など)。
状態	証明書を申請している事業体の都道府県や地域例： <b>Tokyo、Osaka、Kanagawa</b> など)。 <b>メモ</b> ：略語は使用しないでください。 <b>有効</b> ：英数字 (大文字と小文字、0 ~ 9) と空白文字。 <b>無効</b> ：上記の英数字以外の文字 (@ # \$ % & * など)。
国	証明書を申請している組織の所在国。



表 5-49. 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
E- メール	会社の E- メールアドレス CSR と関連付ける任意の E- メールアドレスを入力できます。E- メールアドレスはアットマーク (@) を含む有効な E- メールアドレスでなければなりません (例: <b>name@xyzcompany.com</b> )。 <b>メモ:</b> この E- メールアドレスはオプションフィールドです。

## サーバー証明書のアップロード

サーバー証明書をアップロードするには、次の手順を実行します。

- 1 **SSL メインメニュー** ページで、**OSR に基づいて生成されたサーバー証明書のアップロード** を選択して **次へ** をクリックします。**証明書のアップロード** ページが表示されます。
- 2 テキストフィールドにファイルのパスを入力するか、**参照** をクリックしてファイルを選択します。
- 3 **適用** をクリックします。証明書が無効の場合は、エラーメッセージが表示されます。



**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。

**証明書のアップロード** ページの内容を更新するには、**更新** をクリックします。

**証明書のアップロード** ページの内容を印刷するには、**印刷** をクリックします。

## ウェブサーバーキーと証明書のアップロード

ウェブサーバーキーと証明書をアップロードするには、次の手順を実行します。


- 1 **ウェブサーバーキーと証明書のアップロード** オプションを選択してから、**次へ** をクリックします。
- 2 ブラウザメニューでプライベートキーファイルを入力します。
- 3 ブラウザメニューで証明書ファイルを入力します。
- 4 両ファイルがアップロードされたら、**適用** をクリックします。ウェブサーバーキーと証明書が一致しない場合、エラーメッセージが表示されます。



**メモ:** CMC が受け入れるのは、X509、Base 64 エンコードの証明書のみです。DER など、他のエンコードスキームを使用している証明書は、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、CMC で受け取ったデフォルトの証明書が置き換えられます。



**メモ:** ウェブサーバーキーとサーバー証明書をアップロードするには、**シャーシ設定システム管理者** 権限が必要です。

 **メモ**：証明書が正常にアップロードされると、CMC がリセットされ、一時的に使用できなくなります。リセット中に他のユーザーが切断されないようにするため、CMC にログインしている可能性のある権限を持つユーザーに通知し、**ネットワーク** タブの **セッション** ページで、アクティブなセッションを確認してください。

## サーバー証明書の表示

**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。**サーバー証明書の表示** ページが表示されます。

表 5-50 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。

表 5-50. 証明書情報


フィールド	説明
シリアル	証明書のシリアル番号です。
件名	タイトルによって入力された証明書の属性です。
発行者	発行者によって返された証明書の属性です。
有効期限の開始日	証明書の発行日です。
有効期限の終了日	証明書の失効日です。

**サーバー証明書の表示** ページの内容を更新するには、**更新** をクリックします。

**サーバー証明書の表示** ページの内容を更新するには、**印刷** をクリックします。

## セッションの管理

**セッション** ページにシャースへの接続セッションをすべて表示し、どのアクティブセッションを終了することもできます。

 **メモ**：セッションを終了するには、**シャース設定システム管理者** の権限が必要です。

セッションを管理または終了するには：

- 1 ウェブ経由で CMC にログインします。
- 2 **ネットワーク** タブをクリックしてから、**セッション** サブタブをクリックします。
- 3 **セッション** ページで、終了するセッションを見つけ、適切なボタンをクリックします。表 5-51 にセッションのプロパティを示します。

表 5-51. セッションのプロパティ

プロパティ	説明
セッション ID	ログインの各インスタンスに生成される連番の ID 番号を表示します。
ユーザー名	ユーザーのログイン名が表示されます（ローカルユーザーまたは Active Directory ユーザー）。Active Directory ユーザー名の例として、名前 <u>@domain.com</u> 、 <u>domain.com/</u> 名前、 <u>domain.com\</u> 名前などがあります。
IP Address (IP アドレス)	ユーザーの IP アドレスを表示します。
セッションの種類	セッションの種類（Telnet、シリアル、SSH、リモート RACADM、SMASH CLP、WSMAN、GUI セッション）が表示されます。
終了	表示されているセッションはどれでも終了できます（自分のセッションを除く）。関連セッションを終了するには、ボタンをクリックします。この欄は、 <b>シャージ設定システム管理者</b> 権限がある場合にのみ表示されます。

## サービスの設定

CMC には Web サーバーが含まれており、インターネット上でクライアントとの間で暗号化データを送受信するために、業界標準の SSL セキュリティプロトコルを使用するように設定されています。ウェブサーバーには、デルの自己署名 SSL デジタル証明書（サーバー ID）が含まれており、クライアントからのセキュア HTTP 要求を受け入れて応答します。このサービスは、ウェブインタフェースとリモート CLI ツールが CMC と通信するために必要です。



**メモ:** リモート（RACADM）CLI ツールとウェブインタフェースはウェブサーバーを使用します。ウェブサーバーがアクティブではない場合、リモート RACADM とウェブインタフェースは動作しません。



**メモ:** ウェブサーバーがリセットされた場合は、サービスが再び利用可能になるまで少なくとも 1 分間お待ちください。ウェブサーバーのリセットは、通常、次のいずれかのイベントにより発生します。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の変更（CMC ウェブユーザーインタフェースまたは RACADM 経由）、ウェブサーバーのポート設定の変更（ウェブユーザーインタフェースまたは RACADM 経由）、CMC のリセット、新しい SSL サーバー証明書のアップロード。



**メモ:** サービスの設定を変更するには **シャージ設定システム管理者** の権限が必要です。

CMC サービスを設定するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 **ネットワーク** タブをクリックします。
- 3 **サービス** サブタブをクリックします。**サービス** ページが表示されます。
- 4 必要に応じて次のサービスを設定します。
  - CMC シリアルコンソール (表 5-52)
  - ウェブサーバー (表 5-53)
  - SSH (表 5-54)
  - Telnet (表 5-55)
  - リモート RACADM (表 5-56)
  - SNMP (表 5-57)
  - Syslog の削除 (表 5-58)
- 5 **適用** をクリックし、すべてのデフォルトのタイムアウト値および最大タイムアウト制限値を更新します。

表 5-52. CMC シリアルコンソールの設定

設定	説明
有効	CMC の Telnet コンソールインタフェースを有効にします。 <b>デフォルト</b> ：オフ（無効）
リダイレクト有効	CMC からシリアル /Telnet/SSH クライアントを使って、サーバーへのシリアル / テキストのコンソールリダイレクトを有効にします。CMC は、内部的にサーバーの COM2 ポートに接続する iDRAC に接続します。 <b>設定オプション</b> ：オン（有効）、オフ（無効） <b>デフォルト</b> ：チェック済み（有効）
アイドルタイムアウト	アイドル状態のシリアルセッションが自動的に切断されるまでの秒数を示します。 <b>タイムアウト</b> 設定の変更は、次のログインで有効になります。現在のセッションには影響しません。 <b>タイムアウト範囲</b> ：0 または 60 - 10800 秒。アイドルタイムアウト機能を無効にするには、0 を入力します。 <b>デフォルト</b> ：1800 秒
ボーレート	CMC の外部シリアルポートのデータ速度を示します。 <b>有効な設定オプション</b> ：9600、19200、28800、38400、57600、115200 bps <b>デフォルト</b> ：115200 bps
認証無効	CMC シリアルコンソールログイン認証を有効にします。 <b>デフォルト</b> ：オフ（無効）

表 5-52. CMC シリアルコンソールの設定 (続き)

設定	説明
Esc キー	<p><b>connect</b> または <b>racadm connect</b> コマンドを使用するときにシリアル / テキストコンソールリダイレクトを終了する Escape キーの組み合わせを指定できます。</p> <p><b>デフォルト:</b> ^\</p> <p>(&lt;Ctrl&gt; を押しながらバックスラッシュ (\) 文字を入力)</p> <p><b>メモ:</b> キャレット文字 ^ は、&lt;Ctrl&gt; キーを表しています。</p> <p>設定オプション:</p> <ul style="list-style-type: none"> <li>• 10 進値 (例: 95)</li> <li>• 16 進値 (例: 0x12)</li> <li>• 8 進値 (例: 007)</li> <li>• ASCII 値 (例: ^a)</li> </ul> <p>ASCII 値は次のエスケープキーコードを使って表します。</p> <ul style="list-style-type: none"> <li>• Esc の後に英字 (a ~ z, A ~ Z)</li> <li>• Esc の後に特殊文字 [ ] \ ^ _</li> <li>• 最大長: 4</li> </ul>
履歴バッファサイズ	<p>シリアルコンソールに最後に書き込まれた文字を格納しているシリアル履歴バッファの最大サイズを示します。</p> <p><b>デフォルト:</b> 8192 文字</p>
ログインコマンド	<p>ユーザーが CMC シリアルコンソールインタフェースにログインするときに自動的に実行するシリアルコマンドを指定します。</p> <p><b>例:</b> connect server-1</p> <p><b>デフォルト:</b> [Null]</p>

表 5-53. ウェブサーバーの設定

設定	説明
有効	<p>CMC のウェブサーバーのサービス (リモートの RACADM およびウェブインタフェースからのアクセス) を有効にします。</p> <p><b>デフォルト:</b> オン (有効)</p>

表 5-53. ウェブサーバーの設定 (続き)

設定	説明
最大セッション数	<p>シャーシで許可される同時ウェブユーザーインターフェースセッションの最大数を示します。<b>最大セッション数</b> プロパティの変更は次回のログインで有効になります。現在の <b>アクティブセッション</b> (自分自身のセッションを含む) には影響しません。リモート RACADM はウェブサーバーの <b>最大セッション数</b> プロパティの影響は受けません。</p> <p><b>許可範囲</b> : 1 ~ 4</p> <p><b>デフォルト</b> : 4</p> <p><b>メモ</b> : <b>最大セッション数</b> プロパティを現在のアクティブセッション数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。</p>
アイドルタイムアウト	<p>アイドル状態の Web ユーザーインターフェースセッションが自動的に切断されるまでの秒数を示します。<b>タイムアウト</b> 設定の変更は、次回のログインで有効になります。現在のセッションには影響しません。</p> <p><b>タイムアウト範囲</b> : 60 ~ 10800 秒です。</p> <p><b>デフォルト</b> : 1800 秒</p>
HTTP ポート番号	<p>CMC がリスニングに使用するデフォルトポートを示します。</p> <p><b>メモ</b> : ブラウザで HTTP アドレスを入力すると、ウェブサーバーは自動的にリダイレクトして HTTPS を使用します。</p> <p>デフォルト HTTPS ポート (80) を変更した場合は、ブラウザのアドレスフィールドのアドレスにポート番号を次のように入力する必要があります。</p> <p><code>http://&lt;IP アドレス&gt;:&lt;ポート番号&gt;</code></p> <p>IP アドレスはシャーシの IP アドレスで、ポート番号は、デフォルトの 80 以外の HTTP ポート番号です。</p> <p><b>設定範囲</b> : 10 ~ 65535</p> <p><b>デフォルト</b> : 80</p>
HTTPS ポート番号	<p>セキュアなサーバー接続に対するリスニングを行う CMC によって使用されるデフォルトポートを示します。</p> <p>デフォルト HTTPS ポート番号 (443) を変更した場合は、ブラウザのアドレスフィールドのアドレスにポート番号を次のように入力する必要があります。</p> <p><code>https://&lt;IP アドレス&gt;:&lt;ポート番号&gt;</code></p> <p>&lt;IP アドレス&gt; はシャーシの IP アドレスで、&lt;ポート番号&gt; はデフォルトの 443 以外の HTTPS ポート番号です。</p> <p><b>設定範囲</b> : 10 ~ 65535</p> <p><b>デフォルト</b> : 443</p>

表 5-54. SSH の設定

設定	説明
有効	CMC で SSH を有効にします。 <b>デフォルト</b> ：オン（有効）
最大セッション数	シャードで同時に実行できる SSH セッションの最大数。このプロパティの変更は、次のログインで有効になります。現在のアクティブセッション（自分のセッションを含む）には影響しません。 <b>設定可能な範囲</b> ：1～4 <b>デフォルト</b> ：4 <b>メモ</b> ： <b>最大セッション数</b> プロパティを現在の <b>アクティブセッション</b> 数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。
アイドルタイムアウト	アイドル状態の SSH セッションが自動的に切断されるまでの秒数を示します。 <b>タイムアウト</b> 設定の変更は、次のログインで有効になります。現在のセッションには影響しません。 <b>タイムアウト範囲</b> ：0 または 60～10800 秒 アイドルタイムアウト機能を無効にするには、0 を入力します。 <b>デフォルト</b> ：1800 秒
ポート番号	サーバー接続に対するリスニングを行う CMC によって使用されます。 <b>設定範囲</b> ：10～65535 <b>デフォルト</b> ：22

表 5-55. Telnet の設定

設定	説明
有効	CMC の Telnet コンソールインタフェースを有効にします。 <b>デフォルト</b> ：オフ（無効）
最大セッション数	シャードで同時に実行できる Telnet セッションの最大数を示します。このプロパティの変更は、次のログインで有効になります。現在のアクティブセッション（自分のセッションを含む）には影響しません。 <b>許可範囲</b> ：1～4 <b>デフォルト</b> ：4 <b>メモ</b> ：最大セッション数 プロパティを現在のアクティブセッション数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。
アイドルタイムアウト	アイドル状態の Telnet セッションが自動的に切断されるまでの秒数を示します。タイムアウト設定の変更は、次のログインで有効になります。現在のセッションには影響しません。 <b>タイムアウト範囲</b> ：0 または 60～10800 秒 アイドルタイムアウト機能を無効にするには、0 を入力します。 <b>デフォルト</b> ：1800 秒
ポート番号	サーバー接続に対するリスニングを行う CMC によって使用されるポートを示します。 <b>デフォルト</b> ：23



表 5-56. リモート RACADM の設定

設定	説明
有効	CMC へのリモート RACADM ユーティリティのアクセスを有効にします。 <b>デフォルト</b> ：オン（有効）
最大セッション数	シャードで同時に実行できる RACADM セッションの最大数を示します。このプロパティの変更は、次のログインで有効になります。現在の <b>アクティブセッション</b> （自分のセッションを含む）には影響しません。 <b>許可範囲</b> ：1～4 <b>デフォルト</b> ：4 <b>メモ</b> ：最大セッション数プロパティを現在のアクティブセッション数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。
アイドルタイムアウト	アイドル状態の racadm セッションが自動的に切断されるまでの秒数を示します。アイドルタイムアウト 設定の変更は、次のログインで有効になります。現在のセッションには影響しません。アイドルタイムアウト 機能を無効にするには、0 を入力します。 <b>タイムアウト範囲</b> ：0 または 10～1920 秒。アイドルタイムアウト機能を無効にするには、0 を入力します。 <b>デフォルト</b> ：30 秒

表 5-57. SNMP の設定

設定	説明
有効	CMC で SNMP を有効にします。 <b>有効な値</b> ：オン（有効）またはオフ（無効） <b>デフォルト</b> ：オフ（無効）
コミュニティ名	CMC の SNMP デモンからデータを取得するのに使うコミュニティ文字列を示します。

表 5-58. リモートシスログ設定

設定	説明
有効	CMC ログとハードウェアログエントリを指定のサーバーに転送し、リモートで取得できるようにします。 有効な値：オン（有効）またはオフ（無効） デフォルト：オフ（無効）
シスログサーバー 1	3 つのサーバーのうち最初のサーバーが、CMC とハードウェアログエントリのコピーをホストします。ホスト名、IPv6 アドレス、または IPv4 アドレスで指定します。
シスログサーバー 2	3 つのサーバーのうち 2 番目のサーバーが、CMC とハードウェアログエントリのコピーをホストします。ホスト名、IPv6 アドレス、または IPv4 アドレスで指定します。
シスログサーバー 3	3 つのサーバーのうち 3 番目のサーバーが、CMC とハードウェアログエントリのコピーをホストします。ホスト名、IPv6 アドレス、または IPv4 アドレスで指定します。
シスログポート番号	CMC ログおよびハードウェアログのエントリのコピーを受信するためのリモートサーバーのポート番号を指定します。3 つのサーバーすべてに対して、同じポート番号が使用されます。有効なシスログポート番号は 10 ～ 65535 です。 デフォルト：514

## 電力バジェットの設定

CMC では、シャーシへの電力のバジェットを設定して電源を管理することができます。電源管理サービスは電力消費を最適化し、需要に基づいてさまざまなモジュールに電力を割り当て直します。

CMC を介して電源を設定する手順については、303 ページの「電源の設定と管理」を参照してください。

CMC の電力管理サービスの詳細については、285 ページの「電力管理」を参照してください。

## ファームウェアアップデートの管理

本項では、GUI と RACADM コーティリシティを使用してシャーシとサーバーコンポーネントのファームウェアをアップデートする方法について説明します。

RACADM または GUI を使用して、以下のコンポーネントをアップデートできません。GUI では、**シャーシの概要** → **アップデート** または **シャーシコントローラ** → **アップデートページ** を使用してアップデートを行います。

- CMC — アクティブとスタンバイ
- iKVM
- iDRAC — iDRAC6 より前の iDRAC ファームウェア iDRAC は、リカバリインタフェースを使用してアップデートする必要があります。iDRAC6 FW もリカバリインタフェースでアップデートできますが、iDRAC6 およびそれ以降のバージョンでは廃止されています。
- IOM インフラストラクチャデバイス

GUI の **サーバーの概要** → **アップデート** ページでは、以下のサーバーコンポーネントをアップデートできます。

- iDRAC
- BIOS
- Unified Server Configurator
- 32-Bit Diagnostics
- オペレーティングシステムドライバパック
- ネットワークインタフェースコントローラ
- RAID コントローラ


サーバーコンポーネントファームウェアアップデートは、iDRAC 上の Lifecycle Controller サービスを使用して実行されます。Lifecycle Controller は、Dell アップデートパッケージ (DUP) フォーマットのファームウェアイメージをサポートします。デフォルトの CMC 構成では、DUP のサイズについて 48MB の制限があります。オペレーティングシステムドライバパックコンポーネントの DUP はこの制限を超えており、拡張ストレージ機能を使用して別途アップデートする必要があります。詳細については、189 ページの「Lifecycle Controller を使用したサーバーコンポーネントファームウェアのアップデート」を参照してください。

ファームウェアをアップデートするとき、アップデートに失敗した場合にもサービスが失われることを防止できる推奨プロセスがあります。ガイドラインについては、48 ページの「CMC ファームウェアのインストールまたはアップデート」を参照してください。

## 現在のファームウェアバージョンの表示

更新ページには、すべての更新可能なシャーシコンポーネントの現在のバージョンが表示されます。これには、iKVM ファームウェア、アクティブ CMC ファームウェア、スタンドバイ CMC ファームウェア、iDRAC ファームウェア、および IOM インフラストラクチャ デバイス ファームウェアが含まれます。詳細については、186 ページの「IOM インフラストラクチャデバイスファームウェアのアップデート」を参照してください。

更新可能なシャーシコンポーネントを表示するには：

- 1 ウェブインタフェースにログインします。詳細については、99 ページの「CMC 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 システムツリーで **シャーシの概要** をクリックします。  
 **メモ**：または、システムツリーで **シャーシコントローラ** をクリックします。
- 3 **アップデート** タブをクリックします。ファームウェアのアップデート ページが表示されます。

更新可能なサーバーコンポーネントを表示するには：


- 1 ウェブインタフェースにログインします。詳細については、99 ページの「CMC 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 システムツリーで **サーバーの概要** をクリックします。
- 3 **アップデート** タブをクリックします。サーバーコンポーネントアップデート が表示されます。

選択したデバイスのアップデートページを開くには：


- 1 デバイス名をクリックするか、または **すべてを選択 / すべての選択を解除** オプションを選択します。
- 2 アップデートの **適用** をクリックします。  
選択したデバイスのアップデートページが表示されます。

シャーシに iDRAC がリカバリ モードにある前世代のサーバーが存在する場合、または iDRAC のファームウェアが破損していることを CMC が検出した場合には、これらの前世代 iDRAC もファームウェアのアップデート ページに表示されます。CMC を使用して iDRAC ファームウェアを回復する手順については、188 ページの「CMC での iDRAC ファームウェアのリカバリ」を参照してください。

## ファームウェアのアップデート

 **メモ:** CMC 上でファームウェアをアップデートするには、**シャーシ設定システム管理者**の権限が必要です。


 **メモ:** ファームウェアのアップデートでは CMC と iKVM の現在の設定が維持されます。

 **メモ:** システムコンポーネントのファームウェアをアップデートするためにウェブユーザーインターフェースのセッションを利用する場合、ファイル転送時間を十分に許容できるように **アイドルタイムアウト** 時間を設定する必要があります。ファームウェアのファイル転送に 30 分までもかかることがあります。**アイドルタイムアウト** 値を設定するには、173 ページの「サービスの設定」を参照してください。


**コンポーネントファームウェアアップデート** ページには、一覧表示された各コンポーネントに対するファームウェアの現行バージョンが表示され、ファームウェアを最新バージョンにアップデートできます。


デバイスファームウェアの基本的な更新手順：


- 1 アップデートするデバイスを選択します。
- 2 グループ化にある **適用** ボタンをクリックします。
- 3 **参照** ボタンをクリックしてファームウェアイメージを選択します。
- 4 **ファームウェア更新を開始する** をクリックして更新処理を開始します。ステータス進捗ページの後に、**ファイルイメージを転送中** のメッセージが表示されます。


 **メモ:** 必ずファームウェアの最新バージョンを用意してください。最新バージョンのファームウェアのイメージは、デルのサポートサイト [support.dell.com](http://support.dell.com) からダウンロードできます。


## CMC ファームウェアのアップデート

 **メモ:** サーバーの CMC または iDRAC のファームウェアをアップデート中、シャーシ内のファンの一部またはすべてが 100 パーセントの速度で回転します。これは正常な動作です。

 **メモ:** ファームウェアが正常にアップロードされた後、Active CMC がリセットされ、一時的に使用不可になります。スタンバイ CMC が存在する場合、スタンバイとアクティブの役割が入れ替わり、スタンバイ CMC がアクティブ CMC になります。アクティブ CMC のみにアップデートが適用される場合、リセット完了後、アクティブ CMC はそのアップデートされたイメージを実行しません。スタンバイ CMC だけがそのイメージを所持します。一般に、アクティブとスタンバイの CMC の同一ファームウェアバージョンを保存することをお勧めします。

 **メモ:** リセット中に他のユーザーが切断されないようにするため、CMC にログインしている可能性のある権限を持つユーザーに通知し**セッション** ページで、アクティブなセッションを確認してください。**セッション** ページを開くには、ツリーで**シャーシ** を選択し、**ネットワーク** タブをクリックして **セッション** サブタブをクリックします。そのページのヘルプには、ページの右上にある **ヘルプ** リンクからアクセスできます。


 **メモ**：CMC との間でのファイルの転送中は、ファイル転送アイコンが回転します。アイコンが回転する場合は、ブラウザでアニメーションが有効になっているか確認してください。手順については、39 ページの「Internet Explorer でアニメーションの再生」を参照してください。

 **メモ**：Internet Explorer を使って CMC からファイルをダウンロードするときに問題が起きた場合は、**暗号化されたページをディスクに保存しない** オプションを有効にしてください。手順については、38 ページの「Internet Explorer で CMC からファイルのダウンロード」を参照してください。

CMC ファームウェアをアップデートするには、次の手順を実行してください。

1 **ファームウェアアップデート** ページで、CMC の **ターゲットの更新** チェックボックスを選択して、アップデートする CMC を選択します。両 CMC を同時にアップデートすることが可能です。


2 CMC コンポーネントリストの下の **CMC の更新を実行する** ボタンをクリックします。

 **メモ**：デフォルトの CMC ファームウェアイメージ名は、**firmimg.cmc** です。IOM インフラストラクチャデバイスのファームウェアをアップデートする前に、まず CMC ファームウェアをアップデートするようにしてください。

3 **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、**参照** をクリックし、ファイルの保存場所にナビゲートします。


4 **ファームウェアアップデートを開始する** をクリックします。**ファームウェアアップデートの進行状況** セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイル転送にかかる時間は、接続速度によって大きく異なります。内部アップデート処理が開始されると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。次の補足的指示に従って下さい。

- ファイル転送時に、**更新** ボタンの利用、または他のページへ移動しないでください。
- アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時のみ、利用可能です。
- **アップデート状態** フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。


 **メモ**：CMC のアップデートには数分かかる場合があります。


- 5 スタンバイ CMC の場合、アップデートが完了すると、**アップデート状態** フィールドに「完了」と表示されます。アクティブ CMC の場合、ファームウェアのアップデート処理の最終段階では、アクティブ CMC はオフラインになることから、ブラウザセッションと CMC への接続が一時的に失われます。アクティブ CMC の再起動後、数分経過したら、再びログインする必要があります。

CMC がリセットされた後、新しいファームウェアが **ファームウェアアップデート** ページに表示されます。

 **メモ:** ファームウェアアップグレード後、ウェブベースブラウザのキャッシュをクリアします。ブラウザのキャッシュをクリアにする手順については、ご利用のウェブブラウザのオンラインヘルプを参照してください。

### iKVM ファームウェアのアップデート

 **メモ:** ファームウェアが正常にアップロードされると、iKVM がリセットされ、一時的に使用できなくなります。

- 1 CMC Web インタフェースに再びログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **アップデート** タブをクリックします。**ファームウェアのアップデート** ページが表示されます。
- 4 対象となる iKVM の **ターゲットを更新する** チェックボックスを選択して、更新する iKVM を選択します。
- 5 iKVM コンポーネント リストの下の **iKVM の更新を実行する** ボタンをクリックします。
- 6 **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、**参照** をクリックし、ファイルの保存場所にナビゲートします。  
 **メモ:** iKVM ファームウェアイメージのデフォルト名は **ikvm.bin** です。以前のイメージと混同しないようにするため、この名前を変更することも可能です。
- 7 **ファームウェアアップデートを開始する** をクリックします。

8 はい をクリックして続行します。ファームウェアアップデートの進行状況セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイル転送にかかる時間は、接続速度によって大きく異なります。内部アップデート処理が開始されると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。次の補足的指示に従って下さい。

- ファイル転送時に、**更新** ボタンの利用、または他のページへ移動しないでください。
- アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
- **アップデート状態** フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。



**メモ** : iKVM のアップデートに 2 分までもかかる場合があります。

アップデートが完了すると、iKVM がリセットし、新しいファームウェアが **ファームウェアのアップデート** ページに表示されます。

#### IOM インフラストラクチャデバイスファームウェアのアップデート

このアップデートを実行することにより、IOM デバイスのコンポーネント用のファームウェアがアップデートされますが、IOM デバイス自体のファームウェアはアップデートされません。コンポーネントとは、IOM デバイスと CMC の間のインタフェース回路です。コンポーネントのアップデートイメージは、CMC ファイルシステムに常駐しており、コンポーネントは、コンポーネントの現行バージョンと CMC のコンポーネントイメージが一致しない場合に限り、CMC ウェブ GUI にアップデート可能デバイスとして表示されます。IOM インフラストラクチャデバイスファームウェアをアップデートするには、次の手順を実行します。

- 1 CMC Web インタフェースに再びログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **アップデート** タブをクリックします。ファームウェアのアップデート ページが表示されます。
- 4 IOM デバイスに対応する **ターゲットを更新する** チェックボックスを選択して、更新する IOM デバイスを選択します。



- 5 IOM コンポーネントリストの下の **IOM の更新を実行する** ボタンをクリックします。



**メモ:** IOM インフラストラクチャデバイス (IOMINK) ターゲットの場合、必要とするイメージは CMC 上に存在するため、**ファームウェアイメージ** フィールドは表示されません。IOMINF のファームウェアをアップデートする前に、まず CMC ファームウェアをアップデートするようにしてください。

CMC ファイルシステムに含まれているイメージを用いて、IOMINF ファームウェアが古いと判断された場合は、IOMINF のアップデートが CMC により許可されます。IOMINF ファームウェアが最新である場合は、CMC は IOMINF のアップデートを許可しません。最新の IOMINF デバイスはアップデート可能なデバイスとして一覧表示されます。

- 6 **ファームウェアアップデートを開始する** をクリックします。**ファームウェアアップデートの進行状況** セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイル転送にかかる時間は、接続速度によって大きく異なります。内部アップデート処理が開始されると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。次の補足的指示に従ってください。

- ファイル転送時に、**更新** ボタンの利用、または他のページへ移動しないでください。
- **アップデート状態** フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。



**メモ:** IOMINF ファームウェアのアップデート時には、ファイル転送タイマーは表示されません。アップデートが完了すると、デバイスが再起動するため、IOM デバイスとの接続が一時的に失われます。アップデートが完了すると、新ファームウェアが表示され、アップデートされたシステムは以後 **ファームウェアのアップデート** ページに表示されません。

## サーバー iDRAC ファームウェアのアップデート



**メモ:** ファームウェアアップデートのアップロードが正常に行われると、(サーバー上の) iDRAC はリセットされ、一時的に利用できなくなります。



**メモ:** iDRAC ファームウェアは iDRAC を搭載したサーバーではバージョン 1.4 以降、iDRAC6 Enterprise を搭載したサーバーではバージョン 2.0 以降である必要があります。iDRAC ファームウェアを iDRAC 2.3 より前のバージョンから 3.0 以降にアップデートする場合は、iDRAC ファームウェアをバージョン 3.0 以降にアップデートする前にバージョン 2.3 にアップデートする必要があります。

- 1 CMC ウェブインタフェースに再びログインします。
- 2 システムツリーで **シャーシの概要** を選択します。

- 3 **アップデート** タブをクリックします。**ファームウェアのアップデート** ページが表示されます。
- 4 対象のデバイスの **ターゲットを更新する** チェックボックスを選択して、更新する **iDRAC** を選択します。
- 5 **iDRAC** コンポーネント リストの下の **iDRAC のアップデートを実行する** ボタンをクリックします。
- 6 **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、**参照** をクリックし、ファイルの保存場所にナビゲートします。
- 7 **ファームウェアアップデートを開始する** をクリックします。**ファームウェアアップデートの進行状況** セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイル転送にかかる時間は、接続速度によって大きく異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。次の補足的指示に従ってください。
  - ファイル転送時に、**更新** ボタンの利用、または他のページへ移動しないでください。
  - アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時のみ、利用可能です。
  - **アップデート状態** フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。



**メモ** : CMC またはサーバーのアップデートには数分かかる場合があります。

## CMC での iDRAC ファームウェアのリカバリ

iDRAC ファームウェアは通常、iDRAC 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、**support.dell.com** からダウンロードしたオペレーティングシステム固有のアップデートパッケージなどの iDRAC 機能を使ってアップデートします。iDRAC ファームウェアのアップデート手順は、『iDRAC ファームウェアユーザーズガイド』を参照してください。

初期世代のサーバーは、iDRAC ファームウェアの新規更新処理により破損したファームウェアを回復できます。CMC が iDRAC ファームウェアの破損を検知すると、**ファームウェアのアップデート** ページにそのサーバーをリストします。

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

- 1 **support.dell.com** から管理コンピュータに最新の iDRAC ファームウェアをダウンロードします。
- 2 ウェブインタフェースにログインします (99 ページの「CMC ウェブインタフェースへのアクセス」を参照)。

- 3 システムツリーで **シャーシの概要** をクリックします。
- 4 **アップデート** タブをクリックします。**ファームウェアのアップデート** ページが表示されます。
- 5 対象のデバイスの **ターゲットをアップデートする** チェックボックスを選択して、更新対象と同じ型式の **iDRAC** を選択します。
- 6 iDRAC コンポーネント リストの下の **iDRAC のアップデートを実行する** ボタンをクリックします。
- 7 **参照** をクリックして、ダウンロードした iDRAC ファームウェアイメージに移動し、**開く** をクリックします。



**メモ** : デフォルトの iDRAC ファームウェアイメージ名は **firmimg.imc** です。IOM インフラストラクチャデバイスのファームウェアをアップデートする前に、まず CMC ファームウェアをアップデートするようにしてください。

- 8 **ファームウェアアップデートを開始する** をクリックします。次の補足的指示に従って下さい。
  - ファイル転送時に、**更新** ボタンの利用、または他のページへ移動しないでください。
  - アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
  - **アップデート状態** フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。



**メモ** : iDRAC ファームウェアのアップデートには、最大 10 分かかることがあります。

## Lifecycle Controller を使用したサーバーコンポーネントファームウェアのアップデート

Lifecycle Controller は、各サーバー上で使用可能なサービスで、iDRAC によって強化されます。**サーバーコンポーネントのアップデート** ページでは、Lifecycle Controller サービスを使って、サーバー上のコンポートおよびデバイスのファームウェアの管理を行うことができます。Lifecycle Controller はファームウェアのアップデートに最適化アルゴリズムを使用して再起動の数を効率的に減らします。

Lifecycle Controller ベースのアップデート機能を使用する前に、サーバーファームウェアのバージョンをアップデートする必要があります。



**メモ**：サーバーコンポーネントファームウェアモジュールをアップデートする前に、CMC ファームウェアをアップデートする必要があります。

サーバーコンポーネントファームウェアは以下の順序でアップデートしてください。

- BIOS
- Lifecycle Controller
- iDRAC

**support.dell.com/manuals** にある『CMC Readme』の「Recommended Module Firmware Versions」（推奨されるモジュールファームウェアバージョン）の項を参照してください。Lifecycle Controller は、iDRAC6 以降のサーバー向けのモジュールアップデートサポートを提供します。Lifecycle Controller を使用してファームウェアをアップデートするには、iDRAC ファームウェアがバージョン 2.3 以降になっている必要があります。

DUP を使用して手動でファームウェアをアップデートする場合は、以下の順序でファームウェアをアップデートしてください。

- BIOS
- Lifecycle Controller
- iDRAC — iDRAC ファームウェアを iDRAC 2.3 より前のバージョンから 3.0 以降にアップデートする場合は、iDRAC ファームウェアをバージョン 3.0 以降にアップデートする前にバージョン 2.3 にアップデートする必要があります。

### ifecycle Controller の有効化

サーバーが Lifecycle Controller サービスをサポートしない場合、**ファームウェアインベントリ** セクションでは Not Supported（未対応）と表示されます。

サーバー上で Lifecycle Controller が無効になっている場合があり、**ファームウェアインベントリ** セクションで Lifecycle Controller may not be enabled（Lifecycle Controller が有効化されていない可能性があります）と表示されます。

最新世代のサーバーで Lifecycle Controller サービスを有効にするには、Unified Server Configurator（USC）ファームウェアのインストールおよび iDRAC6 ファームウェアのアップデートにより、既存のサーバーをアップグレードします。古い世代のサーバーの場合は、このアップグレードができない場合があります。

通常、USC ファームウェアは、それぞれのサーバーのオペレーティングシステムで実行される必要のある適切なインストールパッケージによりインストールされます。ネイティブの iDRAC Web ブラウザインタフェースでは、拡張子が **.usc** の特別な修復パッケージまたはインストールパッケージを利用できます。このパッケージを使用すると、通常のファームウェアアップデートと同様の方法で USC ファームウェアをインストールできます。詳細については、『Dell Lifecycle Controller Integration for USC/USC-LCE ユーザーズガイド』を参照してください。

Lifecycle Controller サービスは、サーバー起動プロセス時に有効にすることができます。iDRAC6 サーバーの場合は、起動コンソールで、Press <CTRL-E> for Remote Access Setup within 5 sec. (リモートアクセスセットアップを行う場合は 5 秒以内に <CTRL-E> を押してください。) というメッセージが表示されたら、<CTRL-E> を押します。次に、セットアップ画面で、**システムサービス** を有効にします。

保留中のすべてのスケジュール済みジョブをキャンセルして、それらをキューから削除するには、**システムサービスをキャンセル** を選択します。

**サーバーコンポーネントのアップデート** ページでは、お使いのシステムにあるさまざまなファームウェアコンポーネントをアップデートすることができます。このページの機能を使用するには、次が必要です。

- **CMC : サーバー管理者** 権限。
- **iDRAC : iDRAC の設定** 権限および **iDRAC へのログイン** 権限。

権限が不十分である場合には、サーバー上のコンポーネントおよびデバイスのファームウェアインベントリの表示のみが可能となります。そのサーバーでは、どのような Lifecycle Controller 操作にも、選択できるコンポーネントまたはデバイスはありません。

Lifecycle Controller とサーバーコンポーネント、およびデバイスファームウェアの管理についての詳細は、次を参照してください。

- Lifecycle Controller Remote Services 概要。
- **delltechcenter.com/page/Lifecycle+Controller**。

## フィルタリング機構

全サーバーのコンポーネントおよびデバイスすべての情報は、一度に取得されます。この大量な情報に対処するため、**Lifecycle Controller** はさまざまなフィルタリング機構を提供しています。これらのフィルタにより、次が可能になります。

- 簡単に表示できるよう、1 つまたは複数のカテゴリのコンポーネントやデバイスを選択。
- サーバー全体のコンポーネントおよびデバイスのファームウェアのバージョンを比較。
- 選択されたコンポーネントおよびデバイスを自動的にフィルタリングして、タイプやモデルに基づいた特定のコンポーネントやデバイスのカテゴリの絞り込みを実施。



**メモ:** 自動フィルタリング機能は、Dell アップデートパッケージ (DUP) を使用する際に重要です。DUP のアップデートプログラミングは、コンポーネントやデバイスのタイプまたはモデルにもとづいて行うことができます。自動フィルタリングの動作は、最初の選択を行った後は、その後の選択決定を最小化するように設計されています。

## 例

次に、フィルタリング機構の適用例をいくつか示します。

- **BIOS** フィルタが選択されると、全サーバーの **BIOS** インベントリのみが表示されます。複数サーバーモデルで構成される一連のサーバーがあり、そのうちの 1 つのサーバーが **BIOS** アップデートの対象として選択された場合、自動フィルタリングロジックにより、選択されたサーバーのモデルと異なるモデルのサーバーはすべて自動的に除外されます。これにより、選択された **BIOS** ファームウェアのアップデートイメージ (DUP) が、正しいサーバーモデルとの互換性を持っていることを確実にします。

場合によっては、1 つの **BIOS** ファームウェアアップデートイメージが複数のサーバーモデルと互換性を持つことがあります。この互換性が将来失われる場合に備え、このような最適化は無視されます。

- 自動フィルタリングは、ネットワークインタフェースコントローラ (NIC) や **RAID** コントローラのファームウェアアップデートにおいて重要です。これらのデバイスカテゴリには、種々のタイプやモデルが存在します。同様に、ファームウェアアップデートイメージ (DUP) が最適化された形式 (ある特定のカテゴリ内の複数のタイプまたはモデルのデバイスをアップデートできるように DUP がプログラムされている) で利用できる場合もあります。

**サーバーコンポーネントのアップデート** ページには、次の各セクションがあります。

- **コンポーネント / デバイスのアップデートフィルタ**：このセクションは、**ファームウェアインベントリ** セクションのコンポーネントやデバイスの表示方法を制御するために使用されます。コンポーネントやデバイスタイプのためのフィルタを有効にすることにより、**ファームウェアインベントリ** セクションの表示は、全サーバー内の有効なコンポーネントやデバイスのみを表示するように変更されます。

フィルタが選択され、それによってフィルタされたコンポーネントやデバイスがインベントリセクションに表示された後、コンポーネントまたはデバイスがアップデート対象として選択された場合には、さらにフィルタリングが行われる場合があります。たとえば、**BIOS** フィルタが選択されると、インベントリセクションにはすべてのサーバーとその **BIOS** コンポーネントのみが表示されます。それらのうちの 1 つのサーバーの **BIOS** コンポーネントが選択されると、インベントリがさらにフィルタされ、選択されたサーバーと同じモデル名のサーバーのみが表示されます。

フィルタが選択されず、インベントリセクションでコンポーネントまたはデバイスのアップデート用選択が行われた場合には、その選択に関連するフィルタが自動的に有効になります。モデル、タイプ、またはその他の識別要素において選択されたコンポーネントに一致するすべてのサーバーがインベントリセクションに表示される、さらなるフィルタリングが行われる場合もあります。たとえば、1 つのサーバーの **BIOS** コンポーネントがアップデート対象として選択された場合、フィルタがこの **BIOS** に自動的に設定され、インベントリセクションには、選択されたサーバーのモデル名に一致するサーバーが表示されます。

フィルタを有効にすると、関連するコンポーネントやデバイスを **ファームウェアインベントリ** セクションでフィルタできるようにします。フィルタが有効化された後は、シャード内に存在する全サーバーで一致するコンポーネントまたはデバイスのみを表示できます。このフィルタは、パスフィルタです。すなわち、フィルタ条件に一致するコンポーネントやデバイスのみが許可され、それ以外はすべて除外されます。必要に応じて 1 つまたは複数（またはすべて）のフィルタを選択できます。

コンポーネントおよびデバイスは、次のようにグループ化されます。

- **BIOS**
- **iDRAC**
- **Unified Server Configurator (Lifecycle Controller)**
- **32-Bit Diagnostics**
- **オペレーティングシステムドライバパック**
- **ネットワークインタフェースコントローラ (NIC) および RAID コントローラ**

- コンポーネント/デバイスのファームウェアインベントリ：このセクションは、現在シャーシ内に存在するすべてのサーバー上のコンポーネントおよびデバイスのファームウェアバージョンのステータスを要約します。アップデート、ロールバック、再インストール、およびジョブの削除などの、Lifecycle Controller のさまざまな操作のオプションを実行するオプションが利用可能です。一度に実行できる操作は 1 種類のみです。サポートされていないコンポーネントとデバイスがインベントリの一部としてリストされる可能性があります。Lifecycle Controller 操作を許可しないでください。

現在 Lifecycle Controller によってサポートされていないサーバーは、**未対応**としてリストされます。iDRAC ファームウェアのみを直接にアップデートすることができる代替ページに移動することが可能になるハイパーリンクが表示されます。このページでは、サーバー上のコンポーネントやデバイスのアップデートは一切サポートしていません。この代替ページでは、iDRAC ファームウェアのみをアップデートすることができ、Lifecycle Controller 機能に依存しません。

サーバーが **準備中** とリストされる場合は、ファームウェアインベントリが取得された時に、サーバーの iDRAC が初期化中であったことを示します。この場合は、iDRAC が完全に操作可能になるまで待ってからページを更新して、ファームウェアインベントリを再度取得します。

インベントリに表示されるコンポーネントやデバイスの内容が、サーバーに物理的にインストールされている内容を正しく反映していないときは、サーバーの起動プロセス中に **Unified Server Configurator Console (USC)** を起動する必要があります。これは、コンポーネントおよびデバイスの内部情報を更新するために役立ち、現在インストールされているコンポーネントやデバイスを検証する別の手段を提供します。この状況は、次の場合に発生します。

- サーバー管理に新たに Lifecycle Controller 機能を導入するために、サーバーの iDRAC ファームウェアがアップデートされた。
- サーバーに新しいデバイスが新規に挿入された。

このアクションを自動化するため、iDRAC 設定ユーティリティはブートコンソールからアクセス可能なオプションを提供します。

iDRAC6 サーバーの場合は、起動コンソールで、「Press <CTRL-E> for Remote Access Setup within 5 sec. (リモートアクセスセットアップを行う場合は 5 秒以内に <CTRL-E> を押してください。)」というメッセージが表示されたら、<CTRL-E> を押します。次に、セットアップ画面で、**再起動時にシステムインベントリを収集** を有効にします。

iDRAC7 サーバーの場合は、起動コンソールで F2 を選択してシステムセットアップを表示します。セットアップ画面で、iDRAC Settings (iDRAC 設定) を選択して、次に **System Services (USC)** (システムサービス (USC)) を選択します。セットアップ画面で、**再起動時にシステムインベントリを収集** を有効にします。



表 5-59 にサーバーのコンポーネントおよびデバイス情報を示します。


表 5-59. コンポーネントおよびデバイス情報

フィールド	説明
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1 ~ 16 (シャーシには使用できるスロットが 16 個あります) の連番 ID で、シャーシ内のサーバーの場所を識別します。スロットに装着されているサーバーが 16 未満の場合は、サーバーが装着されているスロットのスロット番号のみが表示されます。
名前	各スロットのサーバー名を表示します。
モデル	サーバーのモデルを表示します。
コンポーネント / デバイス	サーバーのコンポーネントおよびデバイスの情報を示します。列幅が狭すぎる場合、マウスオーバーツールを使うと説明が表示されます。
現在のバージョン	サーバーのコンポーネントまたはデバイスの現在のバージョンを示します。現在のバージョンの横にチェックボックスが表示された場合は、そのコンポーネントまたはデバイス用に現在インストールされているファームウェアのファームウェアイメージが、 <b>再インストール</b> 操作のために Lifecycle Controller 内で使用可能であることを示します。
ロールバックバージョン	サーバーのコンポーネントまたはデバイスのロールバックバージョンを示します。現在のバージョンの横にチェックボックスが表示された場合は、そのコンポーネントまたはデバイス用に以前インストールされたファームウェアのファームウェアイメージが、 <b>ロールバック</b> 操作のために Lifecycle Controller 内で使用可能であることを示します。これら機能の可用性は、Lifecycle Controller のバージョン互換性ロジックによって異なります。Lifecycle Controller はまた、以前のバージョンのアップデートが Lifecycle Controller によって行われたものとみなします。
ジョブステータス	そのサーバー上でスケジュールされているすべての操作のジョブステータスを表示します。ジョブステータスは継続して動的にアップデートされます。状態が <b>完了</b> となっているジョブの完了が検出されると、コンポーネントまたはデバイスのいずれかにおいてファームウェアバージョンが変更された場合に備えて、これらのサーバー上のコンポーネントおよびデバイスのファームウェアバージョンが自動的に更新されます。ジョブステータスの横にチェックボックスが表示されている場合は、Lifecycle Controller ジョブが現在実行中および <b>表示中</b> 状態であることを示します。これは、 <b>ジョブの削除</b> 操作にも選択できます。現在の状態の隣には、情報アイコンも表示され、現在のジョブステータスに関する追加情報を提供します。このアイコンをクリックするか、またはカーソルを置くと、情報を表示できます。


表 5-59. コンポーネントおよびデバイス情報（続き）


フィールド	説明
アップデート	<p>サーバーで、ファームウェアアップデート対象のコンポーネントまたはデバイスを選択します。CTRL キーのショートカットを使用して、アップデート対象のコンポーネントまたはデバイスのタイプを、該当する全サーバーで選択できます。CTRL キーを押し下げたままにすると、すべてのコンポーネントが黄色でハイライト表示されます。CTRL キーを押し下げた状態で、<b>アップデート</b>列のチェックボックスを有効にすると、そのコンポーネントまたはデバイスがアップデート対象として選択されます。</p> <p><b>BIOS</b> アップデートは、サーバーのモデルに特有なものです。選択ロジックは、この動作にもとづいています。サーバー内で単一のネットワークインタフェースコントローラ（NIC）デバイスがファームウェアのアップデート対象として選択されていたとしても、そのサーバーのすべての NIC にアップデートが適用されることもあります。このような動作は Lifecycle Controller の機能性、とりわけ Dell アップデートパッケージ（DUP）に含まれるプログラミングに固有です。現時点では、サイズが <b>48MB</b> 未満の Dell アップデートパッケージ（DUP）がサポートされています。</p> <p>アップデートファイルのイメージサイズがより大きい場合、ジョブステータスはダウンロードが失敗したことを示します。サーバーで複数のサーバーコンポーネントのアップデートが試行された場合、すべてのファームウェアアップデートファイルの合計サイズが <b>48M</b> を超えることがあります。このような場合には、これらのアップデートファイルの 1 つのファイルサイズが切り詰められ、そのファイルによるアップデートが失敗します。1 つのサーバー上で複数のコンポーネントをアップデートする場合の方策として、最初に <b>Unified Server Configurator</b> および <b>32-Bit Diagnostics</b> のコンポーネントをまとめてアップデートすることをお勧めします。これらのコンポーネントのアップデートは、サーバーを再起動する必要がなく、比較的短時間で完了します。その後、それ以外のコンポーネントをまとめてアップデートすることができます。</p> <p>すべての Lifecycle Controller アップデートは、即時に実行するようにスケジュールされます。ただし、システムサービスにより、これらの実行が遅延されることもあります。そのような状況では、<b>CMC</b> にホストされているリモート共有が実行時に利用不可となり、その結果アップデートが失敗します。</p>

アップデート対象のコンポーネントまたはデバイスを選択するときは、Dell アップデートパッケージ (DUP) を指定する必要があります。コンポーネント / デバイス、およびファームウェアイメージファイルのセレクトを挙げた 2 番目の表が表示されます。これにより、関連するコンポーネントまたはデバイス用のファームウェアイメージファイルを指定することができます。アップデート対象として選択されたコンポーネント / デバイスのタイプごとに、固有のセレクトが表示されます。

 **メモ:** コンポーネントまたはデバイスのカテゴリごとに、1 つのセレクトのみが表示されます。

これは、ネットワークインタフェースコントローラ (NIC) デバイスおよび RAID コントローラデバイスの場合、より明らかです。これらのデバイスには、多数のタイプやモデルが含まれることがあります。アップデートの選択ロジックは、最初に選択されたデバイスに基づいて、関連するデバイスタイプやモデルを自動的にフィルタします。このような自動的なフィルタ動作の一番の理由は、カテゴリに対して指定できるのが 1 個のファームウェアイメージファイルのみであるということです。ファームウェアイメージファイルは、Microsoft Windows の Dell アップデートパッケージ (DUP) である必要があります。これは、Microsoft Windows の実行形式ファイルです。

 **メモ:** 拡張ストレージ機能がインストールされ、有効になっている場合には、1 つの DUP、または DUP の組み合わせにのどちらについてもサイズの制限が無視されます。拡張ストレージの有効化については、102 ページの「リムーバブルフラッシュメディアの有効化」を参照してください。

 **メモ:** サーバーコンポーネントのファームウェアアップデートを開始する前に、ジョブキューをクリアしておくことをお勧めします。サーバー上の全ジョブのリストは、**Lifecycle Controller ジョブ** ページで利用できます。このページで、単一または複数のジョブを削除したり、サーバー上のすべてのジョブを削除することができます。382 ページの「リモートシステムの Lifecycle Controller ジョブの管理」のトラブルシューティングの項を参照してください。

**サーバーコンポーネントのアップデート** ページでは、表示されるボタンを使用して様々なアクションを行うことができます。ボタンはそれぞれ、関連付けられた Lifecycle Controller 操作の実行を可能にします。操作を行うには、その操作対象として少なくとも 1 つのコンポーネントまたはデバイスを選択する必要があります。コンポーネントまたはデバイスに対して **更新** 操作を選択した場合は、**アップデートフィルタ** および **イメージファイルの選択** のセクションで、そのコンポーネントまたはデバイス用のファームウェアイメージファイルを指定する必要があります。スケジュールのために操作を送信した後は、他のページに移動しないでください。他のページに移動しようとする、ページ移動をキャンセルするための確認のポップアップメッセージが表示されます。キャンセルしない場合は、操作が中断されます。操作の中断、特に **アップデート** 操作中の中断は、ファームウェアイメージファイルのアップロードが正しく完了せずに終了する原因となる

可能性があります。スケジュールのために操作を送信した後は、その操作のスケジュールが正常に行われたことを示すポップアップメッセージを確認するようにしてください。サーバーでスケジュールされた Lifecycle Controller 操作は、完了に 10～15 分かかる場合があります。このプロセスでは、ファームウェアのインストールが実行されるサーバーの再起動が数回行われ、これにはファームウェアの検証ステージも含まれます。プロセスの進行状況は、サーバーコンソールで確認することができます。サーバー上にアップデートの必要があるコンポーネントまたはデバイスが複数ある場合、すべてのアップデートを 1 つの操作に統合してスケジュールすることにより、再起動の必要回数を最小限に減らすことができます。

表 5-60 には、**サーバーコンポーネントのアップデート** ページで利用できるボタンと、実行できるアクションを示します。

**表 5-60. サーバーコンポーネントアップデートのアクション**

ボタン	動作
アップデート	<b>アップデート</b> 操作を実行すると、1 つまたは複数のサーバー全体で選択されたコンポーネントやデバイスのファームウェアアップデートをスケジュールします。
ロールバック	<b>ロールバック</b> 操作を実行すると、1 つまたは複数のサーバー上の選択されたコンポーネントやデバイスのファームウェアのロールバックをスケジュールします。
再インストール	<b>再インストール</b> 操作を実行すると、1 つまたは複数のサーバー上の選択されたコンポーネントやデバイスのファームウェアの再インストールをスケジュールします。
ジョブの削除	<b>ジョブの削除</b> 操作を実行すると、1 つまたは複数のサーバー上の選択されたコンポーネントやデバイスに関連付けられたジョブを削除します。

一部のコンポーネントでは、アップデート、ロールバック、および再インストール操作でサーバーの再起動が必要になることがあります。再起動は、ドロップダウンリストで選択を行うことにより、遅延させることができます。サーバーをただちに再起動する必要がある場合は **今すぐ再起動** を、後で手動で再起動する場合は **後で再起動** を選択してください。

時折、操作が、他のセッションまたはコンテキストを介してスケジュールのため送信されている時に、別の操作が試行されることがあります。この場合、その状況、および操作が送信されないことを示す確認のポップアップメッセージが表示されます。処理中の操作が完了するのを待って、再度送信してください。

## iDRAC の管理

CMC は、iDRAC の導入 ページを提供しており、ユーザーがインストール済みの新規に挿入されたサーバーの iDRAC ネットワークの設定を行うことを可能にします。このページで、ユーザーは、装着されている 1 つまたは複数の iDRAC デバイスを設定できます。また、後でインストールする予定のサーバーのデフォルトの iDRAC ネットワーク設定とルートパスワードを設定することもできます。このデフォルトの設定が **iDRAC QuickDeploy** 設定です。

iDRAC の動作の詳細については、[support.dell.com/manuals](http://support.dell.com/manuals) にある『iDRAC ユーザーズガイド』を参照してください。

### iDRAC QuickDeploy

**iDRAC の導入** ページの **iDRAC QuickDeploy** 選択には、新規に挿入されたサーバーに適用されるネットワーク設定が含まれます。この設定を使って QuickDeploy セクションの **iDRAC ネットワーク設定** テーブルに値を自動入力できます。QuickDeploy を有効にすると、対象サーバーがインストールされたときに QuickDeploy の設定値をサーバーに適用します。iDRAC QuickDeploy 設定の詳細については、41 ページの「LCD 設定ウィザードを使用したネットワーク設定」の手順 8 を参照してください。

**iDRAC QuickDeploy** の設定を有効にし、設定を行うには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **サーバーの概要** を選択します。
- 3 **セットアップ** タブをクリックします。**iDRAC の導入** ページが表示されます。
- 4 必要に応じて QuickDeploy を設定します。

表 5-61. QuickDeploy 設定

設定	説明
<b>QuickDeploy を有効にする</b>	新規に挿入されたサーバーに対してこのページで設定した iDRAC に自動的に表示する <b>QuickDeploy</b> 機能を有効 / 無効にします。自動確認は必ずローカルの LCD パネルで確認します。 <b>メモ</b> ：これには、 <b>サーバー追加時に iDRAC ルートパスワードを設定する</b> ボックスをチェックしたときのルートユーザーパスワードが含まれます。 <b>デフォルト</b> ：オフ（無効）
<b>サーバー挿入時に iDRAC ルートパスワードを設定する</b>	サーバーを挿入したとき、サーバーの iDRAC ルートパスワードを <b>iDRAC ルートパスワード</b> テキストボックスに表示される値に変更するかどうかを指定します。

表 5-61. QuickDeploy 設定 (続き)

設定	説明
<b>iDRAC ルートパスワード</b>	サーバー挿入時に <b>iDRAC ルートパスワードを設定する</b> と <b>QuickDeploy を有効にする</b> がチェックされている場合、シャーシにサーバーが挿入されたときに、このパスワードをサーバーの iDRAC ルートパスワードに割当てます。パスワードは、印刷可能な 1 ~ 20 文字 (スペース含む) で指定します。
<b>確認用 iDRAC ルートパスワード</b>	<b>iDRAC ルートパスワード</b> フィールドに入力されたパスワードを確認します。
<b>iDRAC LAN を有効にする</b>	iDRAC LAN チャンネルを有効 / 無効にします。 <b>デフォルト</b> : オフ (無効)
<b>iDRAC IPv4 を有効にする</b>	iDRAC 上の IPv4 を有効にします。デフォルト設定は有効です。
<b>IPMI オーバー LAN を有効にする</b>	シャーシに搭載されている各 iDRAC の IPMI オーバー LAN チャンネルを有効 / 無効にします。 <b>デフォルト</b> : オフ (無効)
<b>iDRAC DHCP を有効にする</b>	シャーシに搭載されている各 iDRAC の DHCP を有効 / 無効にします。このオプションを有効にすると、 <b>QuickDeploy IP</b> 、 <b>QuickDeploy サブネットマスク</b> 、および <b>QuickDeploy ゲートウェイ</b> フィールドが無効になります。これらの設定は、DHCP を使用して各 iDRAC に自動的に割り当てられるため、変更できません。 <b>デフォルト</b> : オフ (無効)

表 5-61. QuickDeploy 設定 (続き)

設定	説明
<b>iDRAC IPv4 アドレス (スロット 1) を開始する</b>	<p>エンクローージャのスロット 1 に搭載されているサーバーの iDRAC の固定 IP アドレスを指定します。各後続 iDRAC の IP アドレスは、スロットごとにスロット 1 の IP アドレスから 1 ずつ増加します。IP アドレスにスロット数を足した値がサブネットマスクより大きいと、エラー メッセージが表示されます。</p> <p><b>メモ:</b> サブネットマスクとゲートウェイは、IP アドレスのように増加しません。</p> <p>たとえば、IP アドレスが 192.168.0.250 から始まり、サブネットマスクが 255.255.0.0 のとき、スロット 15 の QuickDeploy IP アドレスは 192.168.0.265 です。サブネットマスクが 255.255.255.0 のとき、<b>QuickDeploy 設定の保存</b> または <b>QuickDeploy 設定を使用して自動入力する</b> ボタンを選択すると、QuickDeploy IP address range is not fully within (QuickDeploy Subnet QuickDeploy IP アドレス範囲は QuickDeploy サブネット内ではありません) というエラーメッセージが表示されます。</p>
<b>iDRAC IPv4 ネットマスク</b>	新規に挿入されたすべてのサーバーに割当てられた QuickDeploy サブネットマスクを指定します。
<b>iDRAC IPv4 ゲートウェイ</b>	シャーシに搭載されているすべての iDRAC に割当てる QuickDeploy デフォルトゲートウェイを指定します。
<b>iDRAC IPv6 を有効にする</b>	IPv6 を使用できるシャーシに搭載されている各 iDRAC の IPv6 アドレス指定を有効にします。
<b>iDRAC IPv6 の自動設定を有効にする</b>	iDRAC が DHCPv6 サーバーから IPv6 設定 (アドレスおよびプレフィックス長) を取得できるようにします。また、ステートレスなアドレスの自動構成も有効にします。デフォルト設定は 有効 です。
<b>iDRAC IPv6 ゲートウェイ</b>	デフォルトの IPv6 ゲートウェイが iDRAC に割り当てられるように指定します。デフォルト設定は 「::」 です。
<b>iDRAC IPv6 プレフィックス長</b>	プレフィックス長が iDRAC 上の IPv6 アドレスに対して割り当てられるように指定します。デフォルト設定は 64 です。

- 5 選択を保存するには **QuickDeploy 設定を保存する** ボタンをクリックします。iDRAC ネットワークの設定を変更した場合は、**iDRAC ネットワークの設定を適用する** ボタンをクリックして、iDRAC への設定を適用します。
- 6 表を前回保存した QuickDeploy 設定に更新して、インストールされた各サーバーの iDRAC ネットワーク設定を現在の値に回復するには、**更新** ボタンをクリックします。



**メモ：更新** ボタンをクリックすると、保存されていないすべての iDRAC QuickDeploy および iDRAC ネットワーク構成を削除します。

QuickDeploy 機能は、有効にした場合および、シャシにサーバーを挿入したときのみ実行できます。**サーバー挿入時に iDRAC ルートパスワードを設定する** および **QuickDeploy を有効にする** がチェックされていると、LCD インタフェースでパスワードの変更を有効にする（または無効にする）かどうかのメッセージが表示されます。現行の iDRAC 設定と異なるネットワーク構成がある場合は、変更を許可する（または許可しない）かどうかを尋ねるメッセージが表示されます。



**メモ：**LAN または LAN オーバー IPMI が異なる場合は、QuickDeploy IP アドレス設定を許可するかどうかを尋ねるメッセージが表示されます。DHCP 設定が異なる場合は、DHCP QuickDeploy 設定を許可するかどうかを尋ねるメッセージが表示されます。

QuickDeploy 設定を **iDRAC ネットワーク設定** セクションにコピーするには、**QuickDeploy 設定を使用して自動入力する** をクリックします。QuickDeploy ネットワーク構成設定が、**iDRAC ネットワーク構成設定** テーブルの対応するフィールドにコピーされます。



**メモ：**QuickDeploy フィールドの変更は即座に実施されますが、1 つまたは複数の iDRAC サーバーネットワーク構成を変更した場合は、CMC から iDRAC に反映されるまで数分かかる場合があります。**更新** ボタンを押すタイミングが早すぎると、iDRAC サーバーのデータが部分的にしか正しく表示されない場合があります。

## iDRAC ネットワーク設定

**iDRAC の導入** ページの **iDRAC ネットワーク設定** セクションには、インストールされているすべてのサーバーの iDRAC IPv4 および IPv6 ネットワーク設定が一覧表示されます。この表を使用すると、インストールされている各サーバーの iDRAC ネットワーク設定を行うことができます。各フィールドに表示される初期値は、iDRAC から読み込まれた現在の値です。フィールドを変えて **iDRAC ネットワーク設定を保存する** をクリックすると、変更した iDRAC のフィールドが保存されます。



iDRAC ネットワーク設定を有効にし、その設定を行うには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **サーバーの概要** を選択します。
- 3 **セットアップ** タブをクリックします。  
**iDRAC の導入** ページが表示されます。
- 4 **QuickDeploy を有効にする** チェックボックスを選択して、QuickDeploy 設定を有効にします。
- 5 必要に応じて残りの **iDRAC ネットワーク設定** を設定します。

表 5-62. iDRAC ネットワーク設定

設定	説明
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1 ~ 16 (シャーシには使用できるスロットが 16 個あります) の連番 ID で、シャーシのサーバーの場所を識別します。 <b>メモ:</b> スロットに装着されているサーバーが 16 次の場合、サーバーが装着されているスロットのスロット番号のみが表示されます。
名前	各スロットに装着されているサーバーのサーバー名を表示します。デフォルトでは、スロットは <b>SLOT-01</b> から <b>SLOT-16</b> で表示されます。 <b>メモ:</b> スロット名に空白またはヌルは指定できません。
<b>LAN を有効にする</b>	LAN チャネルを有効 (チェック) または無効 (チェックなし) にします。 <b>メモ:</b> LAN が選択されていない (無効) 場合は、すべての別のネットワーク設定 (IPMI オーバー LAN、DHCP、IP アドレスサブネットマスク および ゲートウェイ) は使用されません。このフィールドはアクセスできません。
<b>ルートパスワードの変更</b>	選択されている場合は、iDRAC ルートユーザーのパスワードの変更を許可できます。この操作を正しく行うためには、 <b>iDRAC ルートパスワード</b> および <b>確認用 iDRAC ルートパスワード</b> フィールドが入力されている必要があります。
<b>DHCP</b>	選択した DHCP を使用して iDRAC IP アドレス、サブネットマスク、およびデフォルト ゲートウェイを取得します。それ以外の場合は、iDRAC ネットワーク設定フィールドで定義された値を使います。このフィールドを設定するには、必ず LAN を有効にしてください。

表 5-62. iDRAC ネットワーク設定（続き）

設定	説明
<b>IPMI オーバー LAN</b>	IPMI LAN チャンネルを有効（チェックあり）または無効（チェックなし）にします。このフィールドを設定するには、必ず LAN を有効にしてください。
<b>IP アドレス</b>	静的 IPv4 または IPv6 アドレスがこのスロットにある iDRAC に割り当てられます。
<b>サブネットマスク</b>	このスロットに装着された iDRAC に割り当てるサブネットマスクを指定します。
<b>ゲートウェイ</b>	このスロットに装着されている iDRAC に割り当てるデフォルトゲートウェイを指定します。
<b>IPv4 を有効にする</b>	スロット内の iDRAC がネットワーク上の IPv4 プロトコルを使用できるようにします。このオプションを有効にするには、 <b>LAN を有効にする</b> オプションを選択する必要があります。デフォルト設定は 有効 です。
<b>IPv6 を有効にする</b>	スロット内の iDRAC がネットワーク上の IPv6 プロトコルを使用できるようにします。このオプションを有効にするには、 <b>LAN を有効にする</b> オプションを選択し、このオプションをアクティブにする <b>自動設定</b> オプションを選択解除する必要があります。デフォルト設定は 無効 です。 <b>メモ</b> ：このオプションは、サーバーが IPv6 を使用できる場合にのみ利用できます。
<b>自動設定</b>	iDRAC が DHCPv6 サーバーから IPv6 設定（アドレスおよびプレフィックス長）を取得できるようにします。また、ステートレスなアドレスの自動構成も有効にします。 <b>メモ</b> ：このオプションは、サーバーが IPv6 を使用できる場合にのみ利用できます。
<b>プレフィックス長</b>	この iDRAC が属する IPv6 サブネットの長さをビット単位で指定します。

- iDRAC に設定を適用するには、**iDRAC ネットワーク設定を適用する** ボタンを押します。QuickDeploy 設定に変更を加えた場合は、それらも保存されます。
- iDRAC ネットワーク設定をインストールされている各ブレードの現在の値に回復し、QuickDeploy 表を前回保存した QuickDeploy 設定に更新するには、**更新** ボタンを押します。



**メモ**：更新 ボタンをクリックすると、保存されていないすべての iDRAC QuickDeploy および iDRAC ネットワーク構成が削除されます。

**iDRAC ネットワーク設定表**は、将来のネットワーク構成を反映するため、インストールされているサーバーに対して表示されている値は、現在インストールされている iDRAC ネットワーク構成と一致しない場合もあります。**更新** ボタンを押すと、変更後の iDRAC ネットワーク構成で **iDRAC の導入** ページを更新します。



**メモ** : QuickDeploy フィールドの変更は即座に実施されますが、1 つまたは複数の iDRAC サーバーネットワーク構成を変更した場合は、CMC から iDRAC に反映されるまで数分かかる場合があります。**更新** ボタンを押すタイミングが早すぎると、象 iDRAC サーバーのデータが部分的にしか正しく表示されない場合があります。

## CMC GUI からリモートコンソールを起動

この機能を使うと、サーバーでキーボード - ビデオ - マウス (KVM) セッションを直接起動できます。

CMC GUI ホームページからサーバーリモートコンソールを起動するには：

- 1 シャーシ図で指定したサーバーをクリックします。
- 2 **クイックリンク** で、**リモートコンソールの起動** リンクをクリックします。

**サーバーステータス** ページからサーバーリモートコンソールを起動するには、

- 1 システムツリーで **サーバーの概要** を選択します。
- 2 表で指定されたサーバーの **リモートコンソールの起動** をクリックします。

個別にサーバーのリモートコンソールを起動するには：

- 1 システムツリーで **サーバーの概要** を展開します。展開されたサーバーリストにすべてのサーバー (1 ~ 16) が表示されます。
- 2 システムツリーで、表示するサーバーをクリックします。**サーバーステータス** ページが表示されます。
- 3 **リモートコンソールの起動** をクリックします。

リモートコンソール機能は、次の条件がすべて満たされた場合のみサポートされます。

- シャーシの電源が入っている
- iDRAC6 と iDRAC7 をサポートしている
- サーバーの LAN インタフェースが有効である
- iDRAC のバージョンが 2.20 以降
- ホストシステムに JRE (Java Runtime Environment) 6 アップデート 16 以降がインストールされている
- ホストシステム上のブラウザで、ポップアップウィンドウが許可されている (ポップアップブロッキングが無効)



**メモ:** リモートコンソールは、iDRAC GUI からでも起動できます。詳細については、iDRAC GUI を参照してください。

### シングルサインオンを使って iDRAC を起動する

CMC は、サーバーなどの個別シャーシコンポーネントの限定された管理機能を提供します。これらの各コンポーネントを完全な管理のため、CMC は、サーバーの管理コントローラ (iDRAC) のウェブベースインタフェースの起動ポイントを提供しています。

サーバー ページから iDRAC 管理コンソールを起動するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **サーバーの概要** を選択します。サーバーステータス ページが表示されます。
- 3 管理するサーバーに対する **iDRAC GUI の起動** アイコンをクリックします。

各サーバーに対する iDRAC 管理コンソールを起動するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **サーバーの概要** を展開します。すべてのサーバー (1 ~ 16) が展開された **サーバー** リストに表示されます。
- 3 表示するサーバーをクリックします。サーバーステータス ページが表示されます。
- 4 **iDRAC GUI の起動** ボタンをクリックします。

この機能は、シングルサインオンを採用しているため、2回目以降に iDRAC GUI を起動する際にユーザーがログインする必要はありません。次に、シングルサインオンの詳細について説明します。

- サーバー管理者の権限を持つ CMC のユーザーは、シングルサインオンで自動的に iDRAC にログインされます。iDRAC のサイトが表示されたら、そのユーザーに管理者権限が自動的に許可されます。これは、iDRAC のアカウントを持たない同じユーザーや、アカウントに管理者権限のない場合でも同様です。
- サーバー管理者の権限を **持たない** CMC ユーザーでも、iDRAC に同じアカウントがある場合は、シングルサインオンで iDRAC に自動ログインできます。iDRAC のサイトが表示されたら、iDRAC アカウントに対して作られた権限が許可されます。
- サーバー管理者の権限、または iDRAC に同じアカウントを持たない CMC ユーザーは、シングルサインオンで iDRAC に自動ログイン **されません**。このユーザーが **iDRAC GUI の起動** ボタンをクリックすると、iDRAC ログインページが表示されます。



**メモ:** ここで言う「同じアカウント」とは、ユーザーが CMC および iDRAC にパスワードが一致する同じログイン名を持っているということです。同じログイン名で、パスワードが一致しないユーザーは、同じアカウントを持つと見なされます。



**メモ:** その場合、ユーザーは、iDRAC のログインページが表示されます（前述のシングルサインオンの 3 つ目の項目参照）。



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



**メモ:** サーバーがシャーシから取り外された、iDRAC IP アドレスを変更した、または iDRAC ネットワーク接続にエラーが発生した場合、iDRAC GUI の起動アイコンをクリックするとエラーページが表示されることがあります。

## サーバークローニング

サーバークローニング機能により、クローン可能なすべての BIOS 設定を、指定されたサーバーから 1 つまたは複数のサーバーに適用することができます。クローン可能な BIOS 設定とは、変更可能で、サーバー間で複製することを目的としている BIOS 設定のことです。

サーバークローニング機能は iDRAC6 サーバーと iDRAC7 サーバーをサポートします。古い世代の iDRAC サーバーがリストされますが、メインページではグレー表示になり、この機能の使用は有効になりません。

サーバークローニング機能を使用するには、以下の条件を満たしている必要があります。

- iDRAC が必要最低限のバージョンになっている。iDRAC6 サーバーは 3.2、iDRAC7 サーバーは 1.0.0 が最低限必要なバージョンです。
- サーバーに、サポートされている世代の iDRAC がある。
- サーバーの電源がオンになっている。

サーバークローニング機能を使用した BIOS 設定は、CMC ウェブインタフェースでのみ行うことができます。BIOS プロファイル ページでこの操作を行います。

BIOS プロファイル ページを開くには、**サーバーの概要** → **セットアップ** → **プロファイル** をクリックします。

ソースサーバーとターゲットサーバーが同じ世代に属している必要はありません。利用できるクローン可能な設定のみが、1 つのサーバープロファイルから他のサーバーに適用されます。

### プロファイルの取得

サーバーの BIOS プロパティをクローニングする前に、まずプロパティを取得して保存プロファイルとして保存する必要があります。

保存プロファイルを作成するときに、各プロファイルに名前と任意の説明を指定します。CMC 不揮発性拡張ストレージメディアに最大 16 個の保存プロファイルを保存できます。

不揮発性ストレージメディアを取り外すか無効にすると、保存プロファイルにアクセスできなくなり、サーバークローニング機能が無効になります。

### プロファイルの適用

CMC 上の不揮発性メディアに保存プロファイルがあるときにサーバークローニング操作を開始するには、保存プロファイルを 1 つまたは複数のサーバーに適用してください。

**プロファイルの適用** 表に、サーバーごとの操作ステータス、スロット番号、スロット名、モデル名が表示されます。保存プロファイルをサーバーに適用した後、サーバーはただちに再起動されます。

## サーバーの BIOS 設定の表示

**プロファイルの適用** 表で選択されたサーバーのサーバー BIOS 設定を表示するには、選択されたエントリの BIOS 設定列で **表示** をクリックします。

**設定の表示** ページが表示されます。

プロファイル（クローン可能な設定）を適用することによって変更できる、サーバー上の BIOS 設定のみが表示されます。設定は、iDRAC BIOS セットアップ画面での表示と同じ方法でグループ分けされています。



**メモ**：コンソールでのブレード BIOS 設定に対する変更は、ブレードでシステムインベントリが実行された後にのみ、**設定の表示** ページに表示されます。このため、**再起動時にシステムインベントリを収集 (CSIOR)** が BIOS で有効になっている必要があります。

## 保存プロファイルの管理

CMC で保存プロファイルを管理するには、**プロファイルの適用** 表で **プロファイルの管理** をクリックします。BIOS プロファイルの管理ページが表示されます。

BIOS プロファイルの管理 ページでは、保存プロファイルの名前または説明の編集、保存プロファイルに含まれる BIOS 設定の表示、保存プロファイルの削除を行うことができます。

## 最近のプロファイルログ

メインブレードクローニングページの **最近のプロファイルログ** 表には、最近のプロファイルログエントリがサーバークローニング操作から直接リストされます。各最新のプロファイルログには、重大度、サーバークローニング操作が実行された日時、クローニングログメッセージの説明が表示されます。

**最近のプロファイルログ** に示されるメッセージは、RAC ログにも書き込まれます。最近のプロファイルログ 表には、10 個の最新のプロファイルログエントリが含まれます。その他の閲覧可能なエントリを表示するには、**プロファイルログを表示** をクリックします。


## 完了ステータスとトラブルシューティング

適用済みの要求された BIOS プロファイルの完了ステータスをチェックするには、次の手順を実行します。

- 1 サーバークローニングメインページの **最近のプロファイルログ** 表から、目的の実行済みジョブのジョブ ID (JID) を取得します。
- 2 **Lifecycle Controller** ジョブ ページの **ジョブ** 表 (**サーバーの概要** → **トラブルシューティング** → **Lifecycle Controller** ジョブ) で同じ JID を探します。

# FlexAddress

本項では、FlexAddress ウェブインタフェース画面について説明します。FlexAddress は、オプションのアップグレードで、工場出荷時にサーバーモジュールに割り当てられた WWN/MAC ID をシャーシで提供される WWN/MAC ID に置き換えることを可能にします。

 **メモ**：設定画面にアクセスするには、FlexAddress のアップグレードを購入し、インストールする必要があります。アップグレードの購およびインストールを行っていない場合は、Web インタフェースに次のメッセージが表示されます。


Optional feature not installed. See the *Dell Chassis Management Controller Users Guide* for information on the chassis-based WWN and MAC address administration feature.

To purchase this feature, please contact Dell at [www.dell.com](http://www.dell.com).

## FlexAddress ステータスの表示

FlexAddress ステータス情報を表示するには、ウェブインタフェースを使用できます。シャーシ全体または個別のサーバーのステータス情報を閲覧することができます。表示される情報には、次が含まれます。

- ファブリック設定。
- アイティブ / アイティブでない FlexAddress。
- スロットの番号および名前。
- シャーシに割り当てられたアドレスとサーバーに割り当てられたアドレス。
- 使用中のアドレス。

 **メモ**：コマンドラインインタフェースを使用して FlexAddress ステータスを表示することもできます。コマンドの詳細については、223 ページの「FlexAddress の使用」を参照してください。

## シャーシ FlexAddress ステータスの表示

シャーシ全体の FlexAddress ステータス情報を表示することが可能です。ステータス情報には、機能が有効であるかどうか、そして各サーバーの FlexAddress ステータスの概要が含まれます。

シャーシに対して FlexAddress がアクティブであるか確認するには、次の手順に従います。

- 1 ウェブインタフェースにログインします（99 ページの「CMC ウェブインタフェースへのアクセス」を参照）。
- 2 システムツリーで **シャーシの概要** をクリックします。



- 3 **セットアップ** タブをクリックします。**一般設定** ページが表示されます。**FlexAddress** エントリには、**アクティブ** または **非アクティブ** の値があります。ここで**アクティブ**とは、シャーシ上でこの機能がインストールされていることを意味します。「無効」は、シャーシ上にこの機能がインストールされておらず、利用もされていないことを意味します。

各サーバーモジュールに関する **FlexAddress** ステータスを表示するには、次の手順を実行します。

- 1 ウェブインタフェース (99 ページの「**CMC ウェブインタフェースへのアクセス**」) にログインします。
- 2 **サーバー概要** → **プロパティ** → **WWN/MAC** とクリックします。
- 3 **FlexAddress サマリ** ページが表示されます。このページでは、シャーシ内のすべてのスロットの **WWN** 設定および **MAC** アドレスを確認することができます。

ステータスページでは、次の情報を提供します。

---

<b>ファブリック構成</b>	<p><b>ファブリック A</b>、<b>ファブリック B</b> および <b>ファブリック C</b> は、取り付けられている I/O ファブリックの種類を表示します。</p> <p><b>iDRAC</b> には、サーバー管理 <b>MAC</b> アドレスが表示されます。</p> <p><b>メモ</b>：ファブリック A を有効にすると、未使用スロットには、装着スロットで使用された場合にファブリック A および <b>MAC</b> のシャーシ指定 <b>MAC</b> アドレス、またはファブリック B および C の <b>WWN</b> が表示されます。</p>
<b>WWN/MAC アドレス</b>	<p>シャーシ内の各スロットの <b>FlexAddress</b> 設定を表示します。表示される情報には、次が含まれます。</p> <ul style="list-style-type: none"><li>• <b>iDRAC</b> 管理コントローラはファブリックではありませんが、その <b>FlexAddress</b> はファブリックのように処理されます。</li><li>• スロット番号および位置</li><li>• <b>FlexAddress</b> の有効/無効ステータス</li><li>• ファブリックタイプ</li><li>• 使用されているサーバー指定およびシャーシ指定の <b>WWN/MAC</b> アドレス</li></ul> <p>緑色のチェックマークは、アクティブなアドレスタイプ（サーバー指定またはシャーシ指定）を示します。</p>

---

- 4 詳細情報については、**ヘルプ** をクリックします。

## サーバー FlexAddress ステータスの表示

各個別サーバーの FlexAddress ステータス情報も表示させることができます。サーバーレベル情報では、対象サーバーの FlexAddress ステータス概要が表示されます。

FlexAddress のサーバー情報を表示するには、次の手順を実行します。

- 1 ウェブインタフェースにログインします (99 ページの「CMC ウェブインタフェースへのアクセス」を参照)。
- 2 システムツリーで **サーバーの概要** を展開します。すべてのサーバー (1 ~ 16) が展開された **サーバー** リストに表示されます。
- 3 表示するサーバーをクリックします。  
**サーバーステータス** ページが表示されます。
- 4 **セットアップ** タブ、**FlexAddress** サブタブを順にクリックします。  
**FlexAddress の展開** ページが表示されます。このページでは、選択したサーバーの WWN 設定および MAC アドレスを確認することができます。  
ステータスページでは、次の情報を提供します。

表 5-63. ステータスページの情報





有効化された FlexAddress	特定スロット上で FlexAddress 機能が有効または無効であるか表示します。		
現在の状態	現在の FlexAddress 設定を表示します。 <ul style="list-style-type: none"> <li>• <b>シャーン指定</b> - 選択したスロットのアドレスには、シャーン指定の FlexAddress を使用しています。新しいサーバーがインストールされた場合でも、スロットベースの WWN/MAC アドレスは維持されます。</li> <li>• <b>サーバー指定</b> - サーバーはコントローラハードウェアに埋め込まれたサーバー指定のアドレスまたはデフォルトアドレスを使用しています。</li> </ul>		
電源状態	サーバーの現在の電源ステータスを表示します。表示される値は、 <b>オン</b> 、 <b>電源投入中</b> 、 <b>電源切断中</b> 、 <b>オフ</b> および <b>N/A</b> （サーバーが存在しない場合）です。		
状態		<b>OK</b>	FlexAddress が存在し、CMC にステータスを提供していることを意味します。CMC と FlexAddress 間で通信障害が発生した場合は、CMC は FlexAddress の正常性ステータスを取得または表示できません。
		情報	正常性ステータス（OK、警告、重要）に変化がない場合に FlexAddress についての情報が表示されます。
		警告	警告アラートのみが発行されたこと、および <b>対応処置を取る必要がある</b> ことを示します。対応措置が取られない場合、サーバーの整合性に影響を与える可能性がある深刻なエラーが生じる場合があります。
		重要	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。重要なステータスはサーバーのシステムエラーを示し、 <b>直ちに対応処置を取る必要があります</b> 。
		値なし	FlexAddress が不在の場合、正常性情報は提供されません。
iDRAC ファームウェア	現在サーバーにインストールされている iDRAC のバージョンを表示します。		
BIOS バージョン	サーバーモジュールの現在の BIOS バージョンを表示します。		
スロット	ファブリックの場所に関連付けられたサーバーのスロット番号。		

表 5-63. ステータスページの情報 (続き)

場所	シャーシ内の入力 / 出力 (I/O) の位置をグループ番号 (A、B、C) とスロット番号 (1 または 2) で示します。スロット名 : A1、A2、B1、B2、C1、C2
ファブリック	ファブリックの種類を表示します。
サーバー指定	サーバー指定 は、コントローラのハードウェアに埋め込まれたサーバー指定の WWN/MAC アドレスを表示します。
シャーシ指定	シャーシ指定 は、特定のスロットで使用されるシャーシ指定の WWN/MAC アドレスを表示します。

5 詳細情報については、ヘルプ をクリックします。

## FlexAddress の設定

FlexAddress をシャーシと一緒に購入された場合はすでにインストール済みであり、システムの電源を入れるとアクティブになります。FlexAddress を別途購入された場合は、『CMC セキュアデジタル (SD) カード技術仕様』に記載されている手順に従って、SD カードに格納されている機能をインストールする必要があります。このマニュアルについては、[support.dell.com/manuals](http://support.dell.com/manuals) を参照してください。

設定を開始する前に、サーバーの電源を落とす必要があります。ファブリックごとに FlexAddress を有効または無効にすることができます。また、スロットごとに、機能を有効 / 無効にすることも可能です。ファブリックごとに機能の有効化を行う場合は、有効にするスロットを選択できます。たとえば、ファブリック -A が有効な場合、有効にしたスロットは、ファブリック -A でのみ FlexAddress が有効になります。その他のファブリックは、工場出荷時に割り当てられた WWN/MAC をサーバー上で使用します。

選択されたスロットには、有効化されたすべてのファブリックに対する FlexAddress が有効化されています。たとえば、ファブリック -A および B を有効にし、ファブリック -A のスロット 1 で FlexAddress を有効にして、ファブリック -B のスロット 1 で無効にすることはできません。



**メモ :** コマンドラインインタフェースを使用して FlexAddress ステータスを表示することもできます。コマンドの詳細については、223 ページの「FlexAddress の使用」を参照してください。



**メモ :** ファブリックレベル (A、B、C、または DRAC) フレックスアドレスを変更する前に、ブレードサーバーの電源がオフになっていることを確認してください。

## ファブリックおよびスロットのシャーシレベルの FlexAddress 設定

シャーシレベルで、FlexAddress 機能をファブリックおよびスロット上で有効または無効にすることができます。FlexAddress はファブリックごとに有効化され、その後、FlexAddress 機能に使用するスロットが選択されます。

FlexAddress を正しく設定するには、ファブリックおよびスロット上で有効にしなければなりません。

FlexAddress 機能をファブリックおよびスロット上で有効または無効にするには、次の手順に従います。

- 1 ウェブインタフェースにログインします (99 ページの「CMC ウェブインタフェースへのアクセス」を参照)。
- 2 システムツリーで **サーバーの概要** をクリックします。
- 3 **設定** タブ → **FlexAddress** サブタブをクリックします。**FlexAddress の展開** ページが表示されます。
- 4 シャーシ指定 **WWN/MAC** のファブリックの選択に、**ファブリック A**、**ファブリック B**、**ファブリック C**、**iDRAC** のチェックボックスが表示されます。
- 5 FlexAddress を有効にしたい各ファブリックのチェックボックスをクリックします。ファブリックを無効にするには、チェックボックスをクリックし、選択をクリアにします。



**メモ:** ファブリックが一つも選択されていない場合、FlexAddress は選択されたスロットに対して有効になりません。

**シャーシ指定 WWN/MAC のスロットの選択** ページには、シャーシの各スロット (1-16) に対して**有効** チェックボックスが表示されます。

- 6 FlexAddress を有効にしたい各スロットの **有効** チェックボックスをクリックします。すべてのスロットを選択したい場合は、**すべて選択 / 選択解除** チェックボックスを利用します。スロットを無効にするには、**有効** チェックボックスをクリックし、選択をクリアにします。



**メモ:** スロットにサーバーが存在する場合、そのスロットで FlexAddress 機能を有効にする前に、ブレードの電源を落とす必要があります。



**メモ:** スロットが一つも選択されていない場合、FlexAddress は選択されたファブリックに対して有効になりません。

- 7 **適用** をクリックして変更を保存します。詳細情報については、**ヘルプ** をクリックします。

## スロットのサーバーレベルの FlexAddress 設定

サーバーレベルで、FlexAddress 機能を個別スロット上で有効または無効にすることができます。

個別のスロット上で FlexAddress 機能の使用を有効または無効にするには、次の手順を実行します。

- 1 ウェブインタフェースにログインします（99 ページの「CMC ウェブインタフェースへのアクセス」を参照）。
- 2 システムツリーで **サーバーの概要** を展開します。展開された **サーバー** リストにすべてのサーバー（1～16）が表示されます。
- 3 表示するサーバーをクリックします。**サーバーステータス** ページが表示されます。
- 4 **セットアップ** タブ、**FlexAddress** サブタブを順にクリックします。**FlexAddress ステータス** ページが表示されます。
- 5 FlexAddress 機能を有効にするには、**FlexAddress の有効化** プルダウンメニューから **はい** を選択し、無効にするには **いいえ** を選択します。
- 6 **適用** をクリックして変更を保存します。詳細情報については、**ヘルプ** をクリックします。

## リモートファイル共有

リモート仮想メディアのファイル共有オプションは、ネットワーク上の共有ドライブのファイルを CMC を介して 1 つまたは複数のサーバーにマッピングし、オペレーティングシステムを導入または更新します。接続が完了すると、リモートファイルはローカルシステムにある場合にアクセス可能です。サポートされている 2 つのメディアの種類はフロッピーディスクと CD/DVD ドライブです。

- 1 ウェブインタフェースにログインします（99 ページの「CMC ウェブインタフェースへのアクセス」を参照）。
- 2 システムツリーで **サーバーの概要** をクリックします。
- 3 **設定** タブ、**リモートファイル共有** サブタブの順にクリックします。**リモートファイル共有の導入** ページが表示されます。
- 4 リモートファイル共有設定を行います。


表 5-64. リモートファイル共有設定

設定	説明
イメージファイルのパス	<p>イメージファイルパスは接続および導入操作でのみ必要です。接続解除操作には適用されません。ネットワークドライブのパス名は、<b>Windows SMB</b> または <b>Linux/Unix NFS</b> プロトコルを使用してサーバーにマウントされます。</p> <p>たとえば、<b>CIFS</b> に接続するには、次を入力します。</p> <pre>&lt;IP to connect for CIFS file system&gt;/ &lt;file path&gt;/&lt;image name&gt;</pre> <p><b>NFS</b> に接続するには、次を入力します。</p> <pre>//&lt;IP to connect for NFS file system&gt;:/&lt;file path&gt;/&lt;image name&gt;</pre> <p>末尾が <b>.img</b> のファイル名は仮想フロッピーとして接続されます。末尾が <b>.iso</b> のファイル名は仮想 CD/DVD として接続されます。最大文字数は <b>511</b> 文字です。</p>
ユーザー名	<p>ユーザー名は接続および導入操作でのみ必要です。接続解除操作には適用されません。このフィールドで指定できる最大文字数は <b>40</b> です。</p>
パスワード	<p>パスワードは接続および導入操作でのみ必要です。接続解除操作には適用されません。このフィールドで指定できる最大文字数は <b>40</b> です。</p>
スロット	<p>スロットの場所を識別します。スロット番号は <b>1 ~ 16</b> (シャーシには使用できるスロットが <b>16</b> 個あります) の連番 ID です。</p>
名前	<p>スロットの名前を示します。スロットはシャーシ内の位置に応じて名前が付けられます。</p>
モデル	<p>サーバーのモデル名を表示します。</p>
電源状態	<p>サーバーの電源状態を表示します。</p> <p><b>該当なし</b> - CMC はサーバーの電源ステータスを特定していません。</p> <p><b>オフ</b> - サーバーまたはシャーシのどちらかの電源がオフです。</p> <p><b>オン</b> - シャーシおよびサーバーともに電源がオンです。</p> <p><b>電源投入中</b> - 電源オフおよび電源オンの間の一時的な状態です。操作が正常に完了すると、電源状態はオンになります。</p> <p><b>電源切断中</b> - 電源オンおよび電源オフの間の一時的な状態です。操作が正常に完了すると、電源状態はオフになります。</p>
接続ステータス	<p>リモートファイル共有接続ステータスを表示します。</p>
すべて選択 / 選択解除	<p>このオプションは、リモートファイル共有操作を行う前に選択します。リモートファイル共有操作には、接続、接続解除、導入の <b>3</b> つの操作があります。</p>

- 5 **接続** をクリックすると、リモートファイル共有に接続されます。リモートファイル共有に接続するには、パス、ユーザー名、およびパスワードを入力する必要があります。操作を正常に完了すると、メディアにアクセスできます。

**接続解除** をクリックすると、前に接続したリモートファイル共有を接続解除できます。

**導入** をクリックすると、メディアデバイスを導入できます。

 **メモ:** このアクションを行うとサーバーが再起動されるため、作業中のファイルをすべて保存してから、`deploy` コマンドを実行してください。

このコマンドでは次のアクションが実行されます。

- リモートファイル共有が接続される。
- ファイルがサーバー用の最初の起動デバイスとして選択される。
- サーバーが再起動される。
- サーバーの電源が切れている場合は、電源がサーバーに投入される。



## よくあるお問い合わせ (FAQ)

表 5-65 では、リモートシステムの管理または復元中に生じるよくある質問が表示されます。

表 5-65. リモートシステムの管理と復元

質問	回答
CMC Web インタフェースにアクセスするとき、SSL 証明書のホスト名と CMC のホスト名が一致しないというセキュリティ警告が表示される。	<p>CMC には、ウェブインタフェースのネットワークセキュリティを保護するため、デフォルトの CMC サーバー証明書と、リモート RACADM 機能が含まれています。この証明書を使用する場合、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、CMC のホスト名（例：IP アドレス）と一致しない <b>CMC デフォルト証明書</b> に対して発行されるためです。</p> <p>このセキュリティ問題に対応するには、CMC の IP アドレスに対して発行された CMC 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) を生成するとき、CSR のコモンネーム (CN) が CMC の IP アドレス（例：192.168.0.120）または登録済みの DNS CMC 名と一致することを確認してください。</p> <p>CSR を登録されている DNS CMC 名と一致させるには：</p> <ol style="list-style-type: none"><li>1 システム ツリーで <b>シャーシの概要</b> をクリックします。</li><li>2 <b>ネットワーク</b> タブをクリックしてから <b>ネットワーク</b> をクリックします。<b>ネットワーク設定</b> ページが開きます。</li><li>3 <b>DNS への CMC の登録</b> チェックボックスを選択します。</li><li>4 <b>DNS CMC 名</b> フィールドに CMC 名を入力します。</li><li>5 <b>変更の適用</b> をクリックします。</li></ol> <p>CSR の生成と証明書の発行については、167 ページの「SSL とデジタル証明書を使用した CMC 通信のセキュリティ確保」を参照してください。</p>

表 5-65. リモートシステムの管理と復元（続き）

質問	回答
<p>プロパティを変更すると、リモート RACADM とウェブベースのサービスを使用できなくなるのはなぜですか。</p>	<p>CMC ウェブサーバーをリセットすると、リモート RACADM サービスとウェブインタフェースに再度アクセスできるようになるまで 1 分ほどかかる場合があります。</p> <p>次のような状況で CMC ウェブサーバーはリセットされます。</p> <ul style="list-style-type: none"> <li>• CMC ウェブインタフェースを使用してネットワーク設定やネットワークセキュリティのプロパティを変更する。</li> <li>• <b>cfgRacTuneHttpsPort</b> プロパティが変更された (<code>config -f &lt;config ファイル&gt;</code> が変更された時も含む)。</li> <li>• <b>racresetcfg</b> が使用されたか、またはシャーシ構成のバックアップがリストアされた。</li> <li>• CMC がリセットされた。</li> <li>• 新しい SSL サーバー証明書がアップロードされた。</li> </ul>
<p>DNS サーバーで CMC を登録できない理由は何ですか？</p>	<p>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。</p>
<p>CMC ウェブインタフェースにアクセスする場合に、SSL 証明書が信頼されていない認証局 (CA) によって発行されましたというセキュリティ警告が表示されます。</p>	<p>CMC には、ウェブインタフェースのネットワークセキュリティを保護するため、デフォルトの CMC サーバー証明書と、リモート RACADM 機能が含まれています。この証明書は、信頼される認証局から発行されていません。このセキュリティ問題に対応するには、信頼された認証局によって発行された CMC サーバー証明書をアップロードします (例: Thawte または Verisign)。証明書の発行の詳細については、167 ページの「SSL とデジタル証明書を使用した CMC 通信のセキュリティ確保」を参照してください。</p>

表 5-65. リモートシステムの管理と復元（続き）

質問	回答
不明な理由で次のメッセージが表示されました。 リモートアクセス：SNMP 認証エラー 原因は何ですか？	検出作業の一部として、IT Assistant はデバイスの <code>get</code> と <code>set</code> コミュニティ名の確認を試みます。IT Assistant には、 <b>コミュニティ名 = public</b> 取得と <b>コミュニティ名 = private</b> の設定があります。CMC エージェントのデフォルトコミュニティ名は <code>public</code> です。IT Assistant が SET リクエストを送信すると、CMC エージェントは SNMP 認証エラーを生成します。これは、CMC エージェントが <b>コミュニティ = public</b> からのリクエストしか受け入れないためです。  RACADM を使用して、CMC のコミュニティ名を変更できます。  CMC 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。 <pre>racadm getconfig -g cfgOobSnmpp</pre> CMC 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。 <pre>racadm config -g cfgOobSnmpp -o cfgOobSnmppAgentCommunity &lt;community name&gt;</pre> SNMP 認証トラップの生成を防ぐには、エージェントに受け入れられるコミュニティ名を入力する必要があります。CMC は 1 つのコミュニティ名しか許可しないため、IT Assistant の検出セットアップと同じ <b>get</b> および <b>set</b> コミュニティ名を入力する必要があります。

## CMC のトラブルシューティング

CMC ウェブインタフェースは、シャーシの識別、診断、およびトラブルシューティングツールを提供します。トラブルシューティングの詳細については、365 ページの「トラブルシューティングとリカバリ」を参照してください。



## FlexAddress の使用

FlexAddress 機能は、オプションのアップグレードです。この機能により、工場出荷時にサーバーモジュールに割り当てられたワールドワイド名前およびメディアアクセスコントロール (WWN/MAC) のネットワーク ID をシャーシで提供される WWN/MAC ID に置き換えることが可能となります。

各サーバーモジュールには、製造過程で一意的 WWN および MAC ID が割り当てられます。FlexAddress 機能が登場する以前は、サーバーモジュールを取り替える際に WWN/MAC ID が変更してしまうため、新しいサーバーモジュールを認識するように Ethernet ネットワーク管理ツールや SAN リソースを再設定する必要がありました。

FlexAddress により、CMC は特定スロットに WWN/MAC ID を割り当て、工場設定の ID を上書きすることが可能になります。サーバーモジュールを取り替えた場合でも、スロットベースの WWN/MAC ID は同じままとなります。この機能により、新しいサーバーモジュールに対応するためにイーサネットネットワーク管理ツールと SAN リソースを再設定する必要がなくなります。

また、工場設定の ID を無効にする処理は、FlexAddress が有効になったシャーシにサーバーモジュールを挿入した場合にのみ行われます。サーバーモジュールに対して永久的な変更は行われません。サーバーモジュールが FlexAddress をサポートしないシャーシに移された場合、工場設定の WWN/MAC IDs が使用されます。

FlexAddress をインストールする前に、SD カードを USB メモリカードリーダーに挿入し、`pwwn_mac.xml` のファイルを表示することで、FlexAddress 機能カードに含まれている MAC アドレスの範囲を特定できます。これにより、この一意的 MAC アドレス範囲のために使用される 16 進数の MAC 開始アドレスである XML タグ `mac_start` が含まれる SD カード上の XML テキストファイルがクリアされます。`mac_count` タグは、SD カードによって割り当てられる MAC アドレスの総数です。割り当てられる MAC 範囲の合計は、次の式で求めることができます。

$$\langle \text{mac\_start} \rangle + 0\text{xCF} (208 - 1) = \text{mac\_end}$$

ここで、208 は MAC アドレス数を表し、次の式で求めることができます。

$$\langle \text{開始 MAC アドレス} \rangle + \langle \text{MAC アドレス数} \rangle - 1 = \langle \text{終了 MAC アドレス} \rangle$$

例：(開始 MAC アドレス) 00188BFFDCFA + 0xCF = (終了 MAC アドレス) 00188BFFDDC9



**メモ：**USB メモリカードリーダーに SD カードを挿入する際、SD カードの内容が誤って変更されないように事前にロックしてください。CMC に挿入する前に SD カードのロックを解除する必要があります。

## FlexAddress の有効化

FlexAddress は SD カードに搭載されており、機能を有効にするには SD カードを CMC に挿入する必要があります。FlexAddress 機能を有効にするには、ソフトウェアのアップデートが必要な場合があります。**FlexAddress を有効にしない場合、これらのアップデートは不要です。**下記の表で記載されるアップデートには、サーバーモジュール BIOS、I/O メザニン BIOS またはファームウェア、および CMC ファームウェアが含まれます。FlexAddress を有効にする前に、これらのアップデートを適用する必要があります。アップデートを適用しないと FlexAddress が正しく機能しない場合があります。

コンポーネント	最低必要なバージョン
Ethernet メザニン カード - Broadcom M5708t、5709、5710	ブートコードファームウェア 4.4.1 以降 iSCSI ブートファームウェア 2.7.11 以降 PXE ファームウェア 4.4.3 以降
FC メザニン カード - QLogic QME2472、FC8	BIOS 2.04 以降
FC メザニン カード - Emulex LPe1105-M4、FC8	BIOS 3.03a3 とファームウェア 2.72A2 以降
サーバーモジュール BIOS	PowerEdge M600 – BIOS 2.02 以降 PowerEdge M605 – BIOS 2.03 以降 PowerEdge M805 PowerEdge M905 PowerEdge M610 PowerEdge M710 PowerEdge M710HD
PowerEdgeM600/M605 LAN (マザーボード上) (LOM)	ブートコードファームウェア 4.4.1 以降 iSCSI ブートファームウェア 2.7.11 以降
iDRAC	PowerEdge xx0x システムのバージョン 1.50 以降 PowerEdge xx1x システムのバージョン 2.10 以降
CMC	バージョン 1.10 以降




**メモ** : 2008 年 6 月以降に注文されたシステムにはすべて、正しいバージョンのファームウェアが搭載されています。


FlexAddress 機能を正しく導入するには、BIOS とファームウェアを次の順序でアップデートしてください。

- 1 メザニンカードのファームウェアと BIOS をすべてアップデートします。
- 2 サーバモジュールの BIOS をアップデートします。
- 3 サーバモジュールの iDRAC ファームウェアをアップデートします。
- 4 シャーシ内の CMC ファームウェアをすべてアップデートします。冗長 CMC がある場合は、必ず両方をアップデートしてください。
- 5 冗長 CMC モジュールシステムではパッシブモジュールに、冗長なしのシステムでは CMC モジュール 1 つに SD カードを挿入します。

 **メモ:** FlexAddress をサポートする CMC ファームウェア (バージョン 1.10 以降) がインストールされていないと、FlexAddress の機能は有効になりません。

SD カードのインストール手順については、『Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様』を参照してください。

 **メモ:** SD カードには、FlexAddress 機能が含まれています。システム機能障害の発生を防ぐため、SD カードに格納されているデータは暗号化されており、いかなる複製や変更も禁止されています。

 **メモ:** SD カードはシャーシ 1 台につき 1 枚のみ使用できます。シャーシが複数台ある場合は、必要な台数分の SD カードを別途購入してください。

SD 機能カードがインストールされている CMC を再起動すると、FlexAddress 機能が自動的に有効になります。これにより、この機能は現在のシャーシにバイインドされます。SD カードを冗長 CMC システムに取り付けた場合は、冗長 CMC が有効になるまで FlexAddress 機能は有効になりません。冗長 CMC をアクティブにする方法については、『Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様』を参照してください。

CMC が再起動したら、225 ページの「FlexAddress 有効化の検証」の項の手順に従って有効化プロセスを確認します。

## FlexAddress 有効化の検証

FlexAddress の正しい有効化を確認するために、RACADM コマンドを使用して、SD 機能カードおよび FlexAddress 有効化を検証します。

SD 機能およびそのステータスを検証するには、次の RACADM コマンドを使用します。

```
racadm featurecard -s
```

表 6-1. featurecard -s コマンドによって返されるステータスメッセージ

ステータスメッセージ	処置
機能カードが挿入されていません。	SD カードが正しく CMC に挿入されていることを確認してください。冗長 CMC 構成では、SD 機能カードが取り付けられている CMC がアクティブ CMC であり、スタンバイ CMC ではないことを確認します。
挿入されている機能カードは有効で、次の FlexAddress 機能が含まれています。機能カードはこのシャーシにバインドされています。	処置の必要はありません。
挿入されている機能カードは有効で、次の FlexAddress 機能が含まれています。機能カードは他のシャーシにバインドされています。 svctag = ABC1234, SD card SN = 01122334455	SD カードを取り外し、現在のシャーシ用の SD カードを見つけて取り付けます。
挿入されている機能カードは有効で、次の FlexAddress 機能が含まれています。機能カードはシャーシにバインドされていません。	機能カードは、他のシャーシに移動したり、現在のシャーシで再び有効にしたりすることができます。現在のシャーシで再び有効にするには、機能カードが取り付けられている CMC モジュールがアクティブになるまで racadm racreset を入力し続けます。

シャーシ上で有効なすべての機能を表示するには、次の RACADM コマンドを使用します。

```
racadm feature -s
```

このコマンドを実行すると、次のステータスメッセージが返されます。

```
機能 = FlexAddress
```

```
アクティブ化された日付 = 2008 年 4 月 8 日 - 10:39:40
```

```
SD- カード SN からインストールされた機能 = 01122334455
```

シャーシ上に有効な機能が存在しない場合は、コマンドは次のメッセージを返します。

```
racadm feature -s
```

このシャーシにアクティブな機能はありません。



Dell 機能カードには、複数の機能が含まれている可能性があります。Dell 機能カードに含まれる機能をシャーシで有効にすると、その Dell 機能カードに含まれている可能性がある他の機能は、別のシャーシで有効にすることはできません。racadm 機能の -s コマンドは、影響される機能について次のメッセージを表示します。

エラー：SD カード上の 1 つまたは複数の機能が別のシャーシでアクティブです。

RACADM コマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **feature** および **featurecard** コマンドの項を参照してください。

## FlexAddress の無効化

RACADM コマンドを使用して、SD カードをインストール前の状態に戻し、FlexAddress 機能を無効にすることができます。ウェブインタフェースでは、無効にする機能は提供されません。無効にすると、SD カードを元の状態に戻し、別のシャーシ上に装着し、有効にすることが可能になります。



**メモ：**SD カードは、物理的に CMC に取り付ける必要があります。また、無効化コマンドを実行する前には、シャーシの電源を切る必要があります。

カードが装着されていない状態、または異なるシャーシのカードを装着した状態で無効化コマンドを実行した場合、機能は無効化されますが、カードに変更は加えられません。

### FlexAddress の無効化

FlexAddress 機能を無効にし、SD カードを復元するには、次の RACADM コマンドを使用します。

```
racadm feature -d -c flexaddress
```

コマンドを実行し、無効化が正常に完了すると、次のステータスメッセージが返されます。


FlexAddress 機能はこのシャーシで正常に非アクティブ化されました。


コマンド実行前にシャーシの電源を切らなかった場合、コマンドは失敗し、次のエラーメッセージが表示されます。

エラー：シャーシの電源が入っているので機能を非アクティブ化できません。

コマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **feature** コマンドの項を参照してください。

## CLI を使用した FlexAddress の設定

 **メモ:** シャーシ指定の MAC アドレスを iDRAC に出力するには、スロットとファブリックの両方を有効にする必要があります。

 **メモ:** グラフィカルユーザーインターフェースを使用して FlexAddress ステータスを表示することもできます。詳細については、210 ページの「FlexAddress」を参照してください。

コマンドラインインターフェースを使用して、ファブリックごとに FlexAddress を有効または無効にすることができます。また、スロットごとに、機能を有効 / 無効にすることも可能です。ファブリックごとに機能の有効化を行う場合は、有効にするスロットを選択できます。たとえばファブリック -A のみが有効化されている場合、有効化されたスロットは全て、ファブリック -A でのみ FlexAddress が有効になります。その他のファブリックは、工場出荷時に割り当てられた WWN/MAC をサーバー上で使用します。この機能が動作するには、ファブリックを有効にし、サーバーの電源を切る必要があります。

FlexAddress が有効なスロットは、すべてのファブリックでも有効になります。たとえば、ファブリック -A および B を有効にし、ファブリック -A のスロット 1 で FlexAddress を有効にして、ファブリック -B のスロット 1 で無効にすることはできません。

ファブリック上で有効または無効にするには、次の RACADM コマンドを使用します。

```
racadm setflexaddr [-f <fabricName> <state>]
```

<fabricName> = A, B, C, or iDRAC

<state> = 0 or 1

**0** は無効、**1** は有効を示します。

スロット上で有効または無効にするには、次の RACADM コマンドを使用します。

```
racadm setflexaddr [-i <slot#> <state>]
```

<slot#> = 1 to 16

<state> = 0 or 1

**0** は無効、**1** は有効を示します。

コマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **setflexaddr** コマンドの項を参照してください。

## Linux 向け FlexAddress の追加設定

Linux ベースのオペレーティングシステム上で、サーバー指定の MAC ID からシャーシ指定の MAC ID に変更する場合は、追加の設定手順が必要となる場合があります。

- SUSE Linux Enterprise Server 9 および 10: ユーザーは、Linux システム上で YAST (Yet another Setup Tool) を実行し、ネットワークデバイスの設定を行い、ネットワークサービスを再起動する必要がある場合があります。
- Red Hat Enterprise Linux 4 および Red Hat Enterprise Linux 5: Kudzu (システムに新しく追加または変更されたハードウェアの検知および設定を行うユーティリティ) を実行します。Kudzu ではハードウェアの検出メニューが表示され、ハードウェアが削除されたり、新しいハードウェアが追加された場合に、MAC アドレスの変更を検出します。

## CLI を使用した FlexAddress ステータスの表示

コマンドラインインタフェースを使用して、FlexAddress のステータス情報を表示することができます。シャーシ全体または特定のスロットのステータス情報の表示が可能です。表示される情報には、次が含まれます。

- ファブリック構成
- FlexAddress 有効化 / 無効化
- スロット番号および名前
- シャーシ指定およびサーバー指定のアドレス
- 使用アドレス

シャーシ全体の FlexAddress ステータスを表示するには、次の RACADM コマンドを使用します。

```
racadm getflexaddr
```

特定のスロットの FlexAddress ステータスを表示するには、次のコマンドを使用します。

```
racadm getflexaddr [-i <slot#>]
```

```
<slot#> = 1 to 16
```

FlexAddress 設定の詳細については、228 ページの「CLI を使用した FlexAddress の設定」を参照してください。コマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』(iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド) の **getflexaddr** コマンドの項を参照してください。

# GUI を使用した FlexAddress の設定

## FlexAddress を利用した Wake-On-LAN の使用

FlexAddress を初めて導入する場合、機能を有効にするには、サーバーモジュールの電源を一度切ってから入れ直す手順が必要です。Ethernet デバイス上の FlexAddress は、サーバーモジュールの BIOS によってプログラムされます。サーバーモジュールの BIOS がアドレスをプログラムするには、サーバーモジュールの電源がオンで動作可能である必要があります。電源オフして電源オンするサイクルが完了すると、Wake-On-LAN (WOL) 機能にシャーシ指定 MAC ID が利用できるようになります。

## FlexAddress のトラブルシューティング

本項には、FlexAddress のトラブルシューティング情報が含まれます。

- 1 機能カードが取り外された場合、どうなりますか？  
何も起こりません。機能カードを取り外したり、保管したり、そのままにすることができます。
- 2 あるシャーシで使用していた機能カードを取り外し、他のシャーシに取り付けた場合、どうなりますか？

Web インタフェースが次のエラーを表示します。

This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature. (この機能カードは異なるシャーシでアクティブ化されています。FlexAddress 機能にアクセスする前にカードを取り外す必要があります。)

Current Chassis Service Tag (現在のシャーシサービスタグ) = XXXXXXXX

Feature Card Chassis Service Tag (機能カードシャーシサービスタグ) = YYYYYYYY

CMC ログに次のエントリが追加されます。

```
'FlexAddress@YYYYYYYY' not activated; chassis ID=
'XXXXXXXX' (「FlexAddress@YYYYYYYY」はアクティブ化されてい
ません; シャーシ ID=「XXXXXXXX」)
```

- 3 機能カードが取り外され、非 FlexAddress カードが取り付けられた場合は、どうなりますか？

カードへの変更または有効化は行われません。カードは CMC によって無視されます。この場合、コマンド **\$racadm featurecard -s** を実行すると、次のメッセージが返されます。

機能カードがインサートされていません

エラー：ファイルを開けることができません

- 4 シャーシのサービスタグが再プログラムされた場合、そのシャーシに機能カードがバインドされていると、どうなりますか？

- 元の機能カードが対象のシャーシまたは別のシャーシ上のアクティブな CMC にある場合は、ウェブインタフェースには次のエラーメッセージが表示されます。

This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature. (この機能カードは異なるシャーシでアクティブ化されています。FlexAddress 機能にアクセスする前にカードを取り外す必要があります。)

Current Chassis Service Tag (現在のシャーシサービスタグ)  
= XXXXXXXX

Feature Card Chassis Service Tag (機能カードシャーシサービスタグ) = YYYYYYYY

この場合元の機能カードは、デルサービスに依頼して元のシャーシサービスタグを別のシャーシに移入するよう再プログラムした上で、元の機能カードを搭載した CMC をそのシャーシ上で有効にする以外は、そのシャーシでも他のシャーシでも無効化できません。

- FlexAddress** 機能は最初にバインドされたシャーシでは有効のままになります。対象のシャーシのバインド機能は新しいサービスタグを反映するように更新されます。
- 5 冗長 CMC システムに 2 つの機能カードが取り付けられている場合は、エラーが発生しますか？
- アクティブ CMC 内の機能カードが有効となり、シャーシにインストールされます。2 つ目のカードは CMC によって無視されます。

6 SD カードには、書き込み防止ロック機能はありますか？

はい、あります。SD カードを CMC モジュールに取り付ける前に、書き込み保護ラッチが「ロック解除」の位置になっていることを確認してください。SD カードが書き込み保護されていると、FlexAddress 機能を有効にできません。この場合、**\$racadm feature -s** コマンドを実行すると、次のメッセージが返されます。

このシャーシにアクティブな機能はありません。エラー：読み取り専用のファイルシステム

7 アクティブな CMC モジュールに SD カードが存在しない場合は、どうなりますか？

**\$racadm featurecard -s** コマンドを実行すると、次のメッセージが返されます。

機能カードが挿入されていません。

8 サーバー BIOS のバージョンがバージョン 1.xx から 2.xx にアップデートされた場合、FlexAddress 機能はどうなりますか？

FlexAddress 機能を使用する前に、サーバーモジュールの電源を一度切る必要があります。サーバーの BIOS 更新が完了した後、サーバーの電源を一度切断して入れ直すまでは、サーバーモジュールはシャーシに割り当てられたアドレスを取得しません。

9 単一の CMC を持つシャーシが、バージョン 1.10 以前のファームウェアにダウングレードされた場合、どうなりますか？

- FlexAddress 機能と設定は、シャーシから削除されます。
- このシャーシで機能を有効するのに使用した機能カードは変更されず、シャーシにバインドされたままになります。このシャーシの CMC ファームウェアがその後バージョン 1.10 以降にアップグレードされると、FlexAddress 機能は、元の機能カードの再挿入（必要な場合）、CMC のリセット（ファームウェアアップグレードの完了後に機能カードが挿入された場合）、および機能の再設定を行うことで再度有効になります。

- 10 冗長 CMC を持つシャーシで、1 つの CMC ユニットのファームウェアを持つ CMC に交換した場合、どうなりますか？

冗長 CMC を持つシャーシの CMC をバージョン 1.10 以前のファームウェアを持つ CMC と交換する場合は、現在の FlexAddress 機能と設定が削除されないように、次の手順に従う必要があります。

- a アクティブな CMC ファームウェアのバージョンが常に 1.10 以降であるようにしてください。
- b スタンバイ CMC を取り外し、新しい CMC を取り付けます。
- c アクティブ CMC から、スタンバイ CMC のファームウェアをバージョン 1.10 以降にアップグレードします。



**メモ:** スタンバイ CMC のファームウェアを 1.10 以降にアップデートしなかった場合にフェイルオーバーが発生すると、FlexAddress 機能は設定されません。機能を再度有効にして設定しなおす必要があります。

- 11 FlexAddress で deactivation コマンドを実行したときに、SD カードがシャーシに挿入されていませんでした。SD カードを復旧するにはどのようにすればよいですか？

ここでの問題は、FlexAddress を無効にしたときに SD カードが CMC に挿入されていなかった場合、その SD カードを使って別のシャーシに FlexAddress をインストールすることはできないということです。カードを使用できるように修復するには、カードをバインド先のシャーシ内の CMC に挿入しなおし、FlexAddress を再インストールしてから、FlexAddress を再度無効にします。

- 12 SD カードを正しく取り付け、すべてのファームウェア/ソフトウェアアップデートもインストールしています。FlexAddress は有効になっていますが、サーバー導入画面に何も表示されません。何が問題なのでしょう？

これは、ブラウザのキャッシュの問題です。ブラウザを一度閉じてから、再度開いてください。

- 13 RACADM コマンド `racresetcfg` を使用してシャーシ設定をリセットする必要がある場合、FlexAddress はどうなりますか？

FlexAddress 機能は引き続き有効であり、そのまま使用できます。すべてのファブリックとスロットがデフォルトとして選択されます。



**メモ:** シャーシの電源を切ってから、RACADM コマンド `racresetcfg` を発行することをお勧めします。

## コマンドメッセージ

下の表に、RACADM コマンドおよび一般的な FlexAddress の状況における出力を示します。

表 6-2. FlexAddress コマンドおよび出力

状況	コマンド	出力
アクティブ CMC モジュールの SD カードが他のサービスタグにバインドされている。	<code>\$racadm featurecard -s</code>	挿入された機能カードは有効で次の機能が含まれています。  FlexAddress: この機能カードは別のシャーシ (svctag = <サービスタグ番号> SD カード SN = <有効な flex address シリアル番号>) にバインドされています。
アクティブ CMC モジュールの SD カードが同じサービスタグにバインドされている。	<code>\$racadm featurecard -s</code>	挿入された機能カードは有効で次の機能が含まれています。  FlexAddress: この機能カードはこのシャーシにバインドされています。
アクティブ CMC モジュールの SD カードがどのサービスタグにもバインドされていない。	<code>\$racadm featurecard -s</code>	挿入された機能カードは有効で次の機能が含まれています。  FlexAddress: この機能カードはどのシャーシにもバインドされていません。
何らかの理由で FlexAddress 機能はシャーシ上で有効になっていない (SD カードが挿入されていない、破損した SD カード、機能が無効、SD カードが異なるシャーシにバインドされている)	<code>\$racadm setflexaddr [-f &lt;fabricName&gt; &lt;slotState&gt;]</code> OR <code>\$racadm setflexaddr [-i &lt;slot#&gt; &lt;slotState&gt;]</code>	エラー: このシャーシでは Flexaddress 機能がアクティブ化されていません。
ゲストユーザーがスロット/ファブリック上で FlexAddress の設定を試みる	<code>\$racadm setflexaddr [-f &lt;fabricName&gt; &lt;slotState&gt;]</code> <code>\$racadm setflexaddr [-i &lt;slot#&gt; &lt;slotState&gt;]</code>	エラー: この操作を行うにはユーザー権限が十分ではありません



表 6-2. FlexAddress コマンドおよび出力 (続き)

状況	コマンド	出力
シャーシの電源がオンの状態での FlexAddress 機能の無効化。	<code>\$racadm feature -d -c flexaddress</code>	エラー：シャーシの電源が入っているのでこの機能を非アクティブ化できません。
ゲストユーザーがシャーシ上の機能の無効化を試みる。	<code>\$racadm feature -d -c flexaddress</code>	エラー：この操作を行うにはユーザー権限が十分ではありません
サーバーモジュールの電源がオンの状態で、スロット / ファブリックの FlexAddress 設定を変更する。	<code>\$racadm setflexaddr -i 1 1</code>	エラー：設定された操作は電源がオンになっているサーバーに影響するので実行できません。
FlexAddressPlus 機能のみを無効にした後 (FlexAddress はアクティブのまま)、まだアクティブな CMC 上で <code>racadm setflexaddr</code> コマンドが失敗するのはなぜですか？		FlexAddressPlus 機能カードがカードスロットに入ったままで、CMC がその後アクティブになると、FlexAddressPlus 機能はもう一度アクティブになり、スロット / ファブリックの FlexAddress 設定の変更が再開されます。

## FlexAddress DELL ソフトウェア製品ライセンス契約

本契約書は、ユーザーであるお客様と Dell Products, L.P または Dell Global B.V. との法的な契約となります。本契約は、Dell 製品に同梱されているすべてのソフトウェア（以下、「本ソフトウェア」と総称します）に適用されます。お客様と本ソフトウェアの制作者または所有者との間で個別にライセンス契約は締結できません。本契約は本ソフトウェアまたはその他の知的財産の販売に関するものではありません。本ソフトウェアの財産所有権および知的所有権は本ソフトウェアの制作者または所有者に属します。本契約で明示的に付与されていない権利はすべて、本ソフトウェアの制作者または所有者が所有します。本ソフトウェアのパッケージを開梱または開封したり、本ソフトウェアをインストールまたはダウンロードしたり、本製品にあらかじめロードまたは組み込まれている本ソフトウェアを使用すると、本契約書の条項に同意したとみなされます。これらの条項に同意できない場合、直ちに本ソフトウェアのすべての製品（ディスク、印刷物、およびパッケージ）を返品し、あらかじめロードまたは組み込まれている本ソフトウェアはすべて削除してください。

本ソフトウェアの複製は、任意の時点において1台のコンピュータにのみインストールして使用することができます。本ソフトウェアの複数のライセンスを所有されている場合は、ライセンスを所有する限りいつでも、ライセンスの数だけ複製を使用できます。コンピュータの一時メモリまたは永久ストレージに本ソフトウェアがロードされている場合を「使用」とします。本ソフトウェアを配布する各コンピュータに個別のライセンスがある場合に限り、これらのコンピュータへの配布を唯一の目的として、ネットワークサーバーにインストールされている場合は「使用」とみなしません。ネットワークサーバーにインストールされた本ソフトウェアを使用するユーザー数が、ライセンス数を超えないようにしてください。ネットワークサーバーにインストールされた本ソフトウェアを使用するユーザー数がライセンス数を超える場合は、ユーザー数とライセンス数が数と同数となるように追加のライセンスを購入してから本ソフトウェアの使用を許可してください。お客様がデルの販売会社または関連会社である場合には、お客様は、デルまたはデルにより指名された代理人に対して、通常の営業時間内に本ソフトウェアの使用に関する監査を行う権利を付与し、監査にあたってはデルに協力することに同意し、かつ、本ソフトウェアの使用に関連するすべての記録をデルに提供することに同意します。監査は、お客様が本契約の条項を遵守しているかどうかに関する確認に限定されます。

本ソフトウェアはアメリカ合衆国の著作権法および国際条約によって保護されています。本ソフトウェアは、バックアップまたはアーカイブの目的でのみ、複製を一部作成できます。また、オリジナルのソフトウェアをバックアップまたはアーカイブの目的でのみ保存することを条件として、1台のハードディスクに本ソフトウェアをインストールできます。お客様は、本ソフトウェアを賃貸またはリースしたり、本ソフトウェアと同梱の印刷物を複製することはできません。ただし、Dell製品の販売または譲渡を目的に、お客様が複製を保持せず、被譲渡者が本条項に同意した場合は、ソフトウェアおよびすべての同梱物を永久的に譲渡することができます。譲渡する場合は、必ず最新のアップデートとすべての旧バージョンが含まれていなければなりません。本ソフトウェアのリバースエンジニアリング、逆コンパイル、または逆アセンブリを行わないでください。お客様のコンピュータに付属のパッケージに、CD-ROM、3.5 インチディスクおよび5.25 インチディスクが同梱されている場合は、お客様のコンピュータに適したディスクのみを使用してください。他のコンピュータまたはネットワークでこれらのディスクを使用したり、本契約で許可される以外の他のユーザーに、貸与、賃貸、リース、または譲渡することはできません。

## 限定保証

Dell では、お客様が本ソフトウェアディスクを受領した日から **90 日間**、通常の使用において材質または製作上の欠陥を生じないことを保証します。この保証はお客様に限定され、譲渡することはできません。すべての黙示的保証は、お客様が本ソフトウェアを入手した日から **90 日間**に制限されます。国や地域によっては、黙示的保証期間が制限されることがないため、この保証期間の制限は適用されない場合があります。Dell およびその供給業者の責任範囲およびお客様の救済措置は、次のいずれかに制限されます。(a) 本ソフトウェアの購入代金を返却する。(b) お客様のコストとリスク負担で、本保証を満たさないディスクが返却承認番号付きで Dell に返却された場合、新しいディスクと交換する。いかなる事故、誤用、乱用、または Dell サポート以外のサービスや修正が原因でディスクの機能に不具合が生じた場合、本限定保証は無効となります。交換されたディスクの保証期間については、オリジナルの残余保証期間、または **30 日間**のいずれか長い方が適用されます。

Dell は、本ソフトウェアの機能がお客様の要求に合うこと、または本ソフトウェアの動作が妨げられない、またはエラーが無いことは保証しません。お客様が期待する成果を得るための本ソフトウェアの選択と、その使用および使用結果につきましては、お客様の責任とさせていただきます。

DELL およびその関連供給会社は、商業性や特定目的への適合性に対する保証を含め、またそれらに限定せず、明示的または黙示的を問わず、本ソフトウェアおよび同梱されるすべての印刷物に対する上記以外のいかなる保証をもちません。本限定保証は、お客様に特定の法的権利を与えるものです。国や地域によってはさらに他の権利が与えられる場合もあります。

本ソフトウェアの使用や使用できなかったことにより発生した利益の損失、営業の中断、データの消失、金銭的喪失などを含むあらゆる損害に対し、DELL またはその供給業者は、そのような損害の可能性を示唆していたとしても、一切の責任を負うものではありません。国や地域によっては、間接的または付随的な損害に対する責任の除外や制限が禁じられているため、一部のお客様にはこの制限は適用されません。

## オープンソースソフトウェア

本 CD にはオープンソースソフトウェアが含まれている場合があります。オープンソースソフトウェアは、そのソフトウェアの配布に関する特定のライセンスの条項および条件に基づいてご使用いただけます。

このオープンソースソフトウェアは有用であることを期待して頒布されていますが、「現状有姿」で提供されており、市場性および特定用途の適合性に関する暗黙的な保障に限らず、明示的または暗黙的にいかなる保証も行いません。いかなる原因によるものであれ、また、いかなる責任理論に基づくものであれ、契約、無過失責任、または不法行為のいずれによるにせよ（過失その他の場合を含む）、使用法の如何を問わず、本ソフトウェアの使用によって発生するいかなる直接的、間接的、偶発的、特別的、典型的、または派生的損害（代替品またはサービスの調達、使用機会、データ、もしくは利益の喪失、または営業の中断を含みますが、それらに限定されません）に対しても、デル、著作権保持者、または提供者は、かかる損害の可能性が示唆されていたとしても、いかなる場合も責任を負いません。

#### 米国 政府機関の制限された権利

本ソフトウェアおよび本マニュアルは、**48 C.F.R. 2.101** 条で定義される「商品」で、**48 C.F.R. 12.212** 条の「商用コンピュータソフトウェア」および「商用コンピュータソフトウェア文書」で構成されます。**48 C.F.R. 12.212** 条 および **48 C.F.R. 227.7202-1** から **227.7202-4** 条で定められているとおり、すべての米国政府機関エンド ユーザーは、本製品につき本契約に記載された権利のみに従ってソフトウェアおよび書類を取得します。契約者 / 製造者は **Dell Products, L.P.** であり、その所在地は **One Dell Way, Round Rock, TX 78682** です。

#### 一般情報

本ライセンスは解約されない限り有効です。上記に定められている条件により、または、お客様が本契約条項のいずれかに違反した場合に本契約は解除されます。解除の際には、お客様は本ソフトウェアとその同梱物、およびすべての複製を破棄するものとします。本契約は、テキサス州法を準拠法とします。本契約書の各条項は分離可能です。施行できない条項があることが判明しても、本契約の他の条項、条件、または要件の施行には影響しません。本契約書は、被譲渡者および譲渡者を拘束します。**Dell** およびお客様は、本ソフトウェアまたは本契約書に関して、陪審裁判を受ける権利を法律で認められた範囲内で放棄することに合意します。本権利の放棄が無効な国や地域では、この合意が適用されない場合があります。本契約をお読みになり、ご理解のうえ、また条件に同意し、本ソフトウェアに関するお客様と **Dell** との契約の完全かつ独占的条件であることをご確認ください。

## よくあるお問い合わせ (FAQ)

表 6-3 には、FlexaddressPlus 機能についての、よくあるお問い合わせ (FAQ) が記載されています。

表 6-3. FlexaddressPlus

質問	回答
FlexAddressPlus 機能のみを無効にした後 (FlexAddress はアクティブのまま)、まだアクティブな CMC 上で <code>racadm setflexaddr</code> コマンドが失敗するのはなぜですか？	FlexAddressPlus 機能カードがカードスロットに入ったままで、CMC がその後にアクティブになると、FlexAddressPlus 機能はもう一度アクティブになり、スロット / ファブリックの FlexAddress 設定の変更が再開されます。



## FlexAddress Plus の使用

FlexAddress Plus は、カードバージョン 2.0 に追加された新機能であり、FlexAddress カードバージョン 1.0 のアップグレード版です。FlexAddress Plus には、FlexAddress よりも多くの MAC アドレスが含まれています。どちらの機能を使っても、シャーシは WWN/MAC（ワールドワイドネーム / メディア アクセスコントロール）アドレスをファイバチャネルと Ethernet デバイスに割り当てられます。シャーシによって割り当てられた WWN/MAC アドレスは、全世界で一意的なアドレスで、サーバスロットに固有なものです。

## FlexAddress Plus の有効化

FlexAddress Plus は、FlexAddress 機能と共に FlexAddress Plus SD カードに含まれています。



**メモ**：FlexAddress とラベル表示されている SD カードには FlexAddress のみが含まれており、FlexAddress Plus とラベル表示されているカードには FlexAddress と FlexAddress Plus が含まれています。機能を有効にするには、カードを CMC に挿入する必要があります。

PowerEdge M710HD などのいくつかのサーバーでは、設定により、FlexAddress (FA) が CMC に提供可能な数よりも多くの MAC アドレスを必要とする場合があります。これらのサーバーでは、FA+ にアップグレードすることで、WWN/MAC の設定を完全に最適化できます。FlexAddress Plus 機能のサポートについては、デルにお問い合わせください。

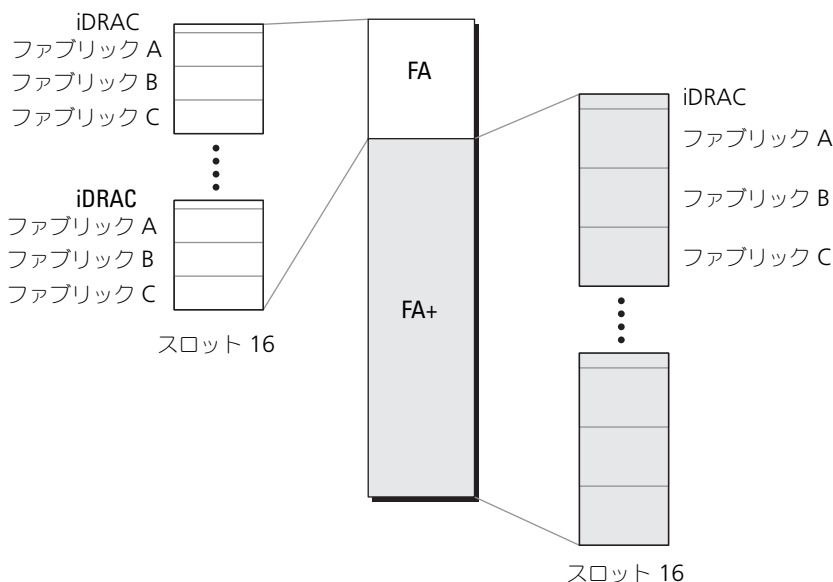
FlexAddress Plus 機能を有効にするには、サーバー BIOS、サーバー iDRAC および CMC ファームウェアのアップデートが必要です。アップデートを適用しない場合は、FlexAddress の機能のみを利用できます。これらのコンポーネントの最低限必要なバージョンについては、[support/dell.com/manuals](https://support.dell.com/manuals) で『CMC 4.0 Readme』を参照してください。

# FlexAddress と FlexAddress Plus

FlexAddress は、208 個のアドレスを 16 のサーバースロットに分けます。つまり、各スロットには、13 個の MAC アドレスが割り当てられます。FlexAddress Plus は、2928 個のアドレスを 16 のサーバースロットに分けます。つまり、各スロットには、183 個の MAC アドレスが割り当てられます。下の表では、両方の機能での MAC アドレスの割り当て方法を示しています。

	ファブリック A	ファブリック B	ファブリック C	iDRAC 管理	合計 MAC 数
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

図 7-1. FlexAddress (FA) と FlexPlusAddress (FA+) の機能





# CMC ディレクトリサービスの 使用

ディレクトリサービスは、ネットワーク上のユーザー、コンピュータ、プリンタなどを制御するのに必要なすべての情報を格納する共通のデータベースを管理しています。Microsoft Active Directory サービスソフトウェアまたは LDAP ディレクトリサービスソフトウェアをお使いの場合、ディレクトリベースのユーザー認証を使用するように CMC を設定することができます。

## CMC と Microsoft Active Directory との併用



**メモ** : Microsoft Windows 2000 および Windows Server 2003 オペレーティングシステムでは、Active Directory を使用して CMC のユーザーを認識できます。IPv6 および IPv4 経由の Active Directory は、Windows 2008 でサポートされています。

### Active Directory スキーマ拡張

Active Directory で CMC へのユーザーアクセスを定義するには、次の 2 つの方法があります。

- 標準 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。
- デルによって定義された Active Directory オブジェクトを使用する拡張スキーマソリューション。

### 標準スキーマと拡張スキーマ

Active Directory を使用して CMC 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。

標準スキーマソリューションの場合

- 標準スキーマでは Active Directory オブジェクトのみが使用されるため、スキーマ拡張は不要です。
- Active Directory の設定はシンプルです。

拡張スキーマソリューションの場合

- アクセス制御オブジェクトのすべてを Active Directory で管理できます。
- さまざまな CMC で異なる特権レベルのユーザーアクセスを設定できるため、最大の柔軟性を実現します。

## 標準スキーマの Active Directory の概要

Active Directory の統合に標準スキーマを使用する場合は、Active Directory と CMC の両方で設定が必要になります。

Active Directory 側では、標準グループオブジェクトが役割グループとして使用されます。CMC のアクセス権を持つユーザーは、役割グループのメンバとなります。

このユーザーに特定の CMC カードへのアクセスを与えるには、役割グループ名とそのドメイン名を特定の CMC カード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、役割と特権レベルは Active Directory ではなく、各 CMC カードで定義されます。各 CMC につき最大 5 つの役割グループを設定および定義できます。図 8-1 に Active Directory と標準スキーマによる CMC の設定を図示します。表 5-43 は役割グループの特権レベルを、表 8-1 は役割グループのデフォルト設定を示したものです。

図 8-1. Active Directory と標準スキーマによる CMC の設定

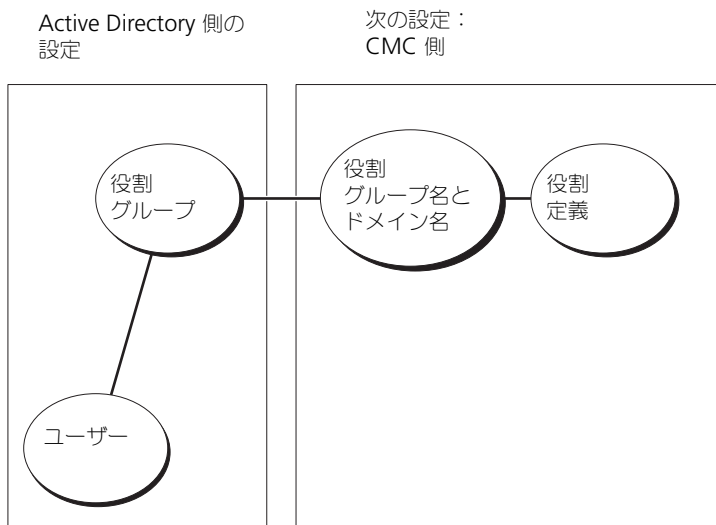


表 8-1. デフォルトのロールグループの権限

役割 グループ	デフォルトの 権限 レベル	許可する権限	ビットマ スク
1	なし	<ul style="list-style-type: none"> <li>• CMC ログインユーザー</li> <li>• シャーシ設定システム管理者</li> <li>• ユーザー設定システム管理者</li> <li>• ログのクリアシステム管理者</li> <li>• シャーシ制御システム管理者</li> <li>• スーパーユーザー</li> <li>• Server Administrator</li> <li>• テストアラートユーザー</li> <li>• コマンドのデバッグシステム管理者</li> <li>• ファブリック A システム管理者</li> <li>• ファブリック B システム管理者</li> <li>• ファブリック C システム管理者</li> </ul>	0x00000fff
2	なし	<ul style="list-style-type: none"> <li>• CMC ログインユーザー</li> <li>• ログのクリアシステム管理者</li> <li>• シャーシ制御システム管理者</li> <li>• Server Administrator</li> <li>• テストアラートユーザー</li> <li>• ファブリック A システム管理者</li> <li>• ファブリック B システム管理者</li> <li>• ファブリック C システム管理者</li> </ul>	0x00000ed9
3	なし	CMC ログインユーザー	0x00000001
4	なし	権限の割り当てなし	0x00000000
5	なし	権限の割り当てなし	0x00000000



**メモ:** ビットマスク値は、RACADM で標準スキーマを設定する場合にのみ使用します。



**メモ:** ユーザー権限の詳細については、149 ページの「ユーザータイプ」を参照してください。

標準スキーマ Active Directory を有効にするには、次の 2 つの方法があります。

- CMC ウェブインタフェースの使用。246 ページの「標準スキーマ Active Directory と Web インタフェースを使用した CMC の設定」を参照してください。
- RACADM CLI ツールの使用。248 ページの「標準スキーマ Active Directory と RACADM を使用した CMC の設定」を参照してください。

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

Active Directory ユーザーが CMC にアクセスできるようになる前に、次の手順を実行して Active Directory を設定します。

- 1 Active Directory サーバー（ドメインコントローラ）で、Active Directory ユーザーとコンピュータスナップイン を開きます。
- 2 グループを作成するか、既存のグループを選択します。グループの名前とこのドメインの名前は、Web インタフェースまたは RACADM を使って CMC 上で設定する必要があります。

詳細については、246 ページの「標準スキーマ Active Directory と Web インタフェースを使用した CMC の設定」および 248 ページの「標準スキーマ Active Directory と RACADM を使用した CMC の設定」を参照してください。

- 3 CMC にアクセスするには、Active Directory ユーザーを Active Directory グループのメンバーとして追加します。

## 標準スキーマ Active Directory と Web インタフェースを使用した CMC の設定

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** を選択します。
- 3 **ユーザー認証** → **ディレクトリサービス** をクリックします。ディレクトリサービス ページが表示されます。
- 4 Microsoft Active Directory（標準スキーマ）の隣にあるラジオボタンを選択します。**Active Directory の設定と管理** ページが表示されます。
- 5 **共通設定** セクションで次の操作を行います。

- a **Active Directory を有効にする** チェックボックスをオンにします。
- b **ルートドメイン名** を入力します。



**メモ：ルートドメイン名** は x.y という命名規則に従った有効なドメイン名でなければなりません。この x は文字間に空白文字が入っていない 1 ~ 256 文字 ASCII 文字列、y は com、edu、gov、int、mil、net、org などの有効なドメインタイプで指定します。

- c **タイムアウト** の時間を秒単位で入力します。タイムアウト範囲は 15 ~ 300 秒です。デフォルトのタイムアウトは 90 秒です。
- 6 ドメインコントローラとグローバルカタログの検索を直接呼び出す場合は、**検索する AD サーバーの検索（オプション）** チェックボックスをオンにし、次の操作を行います。
    - a **ドメインコントローラ** テキストフィールドに、Active Directory サービスがインストールされているサーバーを入力します。

- b **グローバルカタログ** テキストフィールドに、**Active Directory** ドメインコントローラ上のグローバルカタログの場所を入力します。グローバルカタログは **Active Directory** フォレストを検索するためのリソースを提供します。

7 **適用** をクリックして設定を保存します。



**メモ**：次の手順に進む前に、設定を適用する必要があります。設定を適用しなければ、次のページへ移動したとき、入力した設定が失われます。

8 **標準スキーマの設定** セクションで、**役割グループ** をクリックします。**役割グループの設定** ページが表示されます。

9 **グループ名** を入力します。グループ名は、**CMC** カードに関連付けられた **Active Directory** で役割グループを識別します。

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

11 **役割グループの特権** ページで、グループの特権を選択します。

特権を変更すると、既存の**役割グループの特権**（システム管理者、パワーユーザー、ゲストユーザー）がカスタムグループまたは適切な役割グループの特権に変更されます。表 5-43 を参照してください。

12 **適用** をクリックして、役割グループの設定を保存します。

13 **ユーザー設定ページに戻る** をクリックします。

14 ドメインフォレストのルート認証局の署名付き証明書を **CMC** にアップロードします。**証明書のアップロード** ページで、証明書のファイルパスを入力するか、証明書ファイルの場所を指定します。ファイルを **CMC** に転送するには、**アップロード** ボタンをクリックします。



**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。

ドメインコントローラの **SSL** 証明書は、ルート認証局の署名付き証明書で署名されていなければなりません。**CMC** にアクセスする管理ステーションで、ルート認証局の署名付き証明書が使用可能である必要があります。

15 **適用** をクリックします。**適用** をクリックした後、**CMC** ウェブサーバー が自動的に再起動します。

16 **CMC Active Directory** 機能の設定を完了するには、ログアウトしてから **CMC** にログインします。

17 システムツリーで **シャーシ** を選択します。

18 **ネットワーク** タブをクリックします。

19 **ネットワーク** サブタブをクリックします。**ネットワーク設定** ページが表示されます。

- 20 ネットワーク設定 で **DHCP を使用 (CMC ネットワークインターフェース IP アドレス用)** が選択されている場合、**DHCP を使用して DNS サーバーアドレスを取得** を選択します。

DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、プライマリおよび代替 DNS サーバーの IP アドレスを入力します。

- 21 **変更の適用** をクリックします。

これで、CMC 標準スキーマ Active Directory 機能の設定が完了します。

## 標準スキーマ Active Directory と RACADM を使用した CMC の設定

標準スキーマの CMC Active Directory 機能を RACADM CLI を使用して設定するには、次のコマンドを使用します。

- 1 CMC へのシリアル /Telnet/SSH テキスト コンソールを開いて、次を入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <fully qualified root domain name>
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupName <common name of the role group>
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupDomain <fully qualified domain name>
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Bit mask number for
specific user permissions>
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate>
racadm sslcertdownload -t 0x1 -f <RAC SSL
certificate>
```



**メモ:** ビットマスクの番号については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）のデータベースプロパティ章の表 3-1 を参照してください。

2 次のいずれかのオプションを使用して DNS サーバーを指定します。

- CMC で DHCP が有効化されており、DHCP サーバーによって自動取得される DNS アドレスを使用したい場合は、次のコマンドを入力します。

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

- CMC で DHCP が無効になっている場合や、手動で DNS の IP アドレスを入力する場合は、次のコマンドを入力します。

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

```
racadm config -g cfgLanNetworking -o  
cfgDNSServer1 <primary DNS IP address>
```

```
racadm config -g cfgLanNetworking -o  
cfgDNSServer2 <secondary DNS IP address>
```

## 拡張スキーマの概要

Active Directory で拡張スキーマを有効にするには、次の 2 つの方法があります。

- CMC ウェブインタフェースを使用する。手順については、263 ページの「拡張スキーマ Active Directory と Web インタフェースを使用した CMC の設定」参照してください。
- RACADM CLI ツールを使用する。手順については、266 ページの「拡張スキーマ Active Directory と RACADM を使用した CMC の設定」参照してください。

### Active Directory スキーマ拡張

Active Directory データは、属性とクラスの分散データベースです。Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。

データベースに格納されるクラスの一例として、ユーザークラスがあります。ユーザークラスの属性には、ユーザーの姓、名、電話番号などが含まれます。

貴社の環境の固有なニーズを満たす独自の属性やクラスを追加して、データベースを拡張できます。デルでは、スキーマを拡張して、リモート管理の認証と許可をサポートするために必要な変更を含めました。

既存の Active Directory スキーマに追加した属性やクラスは、それぞれ固有の ID で定義する必要があります。業界全体で一意的 ID を維持できるように、Microsoft は Active Directory オブジェクト識別子 (OID) のデータベースを管理しています。Microsoft の Active Directory でスキーマを拡張するために、デルは固有の OID、固有の名前拡張子、デル固有の属性とクラスに一意的に関連付けた属性 ID を確立しました。

デルの拡張子：dell

デルのベース OID：1.2.840.113556.1.8000.1280

RAC LinkID 範囲：12070–2079

## RAC スキーマ拡張の概要

デルは管理者が設定できるプロパティのグループを提供しています。デルの拡張スキーマには、関連、デバイス、特権などのプロパティが含まれます。

関連プロパティは、特定の特権セットのあるユーザーまたはグループを 1 台または複数台の RAC デバイスに関連付けます。このモデルでは、ユーザー、RAC 特権、およびネットワーク上の RAC デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

## Active Directory オブジェクトの概要

認証と承認を Active Directory と統合したい CMC が 2 つネットワーク上にある場合は、各 CMC につき少なくとも 1 つの関連オブジェクトと 1 つの RAC デバイスオブジェクトを作成する必要があります。関連オブジェクトは必要なだけいくつでも作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数にも制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバでもかまいません。

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

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

図 8-2 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。

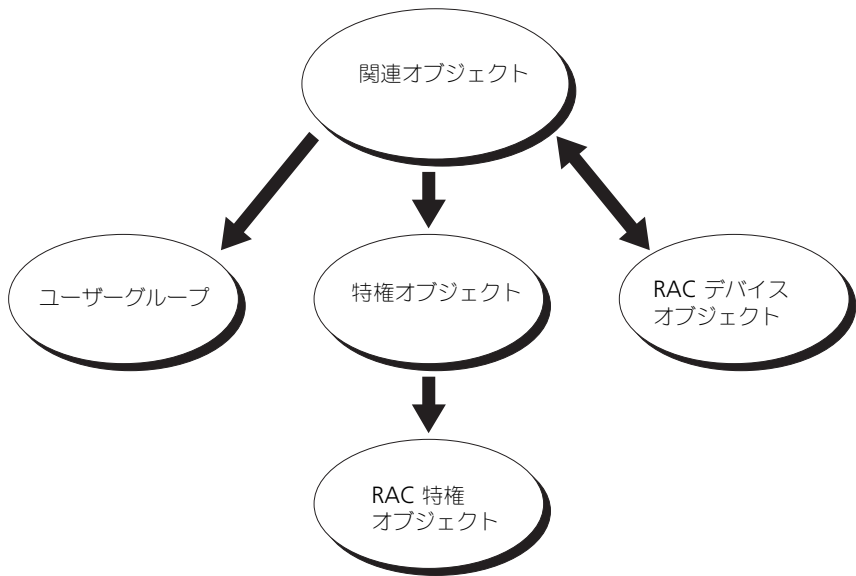


**メモ**：RAC 特権オブジェクトは DRAC 4、DRAC 5、および CMC に適用されます。



作成する関連オブジェクトの数に制限はありません。ただし、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 と統合する各 RAC (CMC) につき 1 つの RAC デバイスオブジェクトが必要です。

図 8-2. Active Directory オブジェクトの標準的なセットアップ

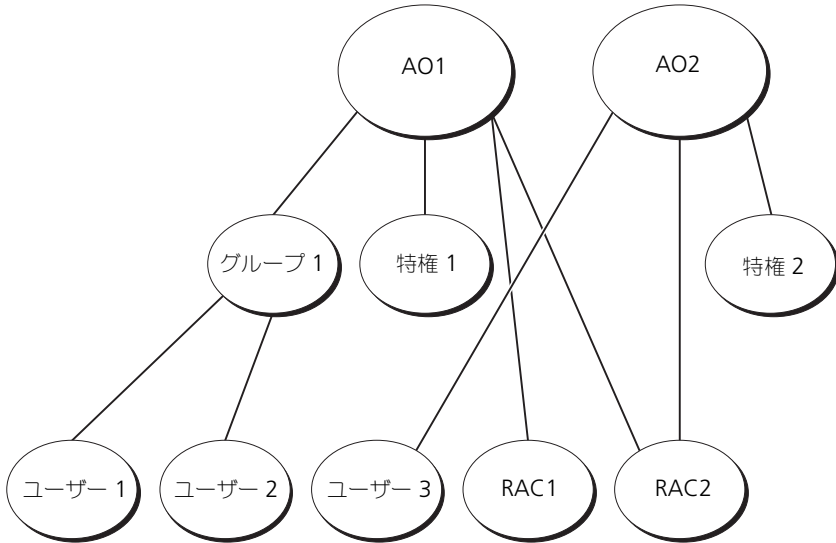


関連オブジェクトに含むことができるユーザー、グループ、RAC デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる特権オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは、RAC (CMC) に「特権」を持つ「ユーザー」を接続します。

また、Active Directory オブジェクトは、単一ドメイン、複数のドメインのいずれに設定することも可能です。たとえば、CMC が 2 つ (RAC1、RAC2) と、既存の Active Directory ユーザーが 3 つ (ユーザー 1、ユーザー 2、ユーザー 3) あるとし、ユーザー 1 とユーザー 2 に両方の CMC へのシステム管理者特権を与え、ユーザー 3 に RAC2 カードへのログイン特権を与えたいとします。図 8-3 に、このシナリオで Active Directory オブジェクトを設定する方法を示します。

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

図 8-3. 単一ドメインでの Active Directory オブジェクトの設定



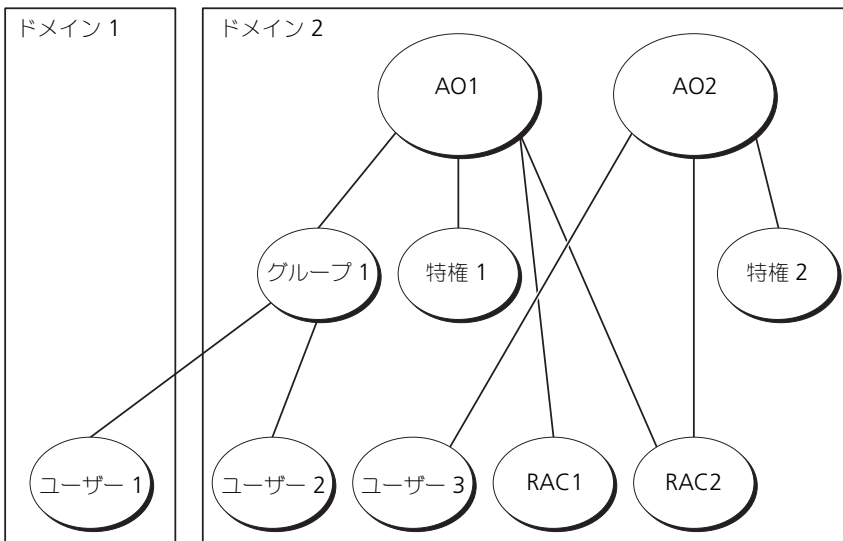
単一ドメインのシナリオでオブジェクトを設定するには

- 1 関連オブジェクトを 2 つ作成します。
- 2 2 つの CMC を表す 2 つの RAC デバイスオブジェクト、RAC1 と RAC2 を作成します。
- 3 2 つの特権オブジェクト、特権 1 と特権 2 を作成します。特権 1 にはすべての特権（システム管理者）、特権 2 にはログイン特権を与えます。
- 4 ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。
- 5 グループ 1 を関連オブジェクト 1 (A01) のメンバ、特権 1 を A01 の特権オブジェクトとして、RAC1 と RAC2 を A01 の RAC デバイスとして追加します。
- 6 ユーザー 3 を関連オブジェクト 2 (A02) のメンバ、特権 2 を A02 の特権オブジェクト、RAC2 を A02 の RAC デバイスとして追加します。

詳細な手順については、「261 ページの「Active Directory への CMC ユーザーと特権の追加」」を参照してください。

図 8-4 に、複数ドメインの Active Directory オブジェクトの例を示します。このシナリオでは、CMC が 2 つ（RAC1 と RAC2）と、既存の Active Directory ユーザーが 3 つ（ユーザー 1、ユーザー 2、ユーザー 3）あるとします。ユーザー 1 はドメイン 1 に存在し、ユーザー 2 とユーザー 3 はドメイン 2 に存在しています。このシナリオでは、ユーザー 1 とユーザー 2 に両方の CMC へのシステム管理者特権を持つように設定し、ユーザー 3 に RAC2 カードへのログイン特権を持つようにします。

図 8-4. 複数ドメインでの Active Directory オブジェクトの設定



複数ドメインのシナリオでオブジェクトを設定するには

- 1 ドメインのフォレスト機能がネイティブまたは Windows 2003 モードになっていることを確認します。
- 2 2 つの関連オブジェクト A01（ユニバーサルスコープの）と A02 を任意のドメインに作成します。

図 8-4 に、ドメイン 2 のオブジェクトを示します。

- 3 2 つの CMC を表す 2 つの RAC デバイスオブジェクト、RAC1 と RAC2 を作成します。
- 4 2 つの特権オブジェクト、特権 1 と特権 2 を作成します。特権 1 にはすべての特権（システム管理者）、特権 2 にはログイン特権を与えます。

- 5 ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。グループ 1 のグループスコープはユニバーサルでなければなりません。
- 6 グループ 1 を関連オブジェクト 1 (A01) のメンバ、特権 1 を A01 の特権オブジェクトとして、RAC1 と RAC2 を A01 の RAC デバイスとして追加します。
- 7 ユーザー 3 を関連オブジェクト 2 (A02) のメンバ、特権 2 を A02 の特権オブジェクト、RAC2 を A02 の RAC デバイスとして追加します。

## 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 CMC にアクセスする前に、Active Directory ソフトウェアと CMC を設定します。

- 1 Active Directory スキーマを拡張します (254 ページの「Active Directory スキーマの拡張」を参照)。
- 2 Active Directory ユーザーおよびコンピュータスナップイン を拡張します (260 ページの「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 CMC ユーザーとその権限を Active Directory に追加します (261 ページの「Active Directory への CMC ユーザーと特権の追加」を参照)。
- 4 各ドメインコントローラ上で SSL を有効にします。
- 5 CMC ウェブインタフェースまたは RACADM を使用して、CMC Active Directory プロパティを設定します (263 ページの「拡張スキーマ Active Directory と Web インタフェースを使用した CMC の設定」または 266 ページの「拡張スキーマ Active Directory と RACADM を使用した CMC の設定」を参照)。

## Active Directory スキーマの拡張

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前に、ドメインフォレストのスキーママスター Flexible Single Master Operation (FSMO) Role Owner にスキーマ管理者特権を持っていることを確認してください。

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』（Dell システム管理ツールおよびマニュアル 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<インストールタイプ>\LDIF Files
- <DVD ドライブ>:\SYSMGMT\ManagementStation\support\OMActiveDirectory\_Tools<インストールタイプ>\Schema Extender

LDIF ファイルを使用するには、**LDIF\_Files** ディレクトリにある **readme** の説明を参照してください。Active Directory スキーマを拡張するために Dell Schema Extender を利用する手順については、255 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



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

- 1 **よろこそ** 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 **Use Current Log In Credentials**（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。スキーマ拡張子を確認するには、Microsoft 管理コンソール（MMC）と Active Directory スキーマスナップインを使用し、次のものがあることを確認します。

- クラス — 表 8-2 ～表 8-7 参照
- 属性 — 表 8-8 参照

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

表 8-2. 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)
<b>dellRacDevice</b>	1.2.840.113556.1.8000.1280.1.1.1.1
<b>dellAssociationObject</b>	1.2.840.113556.1.8000.1280.1.1.1.2
<b>dellRACPrivileges</b>	1.2.840.113556.1.8000.1280.1.1.1.3
<b>dellPrivileges</b>	1.2.840.113556.1.8000.1280.1.1.1.4
<b>dellProduct</b>	1.2.840.113556.1.8000.1280.1.1.1.5

表 8-3. dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.1
説明	Dell RAC デバイスを表します。RAC デバイスは Active Directory では <b>dellRacDevice</b> として設定する必要があります。この設定により、CMC から Active Directory に Lightweight Directory Access Protocol (LDAP) クエリを送信できるようになります。
クラスの種類	構造体クラス
SuperClasses	<b>dellProduct</b>
属性	<b>dellSchemaVersion</b> <b>dellRacType</b>

表 8-4. dellAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.2
説明	Dell 関連オブジェクトを表します。この関連オブジェクトはユーザーとデバイスの間の接続を提供します。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	<b>dellProductMembers</b> <b>dellPrivilegeMember</b>

**表 8-5. dellRAC4Privileges クラス**

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	CMC デバイスの承認権限（特権）を定義します。
クラスの種類	補助クラス
SuperClasses	なし
属性	<b>dellIsLoginUser</b> <b>dellIsCardConfigAdmin</b> <b>dellIsUserConfigAdmin</b> <b>dellIsLogClearAdmin</b> <b>dellIsServerResetUser</b> <b>dellIsTestAlertUser</b> <b>dellIsDebugCommandAdmin</b> <b>dellPermissionMask1</b> <b>dellPermissionMask2</b>

**表 8-6. dellPrivileges クラス**

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	Dell の特権（承認権限）のコンテナクラス。
クラスの種類	構造体クラス
SuperClasses	ユーザー
属性	<b>dellRAC4Privileges</b>

**表 8-7. 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	<b>dellAssociationMembers</b>

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

割り当てられた OID/ 構文オブジェクト識別子	単一値
<b>属性：dellPrivilegeMember</b> 説明：この属性に属する <b>dellPrivilege</b> オブジェクトのリスト。 <b>OID</b> ：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
<b>属性：dellProductMembers</b> 説明：この役割に属する <b>dellRacDevices</b> オブジェクトのリスト。 この属性は <b>dellAssociationMembers</b> 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 <b>OID</b> ：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
<b>属性：dellIsCardConfigAdmin</b> 説明：ユーザーがデバイスの設定権限がある場合には TRUE。 <b>OID</b> ：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
<b>属性：dellIsLoginUser</b> 説明：ユーザーがデバイスでログイン権限がある場合には TRUE。 <b>OID</b> ：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
<b>属性：dellIsCardConfigAdmin</b> 説明：ユーザーがデバイスの設定権限がある場合には TRUE。 <b>OID</b> ：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
<b>属性：dellIsUserConfigAdmin</b> 説明：ユーザーがデバイスのユーザー設定システム管理者権限がある 場合には TRUE。 <b>OID</b> ：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



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

割り当てられた OID/ 構文オブジェクト識別子	単一値
<b>属性: dellLogClearAdmin</b>	
説明: ユーザーがデバイスのログのクリアシステム管理者権限がある場合には TRUE。	
OID: 1.2.840.113556.1.8000.1280.1.1.2.6	TRUE
ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
<b>属性: dellServerResetUser</b>	
説明: ユーザーがデバイスのサーバーリセット権限がある場合には TRUE。	
OID: 1.2.840.113556.1.8000.1280.1.1.2.7	TRUE
ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
<b>属性: dellTestAlertUser</b>	
説明: ユーザーがデバイスのテスト警告ユーザー権限がある場合には TRUE。	
OID: 1.2.840.113556.1.8000.1280.1.1.2.10	TRUE
ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
<b>属性: dellDebugCommandAdmin</b>	
説明: ユーザーがデバイスのデバッグコマンドシステム管理者権限がある場合には TRUE。	
OID: 1.2.840.113556.1.8000.1280.1.1.2.11	TRUE
ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
<b>属性: dellSchemaVersion</b>	
説明: 現在のスキーマバージョンを使用してスキーマをアップデートします。	
OID: 1.2.840.113556.1.8000.1280.1.1.2.12	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
<b>属性: dellRacType</b>	
説明: この属性は dellRacDevice オブジェクトの現在の RAC タイプで、dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。	
OID: 1.2.840.113556.1.8000.1280.1.1.2.13	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	

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

割り当てられた OID/ 構文オブジェクト識別子	単一値
<b>属性 : dellAssociationMembers</b>	
<p><b>説明 :</b> この製品に属する dellAssociationObjectMembers のリスト。 この属性は dellProductMembers リンク属性へのパスワードリンクです。</p> <p>リンク ID : 12071</p>	
<b>OID :</b> 1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
<b>属性 : dellPermissionsMask1</b>	
<b>OID :</b> 1.2.840.113556.1.8000.1280.1.6.2.1 整数 (LDAPTYPE_INTEGER)	
<b>属性 : dellPermissionsMask2</b>	
<b>OID :</b> 1.2.840.113556.1.8000.1280.1.6.2.2 整数 (LDAPTYPE_INTEGER)	

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

Active Directory でスキーマを拡張する場合は、RAC (CMC) デバイス、ユーザーとユーザーグループ、RAC 関連、RAC 特権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』(Dell システム管理ツールおよびマニュアル 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Dell拡張** 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に関する追加手順については、『Dell OpenManage Server Administrator インストールガイド』および『Dell OpenManage Management Station Software インストールガイド』を参照してください。

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

### Administrator Pack のインストール

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

## Active Directory ユーザーとコンピュータスナップインの開始

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

- 1 ドメインコントローラにログインしている場合は、**スタート** → **管理ツール** → **Active Directory ユーザーとコンピュータ** の順にクリックします。  
ドメインコントローラにログインしていない場合は、適切な **Microsoft Administrator Pack** がローカルシステムにインストールされている必要があります。この Administrator Pack をインストールするには、**スタート** → **ファイル名を指定して実行** の順にクリックし、MMC と入力して <Enter> を押します。Microsoft Management Console (MMC) が表示されます。
- 2 **コンソール 1** ウィンドウで、**ファイル** (または Windows 2000 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 **スナップインの追加と削除** をクリックします。
- 4 **Active Directory ユーザーとコンピュータ** スナップインを選択し、**追加** をクリックします。
- 5 **閉じる** をクリックします。

## Active Directory への CMC ユーザーと特権の追加

Dell の拡張 Active Directory ユーザーとコンピュータスナップインを使用して、RAC、関連、および特権オブジェクトを作成すると、CMC のユーザーと特権を追加できます。各オブジェクトタイプを追加するには、次の手順を実行します。

- 1 RAC デバイスオブジェクトの作成
- 2 特権オブジェクトの作成
- 3 関連オブジェクトの作成
- 4 関連オブジェクトへのオブジェクトの追加

### RAC デバイスオブジェクトの作成

RAC デバイスオブジェクトを作成するには、次の手順を実行します。

- 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 RAC オブジェクト** の順に選択します。  
**新規オブジェクト** ウィンドウが表示されます。
- 3 新しいオブジェクトの名前を入力します。この名前は、263 ページの「拡張スキーマ Active Directory と Web インタフェースを使用した CMC の設定」の手順 a で入力する CMC 名と同一である必要があります。
- 4 **RAC デバイスオブジェクト** を選択し、**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。

特権オブジェクトを作成するには：

- 1 **コンソールのルート** (MMC) ウィンドウでコンテナを右クリックします。
- 2 **新規** → **Dell RAC オブジェクト** の順に選択します。  
**新規オブジェクト** ウィンドウが表示されます。
- 3 新しいオブジェクトの名前を入力します。
- 4 **権限オブジェクト** を選択し、**OK** をクリックします。
- 5 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。
- 6 **RAC 特権** タブをクリックし、ユーザーに与える権限を選択します。CMC のユーザー権限の詳細については、149 ページの「ユーザータイプ」を参照してください。

## 関連オブジェクトの作成

関連オブジェクトはグループから派生し、グループタイプが含まれている必要があります。関連スコープは関連オブジェクトのセキュリティグループの種類を指定します。関連オブジェクトを作成する場合は、追加するオブジェクトの種類に適用される関連スコープを選択します。

たとえば、**ユニバーサル** を選択すると、関連オブジェクトは **Active Directory** ドメインがネイティブモード以上で機能している場合にのみ使用可能になります。関連オブジェクトを作成するには

- 1 **コンソールのルート** (MMC) ウィンドウでコンテナを右クリックします。
- 2 **新規** → **Dell RAC オブジェクト** の順に選択します。  
**新規オブジェクト** ウィンドウが開きます。
- 3 新しいオブジェクトの名前を入力します。
- 4 **関連オブジェクト** を選択します。
- 5 **関連オブジェクト** のスコープを選択し、**OK** をクリックします。

## 関連オブジェクトへのオブジェクトの追加

**関連オブジェクトプロパティ** ウィンドウを使用すると、ユーザーまたはユーザーグループ、特権オブジェクト、RAC デバイスまたは RAC デバイスグループ間の関連付けができます。Windows 2000 モード以降のシステムを使用している場合は、ユニバーサルグループを使ってユーザーまたは RAC オブジェクトでドメインを拡張する必要があります。

ユーザーおよび RAC デバイスのグループを追加できます。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

ユーザーまたはユーザーグループを追加するには、次の手順を実行します。

- 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。

**特権オブジェクト** タブをクリックして、RAC デバイスに認証するときにユーザーまたはユーザーグループの特権を定義する関連に、特権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

特権を追加するには、次の手順を実行します。

- 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。

**製品** タブをクリックして、1 台または複数台の RAC デバイスを関連に追加します。関連デバイスは、ネットワークに接続している RAC デバイスのうち、定義したユーザーまたはユーザーグループが使用できるものを指定します。関連オブジェクトには複数の RAC デバイスを追加できます。

### RAC デバイスまたは RAC デバイスグループの追加





RAC デバイスまたは RAC デバイスグループを追加するには、次の手順に従います。


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

### 拡張スキーマ Active Directory と Web インタフェースを使用した CMC の設定


拡張スキーマ Active Directory とウェブインタフェースを使用して CMC を設定するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** を選択します。
- 3 **ユーザー認証** → **ディレクトリサービス** をクリックします。  
ディレクトリサービス ページが表示されます。
- 4 **拡張スキーマ** を選択します。
- 5 **共通設定** セクションで次の操作を行います。：

- a **Active Directory を有効にする** チェックボックスが選択されていることを確認します。
  - b **ルートドメイン名** を入力します。
    -  **メモ:** ルートドメイン名 は x.y の命名規則に従う有効なドメイン名でなければなりません。x は 1 ~ 256 文字の ASCII 文字列で文字間にスペースは挿入できません。y は com、edu、gov、int、mil、net、org などの有効なドメイン名の種類です。
  - c **タイムアウト** の時間を秒単位で入力します。 **設定範囲:** 15 ~ 300 秒 **デフォルト:** 90 秒
- 6 **オプション:** ドメインコントローラとグローバルカタログの検索を直接呼び出す場合は、**検索する AD サーバーの検索 (オプション)** チェックボックスをオンにし、次の操作を行います。
- a **ドメインコントローラ** テキストフィールドに、Active Directory サービスがインストールされているサーバーを入力します。
  - b **グローバルカタログ** テキストフィールドに、Active Directory ドメインコントローラ上のグローバルカタログの場所を入力します。グローバルカタログは Active Directory フォレストを検索するためのリソースを提供します。
    -  **メモ:** IP アドレスを 0.0.0.0 に設定すると、CMC のサーバー検索が無効になります。
    -  **メモ:** コンマ区切りのドメインコントローラまたはグローバルカタログサーバーのリストを指定できます。CMC では、最大 3 個の IP アドレスまたはホスト名を指定できます。
    -  **メモ:** ドメインコントローラまたはグローバルカタログサーバーが、すべてのドメインとアプリケーションに対して正しく設定されていない場合は、既存のアプリケーション / ドメインの動作中に予期しない結果が生成される可能性があります。
- 7 **拡張スキーマの設定** セクションで、次の操作を行います。
- a **CMC 名** を入力します。**CMC 名** は Active Directory で CMC カードを一意に識別します。**CMC 名** は、ドメインコントローラで作成した新しい CMC オブジェクトのコモンネーム (CN) と同じでなければなりません。**CMC 名** は 1 ~ 256 文字の ASCII 文字列で、文字間にスペースは挿入できません。
  - b **CMC ドメイン名** を入力します (例: cmc.com)。**CMC ドメイン名** は、Active Directory CMC オブジェクトがあるドメインの DNS 名 (文字列) です。名前は x.y から成る有効なドメイン名にします。x は文字間に空白文字のない 1 ~ 256 の ASCII 文字列で、y は com、edu、gov、int、mil、net、org などの有効なドメインタイプです。
- 8 **適用** をクリックして設定を保存します。

 **メモ**：次の手順に進んで別のページへ移動する前に、設定を適用する必要があります。設定を適用しない場合、次のページへ移動したときに入力した設定が失われます。

- 9 **証明書**を管理 セクションで、テキストフィールドに証明書のファイルパスを入力するか、または **参照** をクリックして証明書ファイルを選択します。ファイルを CMC に転送するには、**アップロード** ボタンをクリックします。

 **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。

デフォルトでは、SSL 証明書の検証が必要です。**cfgActiveDirectory RACADM** と GUI 内では、証明書の検証を無効にする新しい設定があります。

 **注意**：この証明書を無効にするには危険が伴います。

SSL 証明書検証を有効にするには（デフォルト）：

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

SSL 証明書検証を無効にするには：

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

ドメインコントローラの SSL 証明書には、ルート認証局による署名が必要です。CMC にアクセスする管理ステーションで、ルート認証局の署名付き証明書が使用可能である必要があります。

- 10 **適用** をクリックします。**適用** をクリックした後、CMC ウェブサーバーが自動的に再起動します。
- 11 CMC ウェブインタフェースに再びログインします。
- 12 システムツリーで **シャーシ** を選択し、**ネットワーク** タブをクリックしてから **ネットワーク** サブタブをクリックします。**ネットワーク設定** ページが表示されます。
- 13 CMC ネットワークインターフェースの IP アドレスに **DHCP を使用** が有効の場合は、次のいずれかを行います。
  - **DHCP を使用して DNS サーバーアドレスを取得する** を選択して、DHCP サーバーが DNS サーバーアドレスを自動的に取得できるようにします。
  - **DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにしたままで、フィールドにプライマリおよび代替 DNS サーバーの IP アドレスを入力して DNS サーバーの IP アドレスを手動で設定します。
- 14 **変更の適用** をクリックします。  
CMC 拡張スキーマ Active Directory 機能の設定が完了します。

## 拡張スキーマ Active Directory と RACADM を使用した CMC の設定

ウェブインタフェースではなく、RACADM CLI ツールを使用して、CMC 拡張スキーマ Active Directory 機能を設定するには、次のコマンドを使用します。

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacDomain
<fully qualified CMC domain name>
racadm config -g cfgActiveDirectory -o cfgADRootDomain
<fully qualified root domain name>
racadm config -g cfgActiveDirectory -o cfgADRacName
<CMC common name>
racadm sslcertupload -t 0x2 -f <ADS root CA certificate> -r
racadm sslcertdownload -t 0x1 -f <CMC SSL certificate>
```



**メモ:** このコマンドはリモート RACADM を介してのみ使用できます。リモート RACADM の情報については、74 ページの「RACADM へのリモートアクセス」を参照してください。

**オプション:** DNS サーバーから返されたサーバーを使用せずに、LDAP またはグローバルカタログサーバーを指定してユーザー名を検索する場合は、次の **サーバーの指定** オプションを有効にします。

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



**メモ:** **サーバーの指定** オプションを使用すると、認証局の署名付き証明書が、指定したサーバーの名前と照合されません。IP アドレスだけでなくホスト名も入力できるため、CMC システム管理者にとっては特に便利です。

**サーバーの指定** オプションを有効にした後、サーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN) で LDAP サーバーとグローバルカタログを指定できます。FQDN はサーバーのホスト名とドメイン名で構成されます。


LDAP サーバーを指定するには次のように入力します。


```
racadm config -g cfgActiveDirectory -o
cfgADDomainController <AD domain controller IP address>
```




グローバルカタログサーバーを指定するには次のように入力します。

```
racadm config -g cfgActiveDirectory -o  
cfgADGlobalCatalog <AD global catalog IP address>
```

 **メモ:** IP アドレスを 0.0.0.0 に設定すると、CMC のサーバー検索が無効になります。

 **メモ:** コンマ区切りの LDAP または グローバルカタログサーバーのリストを指定できます。CMC では、最大 3 個の IP アドレスまたはホスト名を指定できます。

 **メモ:** すべてのドメインとアプリケーションに LDAP が正しく設定されていないと、既存のアプリケーション / ドメインの機能中に予期せぬ結果を招くことがあります。

## 2 次のいずれかのオプションを使用して DNS サーバーを指定します。

- CMC で DHCP が有効化されており、DHCP サーバーによって自動取得される DNS アドレスを使用したい場合は、次のコマンドを入力します。

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

- CMC で DHCP が無効になっている場合や、DHCP が有効でも DNS の IP アドレスを手動で指定したい場合は、次のコマンドを入力します。

```
racadm config -g cfgLanNetworking -o  
cfgDNSServersFromDHCP 0  
  
racadm config -g cfgLanNetworking -o  
cfgDNSServer1 <primary DNS IP address>  
  
racadm config -g cfgLanNetworking -o  
cfgDNSServer2 <secondary DNS IP address>
```

これで、拡張スキーマ機能の設定は完了しました。

## よくあるお問い合わせ (FAQ)

表 8-9. CMC と Active Directory の併用：よくあるお問い合わせ (FAQ)

質問	回答
Active Directory が複数のツリーにまたがる場合、これを使って CMC にログインできますか？	はい。CMC の Active Directory クエリアルゴリズムは、1 つのフォレストで複数のツリーをサポートします。
混在モード（すなわちフォレストのドメインコントローラが Microsoft Windows NT 2000 や Windows Server 2003 などの異なるオペレーティングシステムを実行）での Active Directory を使った CMC へのログインは可能ですか？	はい。混在モードでは、CMC クエリプロセスで使用されるすべてのオブジェクト（ユーザー、RAC デバイスオブジェクト、関連オブジェクトなど）が同じドメインになければなりません。デル拡張 Active Directory ユーザーとコンピュータスナップインはモードをチェックし、混合モードであれば、ドメイン間でオブジェクトを作成するためにユーザーを制限します。
CMC と Active Directory の併用は、複数のドメイン環境をサポートしますか？	はい。ドメインフォレストの機能レベルは、ネイティブか Windows 2003 モードであることが必要です。また、関連オブジェクト、RAC ユーザーオブジェクト、および RAC デバイスオブジェクト（関連オブジェクトを含む）にあるグループはユニバーサルグループでなければなりません。
これらの Dell 拡張オブジェクト（Dell 関連オブジェクト、Dell RAC デバイス、および Dell 特権オブジェクト）をいくつかのドメインに分散できますか？	関連オブジェクトと特権オブジェクトは同じドメインの中に置く必要があります。Dell 拡張 Active Directory ユーザーとコンピュータスナップインを使用する場合、これら 2 つのオブジェクトを同じドメインに作成することが強制されます。その他のオブジェクトは別のドメインに作成することができます。
ドメインコントローラの SSL 設定に制限はありますか？	はい。CMC では、信頼できる認証局の署名付き SSL 証明書を 1 つしかアップロードできないため、フォレスト内の Active Directory サーバーの SSL 証明書はすべて同じルート認証局によって署名される必要があります。


表 8-9. CMC と Active Directory の併用：よくあるお問い合わせ (FAQ) (続き)

質問	回答
<p>新しい RAC 証明書を作成しアップロードしましたが、ウェブインタフェースが起動しません。</p>	<p>Microsoft 証明書サービスを使用して RAC 証明書を生成した場合、証明書の作成時に <b>ウェブ証明書</b> でなく <b>ユーザー証明書</b> を誤って選択した可能性があります。</p> <p>回復するには、CSR を生成して、Microsoft 証明書サービスから新しいウェブ証明書を作成し、次の RACADM コマンドを入力してアップロードします。</p> <pre>racadm sslcsrngen [-g] [-f {filename}]  racadm sslcertupload -t 1 -f {web_sslcert}</pre>
<p>Active Directory 認証を使って CMC にログインできない場合は、どうすればよいですか？この問題はどのようにトラブルシューティングできますか？</p>	<ol style="list-style-type: none"> <li>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。</li> <li>2 ローカルの CMC 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 CMC にログインします。 ログインした後、次の手順を実行してください。 <ol style="list-style-type: none"> <li>a CMC Active Directory 設定ページの <b>Active Directory を有効にする</b> チェックボックスがオンになっていることを確認します。</li> <li>b CMC 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。</li> <li>c Active Directory ルート認証局の署名付き証明書から Active Directory 証明書を CMC にアップロードしたことを確認します。</li> <li>d ドメインコントローラの SSL 証明書の有効期限が切れていないことを確認します。</li> <li>e <b>CMC 名、ルートドメイン名、および CMC ドメイン名</b> が Active Directory の環境設定と一致することを確認します。</li> <li>f CMC のパスワードが 127 文字以内であることを確認します。CMC は最大 256 文字のパスワードをサポートしていますが、Active Directory がサポートしているパスワード長は最大 127 文字です。</li> </ol> </li> </ol>

## シングルサインオンの設定

Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista、Windows 7、および Windows Server 2008 では、ネットワーク認証プロトコル Kerberos を認証方法として使用することが可能であるため、ドメインにサインインしたユーザーは、次に使用するアプリケーション（Exchange など）への自動的なサインインまたはシングルサインオンが可能になります。

CMC バージョン 2.10 以降では、CMC は Kerberos を使ってシングルサインオンおよび Smart Card ログオンの 2 つの追加ログインタイプをサポートすることができるようになりました。シングルサインオンでログインする場合、CMC はクライアントシステムの資格情報を使用します。この資格情報は、有効な Active Directory アカウントを使ってログインした後、オペレーティングシステムによってキャッシュされます。

 **メモ**：ログイン方法を選択しても、他のログインインタフェース（SSH など）に対してポリシー属性が設定されるわけではありません。他のログインインタフェースに対しては別のポリシー属性を設定する必要があります。すべてのログインインタフェースを無効にするには、**サービス** ページに移動してからすべて（または一部の）ログインインタフェースを無効にします。

### システム要件

Kerberos 認証を使用するには、ネットワークには次の項目が必要です。

- DNS サーバー
- Microsoft Active Directory Server

 **メモ**：メモ：Windows 2003 で Active Directory を使用する場合は、クライアントシステムに最新のサービスパックとパッチがインストールされていることを確認してください。Windows 2008 で Active Directory を使用する場合は、SP1 と次のホットフィックスがインストールされていることを確認してください。KTPASS ユーティリティ用 **Windows6.0-KB951191-x86.msu**。このパッチがないと、ユーティリティで不良な keytab ファイルが生成されます。LDAP バインド中に GSS\_API および SSL トランザクションに使用する **Windows6.0-KB957072-x86.msu**。

- Kerberos キー配付センター（Active Directory サーバーソフトウェアに同梱）
- DHCP サーバー（推奨）
- DNS サーバー用のリバース（逆引き）ゾーンには Active Directory サーバーと CMC 用のエントリが必要です。

## クライアントシステム

- Smart Card でログインする場合は、クライアントシステムには Microsoft Visual C++ 2005 再頒布可能なプログラムが必要です。詳細については、[www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en) を参照してください。
- シングルサインオンと Smart Card ログインでは、クライアントシステムは Active Directory ドメインと Kerberos 領域の一部である必要があります。

## CMC

- CMC にはファームウェアバージョン 2.10 以降が必要
- 各 CMC には Active Directory アカウントが必要
- CMC は Active Directory ドメインと Kerberos Realm の一部である必要があります。

## 設定の実行

### 必要条件

- Active Directory (AD) の Kerberos 領域とキー配付センター (KDC) が設定済みである (ksetup)。
- クロックドリフトやリバースルックアップに伴う問題を回避するための強固な NTP および DNS インフラストラクチャ。
- 認証されたメンバーを含む CMC 標準スキーマ役割グループ。

## Active Directory の設定

アカウント オプションの **CMC プロパティ** ダイアログボックスで、次の設定を行います。


- **アカウントを信頼して委任** — 転送される資格情報は、このオプションを選択した時点で作成されます。現時点では、CMC はこのオプションの選択時に作成される転送された資格情報を使用しません。このオプションは、他のサービス条件によって、選択できる場合とできない場合があります。
- **アカウントは重要なので委任できない** — このオプションは、他のサービス条件によって、選択できる場合とできない場合があります。
- **このアカウントに Kerberos DES 暗号化を使う** — このオプションを選択します。
- **Kerberos 事前認証を必要としない** — このオプションは選択しません。

Microsoft Windows の一部である ktpass ユーティリティを、Active Directory 内のユーザーアカウントに CMC をマッピングするドメインコントローラ（Active Directory サーバー）上で実行します。たとえば、次のとおりです。

```
C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM  
-mapuser dracname -crypto DES-CBC-MD5 -ptype  
KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

 **メモ** : cmcname.domainname.com には RFC の要求に従って小文字を使用し、領域名 @REALM\_NAME には大文字を使用します。さらに、CMC では Kerberos 認証用の DES-CBC-MD5 タイプの暗号化もサポートされています。

この手順は、CMC にアップロードする必要のある keytab ファイルを作成します。

 **メモ** : keytab には暗号化キーが含まれているので、安全な場所に保管してください。ktpass ユーティリティの詳細については、Microsoft ウェブサイト [technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true](https://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true) を参照してください。

## CMC の設定

 **メモ** : 本項で説明された設定手順は、CMC のウェブアクセスに対してのみ適用されます。

Active Directory で設定した標準スキーマ役割グループ設定を、CMC で使用するように設定します。詳細については、246 ページの「CMC にアクセスするための標準スキーマ Active Directory の設定」を参照してください。

## Kerberos Keytab ファイルのアップロード

Kerberos keytab ファイルは Kerberos データセンター（KDC）に対する CMC のユーザ名とパスワード資格情報として使用され、これによって Active Directory にアクセスすることができます。Kerberos 領域の各 CMC は Active Directory を使って登録し、一意の keytab ファイルがあることが必要です。

keytab ファイルをアップロードするには：

- 1 ユーザー認証 タブ → ディレクトリサービス サブタブに移動します。**Microsoft Active Directory Standard** または **拡張スキーマ** が選択されていることを確認します。選択されていない場合は、任意の設定を選択してから **適用** をクリックします。
- 2 **Kerberos Keytab のアップロード** セクションで **参照** をクリックし、keytab ファイルの保存先フォルダに移動してから **アップロード** をクリックします。

アップロードを完了したら、アップロードに成功または失敗したかを通知するためのメッセージボックスが表示されます。

## シングルサインオンの有効化

- 1 **Chassis Management Controller Network Security** タブ → **Active Directory** → **Active Directory の設定** をクリックします。  
**Active Directory の設定と管理** ページが表示されます。
  - 2 **Active Directory の設定と管理** ページで、次を選択します。
    - シングルサインオン — このオプションを有効にすると、Active Directory にログインしたときに取得した資格情報のキャッシュを使用して CMC にログインできます。
-  **メモ:** このオプションでは、セキュアシェル (SSH)、Telnet、シリアル、リモート RACADM など、すべてのコマンドライン帯域外インタフェースは変更されません。
- 3 ページの下までスクロールし、**適用** をクリックします。

CLI コマンドのテスト機能を使用することにより、Kerberos 認証を使った Active Directory をテストできます。

```
testfeature -f adkrb -u <user>@<domain>
```

ここで、<user> には有効な Active Directory ユーザーアカウントを指します。コマンドが正常に実行されれば、CMC は Kerberos 資格情報を取得することができ、ユーザーの Active Directory アカウントにアクセスできることを示します。コマンドが正常に実行されない場合は、エラーを訂正してコマンドを実行し直してください。詳細については、デルサポートサイト

**support.dell.com/manuals** の『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 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。

## シングルサインオンのログインに使用するブラウザの設定


シングルサインオンは、Internet Explorer バージョン 6.0 以降と Firefox バージョン 3.0 以降でサポートされています。

 **メモ:** 次の手順は、CMC が Kerberos 認証でシングルサインオンを使用する場合にのみ適用されます。


### Internet Explorer

Internet Explorer でシングルサインオンの設定を行うには、次の手順を実行します。


- 1 Internet Explorer で、**ツール** → **インターネットオプション** を選択します。
- 2 **セキュリティ** タブの **セキュリティ設定を表示または変更するゾーンを選択する** の下で、**ローカルイントラネット** を選択します。
- 3 **サイト** をクリックします。  
**ローカルイントラネット** ダイアログボックスが表示されます。

- 4 **詳細** をクリックします。  
**ローカルイントラネットの詳細設定** ダイアログボックスが表示されます。
- 5 このサイトをゾーンに追加するに CMC の名前とそれが属するドメインを入力し、**追加** をクリックします。  
 **メモ** :対象ドメインでは、ワイルドカード (\*) を使用してすべてのデバイス/ユーザーを指定できます。

## Mozilla Firefox

- 1 Firefox では、アドレスバーに **about:config** と入力します。  
 **メモ** :ブラウザに「保証が無効になる場合があります」という警告が表示された場合は、**注意するので大丈夫です** をクリックします。
- 2 **フィルタ** テキストボックスに、`negotiate` と入力します。  
ブラウザには、「`negotiate`」という単語を含んだプリファレンス名のリストが表示されます。
- 3 表示されたリストから、**network.negotiate-auth.trusted-uris** をダブルクリックします。
- 4 **文字列値の入力** ダイアログボックスに、CMC のドメイン名を入力し、**OK** をクリックします。

## シングルサインオンを使用した CMC へのログイン

-  **メモ** :IP アドレスを使って、シングルサインオンまたはスマートカードにログインすることはできません。Kerberos は、完全修飾ドメイン名 (FQDN) に対してユーザーの資格情報を検証します。

シングルサインオンを使用して CMC にログインするには


- 1 ネットワークアカウントを使ってクライアントシステムにログインします。
- 2 次を使用して CMC ウェブページにアクセスします。

`https://<cmcname.domain-name>`

例 : `cmc-6G2WXF1.cmcad.lab`

ここで、`cmc-6G2WXF1` は CMC 名を表します。

`cmcad.lab` はドメイン名を表します。


-  **メモ** :デフォルトの HTTPS ポート番号 (ポート 80) を変更した場合は、`<cmc名.ドメイン名>:<ポート番号>` の書式で CMC ウェブページにアクセスします。ここで、**cmc名** は CMC の CMC ホスト名、**ドメイン名** はドメイン名、**ポート番号** は HTTPS のポート番号をそれぞれ表します。

CMC のシングルサインオン ページが表示されます。




### 3 ログインをクリックします。

CMC は、有効な Active Directory アカウントを使ってログインしたときにブラウザによってキャッシュされた Kerberos 資格情報でユーザーをログインします。ログインに失敗すると、ブラウザは通常の CMC ログインページにリダイレクトされます。

 **メモ** : Active Directory ドメインにログインしないで Internet Explorer 以外のブラウザを使用している場合は、ログインに失敗し、ブラウザには空白ページのみが表示されます。

## スマートカードによる二要素認証の設定

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。一方、2 要素認証ではユーザーがパスワードまたは PIN と秘密キーまたはデジタル証明書を含んだ物理カードを持っている必要があるため、高レベルのセキュリティを実現できます。ネットワーク認証プロトコルの Kerberos では、この 2 要素認証メカニズムを使用しており、これによってシステムはその信頼性を確認できます。Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista、および Windows Server 2008 では、Kerberos を認証方法として優先的に使用します。CMC バージョン 2.10 以降では、CMC は Kerberos を使用してスマートカードログインをサポートできるようになりました。

 **メモ** : ログイン方法を選択しても、他のログインインタフェース (SSH など) に対してポリシー属性が設定されるわけではありません。他のログインインタフェースに対しては別のポリシー属性を設定する必要があります。すべてのログインインタフェースを無効にするには、**サービス** ページに移動してからすべて (または一部の) ログインインタフェースを無効にします。

### システム要件

スマートカードの 270 ページの「システム要件」は、シングルサインオンと同じです。


### 設定の実行

スマートカードの 271 ページの「必要条件」は、シングルサインオンと同じです。

## Active Directory の設定

Active Directory を設定するには、次の手順を実行します。

- 1 Active Directory の Kerberos 領域とキー配付センター (KDC) が設定されていない場合は、設定してください (ksetup)。

 **メモ** : 強力な NTP および DNS インフラストラクチャによって、クロックドリフトやリバースルックアップの問題を確実に回避します。

- 2 各 CMC の Active Directory を作成し、事前認証でなく Kerberos DES 暗号化を使用できるように設定します。
- 3 Ktpass を使用して CMC ユーザーをキー配付センターに登録します (これにより、CMC にアップロードするキーも出力されます)。

## CMC の設定



**メモ**：本項で説明された設定手順は、CMC のウェブアクセスに対してのみ適用されます。

Active Directory で設定した標準スキーマ役割グループ設定を、CMC で使用するよう設定します。詳細については、246 ページの「CMC にアクセスするための標準スキーマ Active Directory の設定」を参照してください。

## Kerberos Keytab ファイルのアップロード


Kerberos keytab ファイルは Kerberos データセンター (KDC) に対する CMC のユーザ名とパスワード資格情報として使用され、これによって Active Directory にアクセスすることができます。Kerberos 領域の各 CMC は Active Directory を使って登録し、一意の keytab ファイルがあることが必要です。

keytab ファイルをアップロードするには：

- 1 **ユーザー認証** タブ → **ディレクトリサービス** サブタブに移動します。  
**Microsoft Active Directory Standard** または **拡張スキーマ** が選択されていることを確認します。選択されていない場合は、任意の設定を選択してから **適用** をクリックします。
- 2 **Kerberos Keytab のアップロード** セクションで **参照** をクリックし、keytab ファイルの保存先フォルダに移動してから **アップロード** をクリックします。  
アップロードを完了したら、アップロードに成功または失敗したかを通知するメッセージボックスが表示されます。

## スマートカード認証の有効化

スマートカード認証を有効にするには、次の手順を実行します。

- 1 **ユーザー認証** タブ → **ディレクトリサービス** サブタブに移動します。  
**Microsoft Active Directory Standard** または **拡張スキーマ** が選択されていることを確認します。
  - 2 **共通設定** セクションで次を選択します。
    - **スマートカード** — このオプションでは、スマートカードをリーダーに挿入し、PIN 番号を入力する必要があります。
-  **メモ**：このオプションでは、セキュアシェル (SSH)、Telnet、シリアル、リモート RACADM など、すべてのコマンドライン帯域外インターフェースは変更されません。
- 3 ページの下までスクロールし、**適用** をクリックします。

CLI コマンドテスト機能を使用すれば、Kerberos 認証によって Active Directory をテストできます。

次のように入力します。

```
testfeature -f adkrb -u <user>@<domain>
```

ここで、<user> には有効な Active Directory ユーザーアカウントを指します。コマンドが正常に実行されれば、CMC は Kerberos 資格情報を取得することができ、ユーザーの Active Directory アカウントにアクセスできることを示します。コマンドが正常に実行されない場合は、エラーを訂正してコマンドを実行し直してください。詳細については、RACADM コマンドの testfeature マニュアルを参照してください。

## スマートカードのログインに使用するブラウザの設定

### Mozilla Firefox

CMC 2.10 では、Firefox ブラウザを使ってスマートカードにログインすることはできません。

### Internet Explorer

インターネットブラウザが Active-X プラグインをダウンロードするように設定されていることを確認します。

## スマートカードを使用した CMC へのログイン



**メモ**：IP アドレスを使って、シングルサインオンまたはスマートカードにログインすることはできません。Kerberos は、完全修飾ドメイン名 (FQDN) に対してユーザーの資格情報を検証します。

スマートカードを使用して CMC にログインするには、次の手順を実行します。

- 1 ネットワークアカウントを使ってクライアントシステムにログインします。
- 2 次を使用して CMC ウェブページにアクセスします。

**https://<cmcname.domain-name>**

例：cmc-6G2WXF1.cmcad.lab

ここで、cmc-6G2WXF1 は CMC 名を表します。

cmcad.lab はドメイン名を表します。



**メモ**：デフォルトの HTTPS ポート番号 (ポート 80) を変更した場合は、<cmc 名.ドメイン名>:<ポート番号> を使って CMC ウェブページにアクセスします。ここで、cmc 名は CMC の CMC ホスト名、ドメイン名 はドメイン名、ポート番号 は HTTPS のポート番号をそれぞれ表します

**CMC のシングルサインオン** ページが表示され、スマートカードを挿入を求められます。

- 3 スマートカードをリーダーに挿入して **OK** 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。

- 4 オプションとしてセッションタイムアウトを選択します。これは、アクティビティを行うことなくログイン状態を継続できる時間を表します。デフォルト値は、ウェブサービスアイドルタイムアウトとして定義されています。詳細については、「サービスの設定」を参照してください。
- 5 パスワードを入力して、**OK** をクリックします。

## スマートカードログイン時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。

特定のクライアントにスマートカード CSP が存在するかどうかを確認する一般的なチェック方法は、Windows のログイン (Ctrl-Alt-Del) 画面でスマートカードをリーダーに挿入し、Windows がスマートカードを検出して PIN ダイアログボックスを表示するかどうかを確認します。

### 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スマートカード発行の担当者に問い合わせてください。

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

Active Directory ユーザーとして CMC 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せずに CMC にログインできるか試してみてください。次のコマンドを使用してローカル RACADM からスマートカードログオンを無効にすることもできます。

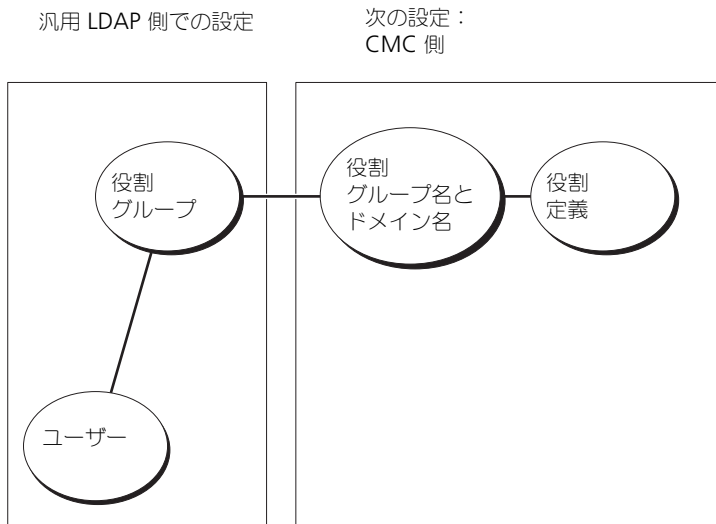
```
racadm config -g cfgActiveDirectory -o cfgADSSCLEnable 0  
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0
```

## 汎用 LDAP と CMC の併用

CMC 管理者は、LDAP サーバーのユーザーログインを CMC と統合することが可能です。この統合を行うには、LDAP サーバーと CMC の両方での設定が必要です。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。CMC 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。特権は、Active Directory サポートを伴う標準スキーマセットアップの動作に似た認証のため、CMC に引き続き保存されます。

LDAP ユーザーが特定の CMC カードにアクセスできるようにするには、その CMC カードに役割グループ名とそのドメイン名を設定する必要があります。各 CMC には、5 つまで役割グループを設定できます。表 5-43 に役割グループの特権レベル、表 8-1 に役割グループのデフォルト設定を示します。図 8-5 に汎用 LDAP を伴う CMC の設定を図示します。

図 8-5. 汎用 LDAP を伴う CMC の設定



### 汎用 LDAP ディレクトリを設定して CMC にアクセス

CMC の汎用 LDAP 実装では、ユーザーにアクセスを許可する際に 2 段階で行います。フェーズ 1 でユーザー認証を行ってから、フェーズ 2 でユーザー承認を行います。

## LDAP ユーザーの認証と承認

一部のディレクトリサーバーでは、特定の LDAP サーバーに対して検索を行う前にバインドが必要です。認証手順は次の通りです。

- 1 オプションでディレクトリサービスにバインドします。デフォルトは匿名バインドです。
- 2 ユーザーログインに基づきユーザーを検索します。デフォルトの属性は **uid** です。
- 3 複数のオブジェクトが検出された場合、プロセスはエラーを返します。
- 4 バインドを解除してから、ユーザーの DN とパスワードを使ってバインド実行します。
- 5 バインドできない場合は、ログインもできません。

これらの手順に問題がなければ、ユーザーは認証されたとみなされます。次のフェーズは承認です。CMD には最大 5 つのグループとそれに対応する特権が保存されています。ユーザーは、オプションでディレクトリサービス内に複数のグループを追加できます。ユーザーが複数グループのメンバの場合、そのグループのすべての特権を取得します。

承認手順は次の通りです。

- 1 設定された各グループで、**member** または **uniquemember** 属性内のユーザーの DN を検索します。このフィールドは、システム管理者により設定が可能です。
- 2 ユーザーが属するグループごとに、特権も一緒に追加します。

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

汎用 Lightweight Directory Access Protocol (LDAP) サービスを使用して、お使いのソフトウェアが CMC へのアクセスを提供するように設定できます。LDAP を使用すると、既存ユーザーの CMC ユーザー権限を追加したり管理することができます。



**メモ** : LDAP を CMC 用に設定するには、**シャージ設定システム管理者** の権限が必要です。

LDAP 設定、汎用 LDAP の設定の情報については、278 ページの「汎用 LDAP と CMC の併用」を参照してください。

LDAP の表示と設定を行うには、

- 1 ウェブインタフェースにログインします。
- 2 **ユーザー認証** タブをクリックしてから、**ディレクトリサービス** サブタブをクリックします。**ディレクトリサービス** ページが表示されます。
- 3 汎用 LDAP に関連付けられるラジオボタンをクリックします。
- 4 表示されているオプションを設定してから、**適用** をクリックします。

表 8-10 に、使用可能なオプションを示します。

表 8-10. 共通設定

設定	説明
汎用 LDAP を有効にする	CMC で汎用 LDAP サービスを有効にします。
識別名を使用してグループメンバーシップを検索	メンバーがデバイスにアクセスを許可されている LDAP グループの識別名 (DN) を指定します。
SSL 証明書検証を有効にする	チェックした場合、CMC は CA 証明書を使用して、SSL ハンドシェイク中に LDAP サーバー証明書を検証します。
バインド DN	ログインユーザーの DN の検索時に、サーバーにバインドするユーザーの識別名を指定します。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。
パスワード	バインド DN と併用するバインドパスワード。 <b>メモ:</b> バインドパスワードは機密データで、適切にセキュリティ保護されている必要があります。
検索するベース DN	すべての検索を開始するディレクトリの分岐の DN。
ユーザーログイン属性	検索対象の属性を指定します。設定されていない場合は、デフォルトで uid を使用します。選択したベース DN 内では一意であることを薦めます。そうでない場合、ログインユーザーの一意性を確保するために、検索フィルタを設定する必要があります。ユーザー DN が属性と検索フィルタの組み合わせを検索するとき一意に識別できない場合、ログインに失敗し、エラーが表示されます。
グループメンバーシップ属性	グループメンバーシップのチェックに使用される 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	有効な LDAP 検索フィルタを指定します。ユーザー属性によって、選択した baseDN 内でログインユーザーを一意的に識別できない場合に使用します。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。このプロパティの最大長は 1024 文字です。
ネットワークタイムアウト (秒)	時間を秒単位で設定すると、アイドルの LDAP セッションが自動的に閉じます。
検索タイムアウト (秒)	時間を秒単位で設定すると、検索が自動的に閉じます。

## LDAP サーバーの選択

サーバーを設定して汎用 LDAP を使用するには、2 つの方法があります。静的サーバーでは、システム管理者がフィールド内に FQDN または IP アドレスを設定できます。代わりに、DN 内で SRV を検索して、LDAP サーバーリストを取得できます。

次に挙げるのは、LDAP サーバーセクションのプロパティです。

- 静的 LDAP サーバーの使用 — このオプションを選択すると、LDAP サービスは、指定したサーバーとポート番号を使用します（次の詳細を参照）。



**メモ:** 静的 または DNS を選択します。

- LDAP サーバーアドレス — LDAP サーバーの FQDN または IP を指定します。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。CMC 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 — LDAP オーバー SSL のポート。設定されていない場合、デフォルトの 636 が使用されます。CMC バージョン 3.0 では、SSL なしでパスワードを転送することができないため、非 SSL ポートはサポートされていません。
- DNS を使用して LDAP サーバーを検索 — このオプションを選択すると、LDAP が DNS 経由で検索ドメインとサービス名を使用します。静的 または DNS を選択します。

次の DNS クエリが SRV レコードに対して実行されます。

```
_<Service Name>._tcp.<Search Domain>
```

ここで、<Search Domain> は、クエリ内で使用するルートレベルドメインで、<Service Name> はクエリ内で使用するサービス名です。たとえば、次のとおりです。

```
_ldap._tcp.dell.com
```

ここで、ldap はサービス名、dell.com は検索ドメインです。

## LDAP グループ設定の管理

グループ管理セクションの表は、役割グループ、関連名、ドメイン、既に設定されている役割グループの権限を表示します。

- 新しい役割グループを設定するには、名前、ドメイン、権限がリストアップされていない役割グループ名をクリックします。
- 既存の役割グループの設定を変更するには、役割グループ名をクリックします。



役割グループ名をクリックすると、**役割グループの設定** ページが表示されます。そのページのヘルプには、ページの右上にある **ヘルプ** リンクからアクセスできます。

## LDAP セキュリティ証明書の管理

この項では、最近 CMC にアップロードされた LDAP 証明書のプロパティを表示します。証明書をアップロードした場合、この情報を使用して証明書が有効で、期限が切れていないことを確認します。



**メモ**：デフォルトでは、認証局が発行した Active Directory 用のサーバー証明書は CMC にありません。認証局が署名した最新のサーバー証明書をアップロードする必要があります。

証明書の次のプロパティが表示されます。

- シリアル番号 - 証明書のシリアル番号。
- 対象者情報 - 証明書の対象者（証明対象の個人名または会社名）。
- 発行者情報 - 証明書の発行者（証明機関名）。
- 有効期限開始日 - 証明書の開始日。
- 有効期限終了日 - 証明書の失効日。

次のコントロールを使用すると、この証明書のアップロードおよびダウンロードが可能になります。

- アップロード - 証明書のアップロードプロセスを初期化します。LDAP サーバー から取得するこの証明書によって CMC へのアクセスが許可されます。
- ダウンロード - ダウンロードプロセスを初期化します。ファイルを保存する場所を問われます。このオプションを選択して **次へ** をクリックすると、**ファイルのダウンロード** ダイアログボックスが表示されます。このダイアログボックスで、管理ステーションまたは共有ネットワークにサーバー証明書を保存する場所を指定します。

## RACADM を使用した汎用 LDAP ディレクトリサービスの設定



**メモ**：この機能は、IPv4 と IPv6 を両方サポートします。

LDAP ログインの設定には、数多くのオプションがあります。大半の場合、デフォルト設定とともにいくつかのオプションを使います。



**メモ**：初めてのセットアップで LDAP 設定をテストするには、「racadm testfeature -f LDAP」コマンドを使用することをお勧めします。この機能は、IPv4 と IPv6 を両方サポートします。

必要なプロパティの変更には、LDAP ログインの有効化、サーバー FQDN または IP の設定、LDAP サーバーのベース DN の設定があります。

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`

- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN  
dc=company,dc=com`

オプションとして、DNS サーバーで SRV 記録のクエリを行うように CMC を設定できます。**cfgLDAPSRVLookupEnable** プロパティが有効の場合、**cfgLDAPServer cfgLDAPServer** プロパティは無視されます。SRV レコードに対して DNS を検索する場合は、次のクエリが使用されます。

```
_ldap._tcp.domainname.com
```

上記のクエリの ldap は、**cfgLDAPSRVLookupServiceName** プロパティです。

**cfgLDAPSRVLookupDomainName** は、**domainname.com** に設定されます。

## 使用状況

LDAP ユーザーを使用して CMC にログインするには、ログインプロンプトでユーザー名を入力し、パスワードプロンプトでパスワードを入力します。LDAP ユーザーが何らかの理由でログインできない場合、CMC はフォールバックし、同じユーザー名とパスワードでのローカルログインの使用を試行します。この操作により、ネットワーク接続がない、または LDAP サーバーが到達可能ではない場合にログインが可能です。

## 困ったときは

CMC のトレースログには、ユーザーがログインに失敗した理由がいくつか記載されています。LDAP ログインの失敗を判断するには、デバッグを有効にして `racadm testfeature -f LDAP` コマンドを使用することをお勧めします。

## 電力管理

Dell PowerEdge M1000e サーバーエンクロージャは、市場で最も電力効率が低いモジュラサーバエンクロージャです。これは、高効率の電源装置とファンを装備するように設計され、システム内の通気を最適化するレイアウトがとられています。また、エンクロージャ内全体を通して電力を最適化するコンポーネントが使用されています。最適化されたハードウェア設計、およびシャーシ管理コントローラ（CMC）、電源装置、iDRAC に内蔵されている高性能の電源管理機能によって、ユーザーは電力効率を向上させ、その電源環境を完全管理することを可能にします。

Dell PowerEdge M1000e モジュラエンクロージャは AC 電力を収容し、すべてのアクティブな内部電源装置ユニット（PSU）に電力を配分します。このシステムは、最大 16685 ワットの AC 電力を提供し、サーバーモジュールとそれに関連したエンクロージャのインフラに割り当てられます。

**電力の測定、低減、管理用コンソール（PM3）** から電力管理を制御することもできます。PM3 が電力を外部から制御すると、CMC は以下を維持できます。

- 冗長性ポリシー
- リモートでの電力ロギング
- 電源冗長性よりサーバーパフォーマンスを優先する
- 電源装置の動的制御
- 110 VAC 動作

PM3 は以下を管理します。

- サーバーの電力
- サーバーの優先度
- システム入力電力容量
- 最大節電モード

詳細については、325 ページの「外部電力管理」を参照してください。



**メモ**：実際の電源供給は、設定と負荷に基づいています。

M1000e の電力管理機能は、管理者が電力消費量を削減できるようにエンクロージャを設定し、独自の要件や環境に対応できるように電源管理をカスタマイズする作業をお手伝いします。

PowerEdge M1000e エンクロージャは、PSU の動作に影響を与え、管理者にシャーシの冗長性状態を報告する方法を決める 3 つの冗長性ポリシーのいずれかに設定可能です。

## AC 冗長性モード

AC 冗長性ポリシーの目的は、モジュラエンクロージャシステムが AC 電源障害に耐えるモードで動作できるようにすることです。電源障害の原因としては、AC 電力グリッド、ケーブル配線、または PSU 自体の障害が考えられます。

AC 冗長性をシステムに設定すると、PSC はグリッドに分割されます。スロット 1、2、3 の PSU は最初のグリッドにあり、スロット 4、5、6 の PSU は 2 番目のグリッドにあります。CMC は、グリッドのいずれかが故障した場合、システムが劣化することなく動作を継続するよう電力を管理します。AC 冗長性は、個々の PSU の障害にも対処します。



**メモ:** AC 冗長性の役割のひとつは、電源グリッド全体に障害が発生してもサーバー動作がシームレスに行えるようにすることです。このため、AC 冗長性を維持するために使用できる電力は、2 つのグリッドの容量がほぼ同等の場合に最大となります。



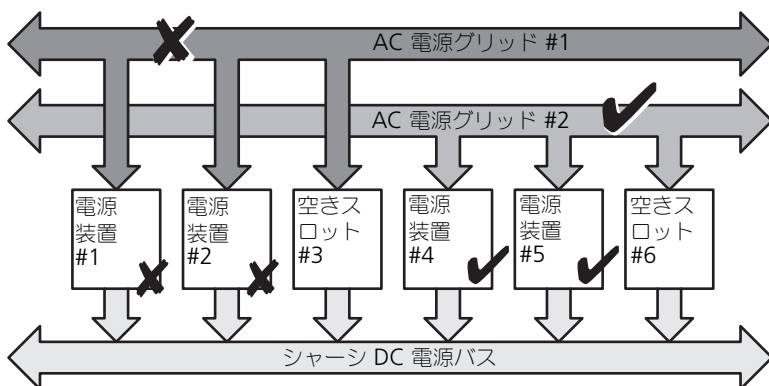
**メモ:** AC 冗長性は、負荷要件が最も弱い電源グリッドの容量を超えない場合のみ満たされます。

## AC 冗長性レベル

各グリッドの PSU は、AC 冗長性として使用するには、最低限の構成が満たされている必要があります。追加の構成は、各グリッドに最低 1 台の PSU を持つそれぞれの組み合わせがあれば可能です。ただし、最大電力を使用できるようにするには、各レグの総電力が実用と同程度である必要があります。AC 冗長性を維持する場合の電力の上限は、最も弱い 2 つのグリッドで利用できる電力です。グリッドにつき PSU が 2 台あり、グリッド 1 に電源障害が発生している例を図 9-1 に図示します。

冗長性喪失イベントを警告するように設定されている場合には、何らかの理由で CMC が AC 冗長性を維持できなくなると、E-メールまたは SNMP（またはその両方）アラートがシステム管理者に送信されます。

図 9-1. グリッドにつき PSU が 2 台とグリッド 1 に電源エラー



**メモ:** この構成で 1 台の PSU に障害が発生すると、障害側の残りの 2 台の PSU にオンラインのマークが付きます。この状態で、残りの PSU のいずれかに障害が発生しても、システムの動作が中断されることはありません。PSU に障害が発生すると、シャーシの正常性に非重要なマークが付きます。小さいグリッドでシャーシ電源をすべて割り当てることができない場合は、AC 冗長性は冗長性なしと報告され、シャーシの正常性は重要と表示されます。

### 電源装置冗長モード

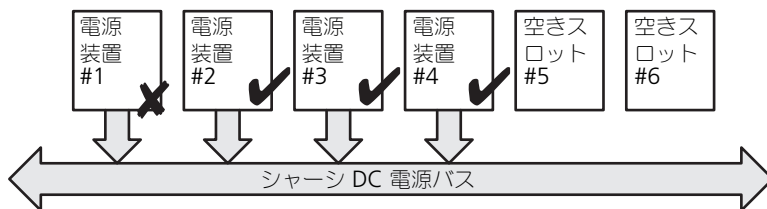
電源装置冗長モードは、冗長電源グリッドが存在しないが、1 台の PSU の障害でモジュラエンクロージャ内のサーバーが停止しないようにする対策に役立ちます。このため、最高容量の PSU は、予備のためにオンラインのままとなっています。これにより、電源装置の冗長性プールが作成されます。図 9-2 に電源装置冗長モードを図示します。

電力と冗長性のために必要な分を超えた PSU を利用することも可能で、これらは障害時に備えて冗長性プールに追加されます。

AC 冗長性の場合と異なり、電源冗長性が選択された場合でも、CMC では、PSU ユニットを特定の PSU スロットの位置に設置する必要がありません。

**メモ:** DPSE（動的電源供給）を使用すると、PSU をスタンバイ状態にできます。スタンバイ状態は、電源の状態ではなく、物理的状态を示します。DPSE を有効にすると、余剰 PSU がスタンバイモードになり、効率アップと節電につながります。

図 9-2. 電源の冗長性：合計 4 台の PSU があり、そのうち 1 台が故障。



デュアルまたはシングル電源グリッド：  
電源装置冗長性は、単一電源装置の障害からの  
保護を提供します。

## 冗長性なしモード

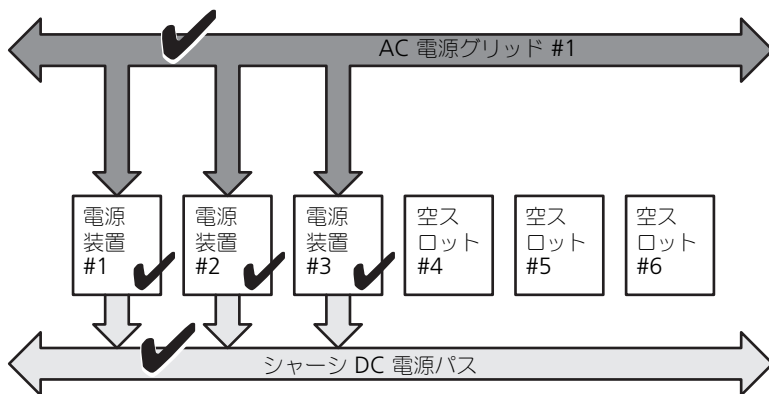
**冗長性なしモード**は、3 台の PSU 構成の工場出荷時のデフォルトであり、シャーシに電源の冗長性が設定されていないことを示します。この構成のとき、シャーシの全体的な冗長性が常に **冗長性なし** であることを示します。3 PSU 構成の場合、**冗長性なし** モードが工場出荷時のデフォルトであることを図 9-3 に図示します。

**冗長性なし** が設定されている場合、CMC では、PSU ユニットを特定の PSU スロット位置に設置する必要はありません。



**メモ**：DPSE が **冗長性なし** モードで無効になっている場合、シャーシ内のすべての PSU は **オンライン** としてリストされています。DPSE が有効な場合、シャーシのすべてのアクティブな PSU は **オンライン** としてリストされ、追加の PSU は **スタンバイ** モードとなり、システムの電力効率が上昇します。

図 9-3. シャーシにある冗長性なしモードの 3 台の PSU



シングル電源グリッド：  
グリッドまたは電源装置の故障に対して、保護しません。

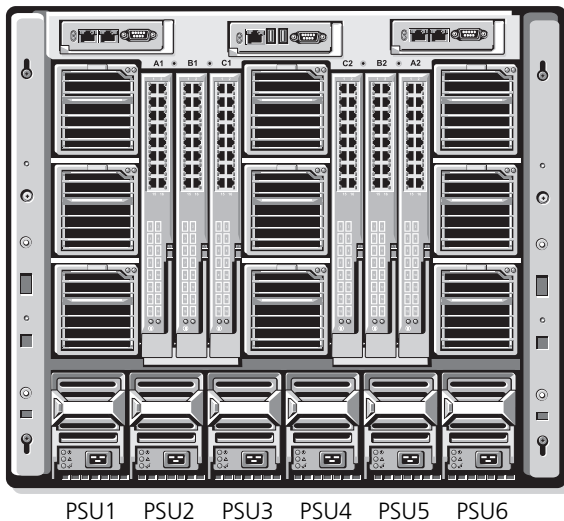
1 台の PSU で障害が発生すると、シャーシの電源割り当てをサポートするために、必要に応じて他の PSU はスタンバイモードが解除されます。PSU が 4 台あり、3 台のみ必要な場合、1 台が故障すると 4 番目の PSU がオンラインとなります。シャーシは、全 6 台をオンラインにできます。

DPSE を有効にすると、余剰 PSU がスタンバイモードになり、効率アップと節電につながります。詳細については、293 ページの「電源装置の動的制御」を参照してください。

### ハードウェアモジュールの電力バジェット

図 9-4 には、6 台の PSU 構成のシャーシが示されています。PSU は、エンクロージャの左端から 1～6 の番号が付けられています。

図 9-4. PSU 6 台構成のシャーシ



CMC は、設置されているすべてのサーバーとコンポーネントに必要なワット数を蓄えるエンクロージャの電力バジェットを維持します。

CMC は、シャーシ内の CMC インフラストラクチャとサーバーに電力を割り当てます。CMC インフラストラクチャは、ファン、I/O モジュール、iKVM（存在する場合）などのシャーシ内のコンポーネントで構成されています。シャーシには、iDRAC 経由でシャーシと通信する最大 16 台のサーバーを搭載できます。詳細については、[support.dell.com/manuals](https://support.dell.com/manuals) にある『iDRAC ユーザーズガイド』を参照してください。

iDRAC は、サーバーの電源を投入する前に、CMC に電力エンベロップ要件を提供します。電力エンベロップは、サーバーを動作し続けるために必要な最大 / 最小電力要件から構成されています。iDRAC の初期予測は、まずサーバーのコンポーネントを理解することにあります。動作が開始し、さらにコンポーネントが見つかり、iDRAC は初期電力要件を増加または減少します。

サーバーがエンクロージャで電源投入されると、iDRAC ソフトウェアは電源要件を推定し直して、電力エンベロップの変更を要求します。



CMC は要求された電力をサーバーに供給し、その割り当てられたワット量は、使用可能なバジェットから減算されます。サーバーに電力要求量が与えられると、サーバーの iDRAC ソフトウェアは実際の電力消費量を継続的に監視します。実際の電力要件に応じて、iDRAC 電力エンベロープは時間の経過に伴い変更される場合があります。iDRAC は、サーバーが割り当てられた電力を完全に消費している場合にのみ、電力アップを要求します。

重い負荷の下では、サーバーのプロセッサのパフォーマンスは、電力消費がユーザーが設定した **システム入力電力の上限値** の下に留まるように低下します。

PowerEdge M1000e エンクロージャは、ほとんどのサーバー設定で最高の性能を発揮するために十分な電力を供給できますが、利用可能なサーバー構成の多くでは、エンクロージャが供給可能な最大電力を消費することはありません。データセンター施設でエンクロージャの電力プロビジョニングを設定するとき、M1000e を使うと、ユーザーは **システム入力電力上限** を指定して、全体的なシャーシの AC 電力が与えられたしきい値を超えないようにできます。CMC はまず、ファン、IO モジュール、iKVM（存在する場合）、および CMC 自体の稼動に十分な電力を確保します。この電力の割当ては、**シャーシインフラに割当てた入力電力** と呼びます。シャーシインフラストラクチャの後に、エンクロージャのサーバーの電源が入ります。**システム入力電力の上限値** を実際の消費量より下に設定しようとしても、そのような設定はできません。

総電力バジェットを **システム入力電力上限** の値より低くする必要がある場合は、CMC が、要求された最大電力より低い値をサーバーに割り当てます。サーバーには個々の **サーバーの優先度** 設定に基づいて電力が割り当てられます。たとえば、優先度 1 のサーバーは最大電力を取得し、優先度 2 のサーバーは優先度 1 のサーバーの後に電力を取得する、というようになります。**システム入力の最大電力容量** とユーザーが設定した **システム入力電力上限** によっては、優先度が低いサーバーが取得する電力量は、優先度 1 のサーバーよりも少ない場合があります。

シャーシにサーバーを追加するなどの構成上の変更を行う場合は、**システム入力電力上限** を上げる必要があることがあります。モジュラエンクロージャに必要な電力は、温度条件が変わり、ファンを高速で運転する必要がある場合、つまり電力消費量を増やす必要が発生した場合にも増加します。また、I/O モジュールや iKVM を追加する場合にも、モジュラエンクロージャの必要電力が増加します。サーバーの電源が入っていない場合でも、管理コンソールへの電源供給を維持するため、サーバーは極めて少ない量の電力を消費します。

供給電力が十分ある場合のみ、追加サーバーへの電源投入をモジュラエンクロージャ内で行うことができます。**システム入力電力上限** をいつでも最大 16685 ワットまで増量して、追加サーバーに電力を供給することができます。

電力の割り当てを削減するモジュラエンクロージャの変更項目は、次のとおりです。

- サーバーの電源オフ
- サーバー
- I/O モジュール
- iKVM の削除
- シャーシの電源オフ状態への移行

シャーシがオンの場合にもオフの場合にも、**システム入力電力上限**を再設定できます。



**メモ:** シングルハイト以外の形状のサーバーを挿入しており、iDRAC への電源が十分ではない場合、そのサーバーは複数台のシングルハイトのサーバーとして表示されます。

## サーバースロットの電力優先度の設定

CMC では、エンクロージャの 16 個のサーバースロットのそれぞれの電力優先度をユーザーが設定できます。優先度設定は、**1**（優先度高）～**9**（優先度低）です。この設定は、シャーシのスロットに割り当てられ、スロットの優先度は、そのスロットに挿入されるサーバーに継承されます。CMC はスロットの優先度を使って、エンクロージャ内の最も優先度の高いサーバーに優先的に電力バジェットを割り当てます。

デフォルトのサーバースロット優先度設定に従って、電力はすべてのスロットに均等に割り当てられます。スロットの優先度を変更することで、システム管理者はどのサーバーに電力供給が必要か優先順位を付けることができます。より重要なサーバー モジュールの優先度をデフォルトの 1 にしたまま、それほど重要でないサーバー モジュールの優先度を 2 以上に設定すると、優先度が 1 のサーバー モジュールに先に電力が供給されます。優先度の高いサーバーには最大電力が割り当てられますが、優先度の低いサーバーには、最大の性能を発揮するために必要な電力が共有されない、または全く電力が供給されない場合があります。

これは、設定された優先度の度合いとサーバーが必要とする電力量に依存します。

システム管理者が優先度の高いサーバーより先に優先度の低いサーバーの電力を手動でオンにすると、優先度のより高いサーバーに電力を割り当てるため、これらの優先度の低いサーバーモジュールが電力割り当ての最小値までの削減が最初に行われるモジュールとなります。利用可能な電力割り当てを使い切ってしまうと、CMC は、優先度の低いまたは同程度のサーバーから、それらの電力が最低限のレベルになるまで電力を再要求します。



**メモ:** I/O モジュール、ファン、および iKVM（存在する場合）に最も高い優先度が指定されます。CMC は、優先度の高いモジュールまたはサーバーの電力ニーズを満たすためのみ、優先度の低いデバイスから電力を再要求します。

## 電源装置の動的制御

DPSE（動的電源供給）モードは、デフォルトで無効に設定されています。

DPSE は、電源からシャーシへの PSU のサーバー管理者を最適化して電力を保存します。この結果、PSU の寿命が高まり、発熱を減らします。

CMC は、エンクロージャ全体の電力割り当てを監視し、PSU を **スタンバイ** 状態にすることで、シャーシの総合電力割り当てをより少数の PSU で賄えるようにします。オンライン PSU の利用率が高いほどより効率的であるため、効率の向上につながると同時に、スタンバイ PSU の寿命も延長できます。

残りの PSU を最大効率で動作するには：

- **DPSE の冗長性なし** モードでは、最適な PSU オンラインであるため、高い電力効率を得られます。必要のない PSU はスタンバイモードになります。
- **DPSE の PSU 冗長性** モードでも、電力効率を得ることができます。最低 2 台の PSU をオンラインにし、1 台には電源設定を行い、もう 1 台には PSU の障害に備えて冗長性を設定します。**PSU 冗長性** モードでは 1 台の PSU の故障に対して保護を提供しますが、AC グリッドを喪失した場合は保護されません。
- **DPSE の AC 冗長性** モードは、6 台のうち最低 2 台をアクティブ（各電力グリッドに 1 台ずつ）にして、部分的に負荷のかかるモジュラエンクロージャ構成の効率と最大電力供給のバランスを保ちます。
- DPSE を無効にすると、6 台すべてを稼働して付加を分散させるため効率性が下がるため、各電源装置の利用率も低下します。

DPSE は、ここで説明された 3 つのすべての電源装置冗長性構成（**冗長性なし**、**電源装置冗長性**、**AC の冗長性**）を有効にできます。

- DPSE の **冗長性なし** 構成では、M1000e は **スタンバイ** 状態で最大 5 台の電源装置を保持できます。PSU 6 台の構成では、一部の PSU ユニットを使用しないでスタンバイ状態にしておくことで、電力効率を向上させます。この構成でオンラインの PSU を取り外したり、障害が発生したりすると、**スタンバイ** 状態の PSU は **オンライン** に切り替わります。ただし、スタンバイ PSU がアクティブになるまでに最大 2 秒間かかるため、**冗長性なし** 構成での移行中に、一部のサーバーモジュールに電力が供給されなくなる場合があります。



**メモ：**この PSU 3 台の構成では、サーバー負荷によって PSU が **スタンバイ** に移行できないことがあります。

- **電源装置冗長性** 構成では、エンクロージャは電源投入に必要な PSU 以外に、追加 PSU の電源を常にオンに保ち、**オンライン** のマークを付けます。電源使用量を監視し、システム全体の負荷に応じて、最大 4 台の PSU を **スタンバイ** 状態に移行できます。PSU 6 台の構成では、最低 2 台の電源装置が常にオンに保たれます。

**電源装置冗長性** 構成のエンクロージャでは、常に 1 台の余剰 PSU がオンになっているため、オンライン PSU の 1 台に障害が発生しても、設置されているサーバーモジュールに十分に電源を供給することができます。オンライン PSU に障害が発生すると、スタンバイ PSU がオンラインになります。複数の PSU に同時に障害が発生すると、スタンバイ PSU を立ち上げている間、いくつかのサーバーモジュールに電源が供給されない場合があります。

- **AC 冗長性** 構成では、シャーシの電源投入時にすべての電源装置がオンになります。電源利用状況は監視され、システム設定と電力利用状況によっては、PSU は **スタンバイ** 状態に移行します。グリッドにある PSU の **オンライン** 状態はミラーしているため、エンクロージャは、グリッドへの電力を喪失してもエンクロージャへの電力に支障なく電力を維持することができます。

**AC 冗長性** 設定で電力需要が増加すると、**スタンバイ** 状態にある PSU が使用されます。こうして、デュアルグリッド冗長性に必要なミラー構成が維持されます。



**メモ** : DPSE を有効にすると、電力需要が 3 つのすべての電源冗長性ポリシーモードで高まった場合、スタンバイ PSU が **オンライン** になり、電力を供給します。

## 冗長性ポリシー

冗長性ポリシーは、CMC によるシャーシ電力供給管理の方法を指定するための、設定可能なプロパティの一連です。次の冗長性ポリシーは、PSU の動的制御の有無にかかわらず設定可能です。

- AC 冗長性
- 電源装置冗長性
- 冗長性なし

シャーシでのデフォルト冗長性構成は、表 9-1 に示す通り、構成する PSU の数に依存します。

表 9-1. デフォルトの冗長構成


PSU 構成	デフォルトの冗長性ポリシー	デフォルトの PSU 動的制御設定
PSU 6 台	AC 冗長性	無効
PSU 3 台	冗長性なし	無効

## AC 冗長性

PSU 6 台の AC 冗長性モードでは、6 台の PSU はすべてアクティブです。左側の PSU 3 台を 1 つの AC 電源グリッドに、そして右側の 3 台を別の電源グリッドに接続する必要があります。

 **注意**：システムエラーを回避し、AC 冗長性を効率的に機能させるには、PSU 一式がバランス良く個別の AC グリッドに適切に接続される必要があります。

一方の AC グリッドが故障した場合、まだ機能している AC グリッドに接続されている 3 台の PSU でサーバーやインフラストラクチャに支障なく引き続き電力を供給します。


 **注意**：AC 冗長性モードでは、バランスのとれた台数の PSU セットが必要で（各グリッドに少なくとも 1 台の PSU が必要）。この条件を満たさない場合、AC 冗長性を実現できない可能性があります。

## 電源装置冗長性

電源装置冗長性を有効にすると、シャーシの PSU を 1 台予備として保持して、どの 1 台の PSU に障害が発生してもサーバーやシャーシへの電力が低下しないようになっています。電源装置冗長性モードでは、最大 4 台の PSU が必要です。DPSE が有効な場合には、追加の PSU が存在すれば、それらが電力効率の改善のために使用されます。冗長性を喪失した後に障害が発生すると、シャーシ内のサーバーの電源が低下する可能性があります。

## 冗長性なし


シャーシが必要とする供給量を超えた電力が、障害発生時においても、シャーシへの電力供給を継続するために利用可能です。

 **注意**：冗長性なしモードは、DPSE がシャーシ要件に関して有効化されている場合、最適な数の PSU を使用します。このモードの場合、1 台の PSU の障害発生により、サーバーの電源とデータが失われる可能性があります。

## 節電と電力バジェットの変更

ユーザー設定の電力上限値に達すると、CMC は節電を実行します。電力需要がユーザー設定の **システム入力電力上限** を超えると、CMC は優先度の低い順にサーバーへの電力供給を低減して、シャーシ内の優先度の高いサーバーおよびその他のモジュールに電力を解放します。

シャーシ内のすべてまたは複数のスロットが同じ優先順位に設定されている場合、CMC はスロット番号の小さい順にサーバーへの電力を低減させます。たとえば、スロット 1 と 2 にあるサーバーが同じ優先順位を持つ場合、スロット 1 のサーバーの電力の方がスロット 2 のサーバーの電力より先に低減されます。

 **メモ**：シャーシ内のサーバーにそれぞれ 1～9 の番号を与えることで優先順位を割り当てることができます。すべてのサーバーのデフォルト優先順位は 1 です。低い番号の方が優先順位が高くなります。

サーバーの優先順位を割り当てる手順は、「317 ページの「RACADM の使用」を参照してください。

GUI を使用してサーバーの優先順位を割り当てることができます。

- 1 システムツリーで **サーバー** をクリックします。
- 2 **電源** → **優先順位** をクリックします。

### 節電と最大節電モード

CMC は、次の場合に最大節電モードを実行します。

- ユーザーが、ウェブインタフェースまたは RACADM を使用して最大節電モードを選択する場合。
- UPS デバイスにより発行された自動コマンドラインスクリプトが、最大節電モードを選択する場合。

最大節電モードで、全サーバーが最低電力レベルで機能を起動し、その後のサーバー電力割り当て要求がすべて拒否される場合。このモードでは、電源がオンのサーバーのパフォーマンスの質が低下します。追加サーバーは、サーバーの優先順位にかかわらず、電源がオンにできません。

ユーザーまたは自動コマンドラインスクリプトが最大節電モードをクリアすると、システムはフルパフォーマンスに復元されます。

### ウェブインタフェースの使用

最大節電モードは、GUI を使用して選択、または選択解除できます。

- 1 システムツリーで **シャーシの概要** をクリックします。
- 2 **電源** → **設定** をクリックします。
- 3 **最大節減モード** ボックスを選択して最大節減モードを有効にしてから、**適用** をクリックします。
- 4 **最大節減モード** をクリアし、通常の動作を復元してから、**適用** をクリックします。

### RACADM の使用

シリアル /Telnet/SSH コンソールを開いて、CMC にログインします。

- 最大節電モードを有効にするには、次を入力します。

```
racadm config -g cfgChassisPower -o  
cfgChassisMaxPowerConservationMode 1
```

- 通常の動作を復元するには、次を入力します。

```
racadm config -g cfgChassisPower -o  
cfgChassisMaxPowerConservationMode 0
```

## 110V の PSU の動作

PSU には、110V の AC 入力で作動する機種があります。この入力は、分岐回路で許容されている数値を超える場合があります。110V の AC に接続される PSU がある場合は、エンクロージャの通常動作のために CMC を設定する必要があります。上記が設定されていない場合に 110V の PSU が検出されると、その後のサーバー電力割り当ての要求が拒否されます。この場合、追加されるサーバーは、優先順位に関係なく電力がオンになりません。110V の PSU を使用するには、ウェブインターフェースまたは RACADM を使って CMC を設定します。

### ウェブインターフェースの使用

110V の回路が予測電流に定格されていることを確認してから、次の手順を実行します。

- 1 システムツリーで **シャーシの概要** をクリックします。
- 2 **電源** → **設定** をクリックします。
- 3 **110 VAC 動作を許可する** を選択してから、**適用** をクリックします。

### RACADM の使用

110V の回路が予測電流の定格になっていることを確認してから、次の手順を実行します。

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
- 2 110 VAC PAC を有効にする：

```
racadm config -g cfgChassisPower -o  
cfgChassisAllow110VACOperation 1
```

### 電源冗長性よりサーバーパフォーマンスを優先する

このオプションを有効にすると、電源冗長性の維持よりも、サーバーのパフォーマンスとパワーアップを優先します。無効にした場合は、サーバーのパフォーマンスよりも電源冗長性の維持を優先します。したがってこのオプションが無効の場合には、冗長性とフルパフォーマンスの両方を維持するために必要な電力をシャーシの電源装置で供給できなくなると、冗長性を維持するために、一部のサーバーにおいて次のような状態が発生することがあります。

- フルパフォーマンスで稼働するのに十分な電力が供給されない。
- 電源がオフになる。

## ウェブインタフェースの使用

電源冗長性よりサーバーパフォーマンスを優先するオプションを有効にするには、次の手順を実行します。

- 1 システムツリーで **シャーシの概要** をクリックします。
- 2 **電源** → **設定** をクリックします。
- 3 **電源冗長性よりサーバーパフォーマンスを優先する** を選択して、**適用** をクリックします。

電源冗長性よりサーバーパフォーマンスを優先するオプションを無効にするには、次の手順を実行します。

- 1 システムツリーで **シャーシの概要** をクリックします。
- 2 **電源** → **設定** をクリックします。
- 3 **電源冗長性よりサーバーパフォーマンスを優先する** をクリアして、**適用** をクリックします。

## RACADM の使用

電源冗長性よりサーバーパフォーマンスを優先するオプションを有効にするには、次の手順を実行します。

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
- 2 電源冗長性よりサーバーパフォーマンスを優先するオプションを有効化するには、次を入力します。

```
racadm config -g cfgChassisPower -o  
cfgChassisPerformanceOverRedundancy 1
```

電源冗長性よりサーバーパフォーマンスを優先するオプションを無効にするには、次の手順を実行します。

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
- 2 電源冗長性よりサーバーパフォーマンスを優先するオプションを無効化するには、次を入力します。

```
racadm config -g cfgChassisPower -o  
cfgChassisPerformanceOverRedundancy 0
```

## リモートロギング

電力消費のレポートを、リモートのシステムログサーバーに出力することができます。一定の期間にわたるシャーシの全電力消費量、最大値、最小値、および平均値のレポートが可能です。この機能の有効化、およびデータ収集とロギング間隔の設定に関する詳細は、次の関連セクションを参照してください。



## ウェブインタフェースの使用

GUI を使用して電力に関するリモートロギングを有効化できます。これを行うには、GUI にログインして、次の手順を実行します。

- 1 システムツリーで **シャーシの概要** をクリックします。
- 2 **電源** → **設定** をクリックします。
- 3 **電力リモートロギング** を選択して、リモートホストへの電力イベントのログを有効にします。
- 4 必要とするロギング間隔を指定します（1～1440 分）。
- 5 **適用** をクリックして変更を保存します。

## RACADM の使用

シリアル/Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次のように電力リモートロギングの設定を行います。

- 1 電力リモートロギング機能を有効にするには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingEnabled 1
```

- 2 電力リモートロギングの間隔を指定するには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingInterval n
```

n は、1～1440 の値（分）を指定します。

- 3 電力リモートロギング機能が有効かどうかを判定するには、次のコマンドを入力します。

```
racadm getconfig -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingEnabled
```

- 4 電力リモートロギングの間隔を確認するには、次のコマンドを入力します。

```
racadm getconfig -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingInterval
```



**メモ:** 電力リモートロギングの機能を使用するには、あらかじめリモート syslog ホストの設定が済んでいる必要があります。1 つまたは複数のリモート syslog ホストへのロギングが有効になっている必要があります。そうでない場合には、電力消費がロギングされます。この設定は、GUI または RACADM CLI のいずれかで行うことができます。詳細については、リモート syslog の設定手順を参照してください。

## 冗長性ポリシーが低下またはない状態の PSU 障害

PSU 障害などの電力不足イベントが発生した場合、CMC はサーバーへの電力を節減します。サーバーへの電力を節減した後、CMC はシャーシの電力必要量を再計算します。電力要件をまだ満たしていない場合、CMC は低優先順位のサーバーの電源をオフにします。

電力必要量が電力バジェット内の間、高優先順位サーバーへの電力供給が増分的に復元されます。



**メモ:** 冗長ポリシーを設定するには、314 ページの「電力バジェットと冗長性の設定」を参照してください。

## 新規サーバーの制御ポリシー

新しく追加されたサーバーに電源が投入された時、その新しいサーバーの追加でシャーシのために利用可能な電力必要量を越えた場合には、CMC は新しいサーバーに十分な電力を供給するために、優先順位が低いサーバーへの電力を節減する必要があります場合があります。これは、システム管理者がサーバーをフルパワーで稼働させるのに必要な電力量より低い電力上限値をシャーシに設定した場合、またはシャーシ内のすべてのサーバーに必要なワーストケース電力に満たない電力しか利用できない場合に発生する可能性があります。優先度の低いサーバーへの電力を低減させることで十分な電力が解放されない場合は、新しいサーバーを起動できないことがあります。

シャーシと新しいサーバーを含むすべてのサーバーをフルパワーで稼働させるのに必要な最大持続電力がワーストケース電力必要量です。この電力量が利用可能な場合、ワーストケース電力必要量より低い電力がサーバーに割り当てられることはなく、新しいサーバーを起動することが可能です。

ワーストケース電力必要量を満たすことができない場合、新しいサーバーを起動するために必要な電力が解放されるまで、優先度の低いサーバーへの電力は低減されます。

表 9-2 は、上記のような状況で新しいサーバーに電源が投入されたときに CMC が行うアクションを説明しています。

表 9-2. サーバーの電源投入が試行されたときの CMC の対応

ワーストケース電力 CMC の対応 が使用可能		サーバー電源 オン
あり	節電は不要	許可
なし	節電を実施	
	• 新しいサーバーに必要な電力が使用可能	許可
	• 新しいサーバーに必要な電力が使用不可	不許可

PSU が失敗すると、非重要な正常性状態になり、PSU 障害イベントが生成されます。PSU を取り外すと、PSU の取り外しイベントが発生します。

いずれかのイベントが発生した結果、冗長性が喪失した場合は、電力割り当てに基づいて、冗長性の喪失イベントが生成されます。

後続の電力容量またはユーザーの電力容量がサーバーの割り当てよりも大きい場合は、サーバーのパフォーマンスが劣化するか、最悪の場合には、サーバーの電源が切断される恐れがあります。これらの電源切断は優先順の逆順に行われます。つまり、優先順位の低いサーバーから電源が切断されます。

表 9-3 では、さまざまな PSU 冗長構成における PSU の電源切断または PSU の取り外しに対するファームウェアの対応を示します。

**表 9-3. PSU の障害または取り外しによるシャーシへの影響**

PSU 構成	PSU 動的制御	ファームウェアの対応
AC 冗長性	無効	CMC はユーザーに AC 冗長性の喪失をアラートします。
電源装置冗長性	無効	CMC はユーザーに電源装置冗長性の喪失をアラートします。
冗長性なし	無効	必要に応じて、優先度の低いサーバーへの電力を低減します。
AC 冗長性	有効	CMC はユーザーに AC 冗長性の喪失をアラートします。PSU の障害または取り外しにより失われた電力パジェットを補うために、スタンバイの PSU（存在する場合）の電源がオンになります。
電源装置冗長性	有効	CMC はユーザーに電源装置冗長性の喪失をアラートします。PSU の障害または取り外しにより失われた電力パジェットを補うために、スタンバイの PSU（存在する場合）の電源がオンになります。
冗長性なし	有効	必要に応じて、優先度の低いサーバーへの電力を低減します。

### 冗長性ポリシーが低下またはない状態の PSU 障害

ユーザーが PSU または PSU の AC コードを取り外すと、CMC は電力の節約を開始します。CMC は、電力の割り当てをシャーシ内の残りの PSU でまかなうことができるようになるまで、優先順位の低いサーバーへの電力を節減します。複数台の PSU を取り外す場合、CMC は 2 台目の PSU が取り外されたときに電力必要量を再計算して、ファームウェアの対応を決定します。電源条件が満たされていない場合、CMC は低優先順位ブレードサーバーの電源を切断する場合があります。

## 制限値

- CMC は、優先順位の高いサーバーに電源投入するために優先順位の低いサーバーの電源を自動的に切ることはありませんが、ユーザーが電源を切ることはできます。
- PSU 冗長性ポリシーの変更は、シャーシ内の PSU の台数によって制限されます。294 ページの「冗長性ポリシー」に記載されている 3 つの PSU 冗長構成のうち、いずれかを選択することもできます。

## システム イベント ログの電源供給および冗長性ポリシーの変更

電源供給状態および電力冗長性ポリシーの変化はイベントとして記録されます。システム イベント ログ (SEL) に記録される電源供給関連のイベントは、電力供給の追加と削除、電力供給入力追加と削除、電源供給出力の追加と削除、およびアサート停止です。

表 9-4 下の一覧は、電源供給の変化に関連する SEL 項目です。

表 9-4. 電源供給の変化に対する SEL イベント

電源供給イベント	システムイベントログ (SEL) の項目
差し込み	電源供給の存在がアサートされた
取り外し	電源供給の存在のアサートが停止された
AC 入力受信	電源供給入力喪失のアサートが停止された
AC 入力喪失	電源供給入力喪失がアサートされた
DC 出力生成	電源供給不良のアサートが停止された
DC 出力喪失	電源供給不良がアサートされた
非承認の 110V の動作が検出された	電源の低入力電力 (110) がアサートされた
110V 動作が確認された	電源の低入力電力 (110) のアサートが解除された

SEL で項目を記録する電源冗長性状態の変更に関連するイベントは、**AC 冗長** 電力ポリシー、または **電源装置冗長** 電力ポリシーのいずれかに設定されているモジュラエンクロージャに対する冗長性の喪失および冗長性の回復です。表 9-5 には、電源供給の変化に関連する SEL をリストしています。

表 9-5. 電源冗長性状態変化の SEL イベント

電力ポリシーイベント	システムイベントログ (SEL) の項目
冗長性喪失	冗長性喪失がアサートされた
冗長性上昇	冗長性喪失のアサートが解除された

## 冗長性状態と全体的な電源状態

冗長性状態は全体的な電源状態を決定する要素です。たとえば、電源冗長性ポリシーが AC 冗長性などに設定され、冗長性状態がシステムが稼動しているとなっている場合は、全体的な電源状態は通常、**OK** になります。しかし、AC 冗長性がある状態で稼動するための条件を満たすことができない場合は、冗長性状態は **いいえ** になり、全体的な電源状態は **重要** になります。これは、設定されている冗長性ポリシーに従ってシステムを動作できないためです。



**メモ** : CMC では、冗長性ポリシーを AC 冗長性に変更したり、または AC 冗長性から他の設定に変更したりする場合に、こうした条件を事前に確認しません。そのため、冗長性ポリシーを設定すると、すぐに冗長性が喪失したり、冗長性が回復する可能性があります。

## 電源の設定と管理

ウェブベースまたは RACADM インタフェースを使って、CMC 上の電源制御の管理と設定を行うことができます。具体的には、次が可能です。

- シャーシ、サーバーおよび PSU への電力割り当て、消費量およびステータスの表示。
- シャーシのシステム入力電力上限と冗長性ポリシーの設定。
- シャーシの電源制御操作（電源投入、電源切断、システムリセット、電源切断と再投入）の実行。

### PSU の正常性ステータスの表示

**電源装置ステータス** ページには、シャーシに関連付けられている PSU の状態が表示されます。

#### ウェブインタフェースの使用

PSU の状態ステータスは、2 つの方法で表示させることができます。1 つは **シャーシステータス** ページの **シャーシグラフィックス** セクション、もう 1 つは **電源装置ステータス** ページです。**シャーシグラフィックス** ページは、シャーシに取り付けられたすべての PSU のグラフィック表示を提供します。

**シャーシグラフィックス** を使用してすべての PSU の正常性ステータスを表示するには

- 1 CMC ウェブインタフェースにログインします。
- 2 **シャーシステータス** ページが表示されます。**シャーシグラフィックス** の下側のセクションには、シャーシの背面図とすべての PSU の状態ステータスが表示されます。PSU の正常性状態は、PSU サブグラフィックの色で示されます。
  - 緑色 — PSU が存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
  - 橙色 — PSU 障害を示します。エラー状態の詳細については、CMC ログを参照してください。
  - 灰色 — PSU の取り付け中、シャーシの電源を投入時または PSU の挿入中に PSU がスタンバイに設定されると生じます。PSU が存在し、電源がオフ。悪条件の兆候は報告されていません。
- 3 個別の PSU サブグラフィック上にマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象 PSU に関する追加情報を提供します。
- 4 PSU サブグラフィックは、該当する CMC GUI ページにハイパーリンクされており、すべての PSU の **電源装置ステータス** ページに即座に移動できます。

**電源装置ステータス** を使用して PSU の正常性状態を表示するには

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **電源装置** を選択します。**電源装置ステータス** ページが表示されます。

表 9-6 および 表 9-7 に、電源装置ステータス ページに表示される情報の説明があります。

**表 9-6. 電源装置**

項目	説明
名前	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。
存在	PSU が <b>存在</b> または <b>不在</b> を示します。

表 9-6. 電源装置 (続き)




項目	説明
状態	<p> OK PSU が存在し、CMC と通信を行っていることを示します。CMC と電源装置との間で通信エラーが発生した場合は、CMC は PSU の状態ステータスを取得または表示できません。</p> <p> 警告 警告のみが発行されたこと、および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、シャーシ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。</p> <p> 重要 少なくとも 1 件の障害アラートが電源供給に対して発行されたことを示します。重大度状態は、シャーシの電源エラーを示し、<b>直ちに対応処置を取る必要があります。</b></p>
電源ステータス	電源装置の電源状態を示します (次のいずれか 1 つ) : <b>初期化中、オンライン、スタンバイ、診断中、故障、オフライン、不明または不在。</b>
容量	電源容量がワット単位で表示されます。

表 9-7. システム電源の状態

項目	説明
全体的な電源正常性	シャーシ全体の電源管理の正常性状態 ( <b>OK、非重要、重要、回復不可、その他、不明</b> ) を示します。
システム電源の状態	シャーシの電源状態 ( <b>オン、オフ、電源オン、電源オフ</b> ) を示します。
冗長性	電源装置冗長性のステータスを示します。有効値は次のとおりです。 <b>いいえ</b> : 電源装置は非冗長です。 <b>はい</b> : 完全冗長化されています。

### RACADM の使用

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm getpminfo
```

出力詳細を含む **getpminfo** の詳細については、デルサポートサイト [support.jp.dell.com/manuals](http://support.jp.dell.com/manuals) の『RACADM Command Line Reference Guide for iDRAC6 and CMC』(iDRAC6 および CMC 用 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。

## 消費電力ステータスの表示

CMC は、システム全体で実際に消費している入力電力を **消費電力ステータス** ページに表示します。

### ウェブインタフェースの使用



**メモ**：電力の管理を行うには、**シャーシ設定システム管理者**の権限が必要です。

ウェブインタフェースを使用して電力消費量ステータスを表示するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **電源** → **消費電力** をクリックします。**消費電力** ページが表示されます。



**メモ**：**システム** ツリー → **ステータス** タブにある **電源装置** から電力冗長性ステータスを表示することもできます。

### RACADM の使用

RACADM を使用して電力消費量ステータスを表示するには、次の手順を実行します。

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm getpminfo
```

表 9-8 から表 9-11 では、**消費電力** ページに表示される情報について説明します。

**表 9-8. リアルタイム電力統計**

項目	説明
システム入力電力	PSU の AC 入力側から測定したシャーシ内のすべてのモジュールの現在の累積電力消費量を示します。システム入力電力の値は、ワットおよび BTU/ 時単位で示されます。
ピークシステム電力	値が最後にクリアされてから消費された最大システムレベル入力電力を表示します。このプロパティによって、経時的に記録されているシステムごと（シャーシとモジュール）の最大電力消費量を追跡できます。表の下にある <b>ピーク / 最少電力統計のリセット</b> ボタンをクリックして、この値をクリアします。ピークシステム電力の値は、ワットおよび BTU/ 時単位で示されます。



表 9-8. リアルタイム電力統計（続き）

項目	説明
ピークシステム電力の開始時間	ピークシステム電力消費量の値が最後にクリアにされた日時を表示します。タイムスタンプは、 <b>hh:mm:ss MM/DD/YYYY</b> の形式で表示されます。 <b>hh</b> は時間（0～24）、 <b>mm</b> は分（00～60）、 <b>ss</b> は秒（00～60）、 <b>MM</b> は月（1～12）、 <b>DD</b> は日（1～31）、そして <b>YYYY</b> は年を表します。この値は、 <b>ピーク / 最小電力統計のリセット</b> ボタンでリセットされます。また CMC のリセットまたはフェイルオーバー時にもリセットされます。
ピークシステム電力のタイムスタンプ	記録期間中に記録されたピークシステム電力消費の発生日時を示します。タイムスタンプは <b>hh:mm:ss MM/DD/YYYY</b> 形式で表示されます。ここで、 <b>hh</b> は時間（0～24）、 <b>mm</b> は分（00～60）、 <b>ss</b> は秒（00～60）、 <b>MM</b> は月（1～12）、 <b>DD</b> は日（1～31）、 <b>YYYY</b> は年を表します。
最小システム電力	ユーザーが前回この値をクリアした後の最小システムレベルの AC 電力消費量をワット単位で表示します。このプロパティによって、経時的に記録されているシステムごと（シャーシとモジュール）の最小電力消費量を追跡できます。表の下にある <b>ピーク / 最小電力統計のリセット</b> ボタンをクリックして、この値をクリアします。最小システム電力の値は、ワットおよび BTU/時単位で示されます。この値は、 <b>ピーク / 最小電力統計のリセット</b> ボタンでリセットされます。また CMC のリセットまたはフェイルオーバー時にもリセットされます。
最小システム電力の開始時間	最小システム電力消費量の値が最後にクリアにされた日時を表示します。タイムスタンプは、 <b>hh:mm:ss MM/DD/YYYY</b> の形式で表示されます。 <b>hh</b> は時間（0～24）、 <b>mm</b> は分（00～60）、 <b>ss</b> は秒（00～60）、 <b>MM</b> は月（1～12）、 <b>DD</b> は日（1～31）、そして <b>YYYY</b> は年を表します。この値は、 <b>ピーク / 最小電力統計のリセット</b> ボタンでリセットされます。また CMC のリセットまたはフェイルオーバー時にもリセットされます。
最小システム電力のタイムスタンプ	記録機間中に記録された最小システム電力消費の発生日時を示します。タイムスタンプの形式は、 <b>ピークシステム電力のタイムスタンプ</b> で説明したとおりです。
システムアイドル電力	シャーシのアイドル状態の推定電力消費量が表示されます。アイドル状態とは、シャーシの電源がオンで、すべてのモジュールが電力を消費しているシャーシの状態のことを指します。これは、推定値であり、測定値ではありません。この推定値は、シャーシ基板コンポーネント（I/O モジュール、ファン、iKVM、iDRAC コントローラおよび前面パネル LCD）に割り当てられた電力、および電源がオンの状態にあるすべてのサーバーに割り当てられた最小電力要件の累積値として算出されます。システムアイドル電力の値は、ワットおよび BTU/時単位で示されます。

表 9-8. リアルタイム電力統計 (続き)

項目	説明
システム潜在電力	シャーシが最大出力で動作している場合の推定電力消費量を表示します。最大電力消費量は、シャーシの電源がオンで、すべてのモジュールが最大出力で電力を消費しているシャーシの状態を示します。 <u>この値は、システム構成の履歴データ (総電力消費量) の推定値であり、測定値ではありません。</u> この推定値は、シャーシ基板コンポーネント (I/O モジュール、ファン、iKVM、iDRAC コントローラおよびフロントパネル LCD) に割り当てられた電力、そして電源がオンの状態になっているすべてのサーバーに割り当てられた最小電力要件の累積値として算出されます。システム潜在電力の値は、ワットおよび BTU/ 時単位で示されます。
システム入力電流測定値	シャーシ内の各 PSU モジュールの入力電流消費量の合計値に基づいて、シャーシの総入力電流消費量を表示します。システム入力電流測定値は、アンプ (Amp) 単位で表示されます。

表 9-9. リアルタイムエネルギー統計ステータス

項目	説明
システムエネルギー消費量	PSU の AC 入力側から測定したシャーシ内のすべてのモジュールの現在の累積エネルギー消費量を示します。この値は、累積値で kWh 単位で表示されます。
システム エネルギー消費開始時間	システムエネルギー消費量の値が最後にクリアされ、新しい測定サイクルが開始された日時を表示します。タイムスタンプは、 <b>hh:mm:ss MM/DD/YYYY</b> の形式で表示されます。 <b>hh</b> は時間 (0 ~ 24)、 <b>mm</b> は分 (00 ~ 60)、 <b>ss</b> は秒 (00 ~ 60)、 <b>MM</b> は月 (1 ~ 12)、 <b>DD</b> は日 (1 ~ 31)、そして <b>YYYY</b> は年を表します。この値は、 <b>エネルギー統計のリセット</b> ボタンでリセットされますが、CMC リセット時またはフェイルオーバー時にはリセットされません。
システムエネルギー消費量タイムスタンプ	システムエネルギー消費量が表示するために算出された日時を表示します。タイムスタンプは、 <b>hh:mm:ss MM/DD/YYYY</b> の形式で表示されます。 <b>hh</b> は時間 (0 ~ 24)、 <b>mm</b> は分 (00 ~ 60)、 <b>ss</b> は秒 (00 ~ 60)、 <b>MM</b> は月 (1 ~ 12)、 <b>DD</b> は日 (1 ~ 31)、そして <b>YYYY</b> は年を表します。

**表 9-10. システム電源の状態**

項目	説明
全体的な電源正常性	シャーシの電源サブシステムの正常性状態を示します。 <ul style="list-style-type: none"> <li>• 緑色のチェックアイコンは <b>OK</b></li> <li>• 橙色の感嘆符のアイコンは <b>非重要</b></li> <li>• 赤色の X アイコンは <b>重要</b></li> </ul>
システム電源の状態	シャーシの電源状態（ <b>オン</b> 、 <b>オフ</b> 、 <b>電源オン</b> 、 <b>電源オフ</b> ）を示します。
冗長性	冗長性の状態を示します。有効値は次のとおりです。 <p><b>いいえ</b> — PSU は非冗長です。</p> <p><b>はい</b> — 完全冗長化されています。</p>


**表 9-11. サーバーモジュール**

項目	説明
スロット	サーバーモジュールの場所を表示します。 <b>スロット</b> は、サーバーモジュールをシャーシ内の場所で識別する連番（1～16）です。
名前	サーバー名を表示します。サーバー名はユーザーによって再定義できます。
存在	サーバーがスロットにあるかどうかを示します（ <b>はい</b> または <b>いいえ</b> ）。フィールドに <b>拡張 #</b> （# は 1～8 の数値）が表示される場合、それに続く番号がマルチスロットサーバーのメインスロットとなります。
実測値（AC）	サーバーが実際に消費する電力をリアルタイムで計測した値です。測定値は、ワット数で表示されます。
電流累積開始時間	<b>開始時間</b> フィールドに指定された時刻移行にサーバーが実際に消費した電力をリアルタイムで測定した値です。測定値は、キロワット時（kWh）で表示されます。
ピーク消費時間スタンプ	サーバーが一度に消費するピーク電力を表示します。ピーク消費電力の発生時間は、 <b>タイムスタンプ</b> フィールドに記録されます。測定値は、ワット単位で表示されます。

## 電力バジェット状態の表示

CMC は **電力バジェットステータス** ページに電源サブシステムの電源状態の概要を表示します。

## ウェブインタフェースの使用

 **メモ**: 電力の管理を行うには、**シャーシ設定システム管理者**の権限が必要です。ウェブインタフェースを使用して電力バジェットステータスを表示するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **電源** → **バジェットステータス** をクリックします。  
**電力バジェットステータス** ページが表示されます。

表 9-12 から表 9-15 では、**電力バジェットステータス** ページに表示される情報について説明します。

この情報の設定については、314 ページの「電力バジェットと冗長性の設定」を参照してください。

## RACADM の使用

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm getpbinfo
```

出力詳細を含む **getpbinfo** の詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **getpbinfo** コマンドの項を参照してください。

### 表 9-12. システム電源のポリシー設定

項目	説明
システム入力電力の上限値	<p>システム全体（シャーシ、CMC、サーバー、I/O モジュール、電源装置、iKVM、ファン）のユーザー定義による電力消費上限値を示します。CMC は、サーバーへの電力割り当てを低減することで、または優先度の低いサーバーモジュールの電源を落とすことで、この上限値を実施します。システム入力電力の上限値は、ワット、BTU/時およびパーセント単位で表示されます。</p> <p>シャーシの電力消費量が <b>システム入力電力上限値</b> を超える場合、総電力消費量が上限値を下回るまで、優先度の低いサーバーのパフォーマンスが低減されます。</p> <p>サーバーが <b>同じ</b> 優先度に設定されている場合は、サーバーのスロット番号の順序に基づいて、電力低減または電源オフされるサーバーが選択されます。たとえば、スロット 1 のサーバーは最初に選択され、スロット 16 のサーバーは最後に選択されます。</p>

表 9-12. システム電源のポリシー設定（続き）

項目	説明
冗長性ポリシー	<p>現在の冗長性の設定：<b>AC 冗長性</b>、<b>電源装置冗長性</b>、<b>冗長性なし</b>を示します。</p> <p><b>AC 冗長性</b> — 入力電力はすべての PSU 間で負荷分散されます。このうち半分は 1 つの AC グリッドに配線され、残り半分は別のグリッドに配線されます。システムが AC 冗長性 モードで最適運用されているとき、電源はアクティブな電源装置すべての間で負荷分散されています。AC グリッドに障害が発生した場合は、機能している AC グリッドに接続されている PSU が中断せずに引き継ぎます。</p> <p><b>電源装置冗長性</b> — どの PSU が故障してもサーバーモジュールやシャーシの電源障害が引き起こされないように、シャーシ内で最大定格の PSU 容量がスベアとして保たれます。</p> <p><b>電力装置冗長性</b> は、6 台全部の PSU を使用しない場合もあります。必要分の PSU を使用して 1 台に障害が発生した場合に、残りの PSU がシャーシに電源を引き続き供給できるようにします。DPSE が有効な場合、他の PSU をスタンバイモードにできます。</p> <p><b>冗長性なし</b> — すべてのアクティブの PSU からの電力は、シャーシ、サーバー、I/O モジュール、iKVM、CMC など、シャーシ全体に電源を供給するのに十分です。DPSE が有効な場合、残りの PSU をスタンバイモードにできます。</p> <p><b>△ 注意：</b>冗長性なしモードは、バックアップなしで、最低限必要な PSU 数を使用します。使用している 1 台に障害が発生すると、サーバーモジュールの電源とデータが消失する可能性があります。</p>
電源装置の動的制御	<p><b>電源装置の動的制御</b> が有効か無効かを示します。この機能を有効にすると、CMC は設定された冗長性ポリシーとシステムの電源要件に基づいて、あまり使用されていない PSU をスタンバイモードにします。使用量の少ない PSU をスタンバイモードにすることで、オンライン PSU の使用率と効率を上げることができ、節電につながります。</p>

表 9-13. 電力バジェット

項目	説明
システム入力最大電力容量	利用可能な電源装置がシステムに供給できる最大入力電力（ワット）。
予備の入力冗長電力	AC グリッドや PSU が故障した場合に利用できる予備の冗長電力量（ワット）を示します。 シャーシが <b>AC 冗長性</b> モードで作動するように設定されている場合、 <b>予備の入力冗長電力</b> は AC グリッドが故障した場合に利用できる予備の電力量となります。 シャーシが <b>電源装置冗長性</b> モードで作動するように設定されている場合、 <b>予備の入力冗長電力</b> は特定の PSU に障害が発生した場合に利用できる予備の電力量となります。
サーバーに割り当てられた入力電力	設定に基づいて CMC がサーバーに割り当てる累積入力電力（ワット）を表示します。
シャーシインフラストラクチャに割り当てられた入力電力	CMC がシャーシインフラストラクチャ（サーバー上のファン、IO モジュール、iKVM、CMC、スタンバイ CMC および iDRAC）に割り当てる累積入力電力（ワット）を表示します。
割り当て可能な総入力電力	割り当て可能な総シャーシ電力をワットで表示します。
スタンバイ入力電力容量	電源装置が故障、またはシステムから電源装置が取り外された場合に、利用できるスタンバイ入力電力（ワット）を表示します。システムに複数の電源装置が搭載され、動的制御が有効になっている場合に、このフィールドに測定値が表示されます。 <b>メモ</b> ：スタンバイ入力電力容量の値に寄与しないスタンバイモードの PSU もあります。この場合、この PSU は、 <b>割り当て可能な総入力電力</b> の値に寄与しています。

表 9-14. サーバーモジュール

項目	説明
スロット	サーバーモジュールの場所を表示します。 <b>スロット</b> は、サーバーモジュールをシャーシ内の場所では識別する連番（1～16）です。
名前	サーバー名を表示します。サーバー名はユーザーが定義します。
タイプ	サーバーのタイプが表示されます。
優先度	<p>シャーシの電力バジェットの目的で、サーバースロットに割り当てられた優先順位を示します。ユーザーが定義した電力制限値に基づいて、または電源装置や電源グリッドが故障のために、電力の節減や再割り当てを行う必要が生じた場合、CMC は計算にこの値を使用します。</p> <p><b>優先順位：1（最高）から 9（最低）</b></p> <p>デフォルト：<b>1</b></p> <p><b>メモ：</b>サーバースロットの優先順位は、スロットに差し込まれたサーバーではなくサーバースロットに関連付けられています。サーバーをシャーシ内の別のスロット、または別のシャーシに移動すると、そのサーバーの優先順位はそれが新しく差し込まれたスロットに割り当てられている優先順位になります。</p>
電源状態	<p>サーバーの電源状態を表示します。</p> <ul style="list-style-type: none"> <li>• <b>該当なし：</b> CMC はサーバーの電源状態を特定していません。</li> <li>• <b>オフ：</b> サーバーまたはシャーシの電源がオフです。</li> <li>• <b>オン：</b> シャーシおよびサーバーともに電源がオンです。</li> <li>• <b>電源投入中：</b> 電源オフおよび電源オンの間の一時的な状態です。電源サイクルが完了すると、電源状態はオンになります。</li> <li>• <b>電源切断中：</b> 電源オンおよび電源オフの間の一時的な状態です。電源サイクルが完了すると、電源状態はオフになります。</li> </ul>
バジェット割り当て - 実測値	<p>サーバーモジュールへの電力バジェットの割り当てを示します。</p> <ul style="list-style-type: none"> <li>• <b>実測値：</b> 各サーバーに割り当てられている電力バジェット</li> </ul>

表 9-15. シャーシの電源装置

項目	説明
名前	PSU の名前が <b>PS-n</b> の形式で表示されます。ここで、 <b>n</b> は電源装置番号です。
電源状態	PSU の電源状態： <b>初期化中、オンライン、スタンバイ、診断中、故障、不明、または不在（欠如）</b> を示します。
入力電圧	電源装置の現在の入力電圧（ボルト）を表示します。
入力電流	電源装置の現在の入力電流を表示します。
定格出力	電源装置の最大定格出力を表示します。

## 電力バジェットと冗長性の設定

CMC の電力管理サービスはシャーシ全体（シャーシ、サーバー、IOM、iKVM、CMC、PSU）の電力消費量を最適化し、電力需要に基づいて各モジュールに電力を再割り当てします。

### ウェブインタフェースの使用



**メモ**：電力の管理を行うには、**シャーシ設定システム管理者**の権限が必要です。

ウェブインタフェースを使用して電力バジェットを設定するには

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **電源** → **設定** をクリックします。  
**バジェット / 冗長性の設定** ページが表示されます。
- 4 必要に応じて、「表 9-16」に記載されるプロパティの一部またはすべてを設定します。
- 5 **適用** をクリックして変更を保存します。

**バジェット / 冗長性の設定** ページの内容を更新するには、**更新** をクリックします。内容を印刷するには、**印刷** をクリックします。



表 9-16. 設定可能な電力バジェット / 冗長性のプロパティ

項目	説明
システム入力電力の上限値	<p>システム入力電力の上限値は、システムがサーバーおよびシャーシインフラストラクチャに割り当てることができる最大 AC 電力です。この値は、電源が投入されたサーバーおよびシャーシインフラストラクチャの最小必要電力を <b>超える</b> 値であれば、任意の意の設定することができます。この最小必要電力値よりも低い値に設定することはできません。</p> <p>サーバーおよびシャーシ インフラストラクチャに割り当てた電力は、<b>電力バジェット</b> セクションにある <b>シャーシの概要</b> → <b>電源</b> → <b>電力バジェット</b> ステータス ページのユーザー インタフェース、または CLI RACADM ユーティリティ コマンド (racadm getphbinfo) を介して確認することができます。</p> <p>現在の電源割り当てを低減するために 1 台以上のサーバーの電源をオフにし、<b>システム入力電力容量</b> を低い値に再設定する、またはサーバーに電源を投入する前に容量限界を設定することができます。</p> <p>この設定を変更する際は、どの単位の値も入力することができます。インタフェースは、最後に変更された単位フィールドが、それらの変更が適用された際に送付された値であることを確かめます。</p> <p><b>メモ</b> : 容量計画については、<a href="http://www.dell.com/calc">www.dell.com/calc</a> の Datacenter Capacity Planner (DCCP) ツールを参照してください。</p> <p><b>メモ</b> : 値の変更がワット数で指定された場合は、実際に適用される値と全く同じになります。しかし、BTU/時 またはパーセント単位で指定した変更は、実際に適用される値と異なる場合があります。これは、これらの単位の数値をワット数に変換してから適用することにより、丸め誤差が発生するためです。</p>

表 9-16. 設定可能な電力バジェット / 冗長性のプロパティ (続き)

項目	説明
冗長性ポリシー	<p>次のオプションから選択できます。</p> <ul style="list-style-type: none"> <li> <b>冗長性なし</b>：電源装置からの電力は、シャーシ、サーバー、I/O モジュール、iKVM、CMC を含むシャーシ全体の電源投入に使用されます。電源装置は予備に保存できません。                 <p><b>メモ</b>：冗長性なしモードは、一度に必要な最低限度の電源装置数を使用します。PSU の最低台数が取り付けられると、バックアップはできません。3 台のうち 1 台の電源装置に障害が発生すると、サーバーの電源が落ち、データを損失する恐れがあります。複数の PSU 最低必要数が表示されると、追加の PSU がスタンバイモードとなり、DPSE が有効になると電力効率上昇します。</p> </li> <li> <b>電源装置冗長性</b>：どの電源装置 が故障してもサーバーモジュールやシャーシの電源が切断されないように、シャーシ内で最大定格の電源装置がスペアとして保持されます (ホットスワップ)。                 <p><b>電源装置の冗長性モード</b>は、取り付けられたすべての電源装置を利用するわけではありません。追加の電源装置が存在する場合は、スタンバイモードにすると、DPSE が有効な場合に電力効率を上げることができます。<b>電源装置冗長性</b> モードは、シャーシの電力消費量が定格電力を超える場合、サーバーモジュールが起動しないようにします。このモードで <b>2 台</b> の電源装置が故障すると、シャーシ内の一部またはすべてのサーバーモジュールの電源が切れてしまう可能性があります。サーバーモジュールの性能はこのモードでは低下しません。</p> </li> <li> <b>AC 冗長性</b>：このモードでは、<b>6 台の PSU が 2 つの電力グリッドに分けられます (PSU 1-3 を電力グリッド 1 に、PSU 4-6 を電力グリッド 2 に接続)</b>。PSU が故障したり、AC 電力を失ったりした場合は、冗長性ステータスは喪失状態になります。                 </li> </ul>
電源冗長性よりサーバーパフォーマンスを優先する	<p>このオプションを有効にすると、電源冗長性の維持よりも、サーバーのパフォーマンスとパワーアップが優先されます。この機能の詳細については、297 ページの「電源冗長性よりサーバーパフォーマンスを優先する」を参照してください。</p>

表 9-16. 設定可能な電力バジェット / 冗長性のプロパティ (続き)

項目	説明
電源装置の動的制御の有効化	<p>オプションで、動的電力制御を有効にします。<b>動的制御</b> モードでは、消費電力に基づいて電源装置の電源を <b>オン</b> (オンライン) または <b>オフ</b> (スタンバイ) にし、シャーシ全体の電力消費量を最適化します。</p> <p>たとえば、電力バジェットが 5000 ワットで、冗長ポリシーが AC 冗長性モードに設定され、6 台の電源装置があると仮定します。CMC は、4 台の電源装置で AC 冗長性を確保でき、残りの 2 台をスタンバイモードにできるものと判定します。新しくインストールしたサーバーにさらに 2000W の電力が必要な場合や、既存のシステム設定の電力効率を向上させる必要がある場合は、2 台のスタンバイ状態の電源装置が追加されます。</p>
シャーシ電源ボタンを無効にする	<p>オプションで、シャーシの電力ボタンを無効にします。チェックボックスがオンになっているときに、シャーシの電源ボタンを押してシャーシの電源状態を変更しようとする、このアクションは無視されます。</p>
110 VAC 動作を許可する	<p>電源装置ユニットが 110V AC 入力に接続されると、オプションで通常の動作が許可されます。詳細については、297 ページの「110V の PSU の動作」を参照してください。</p>
最大節電モード	<p>オプションで、ただちに最大節電モードを入力します。詳細については、296 ページの「節電と最大節電モード」を参照してください。</p>

## RACADM の使用

冗長性を有効にして冗長性ポリシーを設定するには、次の手順を実行します。



**メモ**：電力の管理を行うには、**シャーシ設定システム管理者** の権限が必要です。

1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。

2 必要に応じてプロパティを設定します。

- 冗長性ポリシーを選択するには、次のように入力します。

```
racadm config -g cfgChassisPower -o
cfgChassisRedundancyPolicy <value>
```

ここで、<value> は **0** (冗長性なし)、**1** (AC 冗長性)、**2** (電源装置冗長性) です。デフォルトは **0** です。

例えば、次のコマンド

```
racadm config -g cfgChassisPower -o
cfgChassisRedundancyPolicy 1
```

は、冗長性ポリシーを **1** に設定します。

- PSU の動的制御を有効または無効にするには、次のように入力します。  
`racadm config -g cfgChassisPower -o  
cfgChassisDynamicPSUEngagementEnable <value>`

ここでの `<value>` は **0** (無効) あるいは **1** (有効) です。デフォルトは **0** です。

例えば、次のコマンド

```
racadm config -g cfgChassisPower -o  
cfgChassisDynamicPSUEngagementEnable 0
```

は、PSU の動的制御を無効にします。

シャーシ電源の RACADM コマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC7 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **config**、**getconfig**、**getpbinfo**、**cfgChassisPower** の項を参照してください。

## サーバーに優先度を割り当てる方法

サーバーの優先度により、必要とされる電力が増えたときに CMC がどのサーバーから電力を受けるかが決まります。



**メモ**：サーバーに割り当てる優先度は、サーバー自体ではなく、そのスロットにリンクされます。サーバーを新しいスロットに移動した場合、新しいスロットの場所の優先度を再設定する必要があります。



**メモ**：電力の管理を行うには、**シャーシ設定システム管理者** の権限が必要です。

## ウェブインタフェースの使用

CMC ウェブインタフェースを使用して優先度を割り当てるには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **サーバーの概要** を選択します。**サーバーステータス** ページが表示されます。
- 3 **電源** → **サーバーの優先順位** をクリックします。  
**サーバーの優先度** ページが表示され、シャーシ内のすべてのサーバーが一覧表示されます。
- 4 1 台、複数台、またはすべてのサーバーに対する優先度（1～9、1 が最高の優先度）を選択します。デフォルト値は 1 です。複数のサーバーに同一の優先度を割り当てることも可能です。
- 5 **適用** をクリックして変更を保存します。

## RACADM の使用

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm config -g cfgServerInfo -o cfgServerPriority -i  
<slot number> <priority level>
```

ここで、<slot number> (1 ~ 16) はサーバーの位置を表し、<priority level> は 1 ~ 9 の数値です。

例えば、次のコマンド

```
racadm config -g cfgServerInfo -o cfgServer Priority -i 5 1
```

スロット 5 に装着されたサーバーの優先順位を 1 に設定します。

## 電力バジレットの設定



**メモ**：電力の管理を行うには、**シャーン設定システム管理者** の権限が必要です。

### ウェブインタフェースの使用

CMC ウェブインタフェースを使用して電力バジレットを設定するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーンの概要** をクリックします。 **シャーンの正常性** ページが表示されます。
- 3 **電源** タブをクリックします。 **消費電力ステータス** ページが表示されます。
- 4 **設定** サブタブをクリックします  
**バジレット / 冗長性の設定** ページが表示されます。
- 5 16685 ワットまでのバジレット値を **システム入力電力の上限值** テキストフィールドに入力します。



**メモ**：電力バジレットの上限值は、3 台の PSU のうち設定された最も低い値に制限されます。この値を超える AC 電力バジレット値を設定しようとする  
と、CMC によるエラーメッセージが表示されます。



**メモ**：値の変更がワット数で指定された場合は、実際に適用される値と全く同じになります。しかし、BTU/時 またはパーセント単位で指定した変更は、実際に適用される値と異なる場合があります。これは、これらの単位の数値をワット数に変換してから適用することにより、丸め誤差が発生するためです。

- 6 **適用** をクリックして変更を保存します。

## RACADM の使用

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm config -g cfgChassisPower -o  
cfgChassisPowerCap <value>
```

ここで、<値> は 2715 ~ 16685 の範囲の数値で、電力の上限値をワット数で表します。デフォルト値は 16685 です。

例えば、次のコマンド

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
```

は、最大電力バジェットを 5400 ワットに設定します。



**メモ:** 電力バジェットは 16685 ワットまでに制限されています。お使いのシャーシの電力容量を超える AC 電力バジェット値を設定しようとすると、エラーメッセージが表示されます。

## 電源バジェットを維持するためのサーバー電力の低減

システムの消費電力量をユーザー設定の **システムの入力電力の上限値** の範囲内に保つためにさらに電力が必要な場合は、優先順位の低いサーバーへの電力割り当てが低減されます。たとえば、新しいサーバーが追加された場合 **CMC** は優先順位が低いサーバーへの電力を低減し、新しいサーバーに供給する電力を増やすことがあります。優先順位の低いサーバーへの電力割り当てを低減した後も電力量が不十分である場合は、**CMC** は新しいサーバーへの電力投入に十分な電力が確保されるまで、サーバーの性能を低下させます。

**CMC** は次の 2 つの場合にサーバーの電力割り当てを低減します。

- 合計消費電力量が設定可能な **システムの入力電力の上限値** を超える場合 (319 ページの「電力バジェットの設定」を参照)
- 冗長構成で電力故障が発生した場合。

サーバーへの優先レベルの割り当ての詳細については、320 ページの「シャーシに対する電力制御操作の実行」を参照してください。

## シャーシに対する電力制御操作の実行



**メモ:** 電力の管理を行うには、**シャーシ設定システム管理者** の権限が必要です。







**メモ:** 電源制御操作はシャーシ全体に影響します。IOM に対する電力制御操作については、322 ページの「IOM 上で電源制御操作の実行」を参照してください。サーバーに対する電力制御操作については、323 ページの「サーバーに対する電力制御操作の実行」を参照してください。

**CMC** は、手順に従ったシャットダウンなど、シャーシ全体 (シャーシ、サーバー、IOM、iKVM、PSU) に関するいくつかの電源管理操作を、ユーザーがリモート実行できるようにします。

## ウェブインタフェースの使用

CMC ウェブインタフェースを使用してシャーシの電力制御操作を行うには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **電源** タブをクリックします。  
**消費電力** ステータス ページが表示されます。
- 4 **制御** サブタブをクリックします。 **シャーシ電力制御** ページが表示されます。
- 5 対応するラジオボタンをクリックして、次の **電力制御操作** のうちひとつを選択します。
  - **システムの電源を入れる** — シャーシの電源を入れます（シャーシの電源が **オフ** のときに電源ボタンを押す操作と同じ）。シャーシの電源がすでに **オン** の場合は、このオプションが無効になっています。  
 **メモ:** この操作は、シャーシおよびその他のサブシステム（サーバー上の iDRAC、IOM および iKVM）の電源をオンにします。サーバーの電源はオンになりません。
  - **システムの電源を切る** — シャーシの電源を切ります。シャーシの電源がすでに **オフ** の場合は、このオプションが無効になっています。  
 **メモ:** この操作は、シャーシ（シャーシ、サーバー、IOM、iKVM および電源装置）の電源をオフにします。CMC は電源オンのままですが、仮想スタンバイ状態になります。1 つの電源装置および数個のファンがこの状態にある CMC を冷却します。この電源装置は、低速で動作するファンに対しても電力を供給します。
  - **システムの電源を入れなおす（コールドブート）** — サーバーの電源を切ってから再起動します。シャーシの電源がすでに **オフ** の場合は、このオプションが無効になっています。  
 **メモ:** この操作は、シャーシ全体（シャーシ、常に電源オンに設定されているサーバー、IOM、iKVM および電源装置）の電源をオフにし、再起動します。
  - **CMC のリセット** — 電源を切ることなく CMC をリセットします（ウォームリブート）（CMC の電源がすでにオフの場合は、このオプションは無効です）。  
 **メモ:** この操作では CMC のリセットのみを行います。その他のコンポーネントは影響されません。
  - **強制シャットダウン** — この操作は、シャーシ全体（シャーシ、サーバー、IOM、iKVM および電源装置）を強制的に電源オフにします。この場合、電源をオフにする前に、サーバーのオペレーティングシステムを正常に終了させることはしません。
- 6 **適用** をクリックします。確認を求めるダイアログボックスが表示されます。
- 7 **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

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm chassisaction -m chassis <action>
```

ここで、<action> は、電源投入、電源切断、パワーサイクル、強制シャットダウン または リセット を指します。

## IOM 上で電源制御操作の実行

各 IOM でリセットやパワーサイクルをリモート実行できます。



**メモ**：電力の管理を行うには、**シャーシ設定システム管理者** の権限が必要です。

### ウェブインタフェースの使用

CMC ウェブインタフェースを使用して IOM の電力制御操作を行うには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 **I/O モジュールの概要** を選択します。  
**I/O モジュールのステータス** ページが表示されます。
- 3 **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。
- 4 リストで IOM の隣にあるドロップダウンメニューから実行する操作（**リセット** または **パワーサイクル**）を選択します。
- 5 **適用** をクリックします。  
確認を求めるダイアログボックスが表示されます。
- 6 電力の管理操作を実行するには、**OK** をクリックします（たとえば、IOM をパワーサイクルする場合）。

## RACADM の使用

RACADM ウェブインタフェースを使用して IOM の電力制御操作を行うには、次の手順を実行します。

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm chassisaction -m switch-<n> <action>
```

ここで <n> は、1 ~ 6 の数値で IOM (A1, A2, B1, B2, C1, C2) を指定し、<操作> は、パワーサイクル または リセット のどちらかの実行したい操作を示します。



## サーバーに対する電力制御操作の実行



**メモ**：電力の管理を行うには、**シャーシ設定システム管理者** の権限が必要です。

CMC は、シャーシ内の個別のサーバーに関するいくつかの電源管理操作（手順に従ったシャットダウンなど）を、ユーザーがリモート実行できるようにします。

### ウェブインタフェースの使用

ウェブインタフェースを使用してサーバーの電力制御操作を行うには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリー内の **サーバーの概要** を展開し、電力制御操作の対象とするサーバーを選択します。**サーバーステータス** ページが表示されます。
- 3 **電源** タブをクリックします。  
**サーバーの電力管理** ページが表示されます。
- 4 **電源ステータス** は、次で示すサーバーの電源ステータスを表示します。
  - **該当なし**：CMC はサーバーの電源状況を特定していません。
  - **オフ** - サーバーまたはシャーシのどちらかの電源がオフです。
  - **オン** - シャーシおよびサーバーともに電源がオンです。
  - **電源投入中** - 電源オフおよび電源オンの間の一時的な状態です。操作が完了すると、**電源状態** は **オン** になります。
  - **電源切断中** - 電源オンおよび電源オフの間の一時的な状態です。操作が完了すると、**電源状態** は **オフ** になります。
- 5 次の **電源制御操作** のいずれかのラジオボタンをクリックして選択します。
  - **サーバーの電源を入れる** — サーバーの電源を入れます（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。
  - **サーバーの電源を切る** — サーバーの電源を切ります（サーバーの電源がオンのときに電源ボタンを押す操作と同じ）。
  - **正常なシャットダウン** — サーバーの電源を切ってから再起動します。
  - **サーバーをリセットする（ウォームブート）** — サーバーの電源を切らないで再起動します。サーバーの電源が **オフ** の場合は、このオプションは無効になっています。
  - **サーバーの電源を入れなおす（コールドブート）** — サーバーの電源を切ってから再起動します。サーバーの電源が **オフ** の場合は、このオプションは無効になっています。

- 6 **適用** をクリックします。確認を求めるダイアログボックスが表示されます。
- 7 **OK** をクリックして、電源管理の操作（サーバーのリセットなど）を行います。



**メモ**：すべての電源管理の操作は、**サーバー → 電源管理 → 管理** ページで複数のサーバーに対して行えます。

## RACADM の使用

RACADM ウェブインタフェースを使用してサーバーの電力制御操作を行うには、次の手順を実行します。

シリアル /Telnet/SSH テキストコンソールを開いて **CMC** に進み、ログインした後、次を入力します。

```
racadm serveraction -m <module> <action>
```

ここで、<module> はシャーシ内のスロット番号 **1 ~ 16** でサーバーを指定し、<action> は実行する操作 **powerup**（電源投入）、**powerdown**（電源切断）、**powercycle**（パワーサイクル）、**graceshutdown**（正常シャットダウン）、**hardreset**（ハードリセット）を指定します。

## 110V 動作

電源装置（PSU）には、**220V** と **110V** をメインにして動作する機種もあります。**110V** の電力は容量が制限されています。したがって、**110V** の接続が検出されると、シャーシはユーザーが **110V** の電力設定プロパティを変更して動作を承認するまで、サーバー電力の追加要求を許可しません。ユーザーは、使用中の **110V** の回路が、承認前にシャーシ設定で必要な電力を供給可能であることを確認しなければなりません。承認後、シャーシは今後の適切なサーバー電力要求を許可し、利用可能な電源容量を使用します。

ユーザーは、初めてインストールした後、いつでも **GUI** または **RACADM** から **110V** の承認をリセットできます。電源装置のエントリは、**110V** 電源が検出されたときと除去されたときに、**SEL** ログに記録されます。エントリは、ユーザーによる承認時と非承認時にも、**SEL** ログに記録されます。

全体的な電力の正常性は、シャーシが **110V** モードで動作し、ユーザーがその動作を承認しない場合、少なくとも非重要状態にあります。非重要状態の時は、**GUI** メインページに「警告」アイコンが表示されます。

**110V** と **220V** が混在する動作はサポートされていません。両方の電圧が使用中であることを **CMC** が検出した場合は、一方の電圧が選択され、他方の電圧に接続されている電源装置の電源はオフとなり、故障中と表示されます。

## 外部電力管理

CMC 電力管理は、オプションで、電力の測定、軽減、管理用コンソール (PM3) によって制御できます。詳細については、『PM3 User's Guide』(PM3 ユーザーズガイド) を参照してください。

外部電力管理を有効にすると、PM3 は以下を管理します。

- 第 12 世代サーバーのサーバー電力
- 第 12 世代サーバーのサーバー優先度
- システム入力電力容量
- 最大節電モード

CMC は以下の維持または管理を継続します。

- 冗長性ポリシー
- リモートでの電力ロギング
- 電源冗長性よりサーバーパフォーマンスを優先する
- 電源装置の動的制御
- 第 11 世代以前のサーバーのサーバー電力

PM3 は、シャーシインフラストラクチャと古い世代のブレードサーバーに電力を割り当てた後、使用可能なバジェットから、シャーシ内の第 12 世代ブレードサーバーの優先度と電力を管理します。リモート電力ロギングは、外部電力管理の影響を受けません。

### ウェブインタフェースの使用

PM3 外部管理を有効にするには、以下を行います。

- 1 **シャーシ設定システム管理者** 権限でシャーシにログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **電源** → **設定** をクリックします。**バジェット / 冗長性の設定** ページが表示されます。
- 4 **サーバーベース電力管理モード** を設定します。
- 5 **適用** をクリックします。

**サーバーベース電力管理モード** を有効にすると、シャーシが PM3 管理の対象となります。すべての第 12 世代サーバーの優先度は 1 (高) に設定されています。PM3 がサーバーの電力と優先度を直接管理します。PM3 は互換性のあるサーバー電力割り当てを制御するため、CMC が **最大節電モード** を制御しなくなります。このため、選択が解除されます。

**最大節電モード** が有効になっていると、CMC は **システム入力電力容量** を、シャーシが処理できる最大値に設定します。CMC は電力が最大容量を超えることを許可しません。ただし、PM3 がその他のすべての容量制限を制御します。

外部電力管理を無効にするには、以下を行います。

- 1 **シャーシ設定システム管理者** 権限でシャーシにログインします。
- 2 システムツリーで **シャーシの概要** を選択します。
- 3 **電源** → **設定** をクリックします。  
**バジェット / 冗長性の設定** ページが表示されます。
- 4 **サーバーベース電力管理モード** を解除します。
- 5 **適用** をクリックします。

電力の PM3 管理を無効にすると、CMC は外部管理が有効になる前のサーバー優先度設定に戻されます。



**メモ** : PM3 管理を無効にしたとき、CMC では最大シャーシ電力が以前の設定に戻されません。手動で値を復元するには、**CMC ログ** を参照して以前の設定を確認してください。

## RACADM の使用

**シャーシ設定システム管理者** 権限で、シリアル / Telnet / SSH テキストコンソールの CMC を開きます。

PM3 によるリモート電源管理を有効にするには、以下を入力します。

```
Racadm config -g cfgChassisPower -o  
cfgChassisServerBasedPowerMgmtMode 1
```

CMC 電力管理を復元するには、以下を入力します。

```
Racadm config -g cfgChassisPower -o  
cfgChassisServerBasedPowerMgmtMode 0
```

電力の PM3 管理を無効にすると、CMC は外部管理が有効になる前のサーバー優先度設定に戻されます。



**メモ** : PM3 管理を無効にしたとき、CMC では最大電力が以前の設定に戻されません。手動で値を復元するには、**CMC ログ** を参照して以前の設定を確認してください。

## トラブルシューティング

電源装置および電力に関連する問題のトラブルシューティングは、365 ページの「トラブルシューティングとリカバリ」を参照してください。

# iKVM モジュールの使用

## 概要

Dell M1000e サーバーシャーシのローカルアクセス KVM モジュールは Avocent 内蔵 KVM スイッチモジュールまたは iKVM と呼ばれます。iKVM はキーボード、ビデオ、マウスなどのアナログスイッチで、シャーシに差し込みます。iKVM はシャーシにホットプラグできるオプションモジュールで、シャーシ内のサーバーとアクティブな CMC のコマンドラインにローカルのキーボード、マウス、ビデオでアクセスできるようになります。

## iKVM ユーザーインターフェース

iKVM では、ホットキーでアクティブになる On Screen Configuration and Reporting (OSCAR) グラフィカルユーザーインターフェースが使用されています。OSCAR では、アクセスするサーバーや Dell CMC コマンドラインをローカルのキーボード、ディスプレイ、マウスなどで選択できます。

シャーシ 1 つに 1 つの iKVM セッションのみが許可されています。

## セキュリティ

OSCAR ユーザーインターフェースを使用すると、システムをスクリーンセーバーのパスワードで保護できます。ユーザーが定義した時間が経過すると、スクリーンセーバーモードになり、正しいパスワードを入力して OSCAR を再びアクティブにするまでアクセスが禁止されます。

## スキャン

OSCAR ではサーバーのリストを選択できます。サーバーは OSCAR がスキャンモードの間に、選択した順序で表示されます。

## サーバーの識別

CMC はシャーシ内のすべてのサーバーにスロット名を割り当てます。階層接続から OSCAR インタフェースを使用してサーバーに名前を割り当てることもできますが、CMC が割り当てた名前が優先され、OSCAR を使用してサーバーに割り当てた新しい名前はすべて上書きされます。

CMC は固有の名前を割り当ててスロットを識別します。CMC Web インタフェースを使用してスロット名を変更するには、「スロット名の編集」を参照してください。RACADM を使用してスロット名を変更するには、『RACADM Command Line Reference Guide for iDRAC7 and CMC』(iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド) の **setslotname** の

項を参照してください。

## ビデオ

iKVM ビデオ接続では、640 x 480 (60Hz) から最大 1280 x 1024 (60Hz) までのビデオ画面解像度がサポートされています。

## プラグアンドプレイ

iKVM はデータ表示チャンネル (DDC) プラグアンドプレイをサポートしています。DDC はビデオモニタの設定を自動化するもので、VESA DDC2B 規格に準拠しています。

## FLASH アップグレード可能

CMC ウェブインタフェースまたは RACADM の **fwupdate** コマンドを使用して iKVM ファームウェアをアップデートできます。詳細については、345 ページの「CMC からの iKVM の管理」を参照してください。

## 物理的な接続インタフェース

シャーシのフロントパネル、アナログコンソールインタフェース (ACI)、およびシャーシのリアパネルから、iKVM を介してサーバーまたは CMC CLI コンソールに接続できます。



**メモ:** シャーシの前面にあるコントロールパネルのポートは、オプションの iKVM 専用に設計されています。iKVM がない場合は、前面コントロールパネルのポートを使用できません。

## iKVM の 接続手順

一度に 1 つの iKVM 接続のみが使用可能です。iKVM は各接続タイプに優先順位を割り当てるため、複数の接続がある場合は、1 つの接続だけが使用可能になり、その他は無効になります。

iKVM 接続の優先順位は次のとおりです。

- 1 フロントパネル
- 2 ACI
- 3 リアパネル

たとえば、フロントパネルと ACI に iKVM 接続がある場合、フロントパネルの接続はアクティブなままで、ACI の接続が無効になります。ACI とリアパネルの接続がある場合は、ACI の接続が優先されます。

## ACI 接続の層

iKVM では、リモートコンソールスイッチポートを介してローカルから、または Dell RCS ソフトウェアを使用してリモートからサーバーと iKVM の CMC コマンドラインコンソールとの層接続が可能です。iKVM は、次の製品からの ACI 接続をサポートしています。

- 180AS、2160AS、2161DS-2\*、2161DS-2、または 4161DS Dell Remote Console Switches
- Avocent AutoView スイッチシステム
- Avocent DSR スイッチシステム
- Avocent AMX スイッチシステム

\* Dell CMC コンソール接続はサポートしていません。



**メモ** : iKVM は Dell 180ES と 2160ES への ACI 接続もサポートしていますが、階層化はシームレスではありません。この接続には USB から PS2 への SIP が必要です。

## OSCAR の使用

本項では、OSCAR インタフェースの概要を提供します。

### ナビゲーションの基本

表 10-1. OSCAR キーボードとマウスの操作

キーまたはキーシーケンス	結果
<ul style="list-style-type: none"><li>• &lt;Print Screen&gt;-&lt;Print Screen&gt;</li><li>• &lt;Shift&gt;-&lt;Shift&gt;</li><li>• &lt;Alt&gt;-&lt;Alt&gt;</li><li>• &lt;Ctrl&gt;-&lt;Ctrl&gt;</li></ul>	<p><b>OSCAR の起動</b> の設定によって、これらのどのシーケンスを使用しても OSCAR を開くことができます。<b>メイン</b> ダイアログボックスの <b>OSCAR の起動</b> セクションでチェックボックスをオンにして、<b>OK</b> をクリックすると、2 つ、3 つ、またはすべてのキーシーケンスを有効にできます。</p>
<F1>	現在のダイアログボックスの <b>ヘルプ</b> 画面を開きます。
<Esc>	変更を保存せずに現在のダイアログボックスを閉じて、前のダイアログボックスに戻ります。 <b>メイン</b> ダイアログボックスでは、<Esc> で OSCAR インタフェースを終了して、選択したサーバーに戻ります。 メッセージボックスでは、ポップアップボックスを閉じて現在のダイアログボックスに戻ります。

表 10-1. OSCAR キーボードとマウスの操作（続き）

キーまたは キーシーケンス	結果
<Alt>	下線付きの英字やその他の指定した文字と組み合わせて使用し、ダイアログボックスを開いたり、オプションを選択（チェックボックスをオンに）したり、処置を実行したりします。
<Alt>+<X>	現在のダイアログボックスを閉じて、前のダイアログボックスに戻ります。
<Alt>+<O>	<b>OK</b> ボタンを選択して、前のダイアログボックスに戻ります。
<Enter>	<b>メイン</b> ダイアログボックスでスイッチ操作を完了し、OSCARを終了します。
シングルクリック、 <Enter>	テキストボックスで、編集するテキストを選択し、左矢印キーと右矢印キーを有効にしてカーソルを移動します。<Enter> をもう一度押すと、編集モードが終了します。
<Print Screen>、 <Backspace>	他のキー入力がない場合は、前の選択項目に切り替えます。
<Print Screen>、 <Alt>+<0>	ユーザーをサーバーから即座に切断します。サーバーが選択されません。ステータスフラグには「空き」と表示されます。（この処置はキーボードの =<0> にのみ適用され、キーパッドには適用されません。）
<Print Screen>、 <Pause>	スクリーンセーバーモードを即座にオンにし、パスワード保護されている場合は、そのコンソールにアクセスできなくします。
上下の矢印キー	リストの行から行へとカーソルを移動します。
左右の矢印キー	テキストボックスの編集時に列内でカーソルを移動します。
<Home>/<End>	カーソルをリストの先頭（Home）または一番下（End）に移動します。
<Delete>	テキストボックスの文字を削除します。
数字キー	キーボードまたはキーパッドから入力します。
<Caps Lock>	無効になっています。大文字と小文字を切り替えるには、<Shift> キーを使用します。

## OSCAR の設定

表 10-2. OSCAR 設定メニューの機能

機能	目的
メニュー	サーバーのリスト表示をスロットの番号順と、名前のアルファベット順の間で切り替えます。



表 10-2. OSCAR 設定メニューの機能

機能	目的
セキュリティ	<ul style="list-style-type: none"><li>パスワードを設定してサーバーへのアクセスを制限します。</li><li>スクリーンセーバーを有効にし、スクリーンセーバーが表示されるまでのアイドル時間を設定し、スクリーン保護モードを設定します。</li></ul>
フラグ	ステータスフラグの表示、タイミング、色、配置を変更します。
言語	OSCAR の全画面の言語を変更します。
ブロードキャスト	キーボードとマウスの操作で複数のサーバーを同時に制御するように設定します。
スキャン	最大 16 サーバーのカスタムスキャンパターンを設定します。

**設定** ダイアログボックスにアクセスするには

- 1 <Print Screen> を押して OSCAR インタフェースを起動します。**メイン** ダイアログボックスが表示されます。
- 2 **設定** をクリックします。**設定** ダイアログボックスが表示されます。

#### 表示動作の変更

サーバーの表示順序を変更し、OSCAR の画面遅延時間を設定するには、**メニュー** ダイアログボックスを使用します。

**メニュー** ダイアログボックスにアクセスするには：

- 1 <Print Screen> を押して OSCAR を起動します。**メイン** ダイアログボックスが表示されます。
- 2 **設定**、**メニュー** の順にクリックします。**メニュー** ダイアログボックスが表示されます。

**メイン** ダイアログボックスでサーバーのデフォルトの表示順序を変更するには

- 1 サーバーを名前のアルファベット順に表示するには、**名前** を選択します。  
または  
**スロット** を選択し、サーバーをスロット番号順に表示します。

- 2 **OK** をクリックします。

OSCAR をアクティブにするキーシーケンスを 1 つ以上割り当てるには

**OSCAR の起動** メニューからキーシーケンスを選択し、**OK** をクリックします。

OSCAR を起動するデフォルトのキーは <Print Screen> です。

OSCAR の画面遅延時間を設定するには

- 1 <Print Screen> を押してから OSCAR が表示されるまでの遅延を秒数 (0 ~ 9) で入力します。

<0> と入力すると、遅延なしで OSCAR が起動します。




- 2 **OK** をクリックします。

OSCAR を遅延表示する時間を設定すると、ソフトスイッチを完了できます。ソフトスイッチの実行方法については、335 ページの「ソフトスイッチ」を参照してください。

### ステータスフラグの制御

ステータスフラグはデスクトップに表示され、選択されているサーバーの名前、または選択されているスロットの状態を示します。**フラグ** ダイアログボックスを使用して、サーバーごとに表示するフラグを設定したり、フラグの色、透明性、表示時間、デスクトップ上の配置などを変更します。

表 10-3. OSCAR ステータスフラグ

フラグ	説明
	名前によるフラグの種類
	ユーザーがすべてのシステムから切断されたことを示すフラグ
	ブロードキャストモードが有効であることを示すフラグ

**フラグ** ダイアログボックスにアクセスするには

- 1 <Print Screen> を押します。**メイン** ダイアログボックスが表示されます。
- 2 **設定**、**フラグ** の順にクリックします。**フラグ** ダイアログボックスが表示されます。


ステータスフラグの表示方法を指定するには

- 1 フラグを常に表示するには **表示** を選択し、切り替え後 5 秒間だけフラグを表示するには **表示と時間指定** を選択します。

 **メモ**：時間指定 だけを選択すると、フラグは表示されません。

- 2 **表示色** セクションからフラグの色を選択します。オプションは黒、赤、青、紫です。
- 3 **表示モード** で、無地のカラーフラグには **不透明** を選択し、フラグからデスクトップが透けて見えるようにするには **透明** を選択します。
- 4 ステータスフラグをデスクトップに配置するには
  - a **位置の設定** をクリックします。**フラグの位置設定** が表示されます。

- b タイトルバーを左クリックし、デスクトップ上の任意の場所までドラッグします。
- c **フラグ** ダイアログボックスに戻るには、右クリックします。

 **メモ**: フラグの位置変更は、**フラグ** ダイアログボックスで **OK** をクリックするまでは保存されません。

- 5 **OK** をクリックして設定を保存します。  
変更を保存せずに終了するには、 をクリックします。


## iKVM によるサーバーの管理


iKVM は最大 16 のサーバーをサポートするアナログスイッチマトリックスです。iKVM スイッチは OSCAR ユーザーインターフェースを使用してサーバーの選択と設定を行います。また、iKVM には CMC コマンドラインコンソールから CMC への接続を確立するためのシステム入力が含まれています。

### 周辺機器の互換性とサポート

iKVM は次の周辺機器と互換性があります。


- QWERTY、QWERTZ、AZERTY、および日本語 109 配列の標準 PC USB キーボード。
- DDC をサポートしている VGA モニタ。
- 標準 USB ポインティングデバイス。
- iKVM のローカル USB ポートに接続している電源内蔵式 USB 1.1 ハブ。
- Dell M1000e シャーシのフロントパネルコンソールに接続している電動 USB 2.0 ハブ。


 **メモ**: iKVM のローカル USB ポートではキーボードとマウスを複数使用できます。iKVM は入力信号を統合します。複数の USB キーボードまたはマウスから同時に入力信号があると、予測不能の結果が生じる可能性があります。

 **メモ**: サポートされているキーボード、マウスおよび USB ハブのみ USB 接続できます。iKVM は、その他の USB 周辺機器から送信されるデータをサポートしていません。

### サーバーの表示と選択

iKVM からサーバーを表示、設定、管理するには、**OSCAR メイン** ダイアログボックスを使用します。サーバーは名前またはスロットを基準に表示できます。スロット番号は、サーバーが使用するシャーシスロット番号です。**スロット** 列は、サーバーが取り付けられているスロット番号を示します。

 **メモ**: Dell CMC コマンドラインはスロット 17 を占有しています。このスロットを選択すると、RACADM コマンドを実行し、サーバーのシリアル コンソールまたは I/O モジュールに接続する CMC コマンド ラインを表示します。

 **メモ**：サーバー名とスロット番号は CMC によって割り当てられます。


**メイン** ダイアログボックスにアクセスするには、次の手順を実行します。

<Print Screen> を押して **OSCAR** インタフェースを起動します。**メイン** ダイアログボックスが表示されます。

または

パスワードが割り当てられている場合は、**パスワード** ダイアログボックスが表示されます。パスワードを入力して **OK** をクリックします。**メイン** ダイアログボックスが表示されます。





パスワード設定の詳細に関しては、337 ページの「コンソールのセキュリティの設定」を参照してください。

 **メモ**：OSCAR の起動には 4 つのオプションがあります。**メイン** ダイアログボックスの **OSCAR の起動** セクションでボックスを選択して、**OK** をクリックすると、1 つ、複数、またはすべてのキーシーケンスを有効にできます。

### サーバーのステータス表示

シャーシのサーバーのステータスは、**メイン** ダイアログボックスの右側に表示されます。次の表で、ステータス記号について説明します。

表 10-4. **OSCAR** インタフェースのステータス記号

記号	説明
	(緑色のドット) サーバーはオンラインです。
	(赤色の X) サーバーはオフラインまたはシャーシにありません。
	(黄色のドット) サーバーは利用できません。
	(緑色の A または B) サーバーは、英字：A= リアパネル、B= フロントパネルで示されるユーザーチャネルによってアクセスされ

### サーバーの選択

サーバーを選択するには、**メイン** ダイアログボックスを使用します。サーバーを選択すると、iKVM によってキーボードとマウスがそのサーバーの正しい設定に再構成されます。

- サーバーを選択するには  
サーバー名かスロット番号をダブルクリックします。

または

サーバーのリストがスロット順に表示されている場合は (**スロット** ボタンが押された状態)、スロット番号を入力して <Enter> を押します。

または

サーバーのリストが名前順に表示されている場合は（**名前** ボタンが押された状態）、固有のサーバー名として確立するまで、最初の文字をいくつか入力して <Enter> を 2 回押します。

- 前のサーバーを選択するには  
<Print Screen> を押してから <Backspace> を押します。このキーの組み合わせによって、前の接続と現在の接続が切り替わります。
- サーバーからユーザーを切断するには  
<Print Screen> を押して OSCAR にアクセスしてから **切断** をクリックします。

または

<Print Screen> を押してから <Alt><0> を押します。この操作により、サーバーが選択されていない空きの状態になります。デスクトップのステータスフラグがアクティブな場合は、「空き」と表示されます。332 ページの「ステータスフラグの制御」を参照してください。

## ソフトスイッチ

ソフトスイッチは、ホットキーシーケンスを使用したサーバー間の切り替えです。<Print Screen> を押して、サーバーの名前や数字を先頭から何文字か入力すると、ソフトスイッチでサーバーに切り替えることができます。前に **遅延時間**（<Print Screen> を押してから **メイン** ダイアログボックスが表示されるまでの秒数）を設定した場合は、その時間が経過する前にキーシーケンスを押すと、OSCAR インタフェースは表示されません。

OSCAR にソフトスイッチを設定するには

- 1 <Print Screen> を押して OSCAR インタフェースを起動します。**メイン** ダイアログボックスが表示されます。
- 2 **設定、メニュー** の順にクリックします。**メニュー** ダイアログボックスが表示されます。
- 3 表示 / 並べ替えキーの **名前** または **スロット** を選択します。
- 4 **画面遅延時間** フィールドに遅延時間を秒で入力します。
- 5 **OK** をクリックします。

サーバーにソフトスイッチするには

- サーバーを選択するには、<Print Screen> を押します。  
手順 3 の選択に従ってサーバーのリストがスロット順に表示されている場合は（**スロット** ボタンが押された状態）、スロット番号を入力して <Enter> を押します。

または

手順 3 の選択に従ってサーバーのリストが名前順に表示されている場合は（**名前** ボタンが押された状態）、固有のサーバー名として確立するまで、最初の文字をいくつか入力して <Enter> を 2 回押します。

- 前のサーバーに戻るには、<Print Screen> を押してから <Backspace> を押します。

### ビデオ接続

iKVM はシャーシのフロントパネルとリアパネルにビデオ接続があります。フロントパネルの接続信号がリアパネルの接続信号より優先されます。モニタがフロントパネルに接続していると、ビデオ接続がリアパネルまで通らず、リアパネルの KVM 接続と ACI の接続が無効であるという OSCAR メッセージが表示されます。モニタが無効になると（フロントパネルから取り外すか CMC コマンドで無効にする）、リアパネルの KVM は無効のままですが、ACI の接続がアクティブになります。（接続の優先度の詳細については、iKVM の接続手順を参照してください。）

フロントパネル接続を有効または無効にする手順の詳細については、フロントパネルの有効または無効を参照してください。

### 割り込み警告

通常、iKVM からサーバーコンソールに接続しているユーザーと、iDRAC GUI コンソールリダイレクト機能を使用して同じサーバーコンソールに接続している別のユーザーは、両者ともコンソールにアクセスして同時に入力できます。

この状況を防止するには、リモートユーザーが iDRAC GUI コンソールリダイレクトを開始する前に iDRAC ウェブインタフェースでローカルコンソールを無効にできます。ローカル iKVM ユーザーには、指定された時間内に接続の割り込みが発生することを知らせる OSCAR メッセージが表示されます。ローカルユーザーはサーバーへの iKVM 接続が終了する前に作業を完了する必要があります。

iKVM ユーザーが使用できる割り込み機能はありません。



**メモ:** リモートの iDRAC ユーザーが特定のサーバーのローカルビデオを無効にした場合は、そのサーバーのビデオ、キーボード、およびマウスが iKVM で使用できなくなります。OSCAR メニューでサーバーの状態が黄色のドットで表示され、ローカルでの使用がロックされているか使用不可であることを示します（サーバーのステータス表示を参照）。

## コンソールのセキュリティの設定

OSCAR では iKVM コンソールのセキュリティ設定を指定できます。指定した遅延時間ほどコンソールが使用されなかった場合に作動するスクリーンセーバーモードを設定できます。作動すると、キーを押すかマウスを動かすまでコンソールはロックされたままになります。続行するには、スクリーンセーバーのパスワードを入力します。

**セキュリティ** ダイアログボックスを使用すると、パスワード保護を使用してコンソールをロックしたり、パスワードを設定または変更したり、スクリーンセーバーを有効にしたりできます。



**メモ:** iKVM のパスワードを失くしたり忘れてしまった場合は、CMC ウェブインタフェースまたは RACADM を使用して iKVM 出荷時のデフォルトにリセットできます。「失くしたり忘れてしまったパスワードのクリア」を参照してください。

### セキュリティダイアログボックスへのアクセス

セキュリティダイアログボックスにアクセスするには、次の手順を実行してください。

- 1 <Print Screen> を押します。**メイン** ダイアログボックスが表示されます。
- 2 **設定、セキュリティ** の順にクリックします。**セキュリティ** ダイアログボックスが表示されます。

### パスワードの設定または変更

パスワードを設定または変更するには、次の手順を実行してください。

- 1 **新規** フィールドでシングルクリックして <Enter> を押すか、ダブルクリックします。
- 2 **新規** フィールドに新しいパスワードを入力し、<Enter> を押します。パスワードは大文字と小文字が区別され、5 ~ 12 文字必要です。少なくとも英字が 1 つと数字が 1 つ含まれていなければなりません。有効な文字は A ~ Z、a ~ z、0 ~ 9、スペースおよびハイフンです。
- 3 **再入力** フィールドにパスワードをもう一度入力して <Enter> を押します。
- 4 パスワードを変更するだけの場合は **OK** をクリックして、ダイアログボックスを閉じます。

### コンソールのパスワード保護

コンソールにパスワードを設定するには、次の手順を実行してください。

- 1 前の手順で説明した方法でパスワードを設定します。
- 2 **スクリーンセーバーを有効にする** チェックボックスをオンにします。
- 3 パスワード保護とスクリーンセーバーの起動を遅らせる **アイドル時間** (1 ~ 99) を分で入力します。

- 4 **モード**：モニターが ENERGY STAR 準拠の場合は、**Energy**、それ以外の場合は **スクリーン** を選択します。



**メモ**：モードが **Energy** に設定されている場合は、アプライアンスがモニターをスリープモードにします。これは通常、モニターの電源がオフになり、緑色の電源 LED に代わって橙色が点灯することからわかります。モードが **スクリーン** に設定されている場合は、テスト中 OSCAR フラグが画面上のあちこちを移動します。テストが開始する前に、警告ポップアップボックスに次のメッセージが表示されます。「Energy モードにすると、ENERGY STAR 準拠でないモニターが損傷することがあります。ただし、開始直後にマウスまたはキーボード操作によってテストを中止できます。」



**注意**：Energy Star 準拠ではないモニターで Energy モードを使用すると、モニターが損傷する恐れがあります。

- 5 **オプション**：スクリーンセーバーテストをアクティブにするには、**テスト** をクリックします。**スクリーンセーバーテスト** ダイアログが表示されます。**OK** をクリックしてテストを開始します。  
テストに 10 秒かかります。完了すると、**セキュリティ** ダイアログボックスに戻ります。

## ログイン

Oscar を起動するには：

- 1 <Print Screen> を押して OSCAR を起動します。**パスワード** ダイアログボックスが表示されます。
- 2 パスワードを入力して **OK** をクリックします。**メイン** ダイアログボックスが表示されます。

## 自動ログアウトの設定

一定のアイドル時間が経過すると自動的にログアウトするように OSCAR を設定できます。

- 1 **メイン** ダイアログボックスで **設定**、**セキュリティ** の順にクリックします。
- 2 **アイドル時間** フィールドに、自動的に切断されるまで接続したままにいる時間を入力します。
- 3 **OK** をクリックします。

## コンソールからのパスワード保護の削除


コンソールのパスワード保護を解除するには、次の手順を実行してください。

- 1 **メイン** ダイアログボックスから **設定**、**セキュリティ** の順にクリックします。
- 2 **セキュリティ** ダイアログボックスで、**新規** フィールドをシングルクリックして <Enter> を押すか、ダブルクリックします。




- 3 **新規** フィールドを空にして <Enter> を押します。
- 4 **再入力** フィールドをシングルクリックして <Enter> を押すか、ダブルクリックします。
- 5 **再入力** フィールドを空にして <Enter> を押します。
- 6 パスワードを除去するだけの場合は、**OK** をクリックします。

#### パスワード保護なしでスクリーンセーバーモードを有効にする方法

 **メモ**：コンソールがパスワードで保護されている場合は、最初にパスワード保護を削除する必要があります。つぎの手順を実行する前に、上記の手順を済ませてください。


パスワード保護なしでスクリーンセーバーモードを有効にするには：

- 1 **スクリーンセーバーを有効にする** を選択します。
- 2 スクリーンセーバーの起動を遅らせる時間（1～99）を分で入力します。
- 3 モニターが **ENERGY STAR** 準拠の場合は、**Energy**、それ以外の場合は **スクリーン** を選択します。

 **注意**：Energy Star 準拠ではないモニターで Energy モードを使用すると、モニターが損傷する恐れがあります。

- 4 オプション：スクリーンセーバーテストをアクティブにするには、**テスト** をクリックします。**スクリーンセーバーテスト** ダイアログが表示されます。**OK** をクリックしてテストを開始します。

テストに 10 秒かかります。完了すると、**セキュリティ** ダイアログボックスに戻ります。

 **メモ**：スクリーンセーバーモードを有効にすると、ユーザーがサーバーから切断され、サーバーは選択されません。ステータスフラグには「空き」と表示されます。

#### スクリーンセーバーモードの終了

スクリーンセーバーモードを終了して **メイン** ダイアログボックスに戻るには、キーをどれか 1 つ押すか、マウスを動かします。

スクリーンセーバーをオフにするには

**セキュリティ** ダイアログボックスで、**スクリーンセーバーを有効にする** チェックボックスをオフにして、**OK** をクリックします。

スクリーンセーバーを即座にオンにするには、<Print Screen> を押してから <Pause> を押します。

#### 失くしたり忘れてたりしたパスワードのクリア

iKVM のパスワードを失くしたり忘れてたりした場合は、iKVM の出荷時のデフォルトのパスワードにリセットしてから変更できます。パスワードのリセットには CMC ウェブインタフェースか RACADM を使用します。

失くしたり忘れてしたりした iKVM パスワードを CMC ウェブインタフェースを使用してリセットするには：

- 1 CMC ウェブインタフェースにログインします。
- 2 シャーシサブメニューから **iKVM** を選択します。
- 3 **セットアップ** タブをクリックします。**iKVM 構成** ページが表示されます。
- 4 **デフォルト値の復元** をクリックします。

これで、OSCAR を使用してパスワードをデフォルトから変更できます。「パスワードの設定または変更」を参照してください。

RACADM を使用して、紛失した、または忘れてしまったパスワードをリセットするには、CMC へのシリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログイン後、次を入力します。

```
racadm racresetcfg -m kvm
```



**メモ** : **racresetcfg** コマンドを使用すると、フロントパネル有効と Dell CMC コンソール有効の設定がデフォルト値と異なる場合はリセットされます。

**racresetcfg** コマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **racresetcfg** コマンドの項を参照してください。

### 言語の変更

OSCAR のテキストを対応言語のいずれかに変更するには、**言語** ダイアログボックスを使用します。OSCAR のすべての画面が直ちに選択した言語に変わります。

OSCAR の言語を変更するには

- 1 <Print Screen> を押します。**メイン** ダイアログボックスが表示されます。
- 2 **設定、言語** の順にクリックします。**言語** ダイアログボックスが表示されます。
- 3 使用する言語のラジオボタンをクリックしてから **OK** をクリックします。

### バージョン情報の表示

iKVM ファームウェアとハードウェアのバージョンを表示し、言語とキーボードの設定を確認するには、**バージョン** ダイアログボックスを使用します。

バージョン情報を表示するには

- 1 <Print Screen> を押します。**メイン** ダイアログボックスが表示されます。
- 2 **コマンド、バージョンの表示** の順にクリックします。**バージョン** ダイアログボックスが表示されます。

**バージョン** ダイアログボックスの上半分にアプライアンスのサブシステムのバージョンが一覧になります。

- 3  をクリックするか、<Esc> を押して **バージョン** ダイアログボックスを閉じます。

## システムのスキャン

スキャンモードでは、iKVM が自動的にスロットからスロットへ（サーバーからサーバーへ）とスキャンします。スキャンするサーバーと、各サーバーが表示される時間を秒で指定して、最大 **16** のサーバーをスキャンできます。

スキャンリストにサーバーを追加するには

- 1 <Print Screen> を押します。 **メイン** ダイアログボックスが表示されます。
- 2 **設定、スキャン** の順にクリックします。 **スキャン** ダイアログボックスが表示され、シャーシ内のすべてのサーバーが一覧になります。
- 3 スキャンするサーバーの横にあるチェックボックスをオンにします。  
または  
サーバー名かスロットをダブルクリックします。  
または  
<Alt > と、スキャンするサーバーの番号を押します。最大 **16** のサーバーを選択できます。
- 4 **時間** フィールドに、スキャンがリストの次のサーバーに移動するまで iKVM が待つ時間（**3 ~ 99**）を秒で入力します。
- 5 **追加 / 削除** ボタンをクリックし、 **OK** をクリックします。

サーバーを **スキャン** リストから削除するには

- 1 **スキャン** ダイアログボックスで、削除するサーバーの横にあるチェックボックスをオンにします。  
または  
サーバー名かスロットをダブルクリックします。  
または  
**クリア** ボタンをクリックして、すべてのサーバーを **スキャン** リストから削除します。
- 2 **追加 / 削除** ボタンをクリックし、 **OK** をクリックします。

スキャンモードを開始するには

- 1 <Print Screen> を押します。 **メイン** ダイアログボックスが表示されます。
- 2 **コマンド** をクリックします。 **コマンド** ダイアログボックスが表示されます。
- 3 **スキャン有効** チェックボックスをオンにします。

- 4 **OK** をクリックします。マウスとキーボードがリセットされたというメッセージが表示されます。
- 5  をクリックしてメッセージボックスを閉じます。

スキャンモードをキャンセルするには

- 1 **OSCAR** が開いており、**メイン** ダイアログボックスが表示されている場合は、リストからサーバーを選択します。

または

**OSCAR** が開いていない場合は、マウスを動かすか、キーボードでどれかキーを押します。現在選択されているサーバーでスキャンが停止します。

または

<Print Screen> を押します。**メイン** ダイアログボックスが表示されたら、リストからサーバーを選択します。

- 2 **コマンド** ボタンをクリックします。**コマンド** ダイアログボックスが表示されます。
- 3 **スキャン有効** チェックボックスをオフにします。

## サーバーへのブロードキャスト

システム内の複数のサーバーを同時に制御して、すべてのサーバーが同じ入力を受信するように設定できます。キー入力やマウスの動作を個別にブロードキャストすることもできます。



**メモ:** 最大 16 のサーバーに同時にブロードキャストできます。

サーバーにブロードキャストするには

- 1 <Print Screen> を押します。**メイン** ダイアログボックスが表示されます。
- 2 **設定、ブロードキャスト** の順にクリックします。**ブロードキャスト** ダイアログボックスが表示されます。



**メモ:** キー入力のブロードキャスト：キー入力を使用する場合、キー入力と同じであると解釈されるためには、ブロードキャストを受信するすべてのサーバーでキーボードの状況が同じであることが必要です。つまり、<Caps Lock> と <Num Lock> のモードがすべてのキーボードで同じでなければなりません。iKVM は選択したサーバーにキー入力を同時に送信しますが、一部のサーバーの抑制によって伝送が遅延する場合があります。



**メモ:** マウス動作のブロードキャスト：マウスが正確に機能するには、すべてのサーバーのマウスドライバ、デスクトップ（同じアイコンの配置など）、ビデオ解像度が同じであることが必要です。また、マウスがすべての画面で同じ場所になければなりません。これらの条件を満たすのは難しいため、複数のサーバーにマウスの動作をブロードキャストすると、予測不能な結果が生じることがあります。

- 3 チェックボックスをオンにして、ブロードキャストコマンドを受信するサーバーのマウスやキーボードを有効にします。

または

上下の矢印を押して、目的のサーバーまでカーソルを移動します。キーボードのチェックボックスをオンにするには <Alt><K>、マウスのチェックボックスをオンにするには <Alt><M> を押します。他のサーバーにも同じ操作を繰り返します。

- 4 **OK** を押して設定を保存し、**設定** ダイアログボックスに戻ります。 をクリック、または <Escape> を押して、**メイン** ダイアログボックスに戻ります。
- 5 **コマンド** をクリックします。**コマンド** ダイアログボックスが表示されます。
- 6 **ブロードキャスト有効** チェックボックスをオンにしてブロードキャストをアクティブにします。**ブロードキャスト警告** ダイアログボックスが表示されます。
- 7 **OK** をクリックしてブロードキャストを開始します。  
キャンセルして **コマンド** ダイアログボックスに戻るには、 をクリック または <Esc> を押します。
- 8 ブロードキャストが有効になっている場合は、情報を入力し、ブロードキャストするマウスの動作を管理ステーションから実行します。リスト内のサーバーのみがアクセス可能です。

ブロードキャストをオフにするには

**セキュリティ** ダイアログボックスから、**ブロードキャスト有効** チェックボックスをオフにします。

## CMC からの iKVM の管理

### フロントパネルの有効または無効

RACADM を使用して前面パネルから iKVM へのアクセスを有効または無効にするには、CMC へのシリアル/Telnet/SSH テキストコンソールを開いて CMC へ進み、ログイン後、次を入力します。

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <value>
```

<value> (値) は 1 (有効) または 0 (無効) です。

**config** サブコマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の config コマンドの項を参照してください。

ウェブインタフェースを使用してフロントパネルから iKVM へのアクセスを有効または無効にするには

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで iKVM を選択します。 **iKVM ステータス** ページが表示されます。
- 3 **セットアップ** タブをクリックします。 **iKVM 構成** ページが表示されます。
- 4 有効にするには、 **フロントパネル USB/ ビデオ有効** チェックボックスをオンにします。  
無効にするには、 **フロントパネル USB/ ビデオ有効** チェックボックスをオフにします。
- 5 **適用** をクリックして設定を保存します。

### iKVM を介した Dell CMC コンソールの有効化

RACADM を使用して iKVM から Dell CMC コンソールへのアクセスを有効にするには、CMC へのシリアル /Telnet/SSH テキストコンソールを開いて CMC へ進み、ログインした後、次を入力します。

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

ウェブインタフェースを使用して Dell CMC コンソールを有効にするには

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで iKVM を選択します。 **iKVM ステータス** ページが表示されます。
- 3 **セットアップ** タブをクリックします。 **iKVM 構成** ページが表示されます。
- 4 **iKVM から CMC CLI へのアクセスを許可する** チェックボックスをオンにします。
- 5 **適用** をクリックして設定を保存します。

### iKVM のステータスとプロパティの表示

Dell M1000e サーバシャーシのローカルアクセス KVM モジュールは Avocent 内蔵 KVM スイッチモジュールまたは iKVM と呼ばれます。シャーシに関連付けられた iKVM の正常性の状態は、 **シャーシグラフィックス** セクションの **シャーシのプロパティ正常性** ページで閲覧することができます。

**シャーシグラフィックス** を使用して iKVM の正常性ステータスを表示するには

- 1 CMC ウェブインタフェースにログインします。
- 2 **シャーシステータス** ページが表示されます。 **シャーシグラフィックス** の中央のセクションには、シャーシの背面図と iKVM の正常性状態が表示されます。iKVM の正常性状態は、iKVM サブグラフィックの色で示されます。
  - 緑色 - iKVM が存在し、電源がオンで CMC と通信中。悪条件の兆候なし。

- 橙色 - iKVM が存在するが、電源がオンまたはオフ、または CMC と通信中または通信していない。悪条件が存在する可能性あり。
  - 灰色 - iKVM が存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
- 3 個々の iKVM サブグラフィックにマウスのカーソルを重ねると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象の iKVM に関する追加情報を提供します。
  - 4 iKVM サブグラフィックは、該当する CMC GUI ページにハイパーリンクされており、**iKVM ステータス** ページに即座に移動することができます。

iKVM の詳細については、iKVM モジュールの使用を参照してください。

**iKVM ステータス** ページを使って iKVM のステータスを表示するには

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **iKVM** を選択します。**iKVM ステータス** ページが表示されます。

**表 10-5. iKVM ステータス情報**

項目	説明
存在	iKVM モジュールが <b>存在</b> か <b>不在</b> かを示します。
電源状態	iKVM の電源状態が <b>オン</b> か <b>オフ</b> か <b>該当なし</b> (不在) かを示します。
名前	iKVM のの製品名を表示します。
メーカー	iKVM のメーカーを表示します。
パーツ番号	iKVM のパーツ番号を示します。パーツ番号は、ベンダーが提供する一意の識別子です。
ファームウェアバージョン	iKVM のファームウェアバージョンを表示します。
ハードウェアバージョン	iKVM のハードウェアバージョンを表示します。
フロントパネル接続済み	モニターがフロントパネルの VGA コネクタに <b>接続している</b> かどうかを示します ( <b>はい</b> または <b>いいえ</b> )。この情報は、ローカルユーザーにシャーシへの前面パネルへのアクセスがあるかどうかを CMC が判定できるように提供されます。
リアパネル接続済み	モニターがリアパネルの VGA コネクタに <b>接続している</b> かどうかを示します ( <b>はい</b> または <b>いいえ</b> )。この情報は、ローカルユーザーにシャーシへの背面パネルへのアクセスがあるかどうかを CMC が判定できるように提供されます。

表 10-5. iKVM ステータス情報 (続き)

項目	説明
ポート層接続済み	iKVM は内蔵ハードウェアを使用して Dell と Avocent の外付け KVM アプライアンスにシームレスに層接続できるように設計されています。iKVM が層になっていると、その接続元の外付け KVM スイッチの画面ディスプレイからシャーシ内のサーバーにアクセスできます。
前面パネルの USB/ビデオを有効にする	フロントパネル VGA コネクタが有効かどうかを示します (はいまたは いいえ)。
iKVM から CMC へのアクセスを許可	iKVM からの CMC コマンドコンソールが有効かどうかを示します (はい または いいえ)。

## iKVM ファームウェアのアップデート

CMC ウェブインタフェースまたは RACADM を使用して iKVM ファームウェアをアップデートできます。

CMC ウェブインタフェースを使用して iKVM ファームウェアをアップデートするには

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** をクリックします。
- 3 **アップデート** タブをクリックします。 **アップデート可能なコンポーネント** ページが表示されます。
- 4 iKVM 名をクリックします。 **ファームウェアのアップデート** ページが表示されます。
- 5 **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、 **参照** をクリックし、ファイルの保存場所にナビゲートします。



**メモ** : iKVM ファームウェアイメージのデフォルト名は **ikvm.bin** です。この名前を変更することも可能です。

- 6 **ファームウェアアップデートを開始する** をクリックします。操作の確定を求めるダイアログボックスが表示されます。
- 7 **はい** をクリックして続行します。 **ファームウェアアップデートの進行状況** セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって大きく異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。次の補足的指示に従ってください。
  - ファイル転送時に、 **更新** ボタンの利用、または他のページへ移動しないでください。



- アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
- **アップデート状態** フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。一部の古いブラウザでは、この自動更新はサポートされていません。**アップデート状態** フィールドを手動で更新するには、**更新** をクリックします



**メモ**: iKVM のアップデートに最大 1 分程かかる場合があります。

アップデートが完了すると、iKVM がリセットし、新しいファームウェアにアップデートされ、**アップデート可能なコンポーネント** ページに表示されます。

RACADM を使用して iKVM ファームウェアをアップデートするには、CMC へのシリアル /Telnet/SSH テキスト コンソールを開いて CMC へ進み、ログイン後、次を入力します。

```
racadm fwupdate -g -u -a <TFTP server IP address or FQDN> -d <filepath/filename> -m kvm
```

たとえば、次のとおりです。

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

**fwupdate** サブコマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **fwupdate** コマンドの項を参照してください。

## トラブルシューティング



**メモ**: アクティブなコンソールリダイレクトセッションがあり、推奨解像度以下の画面で iKVM に接続している場合、ローカルコンソールでサーバーを選択すると、サーバーのコンソール解像度がリセットされることがあります。サーバーで Linux オペレーティングシステムが稼働している場合は、ローカルモニタで X11 コンソールが表示されない可能性があります。iKVM で <Ctrl><Alt><F1> キーを押すと、Linux がテキストコンソールに切り替わります。

表 10-6. iKVM のトラブルシューティング

問題	考えられる原因と解決法
フロントパネルに接続しているモニターに「CMC コントロールによってユーザーが無効になりました」というメッセージが表示されます。	<p>フロントパネルの接続が CMC によって無効になりました。</p> <p>CMC ウェブインタフェースか RACADM を使用してフロントパネルを有効にできます。ウェブインタフェースを使用してフロントパネルを有効にするには</p> <ol style="list-style-type: none"> <li>1 CMC ウェブインタフェースにログインします。</li> <li>2 システムツリーで iKVM を選択します。</li> <li>3 セットアップ タブをクリックします。</li> <li>4 フロントパネル USB/ ビデオ有効 チェックボックスをオンにします。</li> <li>5 適用 をクリックして設定を保存します。</li> </ol> <p>RACADM を使用してフロントパネルを有効にするには、CMC へのシリアル /Telnet/SSH テキスト コンソールを開いて CMC へ進み、ログイン後、次を入力します。</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1</pre>
リアパネルのアクセスが機能しません。	<p>フロントパネルの設定が CMC によって有効になり、現在前面パネルにモニターが接続されています。</p> <p>一度に 1 つの接続のみが許可されています。フロントパネルの接続は ACI とリアパネルの接続より優先されます。接続の優先度の詳細については、iKVM の 接続手順 を参照してください。</p>
リアパネルに接続しているモニターに、「現在別のアプライアンスが層にあるため、ユーザーが無効になりました」というメッセージが表示されます。	<p>ネットワークケーブルが iKVM の ACI ポートコネクタとセカンダリ KVM アプライアンスに接続しています。</p> <p>一度に 1 つの接続のみが許可されています。ACI 層接続はリアパネルのモニタ接続より優先されます。優先順位はフロントパネル、ACI、リアパネルの順になります。</p>

表 10-6. iKVM のトラブルシューティング (続き)

問題	考えられる原因と解決法
<p>iKVM のオレンジの LED が点滅しています。</p>	<p>3 つの原因が考えられます。</p> <p><b>iKVM に問題があり、iKVM の再プログラミングが必要です。</b>問題を解決するには、iKVM ファームウェアのアップデート手順に従ってください (iKVM ファームウェアのアップデート を参照)。</p> <p><b>iKVM が CMC コンソールのインタフェースを再プログラミングしています。</b>この場合は、CMC コンソールが一時的に使用不可になり、OSCAR インタフェースで黄色のドットで表されます。このプロセスに最大 15 分かかります。</p> <p><b>iKVM ファームウェアがハードウェアのエラーを検出しました。</b>詳細については、iKVM ステータスを参照してください。</p> <p>ウェブインタフェースを使用して iKVM ステータスを表示するには</p> <ol style="list-style-type: none"> <li>1 CMC ウェブインタフェースにログインします。</li> <li>2 システムツリーで iKVM を選択します。</li> </ol> <p>RACADM を使用して iKVM ステータスを表示するには、CMC へのシリアル/Telnet/SSH テキスト コンソールを開いて CMC へ進み、ログイン後、次を入力します。</p> <pre>racadm getkvmInfo</pre>

表 10-6. iKVM のトラブルシューティング (続き)

問題	考えられる原因と解決法
<p>使用している iKVM は ACI ポートから外部 KVM スイッチまで層になっていますが、ACI 接続のすべてのエントリが使用不可です。</p> <p>OSCAR インタフェースで状態のすべてに黄色のドットが表示されます。</p>	<p>フロントパネルの接続が有効になり、モニターが接続しています。フロントパネルはその他すべての iKVM 接続より優先されるため、ACI とリアパネルの接続は無効になります。</p> <p>ACI ポートの接続を有効にするには、最初にフロントパネルのアクセスを無効にするか、フロントパネルに接続しているモニターを取り外します。外部 KVM スイッチ OSCAR のエントリがアクティブになり、アクセス可能になります。</p> <p>ウェブインタフェースを使用してフロントパネルを無効にするには</p> <ol style="list-style-type: none"> <li>1 CMC ウェブインタフェースにログインします。</li> <li>2 システムツリーで iKVM を選択します。</li> <li>3 <b>セットアップ</b> タブをクリックします。</li> <li>4 <b>フロントパネル USB/ビデオ有効</b> チェックボックスをオフにします。</li> <li>5 <b>適用</b> をクリックして設定を保存します。</li> </ol> <p>RACADM を使用してフロントパネルを無効にするには、CMC へのシリアル /Telnet/SSH テキスト コンソールを開いて CMC へ進み、ログイン後、次を入力します。</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0</pre>

表 10-6. iKVM のトラブルシューティング (続き)

問題	考えられる原因と解決法
<p>OSCAR メニューで、Dell CMC 接続に赤い「X」が表示され、CMC に接続できません。</p>	<p>2 つの原因が考えられます。</p> <p><b>Dell CMC コンソールが無効になっています。</b>この場合は、CMC ウェブインタフェースか RACADM を使用してこれを有効にできます。</p> <p>ウェブインタフェースを使用して Dell CMC コンソールを有効にするには</p> <ol style="list-style-type: none"> <li>1 CMC ウェブインタフェースにログインします。</li> <li>2 システムツリーで <b>iKVM</b> を選択します。</li> <li>3 <b>セットアップ</b> タブをクリックします。</li> <li>4 <b>iKVM から CMC CLI へのアクセスを許可する</b> チェックボックスをオンにします。</li> <li>5 <b>適用</b> をクリックして設定を保存します。</li> </ol> <p>RACADM を使用して Dell CMC 接続を有効にするには、CMC へのシリアル/Telnet/SSH テキスト コンソールを開いて CMC へ進み、ログイン後、次を入力します。</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre> <p><b>CMC が初期化中、スタンバイ CMC への切り替え中、または再プログラミングを実行中のため、使用できません。</b>この場合は、CMC が初期化が終了するまで待ってください。</p>
<p>OSCAR でサーバーのスロット名が「初期化中」と表示され、選択できません。</p>	<p>サーバーが初期化中か、そのサーバーの iDRAC が初期化に失敗しました。</p> <p>まず 60 秒待ちます。サーバーがまだ初期化中である場合、初期化が完了するとすぐにスロット名が表示され、サーバーを選択できるようになります。</p> <p>60 秒後、OSCAR にスロットが初期化中であると示された場合は、サーバーをシャーシから取り出して再び挿入します。この措置によって iDRAC は再初期化が可能になります。</p>



## I/O ファブリック管理

シャーシは、最大 6 つのパススルーまたはスイッチ式の I/O モジュール (IOM) を収容できます。

これらの IOM は A、B、C の 3 つのグループに分類されます。各グループには、スロット 1 とスロット 2 があります。スロットには、シャーシの背面に左から右へ A1 | B1 | C1 | C2 | B2 | A2 と文字が割り当てられています。各サーバーは IOM に接続するためのメザニカード (MC) 用スロットを 2 つ持ちます。各 MC とそれに対応する IOM は同じファブリックでなければなりません。

シャーシの IO は文字 A、B、C により 3 つの個別のデータバスに分割されます。これらのバスは「ファブリック」と呼ばれ、Ethernet、ファイバチャネルまたは InfiniBand をサポートします。これらの個別のファブリックバスは、2 つの「バンク」、すなわち、バンク 1 とバンク 2 に分割されます。各サーバー IO アダプタ (メザニカードまたは LOM) は、機能に応じて 2 つまたは 4 つのポートを備えています。これらのポートは、冗長性を設定するために IOM バンクの 1 と 2 に均等に分割されます。Ethernet、iSCSI またはファイバチャネルネットワークを導入する場合、可用性を最大限にするために、バンク 1 と 2 を使用して冗長性を確保します。個々の IOM をファブリック識別子とバンク数で表します。

例：「A1」はバンク「1」のファブリック「A」を表します。「C2」はバンク「2」のファブリック「C」を表します。

シャーシは 3 つのファブリックまたはプロトコルタイプをサポートします。グループ内の IOM および メザニカードは、同一または互換性のあるファブリックタイプでなければなりません。

- **グループ A IOMS** は常にサーバーのオンボードイーサネットアダプタに接続されています。グループ A のファブリックタイプは常にイーサネットです。
- **グループ B** については、IOM スロットは各サーバーモジュールの**最初の MC (メザニカード)** スロットに永久的に接続されています。
- **グループ C** については、IOM スロットは各サーバーモジュールの**2 つめの MC (メザニカード)** に永久的に接続されています。



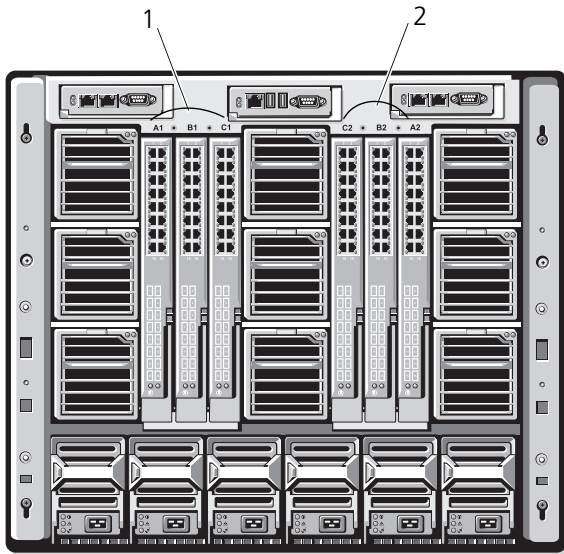
**メモ** : CMC CLI では、IOM は慣習的に switch-*n* と命名されます (A1=switch-1、A2=switch-2、B1=switch-3、B2=switch-4、C1=switch-5)。

## ファブリック管理

ファブリック管理は、シャーシの確立されているファブリックタイプと互換性のないファブリックタイプを持つ IOM および MC の取り付けにより発生する電氣的、構成上、または接続性の問題を回避するのに役立ちます。無効なハードウェア構成は、シャーシまたはそのコンポーネントに電氣的または機能上の問題を引き起こす可能性があります。ファブリック管理により、無効な構成への電源投入が防止されます。

図 11-1 は、シャーシ内の IOM の位置を表示します。各 IOM の場所は、グループ番号 (A、B または C) で示されます。これら個々のファブリックパスは、2 つの IO バンク、バンク 1 と 2 に分割されます。シャーシ上で、IOM スロット名は A1、A2、B1、B2、C1、C2 とマークされています。

図 11-1. IOM の位置を示すシャーシの背面図



- 1   バンク 1 (スロット A1、B1、C1)   2   バンク 2 (スロット A2、B2、C2)



CMC は、無効なハードウェア構成に関するエントリを、ハードウェアログと CMC ログの両方に作成します。

たとえば、次のとおりです。

- ファイバチャンネル IOM に接続された Ethernet MC は無効な構成です。ただし、同じ IOM グループに取り付けられた Ethernet スイッチおよび Ethernet パススルー IOM に接続された Ethernet MC は有効な構成です。
- スロット B1 と B2 にファイバチャンネルパススルー IOM とファイバチャンネルスイッチ IOM を実装した構成は、各サーバー上の最初の MC もファイバチャンネルである場合は有効です。この場合、CMC は IOM とサーバーに電源を投入します。ただし、特定のファイバチャンネル冗長性ソフトウェアはこの構成に対応していないものもあり、すべての有効な構成が対応する構成であるとは限りません。



**メモ:** サーバー IOM と MC のファブリック検証は、シャーシの電源がオンのときにのみ実行されます。シャーシがスタンバイ電源で稼働している場合、サーバーモジュール上の iDRAC の電源は切れたままであるため、サーバーの MC ファブリックタイプを報告できません。MC ファブリックタイプは、サーバー上の iDRAC に電源が投入されるまでは、CMC に報告されません。さらに、シャーシの電源がオンのときは、ファブリック検証はサーバーまたは IOM が挿入される時実行されます (オプション)。ファブリックの不一致が検出された場合、サーバーまたは IOM は電源がオンとなり、ステータス LED は **橙色** に点滅します。

## 無効な構成

無効な構成には、3 種類あります。

- 無効な MC または LOM 構成：新しく取り付けられたサーバーのファブリックタイプが既存の IOM ファブリックと異なる場合
- 無効な IOM-MC 構成：新しく取り付けられた IOM のファブリックタイプと冗長 MC のファブリックタイプが異なるかまたは互換性がない場合
- 無効な IOM-IOM 構成：新しく取り付けられた IOM とグループ内の既存の IOM のファブリックタイプが異なるか互換性がない場合

### 無効なメザニンカード (MC) 構成

1 台のサーバーの LOM または MC がそれに対応する IOM でサポートされていない場合に、MC 構成は無効になります。この場合、MC カードと一致しないサーバーは電源を入れることができませんが、シャーシ内の他のサーバーはすべて稼働可能です。サーバーの電源ボタンが橙色に点滅し、ファブリックの不一致を警告します。CMC ログおよびハードウェアログの詳細については、388 ページの「イベントログの表示」を参照してください。

## 無効な IOM- メザニンカード (MC) 構成

不一致の IOM は電源オフ状態のままとなります。CMC は、CMC ログ とハードウェアログ にエントリを追加して、無効な構成および IOM 名を記録します。CMC は無効の原因となっている IOM のエラー LED も点滅させます。CMC がアラートを送信する設定になっている場合は、このイベントに関する E-メールまたは SNMP アラートを送信します。CMC ログ およびハードウェアログの詳細については、388 ページの「イベントログの表示」を参照してください。

## 無効な IOM-IOM 構成

CMC は、新しく取り付けられた IOM を電源オフの状態で保持し、IOM のエラー LED を点滅させ、不一致に関するエントリを CMC ログとハードウェアログに作成します。CMC ログおよびハードウェアログの詳細については、388 ページの「イベントログの表示」を参照してください。

## 初期電源投入シナリオ

シャーシをプラグインして電源を入れるとき、I/O モジュールがサーバーに優先されます。各グループの最初の IOM は他の IOM より先に電源投入できます。このとき、ファブリックタイプの検証は行われません。グループの最初のスロットに IOM がない場合は、そのグループの 2 番目のモジュールに電源が投入されます。両方のスロットに IOM がある場合は、2 番目のスロットにあるモジュールは最初のスロットにあるモジュールとファブリックタイプが比較されます。

IOM に電源が投入された後、サーバーに電源が投入され、CMC はサーバーのファブリックタイプの整合性を検証します。

ファブリックが同じである限り、パススルーとスイッチを同じグループに共存させることができます。スイッチとパススルーモジュールは、異なるベンダー製でも同じグループに入れることができます。

## IOM 状態の監視

IOM の状態ステータスは、2 つの方法で確認することができます。1 つは **シャーシステータス** ページの **シャーシグラフィックス** セクション、もう 1 つは **I/O モジュールステータス** ページです。**シャーシグラフィックス** ページには、シャーシに取り付けられた IOM の図が表示されます。

シャーシグラフィックスを使用して IOM の正常性ステータスを閲覧するには

- 1 CMC ウェブインタフェースにログインします。
- 2 **シャーシステータス** ページが表示されます。**シャーシグラフィックス** の右側のセクションは、シャーシの背面図を表し、IOM の状態ステータスが含まれます。IOM の状態ステータスは、IOM のサブグラフィックの色で示されます。
  - 緑色 - IOM が存在し、電源がオンで CMC と通信中。悪条件の兆候はなし。

- 橙色 - IOM が存在するが、電源がオンまたはオフである場合がある、または CMC と通信中または通信していない場合がある。悪条件が存在する可能性あり。
  - 灰色 - IOM が存在するが、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
- 3 特定の IOM サブグラフィック上にカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、IOM に関する追加情報を提供します。
  - 4 IOM サブグラフィックは、該当する CMC GUI ページにハイパーリンク付けられ、対象の IOM と関連付けられた **I/O モジュールステータス** ページに瞬時に移動することができます。

**I/O モジュールステータス** ページを使用してすべての IOM の状態ステータスを閲覧するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーの **シャーシ** メニューで、**I/O モジュール** を選択します。
- 3 **プロパティ** タブをクリックします。
- 4 **ステータス** サブタブをクリックします。**I/O モジュールステータス** ページが表示されます。

表 11-1. I/O モジュールの情報



項目	説明	
スロット	シャーシ内の I/O モジュールの位置をグループ番号（A、B、C）とバンク（1 または 2）で示します。IOM 列挙： <b>A1、A2、B1、B2、C1</b> または <b>C2</b> 。	
存在	IOM が存在するかどうかを示します（はい または いいえ）。	
状態	 OK	IOM が存在し、CMC と通信を行っていることを示します。CMC とサーバー間で通信エラーが発生した場合は、CMC はサーバーの状態ステータスを取得または表示できません。
	 情報	状態ステータス（OK、警告、重要）に変化がない場合に IOM についての情報を表示します。
	 警告	警告アラートが発行されたこと、および <b>対応処置を取る</b> 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、IOM の健全性に影響するような重要または重大なエラーを引き起こす可能性があります。  警告が出される状態の例：IOM ファブリックとサーバーのメザニンカードファブリックが不一致、無効な IOM 構成、新しく取り付けた IOM と同じグループの既存の IOM との不一致
	 重要	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。重要な状態は IOM のシステムエラーを示し、 <b>直ちに対応処置を取る必要があります</b> 。  重要な状態を引き起こす状態の例：IOM にエラーが検出された場合、IOM が取り外された場合
	<b>メモ</b> ：状態に変化があれば、ハードウェアと CMC ログの両方に記録されます。詳細については、388 ページの「イベントログの表示」を参照してください。	
ファブリック	IOM のファブリックタイプを示します（ギガビット Ethernet、10GE XAUI、10GE KR、10GE XAUI KR、FC 4 Gbps、FC 8 Gbps、SAS 3 Gbps、SAS 6 Gbps、Infiniband SDR、Infiniband DDR、Infiniband QDR、PCIe バイパス Generation 1、PCIe バイパス Generation 2）。 <b>メモ</b> ：シャーシに搭載された IOM のファブリックタイプがわかっていると、同じグループ内で IOM の不一致が発生するのを防ぐのに効果的です。I/O ファブリックの詳細については、353 ページの「I/O ファブリック管理」を参照してください。	
名前	IOM 製品名が表示されます。	

表 11-1. I/O モジュールの情報（続き）

項目	説明
IOM 管理コンソールの起動	<p>特定の I/O モジュールを示すアイコンが存在する場合は、アイコンをクリックして新しいブラウザ ウィンドウまたはタブで IOM 管理コンソールを起動します。</p> <p><b>メモ：</b>このオプションは、管理されているスイッチ I/O モジュールに対してのみ利用可能です。パススルー I/O モジュールまたは管理されていない Infiniband スイッチには使えません。</p> <p><b>メモ：</b>I/O モジュールの電源がオフのためアクセスできない、その LAN インタフェースが無効である、またはモジュールが有効な IP アドレスに割当てられていない場合は、IOM GUI の起動オプションはその I/O モジュールに表示されません。</p> <p><b>メモ：</b>その場合は、I/O モジュールの管理インタフェースにログインするように求められます。</p> <p><b>メモ：</b>361 ページの「個別 IOM のネットワーク設定」の説明に従って、CMC GUI で I/O モジュールの IP アドレスを設定することができます。</p>
役割	<p>I/O モジュール同士がリンク付けされると、役割は I/O モジュールスタックメンバーを表示します。<b>メンバー</b> とは、モジュールはスタックセットの一部です。<b>マスター</b> とは、モジュールはプライマリアクセスポイントです。</p>
電源ステータス	<p>IOM の電源状態：<b>オン</b>、<b>オフ</b>、<b>該当なし</b>（不在）を示します。</p>
サービスタグ	<p>IOM のサービスタグを表示します。サービス タグはサポートおよびメンテナンス用に Dell が提供する固有の識別子です。</p> <p>状態に変化があれば、ハードウェアと CMC ログの両方に記録されます。詳細については、388 ページの「イベントログの表示」を参照してください。</p> <p><b>メモ：</b>パススルーには、サービスタグがありません。サービスタグがあるのは、スイッチだけです。</p>





## 個別の IOM の状態ステータスの表示

I/O モジュールステータス ページ (I/O モジュールステータス ページとは別) に、個々の IOM の概要が表示されます。

個々の IOM の状態ステータスを表示するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **I/O モジュール** を展開します。すべての IOM (1 ~ 6) が展開された **I/O モジュール** リストに表示されます。
- 3 システムツリーの **I/O モジュール** リストで表示したい IOM をクリックします。
- 4 **ステータス** サブタブをクリックします。**I/O モジュールステータス** ページが表示されます。

表 11-2. I/O モジュール状態ステータスの情報

項目	説明	
場所	シャーシ内の IOM の場所をグループ番号 (A、B、C) とスロット番号 (1 または 2) で示します。スロット名: <b>A1、A2、B1、B2、C1、C2</b>	
名前	IOM の名前が表示されます。	
存在	IOM が <b>存在</b> または <b>不在</b> を示します。	
状態	 OK	IOM が存在し、CMC と通信を行っていることを示します。CMC とサーバー間で通信エラーが発生した場合は、CMC はサーバーの状態ステータスを取得または表示できません。
	 情報	状態ステータス (OK、警告、重要) に変化がない場合に IOM についての情報を表示します。 情報ステータスを引き起こす状態の例: IOM の存在が検出された場合、ユーザーが IOM のパワーサイクルを要求した場合
	 警告	警告アラートが発行されたこと、および <b>対応処置を取る</b> 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、IOM の健全性に影響するような重要または重大なエラーを引き起こす可能性があります。 警告が出される状態の例: IOM ファブリックとサーバーのメザニンカードファブリックとの不一致、無効な IOM 構成、新しく取り付けられた IOM と同じグループの既存の IOM との不一致
	 重要	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。重要な状態は IOM のシステムエラーを示し、 <b>直ちに対応処置を取る必要があります</b> 。 重要な状態を引き起こす状態の例: IOM にエラーが検出された場合、IOM が取り外された場合
電源ステータス	IOM の電源状態: <b>オン、オフ、該当なし</b> (不在) を示します。	
サービスタグ	IOM のサービスタグを表示します。サービス タグはサポートおよびメンテナンス用に Dell が提供する固有の識別子です。	

**メモ:** 状態に変化があれば、ハードウェアと CMC ログの両方に記録されます。ログの表示の詳細については、388 ページの「ハードウェアログの表示」および 391 ページの「CMC ログの表示」を参照してください。

表 11-2. I/O モジュール状態ステータスの情報（続き）

項目	説明
ファブリック	<p>IOM のファブリックタイプを示します（ギガビット Ethernet、10GE XAUI、10GE KR、10GE XAUI KR、FC 4 Gbps、FC 8 Gbps、SAS 3 Gbps、SAS 6 Gbps、Infiniband SDR、Infiniband DDR、Infiniband QDR、PCIe バイパス Generation 1、PCIe バイパス Generation 2）。</p> <p><b>メモ：</b>シャーシに搭載された IOM のファブリックタイプがわかっていると、同じグループ内で IOM の不一致が発生するのを防ぐのに効果的です。I/O ファブリックの詳細については、353 ページの「I/O ファブリック管理」を参照してください。</p>
MAC アドレス	<p>IOM の MAC アドレスを表示します。MAC アドレスは識別手段としてハードウェアベンダーによって割り当てられた固有のアドレスです。</p> <p><b>メモ：</b>パススルーには MAC アドレスはありません。MAC アドレスがあるのは、スイッチだけです。</p>
役割	<p>モジュール同士がリンク付けされた場合の I/O モジュールのスタックメンバーシップを表示します。</p> <ul style="list-style-type: none"> <li>• <b>メンバー</b> - モジュールはスタックセットの一部です。</li> <li>• <b>マスター</b> - モジュールはプライマリアクセスポイントです。</li> </ul>

## 個別 IOM のネットワーク設定

I/O モジュールセットアップ ページでは、IOM の管理に使うインタフェースのネットワーク設定を指定できます。イーサネットスイッチの場合、帯域外管理ポート（IP アドレス）が設定されます。帯域内管理ポート（VLAN 1）の場合、このインタフェースを介して設定は行われません。



**メモ：**I/O モジュール構成 ページで設定を変更する際、IOM グループ A を設定するにはファブリック A 管理者権限が必要となり、IOM グループ B の場合はファブリック B 管理者権限、IOM グループ C の場合はファブリック C 管理者権限が必要となります。



**メモ：**イーサネットスイッチの場合、帯域内（VLAN1）および帯域外の管理 IP アドレスが同じであったり、同じネットワーク上にないようにします。同じにすると、帯域外 IP アドレスが設定されなくなります。デフォルトの帯域内管理 IP アドレスについては、IOM 文書を参照してください。



**メモ：**シャーシに存在する IOM のみ、表示されます。



**メモ：**イーサネットパススルー スイッチまたは Infiniband スイッチ用に I/O モジュールのネットワーク設定を行わないでください。

個々の IOM のネットワーク設定を行うには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **I/O モジュール** を展開します。**セットアップ** サブタブをクリックします。**I/O モジュールネットワーク設定** ページが表示されます。
- 3 I/O モジュールのネットワーク設定を行うには、次のプロパティ値を入力または選択して、**適用** をクリックします。



**メモ**：電源を投入できる IOM のみ、設定することが可能です。



**メモ**：CMC で IOM に設定した IP アドレスは、スイッチの永続的なスタートアップ設定に保存されません。IP アドレスの設定を永久的に保存するには、`connect switch -n` コマンドまたは `racadm connect switch -n RACADM` コマンドを入力するか、または IOM GUI への直接インタフェースを使用してこのアドレスをスタートアップ設定ファイルに保存する必要があります。

表 11-3. I/O モジュールのネットワーク設定

項目	説明
スロット	シャーシ内の IOM の場所をグループ番号 (A、B、C) とスロット番号 (1 または 2) で示します。スロット名：A1、A2、B1、B2、C1、C2 (スロット値を変更することはできません。)
名前	IOM 製品名が表示されます。(IOM 名を変更することはできません。)
電源状態	IOM の電源状況が表示されます。(このページから電源状況を変更することはできません。)
DHCP の有効	シャーシ上の IOM が動的ホスト構成プロトコル (DHCP) サーバーに自動的に IP アドレスを要求して取得できるようになります。 デフォルト：オン (有効) このオプションがオンの場合、IOM は IP 設定 (IP アドレス、サブネットマスク、ゲートウェイ) をネットワーク上の DHCP サーバーから自動的に取得します。 <b>メモ</b> ：この機能が有効な場合、IP アドレス、ゲートウェイおよびサブネットマスクのプロパティフィールド (このオプションのすぐ隣に位置する) は無効になり、過去に入力されたプロパティ値は無視されます。 このオプションがオフの場合、このオプションのすぐ隣の該当するテキストフィールドに、有効な IP アドレス、ゲートウェイおよびサブネットマスクを手動で入力する必要があります。
IP アドレス	IOM ネットワークインタフェースの IP アドレスを指定します。
サブネットマスク	IOM ネットワークインタフェースの サブネットマスクを指定します。
ゲートウェイ	IOM ネットワークインタフェースの ゲートウェイを指定します。



## IOM ネットワーク設定のトラブルシューティング

次のリストでは、IOM ネットワーク設定のトラブルシューティングを行う際の項目が含まれます。

- CMC は IP アドレスの設定変更後、早すぎる時期にアドレスを読み込んでしまう場合があります、**適用** をクリックすると **0.0.0.0** が表示されます。スイッチに正しい IP アドレスが設定されているか確認するには、更新ボタンをクリックします。
- IP/ マスク / ゲートウェイの設定にエラーがあった場合、スイッチは IP アドレスを設定せず、すべてのフィールドに **0.0.0.0** が表示されます。  
一般的なエラーには、次が含まれます。
  - 帯域外 IP アドレスを帯域内管理 IP アドレスと同じ IP アドレス、または同じネットワーク上のアドレスに設定。
  - 無効なサブネットマスクの入力。
  - スイッチに直接接続しているネットワーク以外のアドレスにデフォルトゲートウェイを設定。

IOM ネットワーク設定の詳細については、『Dell PowerConnect M6220 Switch Important Information』（Dell PowerConnect M6220 の重要な情報）マニュアル、および『Dell PowerConnect 6220 Series Port Aggregator ホワイトペーパー』を参照してください。



# トラブルシューティングとリカバリ

## 概要

本項では、リモートシステムで問題が発生した場合に CMC ウェブインタフェースを使って行うリカバリとトラブルシューティングに関連したタスクの実行方法について説明します。

- 設定情報、エラーステータス、エラーログの収集。
- リモートシステムの電源管理。
- リモートシステムの Lifecycle Controller ジョブの管理。
- シャーシ情報の表示。
- イベントログの表示。
- 診断コンソールの使用。
- コンポーネントのリセット。
- ネットワークタイムプロトコル (NTP) 問題に関するトラブルシューティング。
- ネットワーク問題に関するトラブルシューティング。
- アラート問題に関するトラブルシューティング。
- システム管理者パスワードを忘れた場合のリセット。
- シャーシ構成設定および資格情報の保存と復元。
- エラーコードおよびログ。

# シャーシ監視ツール

## 設定情報、シャーシステータス、ログの収集

**racdump** サブコマンドは、全般的なシャーシステータス、設定状況情報、イベントログの履歴を収集するコマンドを提供します。

## 使用状況

```
racadm racdump
```

**racdump** サブコマンドは、次の情報を表示します。

- システム / RAC の一般情報
- CMC 情報
- シャーシの情報
- セッション情報
- センサー情報
- ファームウェアビルド情報

## 対応インタフェース

- CLI RACADM
- リモート RACADM
- Telnet RACADM

**RACDUMP** コマンドは、シリアル、Telnet、SSH コンソールのコマンド プロンプト、または通常のコマンドプロンプトからリモートで実行できます。

**RACDUMP** サブコマンドの構文とコマンドラインオプションを表示するには、次のように入力します。

```
racadm help <racdump>
```

## CLI RACDUMP

Racdump には、次のサブシステムが含まれ、次の RACADM コマンドを集約します。

表 12-1. サブシステムと RACADM コマンド

サブシステム	RACADM コマンド
システム / RAC の一般情報	getsysinfo
セッション情報	getssinfo
センサー情報	getsensorinfo
スイッチ情報 (IO モジュール)	getioinfo
メザニンカード情報 (ドーターカード)	getdcinfo
すべてのモジュール情報	getmodinfo
電力バジェット情報	getpbinfo
KVM 情報	getkvminfo
NIC 情報 (CMC モジュール)	getniccfg
冗長性情報	getredundancymode
トレースログ情報	gettracelog
RAC イベントログ	gettraclog
システムイベントログ	getsel

### 使用状況

```
racadm racdump
```

## リモート RACDUMP

リモート RACADM はクライアント側のユーティリティで、管理ステーションから帯域外ネットワークインタフェースを使用して実行できます。リモート機能のオプション **-r** 使用すると、管理下システムに接続して、リモートコンソールまたは管理ステーションから RACADM サブコマンドを実行できます。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 CMC の IP アドレスが必要です。



**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 <file name>
- racadm sslcertdownload -t <type> [-f <filename>]
```

## リモート RACDUMP の使用

RACDUMP サブコマンドをリモートで使用するには、次のコマンドを入力します。

```
racadm -r <CMC IP address> -u <username> -p <password>
<subcommand> <subcommand options>
racadm -i -r <CMC IP address> <subcommand> <subcommand
options>
```



**メモ:** **-i** オプションは、RACADM にユーザー名とパスワードの入力をインタラクティブにプロンプトするよう指示します。**-i** オプションを指定しない場合は、コマンドラインで **-u** と **-p** オプションを使ってユーザー名とパスワードを指定する必要があります。

たとえば、次のとおりです。

```
racadm -r 192.168.0.120 -u root -p calvin racdump
racadm -i -r 192.168.0.120 racdump
```

CMC 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、次の構文を使用する必要があります。

```
racadm -r <CMC IP address>:<port> -u <username> -p
<password> <subcommand> <subcommand options>
racadm -i -r <CMC IP address>:<port> <subcommand>
<subcommand options>
```

## Telnet RACDUMP

SSH/Telnet RACDUMP は、SSH または Telnet プロンプトから RACDUMP コマンドの使用状況を参照するために使用されます。

RACDUMP の使い方の詳細については、[support.dell.com/manuals](https://support.dell.com/manuals) にある『RACADM Command Line Reference Guide for iDRAC and CMC』（iDRAC6 および CMC 用 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。

### シャーシ上のコンポーネントを識別するための LED の設定

すべてのまたは個別のコンポーネント（シャーシ、サーバー、IOM）のコンポーネント LED を点滅させてシャーシ上のコンポーネントを識別することができます。



**メモ：**これらの設定を変更するには **シャーシ設定システム管理者** の権限が必要です。

### ウェブインタフェースの使用

1 つ、複数、またはすべてのコンポーネント LED を点滅させるには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** をクリックします。
- 3 **トラブルシューティング** タブをクリックします。
- 4 **識別** サブタブをクリックします。**識別** ページが開いて、シャーシ上のすべてのコンポーネントの一覧が表示されます。
- 5 特定のコンポーネント LED の点滅を有効にするには、そのデバイス名の横のボックスを選択し、**点滅** をクリックします。
- 6 特定のコンポーネント LED の点滅を無効にするには、そのデバイス名の横のボックスを選択し、**点滅解除** をクリックします。

### RACADM の使用

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm settled -m <module> [-l <ledState>]
```

ここで、<module> は LED の設定を行うモジュールを指定します。設定オプション：

- server-*n* (*n*=1 ~ 16)
- switch-*n* (*n*=1 ~ 6)
- cmc-active

および <ledState> は LED を点滅させるかどうかを指定します。設定オプション：

- 0 — 点滅なし（デフォルト）

- 1 — 点滅

## SNMP アラートの設定

シンプル ネットワーク 管理プロトコル (SNMP) トラップまたは イベントトラップは、E-メール イベントアラートと似ています。CMC からの未承諾データを受信するために、管理ステーションによって使用されます。

イベントトラップを生成するように CMC を設定することが可能です。表 12-2 は、SNMP および E-メールアラートをトリガーするイベントの概要を提供します。E-メールアラートの詳細は、375 ページの「E-メール警告の設定」を参照してください。



**メモ:** CMC バージョン 2.10 以降、SNMP では IPv6 を使用できるようになりました。イベントアラートの宛先として IPv6 アドレスまたは完全修飾されたドメイン名 (FQDN) を入力できます。

表 12-2. SNMP や E-メール警告を生成するシャードイベント

イベント	説明
ファンロープエラー	ファンの稼働速度が遅すぎるか、稼働していません。
バッテリーロープ警告	バッテリーが機能停止しました。
温度プロープ警告	温度が高温、低温の限界に近づいています。
温度プロープエラー	温度が高すぎるか低すぎて適切な操作が行えません。
冗長性低下	ファンおよび / または電源装置の冗長性が少なくなりました。
冗長性喪失	ファンまたは電源装置に冗長性がありません。
電源装置警告	電源装置がエラー状態に近づいています。
電源装置エラー	電源装置が故障しました。
電源装置の不在	あるはずの電源装置がありません。
ハードウェアログエラー	ハードウェアのログが機能していません。
ハードウェアログ警告	ハードウェアログがほとんど一杯です。
サーバーの不在	存在するはずのサーバーがありません。
サーバーエラー	サーバーが機能していません。
KVM の不在	存在するはずの KVM がありません。
KVM エラー	KVM が機能していません。
IOM の不在	存在するはずの IOM がありません。
IOM エラー	IOM が機能していません。



表 12-2. SNMP や E-メール警告を生成するシャージイベント (続き)

イベント	説明
ファームウェアバージョンの不一致	シャージまたはサーバーのファームウェアが一致していません。
シャージ電力しきい値エラー	シャージ内の電力消費量がシステム入力電力上限を超えました。
SDCARD 不在	CMC SD カードスロットにメディアが挿入されていませんが、設定されている CMC 機能ではセキュアデジタル (SD) カードが必要です。
SDCARD エラー	CMC のセキュアデジタル (SD) カードスロット内のメディアへのアクセス中に、エラーが発生しました。
シャージグループエラー	シャージグループに設定エラーがあります。

ウェブインタフェースまたは RACADM を使って SNMP アラートを追加、設定できます。

#### ウェブインタフェースの使用



**メモ:** SNMP アラートを追加または設定するには、**シャージ設定システム管理者**の権限が必要となります。



**メモ:** セキュリティを強化するために、ルート (ユーザー 1) アカウントのデフォルトパスワードを変更することを強くお勧めします。ルートアカウントは、CMC 出荷時のデフォルトの管理者アカウントです。ルートアカウントのデフォルトパスワードを変更するには、ユーザー ID 1 をクリックして **ユーザー設定** ページを開きます。そのページのヘルプには、ページの右上にある **ヘルプ** リンクからアクセスできます。

CMC ウェブインタフェースを使って SNMP アラートを追加、設定するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャージ** を選択します。
- 3 **アラート** タブをクリックします。**シャージイベント** ページが表示されます。
- 4 アラートの有効化:
  - a アラートを有効にするイベントのチェックボックスを選択します。すべてのイベントのアラートを有効にするには、**すべて選択** チェックボックスを選択します。
  - b **適用** をクリックして設定を保存します。
- 5 **トラップ設定** サブタブをクリックします。**シャージイベントアラート送信先** ページが表示されます。

- 6 空の **送信先** フィールドに有効なアドレスを入力します。



**メモ**：有効なアドレスとは、トラップアラートを受信するアドレスを指します。「ドットで 4 つに区切られた」IPv4 フォーマット、標準 IPv6 アドレス表記、または FQDN を使用します。例：123.123.123.123、2001:db8:85a3::8a2e:370:7334、dell.com

- 7 送信先管理ステーションが属する **SNMP コミュニティ文字列** を入力します。



**メモ**：**シャーシイベントアラート送信先** ページのコミュニティ文字列は、**シャーシ** → **ネットワーク** → **サービス** ページのコミュニティ文字列とは異なります。SNMP トラップのコミュニティ文字列は、CMC が管理ステーション宛の送信トラップに使用するものです。**シャーシ** → **ネットワーク** → **サービス** ページのコミュニティ文字列は、管理ステーションが CMC の SNMP データベースにクエリを行うために使用します。

- 8 **Apply** (適用) をクリックして変更を保存します。

アラート送信先へのイベントトラップをテストするには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** を選択します。
- 3 **アラート** タブをクリックします。**シャーシイベント** ページが表示されます。
- 4 **トラップ設定** タブをクリックします。**シャーシイベントアラート送信先** ページが表示されます。
- 5 送信先の隣にある **テストトラップ** 行の **送信** をクリックします。



**メモ**：トラップ送信先は適切にフォーマットされた数値アドレス (IPv6 または IPv4)、または完全修飾されたドメイン名 (FQDN) で指定できます。お使いのネットワーク技術 / インフラストラクチャと一貫性のあるフォーマットを選択します。**テストトラップ** 機能では、現在のネットワーク設定に不適切な選択項目は検出されません (IPv4 専用の環境で IPv6 送信先を使用する場合など)。

## RACADM の使用

- 1 シリアル / Telnet / SSH テキストコンソールを開いて CMC に進み、ログインします。



**メモ**：SNMP と E-メールアラートの両方に設定できるフィルタマスクは 1 つだけです。既にフィルタマスクを選択している場合は、手順 2 をスキップできます。

- 2 アラートを有効にするには、次を入力します。

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

### 3 CMC に生成させたいイベントを指定するには、次を入力します。

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask  
<mask value>
```

ここで、<mask value> は 0x0 ~ 0xffffffff の 16 進値です。

マスク値を得るには、科学計算用電卓を 16 進モードで使い、<OR> キーで各マスクの第 2 値 (1、2、4、...) を追加します。

たとえば、バッテリープローブ警告 (0x2)、電源装置エラー (0x1000)、KVM エラー (0x80000) 用トラップ警告を有効にするには、2 <OR> 1000 <OR> 200000 を入力して <=> キーを押します。

結果の 16 進値は 208002 で、RACADM コマンドのマスク値は 0x208002 です。

表 12-3. イベントトラップのフィルタマスク

イベント	フィルタマスク値
ファンプローブエラー	0x1
バッテリープローブ警告	0x2
温度プローブ警告	0x8
温度プローブエラー	0x10
冗長性低下	0x40
冗長性喪失	0x80
電源装置警告	0x800
電源装置エラー	0x1000
電源装置の不在	0x2000
ハードウェアログエラー	0x4000
ハードウェアログ警告	0x8000
サーバーの不在	0x10000
サーバーエラー	0x20000
KVM の不在	0x40000
KVM エラー	0x80000
IOM の不在	0x100000
IOM エラー	0x200000
ファームウェアバージョンの不一致	0x400000
シャーシ電力しきい値エラー	0x1000000

表 12-3. イベントトラップのフィルタマスク (続き)

イベント	フィルタマスク値
SDCARD 不在	0x2000000
SDCARD エラー	0x4000000
シャーシグループエラー	0x8000000

- 4 トラップアラートを有効にするには、次を入力します。

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
```

ここで、<index> は 1～4 の値です。インデックス番号は、トラップアラート用の設定可能送信先を最大 4 つ識別するために CMC が使用するものです。送信先は適切にフォーマットされた数値アドレス (IPv6 または IPv4)、または完全修飾されたドメイン名 (FQDN) で指定できます。

- 5 トラップアラートの送信先 IP アドレスを指定するには、次を入力します。

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr  
<IP address> -i <index>
```

ここで、<IP address> は有効な IP アドレスで、<index> は手順 4 で指定したインデックス値です。

- 6 コミュニティ名を指定するには、次を入力します。

```
racadm config -g cfgTraps -o cfgTrapsCommunityName  
<community name> -i <index>
```

ここで <community name> はシャーシが属する SNMP コミュニティの名前で、<index> は手順 4 および 5 で指定したインデックス値です。

トラップアラートの送信先 IP アドレスを 4 つまで設定できます。送信先をさらに追加するには、手順 2～6 を繰り返します。



**メモ:** 手順 2～6 のコマンドは、指定するインデックス (1～4) の既存の設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、**racadm getconfig -g cfgTraps -i <インデックス>** を入力します。インデックスが設定されていると、その値が **cfgTrapsAlertDestIPAddr** と **cfgTrapsCommunityName** オブジェクトに表示されます。

アラート送信先へのイベントトラップをテストするには、次を入力します：

```
racadm testtrap -i <index>
```

ここで、<index> は 1～4 の値で、テストするアラート送信先を表します。インデックス番号がわからない場合は、次を入力します。

```
racadm getconfig -g cfgTraps -i <index>
```

## SNMP Management Information Base (MIB) ファイルのダウンロード

CMC SNMP MIB ファイルは、シャーシタイプ、イベント、およびインジケータを定義します。

CMC では、ウェブインタフェースを使用して MIB ファイルをダウンロードできます。

ウェブインタフェースを使用して CMC の SNMP Management Information Base (MIB) ファイルをダウンロードするには、次の手順を実行します。

- 1 **CMC ウェブインタフェース** にログインします。
- 2 システムツリーで **シャーシ** を選択します。
- 3 **ネットワーク** → **サービス** → **SNMP** をクリックします。  
**SNMP 設定** の項が表示されます。
- 4 **保存** をクリックして CMC MIB ファイルをローカルシステムにダウンロードします。

SNMP MIB ファイルの詳細については、[support.dell.com/manuals](https://support.dell.com/manuals) にある『Dell OpenManage Server Administrator SNMP Reference Guide』（Dell OpenManage Server Administrator SNMP リファレンスガイド）を参照してください。

## E- メール警告の設定

CMC が環境についての警告やコンポーネント障害などのシャーシイベントを検出した場合、1 つ、または複数の E- メールアドレスに E- メール警告を送信するように設定できます。

表 12-2 は、SNMP および E- メール警告をトリガーするイベントの概要を提供します。E- メール警告の詳細については、370 ページの「SNMP アラートの設定」を参照してください。

ウェブインタフェースまたは RACADM を使って SNMP アラートを追加および設定できます。


### ウェブインタフェースの使用



**メモ**：E- メール警告を追加または設定するには、**シャーシ設定管理者** の権限が必要です。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** を選択します。
- 3 **アラート** タブをクリックします。**シャーシイベント** ページが表示されます。

- 4 アラートの有効化：
  - a アラートを有効にするイベントのチェックボックスを選択します。すべてのイベントのアラートを有効にするには、**すべて選択** チェックボックスを選択します。
  - b **適用** をクリックして設定を保存します。
- 5 **E-メールアラート設定** サブタブをクリックします。**E-メールアラートの送信先** ページが表示されます。
- 6 SMTP サーバー IP アドレスを指定します。
  - a **SMTP (E-メール) サーバー** フィールドを見つけて、SMTP ホスト名または IP アドレスを入力します。

 **メモ**：CMC の IP アドレスから送信された E-メールを受け入れるように SMTP E-メールサーバーを設定する必要があります。この機能は通常、セキュリティ上、ほとんどのメールサーバーでオフになっています。この設定をセキユアに行う手順は、SMTP サーバーのマニュアルを参照してください。
  - b アラートを発信する送信元 E-メールアドレスを入力します。デフォルトの送信元 E-メールアドレスを使用する場合は、空白のままにします。デフォルトのアドレスは、`cmc@<IP アドレス>` です。ここで、`<IP アドレス>` は、CMC の IP アドレスを指します。値を入力する場合は、E-メール名の構文は、`<E-メール名>[<@ドメイン>]` です。E-メールアドレスは、オプションで指定することができます。

`@<ドメイン>` が指定されず、かつアクティブな CMC ネットワークドメインが存在する場合、送信元 E-メールアドレスとして `<E-メール名> @<cmc.ドメイン>` が使用されます。`@<ドメイン>` が指定されず、かつアクティブなネットワークドメインが CMC に存在しない場合、CMC の IP アドレスが使用されます（例：`<E-メール名>@<IP アドレス>`）。
  - c **適用** をクリックして変更を保存します。
- 7 アラートを受け取る E-メールアドレスを指定します。
  - a 空白の **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。
  - b オプションで **名前** も入力できます。この名前は、E-メールを受信するエンティティとなります。無効な E-メールアドレスに入力された名前は、無視されます。
  - c **適用** をクリックして設定を保存します。

CMC ウェブインタフェースを使用して、テスト E- メールをアラートの送信先 E- メールアドレスに送信するには、次の手順を実行します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** を選択します。
- 3 **アラート** タブをクリックします。**シャーシイベント** ページが表示されます。
- 4 **E- メールアラート設定** サブタブをクリックします。**E- メールアラートの送信先** ページが表示されます。
- 5 送信先の隣にある **送信先 E- メールアドレス** 行の **送信** をクリックします。

### RACADM の使用

RACADM を使用して、テスト E- メールをアラートの送信先 E- メールアドレスに送信するには、次の手順を実行します。

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
- 2 アラートを有効にするには、次を入力します。

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```



**メモ:** SNMP と E- メールアラートの両方に設定できるフィルタマスクは 1 つだけです。既にフィルタマスクを選択している場合は、手順 3 をスキップできます。

- 3 CMC に生成させたいイベントを指定するには、次を入力します。

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask  
<mask value>
```

ここで、<mask value> は 0x0 ~ 0xffffffff の 16 進数値で、0x で始まる形式である必要があります。表 12-3 は、各イベントタイプのフィルタマスクを提供します。有効にするフィルタマスクの 16 進値の計算方法は、372 ページの「RACADM の使用」の手順 3 を参照してください。

- 4 E- メールアラートを有効にするには、次を入力します。

```
racadm config -g cfgEmailAlert -o  
cfgEmailAlertEnable 1 -i <index>
```

ここで、<index> は 1 ~ 4 の値です。インデックス番号は、設定可能送信先 E- メールアドレスを最大 4 つ識別するために CMC が使用するものです。

- 5 E- メールアラートを受け取る送信先 E- メールアドレスを指定するには、次を入力します。

```
racadm config -g cfgEmailAlert -o  
cfgEmailAlertAddress <email address> -i <index>
```

ここで、<email address> は有効な E- メールアドレスで、<index> は手順 4 で指定したインデックス値です。

- 6 E- メールアラートの受信者の名前を指定するには、次を入力します。

```
racadm config -g cfgEmailAlert -o  
cfgEmailAlertEmailName <email name> -i <index>
```

ここで、<email name> は、E- メールアラートを受信する人またはグループの名前で、<index> は手順 手順 4 と 手順 5 で指定したインデックス値です。E- メール名は、32 文字以内の英数字、ハイフン、下線、ピリオドで指定します。スペースは使用できません。

- 7 `cfgRhostsSmtplibServerIpAddr` データベース プロパティを設定して SMTP ホストを設定するには、次を入力します。

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSmtplibServerIpAddr host.domain
```

ここで、`host.domain` は、正式なドメイン名です。

E- メールアラートを受け取る送信先 E- メールアドレスは、最大 4 件設定できます。さらに E- メールアドレスを追加するには、手順 6 ~ 手順 2 を繰り返します。



**メモ:** 手順 2 ~ 6 のコマンドは、指定するインデックス (1 ~ 4) の既存の設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、**racadm getconfig -g cfgEmailAlert -i <インデックス>** を入力します。インデックスが設定されていると、その値が **cfgEmailAlertAddress** と **cfgEmailAlertEmailName** オブジェクトに表示されます。

## リモートシステムのトラブルシューティングの最初の手順

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？



## シャーシ上の電源監視と電源制御コマンドの実行

ウェブインタフェースまたは RACADM を使用して、次を行うことができます。

- システムの現在の電源状態の表示。
- 再起動するとき、オペレーティングシステムから正常なシャットダウンを実行して、システムをオンまたはオフにします。

CMC における電源管理、および電力バジェット、冗長性、電源制御の設定の詳細は、285 ページの「電力管理」を参照してください。

### 電力バジェット状態の表示

ウェブインタフェースまたは RACADM を使ってシャーシ、サーバー、PSU の電力バジェット状態を表示する方法は、306 ページの「消費電力ステータスの表示」を参照してください。

### 電源制御操作の実行

CMC ウェブインタフェースまたは RACADM を使ってシステムの電源オン、電源オフ、リセットまたは電源サイクルを行う手順は、320 ページの「シャーシに対する電力制御操作の実行」、322 ページの「IOM 上で電源制御操作の実行」および 323 ページの「サーバーに対する電力制御操作の実行」を参照してください。

## 電源のトラブルシューティング

電源装置および電源関係の問題のトラブルシューティングには、次の情報が役立ちます。

- **問題：電源の冗長性ポリシー に AC 冗長性 に設定すると、電源装置の冗長性喪失イベントが生じた。**
  - **解決策 A：**この設定では、モジュラエンクロージャ内のサイド 1（左の 3 つのスロット）とサイド 2（右の 3 つのスロット）で電源装置が最低 1 つずつ必要です。さらに、各サイトは、**AC 冗長性** を維持するために、シャーシの総電源割り当てをサポートするのに十分な容量が必要です。（完全な AC 冗長性を実現するには、6 つの電源装置から成る、完全な PSU 構成になっていることを確認します。
  - **解決策 B：**すべての電源装置が 2 つの AC グリッドに正しく接続されていることを確認します。サイド 1 の電源装置は一方の AC グリッドに、サイド 2 の電源装置は他方の AC グリッドに接続し、両方の AC グリッドが機能していることが必要です。AC グリッドのどちらかが機能しない場合、**AC 冗長性** は失われます。

- **問題：**AC コードが接続されており、電力配分装置も AC に電力を送っているのにも関わらず、PSU に **エラー (AC なし)** が表示される。
  - **解決策 A：**AC コードを確認して交換してください。電力配分装置が供給する電力が十分であるかを点検および確認してください。それでも不具合が解消されない場合は、デルのカスタマーサービスに電源装置装置の交換を依頼してください。
  - **解決策 B：**PSU が他の PSU と同じ電圧で接続されていることを確認します。ある PSU が異なる電圧で作動していることを CMC が検出すると、その PSU の電源はオフとなり、障害としてマークされます。
- **問題：**電源装置の動的制御を有効にしても、どの電源装置も **スタンバイ** 状況として表示されない。
  - **解決策 A：**余剰電力が十分ではありません。1 つまたは複数の電源装置がスタンバイ状況に移行するのは、エンクロージャで利用できる余剰電力が、少なくとも 1 つの電源装置の容量を超えた場合に限られます。
  - **解決策 B：**エンクロージャにある電源装置では、動的電源供給機能が完全にサポートされていません。このケースが該当するか確認するには、ウェブインタフェースを使用して動的電源供給機能をオフにしてから、再びオンにします。動的電源供給機能が完全にサポートされない場合は、メッセージが表示されます。
- **問題：**新しいサーバーを十分な電源装置があるエンクロージャに挿入しましたが、電源がオンになりません。
  - **解決策 A：**システムの電源入力設定を確認します。追加サーバーに電源を供給するには低すぎる電源構成になっているかもしれません。
  - **解決策 B：**110V での動作をチェックします。電源装置のいずれかが 110V の分岐回路に接続されている場合、その構成が有効であることを確認するまでは、サーバーの電源をオンにしないでください。詳細については、電源設定を参照してください。
  - **解決策 C：**最大節電設定を参照してください。これが設定されていると、サーバーへの電源投入が可能です。詳細については、電源設定を参照してください。
  - **解決策 D：**新しく挿入したサーバーと関連付けられるスロットの電源優先度を確認し、他のサーバーのスロットの電源優先度と比べて低く設定されていないかを確認してください。

- **問題：**モジュラエンクロージャ構成を変更していないのに、利用可能な電力の表示が頻繁に変わる。
  - **解決策：**CMC 1.2 以降のバージョンには、エンクロージャがユーザーが設定した電力容量のピークに近づくとサーバーへの電力割当を一時的に減少させるダイナミックファン電源管理機能が搭載されています。これは、ファンに電力を割り当てる際に、電力入力が **システム入力電力上限** を超えないようにするため、サーバーのパフォーマンスを下げる原因になっています。これは、正常な状態です。
- **問題：**ピーク時の余剰電力に 2000 W と表示される。
  - **解決策：**現行の構成ではエンクロージャに 2000 W の余剰電力があり、**システム入力電力上限** はサーバーの性能に影響を与えることなくこの報告された量まで安全に下げることができます。
- **問題：**シャーシが 6 台の電源装置による **AC 冗長性** 構成で動作しているにも関わらず、AC グリッドにエラーが発生した後、サーバーのサブセットに電力が供給されなくなった。
  - **解決策：**この現象は、AC グリッドのエラーが発生したときに電源装置が適切に AC グリッドに接続されていない場合に発生します。**AC 冗長性ポリシー** では、左側の 3 台の電源装置を 1 つの AC グリッドに接続し、右側の 3 台の電源装置を別の AC グリッドに接続することが必要です。PSU3 と PSU4 が間違った AC グリッドに接続されている場合など、2 台の PSU が適切に接続されていないと、AC グリッドに何らかの障害が起きた場合、優先順位が最も低いサーバーへの電源を失う原因となります。
- **問題：**PSU にエラーが発生した後、優先順位の低いサーバーに電力が供給されなくなった。
  - **解決策：**これは、エンクロージャの電力ポリシーが **冗長性なし** に設定されている場合には正常な動作です。今後サーバーの電源がオフになる電源装置エラーを回避するには、シャーシを 4 台以上の電源装置構成にし、**電源装置冗長性ポリシー** を PSU 障害がサーバーの運用に影響しない設定にしてください。
- **問題：**データセンターの周囲温度が上がるとサーバー全体の性能が低下する。
  - **解決策：**これは、**システム入力電力上限** がサーバーへの割り当て電力を減らすことでファンに電力を供給しなければならない電源構成に設定されている場合に発生する可能性があります。**システム入力電力上限** を、サーバーの性能に影響を与えずにファンに十分な電力を供給できる値に増やしてください。

# リモートシステムの Lifecycle Controller ジョブの管理

Lifecycle Controller サービスは各サーバー上で利用することができ、iDRAC により促進されます。CMC によりサーバー上の Lifecycle Controller ジョブのリストが提供されるため、ウェブインタフェースを使用して既存のジョブの削除や除去を行うことができます。Lifecycle Controller の有効化に関する情報については、189 ページの「Lifecycle Controller を使用したサーバーコンポーネントファームウェアのアップデート」を参照してください。

Lifecycle Controller ジョブのリストは、サーバー上の既存のジョブに関する静的なリストです。最新のジョブリストおよび各ジョブのステータスを見るには、リストをリフレッシュする必要があります。

表 12-4 で、Lifecycle Controller ジョブリストに表示される情報について説明しています。

表 12-4. Lifecycle Controller ジョブのステータス

イベント	フィルタマスク値
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1 ~ 16（シャーシには使用できるスロットが 16 個あります）の連番 ID で、シャーシ内でのサーバーの場所を識別するために役立ちます。スロットに装着されているサーバーが 16 未満の場合は、サーバーが装着されているスロットのスロット番号のみが表示されます。
名前	各スロットのサーバー名を表示します。
モデル	サーバーのモデルを表示します。
ジョブ ID	Lifecycle Controller によって、特定のジョブに割り当てられた番号。
説明	更新ジョブや再起動ジョブなど、サーバー上のジョブの種類を示す語句。
状態	サーバー上のジョブのステータスを示します。

Lifecycle Controller ジョブページでは、サーバー上の既存のジョブの削除または除去を行うことができます。

## ジョブの削除

**削除** 操作はデフォルトの操作であり、サーバー上のすべてまたは個々のジョブを削除することができます。削除操作を行うと、選択されたジョブを Lifecycle Controller のジョブキューから取り除きます。**モデル** フィールドに続くチェックボックスをチェックすると、1 つのサーバー上のすべてのジョブを選択できます。個別にジョブを選択するには、そのジョブのステータスフィールドに続くチェックボックスを使用します。

## ジョブの除去

既存の（1 つまたは複数）ジョブが不明な状態となり、ジョブの削除操作を行っても削除できない場合、**除去** 操作が必要になる場合があります。除去操作を行うと、データ管理サービスがリセットされ、すべてのジョブがサーバーから取り除かれます。この操作は、数分かかることがあります。モデルフィールドにつづくチェックボックスをチェックすると、1 つのサーバー上のすべてのジョブを、除去操作の対象として選択できます。



**メモ**: 操作のスケジュールを送信したときは、他のページに移動しないでください。

## シャーシサマリの表示

CMC は、シャーシ、アクティブおよびセカンダリ CMC、iKVM、ファン、温度センサー、I/O モジュール (IOM) のロールアップ概要を表示します。

### ウェブインタフェースの使用

シャーシ、CMC、iKVM、IOM のサマリを表示するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** を選択します。
- 3 **サマリ** タブをクリックします。**シャーシサマリ** ページが表示されます。

表 12-5、表 12-6、表 12-7 および 表 12-8 では、**シャーシサマリ** ページに表示される情報について説明します。

**表 12-5. シャーシサマリ**

項目	説明
<b>名前</b>	シャーシの名前を表示します。名前はネットワーク上のシャーシを識別します。シャーシの名前の設定については、123 ページの「スロット名の編集」を参照してください。
<b>モデル</b>	シャーシのモデルまたはメーカーを表示します。 例：PowerEdge 2900
<b>サービスタグ</b>	シャーシのサービスタグを表示します。サービスタグは、サポートとメンテナンスのためにメーカーが提供する一意の識別子です。
<b>資産タグ</b>	シャーシの管理タグを表示します。
<b>場所</b>	シャーシの場所を表示します。
<b>CMC フェールオーバー準備完了</b>	フェールオーバー状態の場合、スタンバイ CMC（存在する場合）が引き継がれるかどうか（はいまたはいいえ）が表示されます。
<b>システム電源の状態</b>	システムの電源状態を表示します。

**表 12-6. CMC サマリ**

項目	説明
<b>アクティブ CMC の情報</b>	
<b>名前</b>	CMC の名前を表示します。例：アクティブ CMC、スタンバイ CMC
<b>説明</b>	CMC の目的を簡単に説明します。
<b>日時</b>	アクティブ CMC で現在設定されている日時を表示します。
<b>アクティブ CMC ロケーション</b>	アクティブ CMC のスロットの場所を表示します。
<b>冗長モード</b>	スタントバイ CMC がシャーシに存在するかどうかを表示します。
<b>プライマリファームウェアバージョン</b>	アクティブ CMC のファームウェアバージョンが表示されます。
<b>ファームウェア最終更新日</b>	ファームウェアが最後に更新された日付を示します。アップデートが行われていない場合は、このプロパティには <b>なし</b> と表示されます。

表 12-6. CMC サマリ (続き)

項目	説明
ハードウェアバージョン	アクティブ CMC のハードウェアバージョンが表示されます。
MAC アドレス	CMC ネットワークインタフェースの MAC アドレスを表示します。MAC アドレスはネットワーク上の CMC の一意の識別子です。
IP アドレス	CMC ネットワークインタフェースの IP アドレスを表示します。
ゲートウェイ	CMC ネットワークインタフェースのゲートウェイを表示します。
サブネットマスク	CMC ネットワークインタフェースのサブネットマスクを表示します。
DHCP を使用 (ネットワークインタフェース IP アドレス用)	CMC が動的ホスト構成プロトコル (DHCP) サーバーに IP アドレスを自動的に要求して取得できるかどうかを示します (はいまたは いいえ)。このプロパティのデフォルト設定は いいえ です。
プライマリ DNS サーバー	プライマリ DNS サーバーの名前を表示します。
代替 DNS サーバー	代替 DNS サーバーの名前を表示します。
DNS ドメイン名に DHCP を使用	DNS ドメイン名を取得するために DHCP を使用するかどうかを表示します (はい、いいえ)。
DNS ドメイン名	DNS ドメイン名を表示します。
<b>スタンバイ CMC 情報</b>	
存在	セカンダリ (スタンバイ) CMC が設置されているかを示します (はいまたは いいえ)。
スタンバイファームウェアバージョン	スタンバイ CMC にインストールされているファームウェアバージョンを表示します。

表 12-7. iKVM サマリ

項目	説明
存在	iKVM モジュールが存在するかどうかを表示します (はいまたは いいえ)。
名前	iKVM の名前を表示します。名前はネットワーク上の iKVM を識別します。
メーカー	iKVM のモデルまたはメーカーを表示します。

表 12-7. iKVM サマリ (続き)

項目	説明
パーツ番号	iKVM のパーツ番号を示します。パーツ番号は、ベンダーが提供する一意の識別子です。パーツ番号の命名規則はベンダーによって異なります。
ファームウェアバージョン	iKVM のファームウェアバージョンを表示します。
ハードウェアバージョン	iKVM のハードウェアバージョンを表示します。
電源ステータス	iKVM の電源状態： <b>オン</b> 、 <b>オフ</b> 、 <b>なし</b> （不在）を表示します
前面パネルの USB/ビデオを有効にする	前面パネルの VGA または USB コネクタが有効になっているかどうかを表示します（ <b>はい</b> または <b>いいえ</b> ）。
CMC CLI への iKVM からのアクセスを許可する	iKVM 上で CLI アクセスが有効になっているかどうかを示します（ <b>はい</b> または <b>いいえ</b> ）。

表 12-8. IOM サマリ

項目	説明
場所	IOM が占有するスロットを示します。6 つのスロットがグループ名 (A、B、C) とスロット番号 (1 または 2) によって識別されます。スロット名： <b>A-1</b> 、 <b>A-2</b> 、 <b>B-1</b> 、 <b>B-2</b> 、 <b>C-1</b> 、 <b>C-2</b>
存在	IOM が存在するかどうかを示します（ <b>はい</b> または <b>いいえ</b> ）。
名前	IOM 名を表示します。
ファブリック	ファブリックの種類を表示します。
電源ステータス	IOM の電源状態： <b>オン</b> 、 <b>オフ</b> 、 <b>なし</b> （不在）を表示します。
サービスタグ	IOM のサービスタグを表示します。サービスタグは、サポートとメンテナンス用にデルが提供する一意の識別子です。



## RACADM の使用

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
- 2 シャーシと CMC のサマリを表示するには、次を入力します。  
`racadm getsysinfo`
- 3 iKVM サマリを表示するには、次を入力します。  
`racadm getkvminfo`
- 4 IOM サマリを表示するには、次を入力します。  
`racadm getioinfo`

## シャーシとコンポーネントの正常性状態の表示

### ウェブインタフェースの使用

シャーシとシャーシコンポーネントの正常性を表示するには、次を入力します。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** を選択します。 **コンポーネントの状態** ページが表示されます。

**シャーシグラフィックス** セクションは、シャーシの前面および背面図をグラフィック表示します。この表示により、シャーシに内蔵されたコンポーネントおよびステータスの概要を視覚的に把握することができます。

各グラフィックは、取り付けられたコンポーネントをリアルタイムに表示します。コンポーネントの状態は、コンポーネントのサブグラフィックの色で示されます。

- オーバーレイなしコンポーネントが存在し、電源がオンで CMC と通信中です。悪条件の兆候は認められません。
- 橙色の警告サイン—警告アラートが発せられているため、対応措置を取る必要があります。
- 赤色の X—最低 1 つエラー条件が存在することを示します。CMC は引き続きコンポーネントと通信できますが、正常性ステータスが重要として報告されていることを示します。

- グレー表示コンポーネントが存在しますが、電源がオンではありません。CMC と通信しておらず、悪条件の兆候なし。

コンポーネントのサブグラフィックにマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。コンポーネントステータスは動的に更新され、現在の状態を反映するように、コンポーネントのサブグラフィックの色およびテキストヒントも自動的に変更します。

コンポーネントのサブグラフィックをクリックすると、シャードグラフィックの下にコンポーネント情報とクイックリンクが表示されます。

CMC ハードウェアログのセクションは、CMC ハードウェアログの最新の 10 エントリを参照用として表示します。

## RACADM の使用

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm getmodinfo
```

## イベントログの表示

ハードウェアログと CMC ログ ページに、管理下システムで発生したシステムの重要イベントが表示されます。

### ハードウェアログの表示

CMC は、シャードで発生したイベントのハードウェアログを生成します。ハードウェアログは、ウェブインタフェースとリモート RACADM を使用して表示できます。



**メモ**：ハードウェアログをクリアするには、**ログのクリアシステム管理者**の権限が必要です。



**メモ**：特定のイベントが発生したときに E-メールまたは E-メール SNMP トラップを送信するように CMC を設定できます。アラートを送信するように CMC を設定する方法については、370 ページの「SNMP アラートの設定」および 375 ページの「E-メール警告の設定」を参照してください。

## ハードウェアログのエントリ例

critical System Software event: redundancy lost

Wed May 09 15:26:28 2007 normal System Software event: log cleared was asserted

Wed May 09 16:06:00 2007 warning System Software event: predictive failure was asserted

Wed May 09 15:26:31 2007 critical System Software event: log full was asserted

Wed May 09 15:47:23 2007 unknown System Software event: unknown event

## ウェブインタフェースの使用

CMC ウェブインタフェースではハードウェアログの表示や削除、テキストファイルバージョンの保存が可能です。

表 12-9 に、CMC ウェブインタフェースの **ハードウェアログ** ページに表示される情報とその説明を示します。

ハードウェアログを表示するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** をクリックします。
- 3 **ログ** タブをクリックします。
- 4 **ハードウェアログ** サブタブをクリックします。**ハードウェアログ** ページが表示されます。

ハードウェアログのコピーを管理ステーションまたはネットワークに保存するには：

- 1 **ログの保存** をクリックします。  
ダイアログボックスが開きます。
- 2 ログのテキストファイルの場所を選択します。



**メモ：**ログはテキストファイルとして保存されるため、ユーザーインタフェースで重大度を示すのに使用されるグラフィックイメージは表示されません。重大度は、テキストファイルで OK、情報、不明、警告、重要と示されます。日付 / 時刻のエントリは昇順で表示されます。<システム起動> が日付 / 時刻列に表示される場合は、日時を記録できないモジュールのシャットダウンまたはスタートアップ中にイベントが発生したという意味です。

ハードウェアログをクリアするには、**ログのクリア** をクリックします。



**メモ** : CMC はログがクリアされたことを示す新しいログエントリを作成します。

表 12-9. ハードウェアログ情報

項目	説明
重大度	OK 対応処置を必要としない正常なイベントを示します。 情報 重大度の状態が変化していないイベントに関する情報のエントリを示します。 不明 システムエラーを防ぐために <b>早めに対応処置を講じる必要のある</b> 非重要イベントを示します。 警告 システムエラーを防ぐために直ちに対応処置を講じる必要のある <b>重要</b> イベントを示します。 重要 システムエラーを防ぐために、 <b>直ちに対応処置を講じる必要のある</b> 重要イベントを示します。
日時	イベントが発生した正確な日時を示します（例： <b>Wed May 02 16:26:55 2007</b> ）。日付 / 時刻が空白の場合は、システム起動時にイベントが発生しました。
説明	CMC が生成したイベントについて短い説明を提供します（例：冗長性喪失、サーバー挿入など）

## RACADM の使用

RACADM を使用してハードウェアログを表示するには、次の手順を実行します。

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。

- 2 ハードウェアログタイプを表示するには、次を入力します。

```
racadm getssel
```

ハードウェアログをクリアするには、次を入力します。

```
racadm clrssel
```

## CMC ログの表示

CMC は、シャージ関連のイベントのログを生成します。



**メモ**：ハードウェアログをクリアするには、**ログのクリアシステム管理者**の権限が必要です。

### ウェブインタフェースの使用

CMC ウェブインタフェースでは、ハードウェアログの表示や削除、テキストファイルバージョンの保存が可能です。

ログは、行見出しをクリックすることにより、ソース、日付 / 時刻、または 説明を基準に並べ替えることができます。再度、行見出しをクリックすると、並び順序が逆になります。

表 12-10 に、CMC ウェブインタフェースの **CMC ログ** ページに表示される情報とその説明を示します。

CMC ログを表示するには：

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャージ** をクリックします。
- 3 **ログ** タブをクリックします。
- 4 **CMC ログ** サブタブをクリックします。**CMC ログ** ページが表示されます。
- 5 CMC ログのコピーを管理下ステーションまたはネットワークに保存するには、**ログを保存** をクリックします。

ダイアログボックスが開いたら、ログのテキストファイルの保存場所を選択します。

表 12-10. CMC ログ情報

コマンド	結果
ソース	イベントを発生させたインタフェース (CMC など) を示します。
日時	イベントが発生した正確な日時を示します (例: <b>Wed May 02 16:26:55 2007</b> )。
説明	処置について短い説明を表示します (例: ログアウト、ログインエラー、ログクリア)。説明は CMC によって生成されます。

## RACADM の使用

RACADM を使用して CMC ログ情報を表示するには、次の手順を実行します。

- 1 シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
- 2 ハードウェアログタイプを表示するには、次を入力します。

```
racadm getraclog
```

ハードウェアログをクリアするには、次を入力します。

```
racadm clrraclog
```

## 診断コンソールの使用

**診断コンソール** ページは、上級ユーザーやテクニカルサポートを受けているユーザーが CLI コマンドを使って CMC ハードウェアに関連した問題を診断するために使用します。



**メモ**：これらの設定を変更するには **デバッグコマンドシステム管理者** の権限が必要です。

**診断コンソール** ページにアクセスするには、次の手順を行います。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** をクリックします。
- 3 **トラブルシューティング** タブをクリックします。
- 4 **診断** サブタブをクリックします。 **診断コンソール** ページが表示されます。

診断 CLI コマンドを実行するには、**RACADM コマンドの入力** フィールドにコマンドを入力して **送信** をクリックします。診断結果ページが表示されます。

**診断コンソール** ページに戻るには、**診断コンソール ページに戻る** または **更新** をクリックします。

診断コンソールは、RACADM コマンドと共に、表 12-11 に記載されるコマンドをサポートしています。

表 12-11. 対応診断コマンド

コマンド	結果
arp	アドレス解決プロトコル (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。
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表示します。

表 12-11. 対応診断コマンド（続き）

コマンド	結果
ping <IP アドレス>	現在のルーティングテーブルの内容で、CMC から送信先の <IP アドレス> に到達可能かどうかを確認します。このオプションの右側のフィールドに送信先の IP アドレスの入力が必要です。現在のルーティングテーブルの内容に基づいて、ICMP（インターネットコントロールメッセージプロトコル）エコーパケットが宛先 IP アドレスに送信されます。
gettracelog	<p>トレースログを表示します（ログが表示されるまでに数秒かかることがあります）。<b>gettracelog -i</b> コマンドはトレースログ内のコード数を返します。</p> <p><b>メモ：</b> gettracelog コマンドの詳細については、『RACADM Command Line Reference Guide for iDRAC7 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の gettracelog コマンドの項を参照してください。</p>

## コンポーネントのリセット

コンポーネントのリセット ページで、ユーザーは、アクティブ CMC をリセットしたり、仮想的にサーバーを装着し直すことができます。シャーシにスタンバイ CMC がある場合にアクティブ CMC をリセットすると、フェールオーバーが発生し、スタンバイ CMC がアクティブになります。






**メモ：**コンポーネントをリセットするには、**デバッグ コマンド管理者** の権限が必要です。

診断コンソール ページにアクセスするには、次の手順を行います。

- 1 CMC ウェブインタフェースにログインします。
- 2 システムツリーで **シャーシ** をクリックします。
- 3 **トラブルシューティング** タブをクリックします。
- 4 **コンポーネントのリセット** サブタブをクリックします。**更新可能なコンポーネント** ページが表示されます。**コンポーネントのリセット** ページの **CMC サマリ** の部分には次の情報が表示されます。

表 12-12. CMC サマリ

属性	説明
状態	<p> OK CMC が存在し コンポーネントと通信しています。</p> <p> 情報 状態ステータス（OK、警告、重要）に変化がない場合に CMC についての情報を表示します。</p> <p> 警告 警告アラートが発行されたこと、および <b>対応処置を取る必要がある</b> ことを示します。対応処置を取らない場合には、CMC の保全性に影響するような重要または重大なエラーを引き起こす可能性があります。</p> <p> 重要 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。重要な状態は CMC のシステムエラーを示し、<b>直ちに対応処置を取る必要があります</b>。</p>
日時	CMC の日付と時刻を MM/DD/YYYY の形式で表示します。このとき、MM は月、DD は日、YYYY は年を示します。
アクティブ CMC ロケーション	アクティブ CMC の場所を表示します。
冗長モード	シャーシにスタンドバイ CMC がある場合は <b>冗長</b> を表示し、シャーシにスタンドバイ CMC がない場合は <b>冗長なし</b> が表示されます。

5 コンポーネントのリセット ページの **仮想サーバーの装着** の部分には次の情報が表示されます。

表 12-13. 仮想サーバーの装着





属性	説明
スロット	シャーシでサーバーが装着されているスロットを示します。スロット名は、1 ~ 16 の連番 ID で、シャーシでサーバーが装着されている場所を示します。
名前	各スロットのサーバー名を表示します。
存在	サーバーがスロットにあるかどうかを示します（はいまたはいいえ）。
状態	<p> OK サーバーが存在し CMC と通信しています。CMC とサーバー間で通信エラーが発生した場合は、CMC はそのサーバーの状態ステータスを取得または表示できません。</p>



表 12-13. 仮想サーバーの装着（続き）

属性	説明
 情報	正常性の状態（OK、警告、重要）に変化がない場合にサーバーについての情報を表示します。
 警告	警告アラートが発行されたこと、および <b>対応処置を取る必要がある</b> ことを示します。管理者が指定した時間内に対応処置を取らなかった場合は、サーバーの健全性に影響するような重要または重大なエラーを引き起こす可能性があります。
 重要	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。重要な状態は CMC のシステム エラーを示し、 <b>直ちに対応処置を取る必要があります</b> 。
iDRAC ステータス	<p>iDRAC に管理コントローラを内蔵するサーバーの状態を表示します。</p> <ul style="list-style-type: none"> <li>• <b>該当なし</b> - サーバーがない、またはシャーシの電源が入っていません。</li> <li>• <b>レディ</b> - iDRAC が利用可能状態であり、正常に動作しています。</li> <li>• <b>障害あり</b> - iDRAC ファームウェアが破損しています。iDRAC ファームウェア更新ユーティリティを使ってファームウェアを修復します。</li> <li>• <b>エラー</b> - iDRAC と通信できません。仮想装着チェックボックスを使ってエラーを消去します。これがうまくできない場合は、手動でサーバーを削除および交換してエラーを消去してください。</li> <li>• <b>FW 更新</b> - iDRAC ファームウェアを更新しています。更新が完了するまで別の操作をしないでください。</li> <li>• <b>初期化</b> - iDRAC をリセットしています。コントローラの電源サイクルが完了するまで別の操作をしないでください。</li> </ul>
電源状態	<p>サーバーの電源状態を表示します。</p> <ul style="list-style-type: none"> <li>• <b>該当なし</b> - CMC はサーバーの電源状態を特定できていません。</li> <li>• <b>オフ</b> - サーバーまたはシャーシに電源がオフです。</li> <li>• <b>オン</b> - シャーシおよびサーバーともに電源がオンです。</li> <li>• <b>電源投入中</b> - 電源オフおよび電源オンの間の一時的な状態です。電源サイクルが完了すると、電源状態は <b>オン</b> になります。</li> <li>• <b>電源切断中</b> - 電源オンおよび電源オフの間の一時的な状態です。電源サイクルが完了すると、電源状態は <b>オフ</b> になります。</li> </ul>
仮想装着	チェックボックスを選択して仮想的にサーバーの抜き差しを行います。

- 6 サーバーを仮想的に抜き差しするには、対象のサーバーのチェックボックスを選択して **選択の適用** を選択します。この操作を行うと、サーバーの抜き差し動作が可能になります。
- 7 **CMC のリセット / フェールオーバー** を選択すると、アクティブ CMC をリセットします。スタンバイ CMC が存在し、シャーシが完全冗長化されている場合は、フェールオーバーが発生し、スタンバイ CMC がアクティブになります。

# ネットワークタイムプロトコル (NTP) 問題の トラブルシューティング

CMC のクロックをネットワーク上のリモートタイムサーバーの時刻と同期化するよう設定した後は、日付と時刻が変更されるまで数分かかる場合があります。その後も変更されない場合は、トラブルシューティングを行ってください。次のような理由で CMC のクロックが同期化できない場合があります。

- NTP Server 1、NTP Server 2、NTP Server 3 の設定に問題がある
- 間違ったホスト名または IP アドレスが入力された
- 設定されているいずれの NTP サーバーと CMC との通信を妨げるネットワーク接続上の問題がある
- NTP サーバーホストの解決を妨げる DNS の問題がある

CMC は、このような問題を解決するためのツールを提供します。それにはトラブルシューティングの主要な情報源となる CMC トレースログが含まれています。このログには、NTP 関連の障害に関するエラーメッセージが含まれます。CMC が設定されているいずれのリモート NTP サーバーとも同期できない場合、CMC はローカルシステムのクロックから時刻情報を取得します。

CMC がリモートタイムサーバーではなくローカルシステムクロックと同期する場合は、トレースログに次のようなエントリが記録されます。

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0),  
stratum 10
```

次の `racadm` コマンドを入力することで、`ntpd` ステータスを確認することもできます。

```
racadm gettractime -n
```

設定されているいずれかのサーバーに対して `*` が表示されていない場合は、設定が正しくない可能性があります。上記コマンドの出力には、サーバーが同期しない原因をデバッグする場合に役立つ詳細な NTP 統計も含まれています。

Windows ベースの NTP サーバーを設定しようとする場合は、`ntpd` の `MaxDist` パラメータを増やすと問題が解決される場合があります。このパラメータを変更する場合は、事前に変更に伴う影響について読んで理解しておいてください。特に、デフォルト設定は、ほとんどの NTP サーバーを動作するのに十分な大きさを持っています。パラメータを変更するには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

変更後は、NTP を無効にして `ntpd` を再起動し、5 ~ 10 秒後に NTP を再度有効にします。



**メモ** : NTP を再同期するにはさらに 3 分かかることがあります。

NTP を無効にするには、次を入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 0
```

NTP を有効にするには、次を入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 1
```

NTP サーバーが正しく設定されているにもかかわらず、このエントリがトレースログに存在する場合は、CMC が設定された NTP サーバーのいずれとも同期できないことが確実になります。

問題解決に役立つその他の NTP 関連のトレースログエントリが存在する可能性もあります。NTP サーバーの IP アドレス設定ミスの場合は、次のような記録が残されます。

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing  
interface for address 1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]:  
configuration of 1.2.3.4 failed
```

NTP サーバーの設定に間違ったホスト名があると、次のようなトレースログが記録されます。

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found:  
blabla Aug 21 14:34:27 cmc ntpd_initres[1298]: couldn't  
resolve `blabla', giving up on it
```

CMC GUI から `gettracelog` コマンドを入力してトレースログを表示する方法については、392 ページの「診断コンソールの使用」を参照してください。

## LED の色と点滅パターンの解釈

シャーシ上の LED は、色および点滅 / 点滅なしで情報を提供します。

- 緑色の LED の点灯は、コンポーネントの電源がオンであることを示します。緑色の LED の点滅は、ファームウェアアップデートなど、重要ではあるが日常的なイベントを示します。この間、装置は作動していません。これはエラーではありません。
- モジュール上のオレンジの LED の点滅は、モジュールのエラーを示します。
- 青色の LED の点滅は、ユーザーによって設定可能で、識別に利用できます (369 ページの「シャーシ上のコンポーネントを識別するための LED の設定」を参照)。

表 12-14. LED の色と点滅パターン

コンポーネント	LED の色、点滅パターン	意味
CMC	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、無灯	電源オフ
	青色、点灯	アクティブ
	青色、点滅	ユーザー設定のモジュールの識別
	橙色、点灯	不使用
	橙色の点滅	障害
	青色、無灯	スタンバイ
iKVM	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、無灯	電源オフ
	橙色、点灯	不使用
	橙色の点滅	障害
	橙色、無灯	エラーなし
サーバー	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、無灯	電源オフ
	青色、点灯	正常
	青色、点滅	ユーザー設定のモジュールの識別
	橙色、点灯	不使用
	橙色の点滅	障害
	青色、無灯	エラーなし


表 12-14. LED の色と点滅パターン (続き)

コンポーネント	LED の色、点滅パターン	意味
IOM (共通)	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、無灯	電源オフ
	青色、点灯	正常 / スタックマスター
	青色、点滅	ユーザー設定のモジュールの識別
	橙色、点灯	不使用
	橙色の点滅	障害
	青色、無灯	エラーなし / スタックスレープ
IOM (パススルー)	緑色、点灯	電源オン
	緑色、点滅	不使用
	緑色、無灯	電源オフ
	青色、点灯	正常
	青色、点滅	ユーザー設定のモジュールの識別
	橙色、点灯	不使用
	橙色の点滅	障害
	青色、無灯	エラーなし
ファン	緑色、点灯	ファン作動中
	緑色、点滅	不使用
	緑色、無灯	電源オフ
	橙色、点灯	ファンタイプを認識できません、CMC ファームウェアをアップデートしてください。
	橙色の点滅	ファンエラー。タコメーターの範囲外です。
	橙色、無灯	不使用

表 12-14. LED の色と点滅パターン（続き）

コンポーネント	LED の色、点滅パターン	意味
電源装置	（楕円）緑色、点灯	AC OK
	（楕円）緑色、点滅	不使用
	（楕円）緑色、無灯	AC エラー
	橙色、点灯	不使用
	橙色の点滅	障害
	橙色、無灯	エラーなし
	（円）緑色、点灯	DC OK
	（円）緑色、無灯	DC エラー

## 無応答 CMC のトラブルシューティング

 **メモ:** シリアルコンソールを使ってスタンバイ CMC にログインすることはできません。

いずれのインタフェース（ウェブインタフェース、Telnet、SSH、リモート RACADM、シリアルなど）を使用しても CMC にログインできない場合は、CMC 上の LED の観察、DB-9 シリアルポートを使用したリカバリ情報の取得、または CMC ファームウェアイメージのリカバリなどを行うことにより、CMC が機能しているかどうかを確認できます。

### LED を観察して問題を特定する

シャーシに取り付けられている CMC の前面から見て、カードの左側に LED が 2 つあります。

上部の LED — 上部の緑の LED は電源の状態を示します。オンでない場合：

- 1 AC 電源があり、少なくとも 1 台の電源装置があることを確認してください。
- 2 CMC カードが正しく取り付けられていることを確認してください。取り出しハンドルを解除して引き、CMC を取り外した後、再度挿入します。基板が完全に挿入されており、ラッチが正しく閉まることを確認します。

下部の LED — 下部の LED はマルチカラーです。CMC がアクティブで作動しており、問題がないときは、下部の LED は青色になります。問題が検出されると、橙色になります。これらの問題は、次の 3 つのいずれかのイベントによって引き起こされたものです。

- コアエラー この場合、CMC ボードを取り替える必要があります。
- セルフテストエラー この場合、CMC ボードを取り替える必要があります。
- イメージの破損 この場合、CMC ファームウェアイメージをアップロードすることで CMC を回復できます。



**メモ**：標準の CMC 起動およびリセットには、CMC が OS に完全に読み込まれ、ログインできるまでに 1 分以上かかります。アクティブ CMC では青色 LED が点灯しています。冗長 2 台の CMC 構成の場合は、スタンバイ CMC では上部の緑色の LED だけが点灯しています。

## DB-9 シリアルポートからのリカバリ情報の取得

下部の LED が橙色の場合、CMC の前面にある DB-9 シリアル ポートからリカバリ情報を取得できます。

リカバリ情報を得るには：

- 1 CMC とクライアントコンピュータの間に NULL モデムケーブルを取り付けます。
- 2 任意のターミナルエミュレータ（ハイパーターミナル や Minicom など）を開けます。8 ビット、パリティなし、フロー制御なし、ボーレート 115200 に設定します。  
5 秒おきにコアメモリ障害のエラーメッセージが表示されます。

- 3 <Enter> を押します。リカバリ プロンプトが表示されたら、追加情報が利用できます。プロンプトは、CMC スロット番号と障害タイプを示します。問題の原因といくつかのコマンドの構文を表示するには、次を入力します。

```
recover
```

その後 <Enter> を押します。プロンプト例：

```
recover1 [セルフテスト] CMC 1 セルフテストエラー
```

```
recover2 [ファームウェアイメージ不良] CMC2 のイメージが破損しています
```

- プロンプトがセルフテストの失敗を示している場合、CMC にはサービス可能なコンポーネントはありません。この CMC は故障しているため、デルに返品する必要があります。
- プロンプトが **FW イメージ不良** を示している場合は、402 ページの「ファームウェアイメージのリカバリ」の手順に従って問題を解決してください。

## ファームウェアイメージのリカバリ

正常な CMC OS の起動ができない場合、CMC はリカバリモードになります。リカバリモードでは、少数のコマンドのサブセットを使用してファームウェアアップデートファイルの **firmimg.cmc** をアップロードすることでフラッシュデバイスを再プログラムできます。これは、正常のファームウェアアップデートで使用されるのと同じファームウェアイメージファイルです。リカバリプロセスでは、現在の進行状況を示し、回復が完了後、CMC OS を起動します。

**リカバリ** プロンプトで `recover` と入力して `<Enter>` を押すと、回復理由と使用可能なサブコマンドが表示されます。リカバリシーケンス例：

```
recover getniccfg

recover setniccfg 192.168.0.120    255.255.255.0
192.168.0.1

recover ping 192.168.0.100

recover fwupdate -g -a 192.168.0.100
```



**メモ**：ネットワークケーブルを左端 RJ-45 に接続します。

**メモ**：リカバリモードでは、アクティブなネットワークスタックがないため、通常の方法で CMC を ping することはできません。**recover ping <TFTP サーバー IP アドレス>** コマンドを使うことで、TFTP サーバーを ping して LAN 接続を確認できます。一部のシステムでは、**setniccfg** 後に **recover reset** コマンドを使う必要があるかもしれません。

## ネットワーク問題のトラブルシューティング

内部 CMC トレースログを使うと、CMC の警告とネットワークのデバッグを行うことができます。CMC ウェブインタフェース（「診断コンソールの使用」を参照）または RACADM（「RACADM コマンドラインインタフェースの使用」および『RACADM Command Line Reference Guide for iDRAC6 and CMC』（iDRAC6 および CMC 用 RACADM コマンドラインリファレンスガイド）の **gettracelog** コマンドを参照）を使ってトレースログにアクセスできます。


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。
- DDNS — DNS の動的アップデート要求と応答を追跡します。
- ネットワークインタフェースへの設定変更。


トレースログには、管理下システムのおペレーティングシステムではなく、CMC の内部ファームウェアに関連する CMC 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。




## 忘れたシステム管理者パスワードのリセット


 **注意**：修理作業の多くは、認定されたサービス技術者のみが行うことができます。製品マニュアルで許可されている範囲に限り、またはオンラインサービスもしくはテレホンサービスとサポートチームの指示によってのみ、トラブルシューティングと簡単な修理を行うようにしてください。デルで認められていない修理による損傷は、保証の対象となりません。製品に付属しているマニュアルの安全にお使いいただくための周囲をお読みになり、指示に従ってください。

管理操作を行うには、**システム管理者** の権限が必要となります。CMC ソフトウェアには、ユーザーアカウントをパスワード保護するセキュリティ機能が搭載されていますが、システム管理者アカウントのパスワードをお忘れになった場合、この機能を無効にすることができます。システム管理者アカウントのパスワードを忘れた場合、CMC ボードの `PASSWORD_RSET` ジャンパを利用して回復することができます。

CMC ボードには、 12-1 で示すように、2 ピンのパスワードリセットコネクタが搭載されています。リセットコネクタにジャンパが取り付けられている場合、デフォルトのシステム管理者アカウントおよびパスワードが有効になり、**ユーザー名：root** および **パスワード：calvin** に設定されます。システム管理者アカウントは、アカウントが削除された場合やパスワードが変更された場合でも、リセットされます。

 **メモ**：作業を開始する前に、CMC モジュールがパッシブ状態にあることを確認してください。

管理操作を行うには、**システム管理者** の権限が必要となります。システム管理者アカウントのパスワードを忘れた場合、CMC ボードの `PASSWORD_RSET` ジャンパを利用して回復することができます。

`PASSWORD_RST` ジャンパは  12-1 で表示されているように 2 ピンコネクタを使用します。

`PASSWORD_RST` ジャンパが取り付けられている場合、デフォルトのシステム管理者アカウントとパスワードは次のデフォルト値に設定されます。

ユーザー名：root

パスワード：calvin

システム管理者アカウントは、削除されている場合、またはパスワードが変更された場合でも、一時的にリセットされます。



**メモ**：PASSWORD\_RST ジャンパが取り付けられると、次のように（設定プロパティ値ではなく）デフォルトのシリアルコンソールの設定が使用されます。

```
cfgSerialBaudRate=115200  
cfgSerialConsoleEnable=1  
cfgSerialConsoleQuitKey=^\  
cfgSerialConsoleIdleTimeout=0  
cfgSerialConsoleNoAuth=0  
cfgSerialConsoleCommand=""  
cfgSerialConsoleColumns=0
```

- 1 ハンドルに付いている CMC リリースラッチを押し、ハンドルを回してモジュールの前面パネルから離します。CMC モジュールをエンクロージャから引き出します。



**メモ**：静電気障害（ESD）イベントで CMC を損傷する可能性があります。その状況によっては、ESD は人体や物体に蓄積され、CMC などの別の物体に放出されることがあります。ESD による損傷を避けるため、シャーシ外部で CMC を取り扱う場合は、体から帯電を除去するための予防措置を取る必要があります。

- 2 パスワードリセットコネクタからジャンププラグを取り外し、2 ピンのジャンパを取り付けて、デフォルトのシステム管理者アカウントを有効にします。CMC ボード上のパスワードジャンパの位置については、図 12-1 を参照してください。

図 12-1. パスワードリセットジャンパの位置

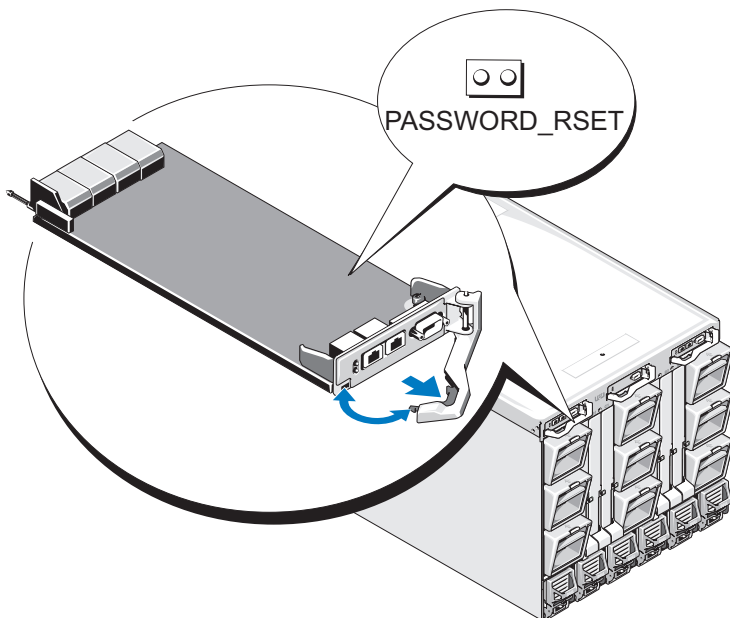





表 12-15. CMC パスワードジャンパの設定

PASSWORD_RESET		(デフォルト) パスワードリセット機能は無効です。
		パスワードリセット機能は有効です。

- 3 CMC モジュールをエンクロージャの中に入れます。切断したケーブルをすべて再接続します。

 **メモ:** CMC モジュールがアクティブになり、残りの手順が終了するまで CMC がアクティブであることを確認します。

- 4 ジャンパを取り付けた CMC モジュールが唯一の CMC である場合、再起動が終了するまでお待ちください。シャーシに冗長 CMC がある場合は、ジャンパを取り付けた CMC モジュールをアクティブに切り替えます。GUI インタフェースで次のように作業します。
  - a シャーシ ページに移動し、電源 タブ → コントロール サブタブの順にクリックします。
  - b **Reset CMC (ウォームブート)** ボタンを選択し、**適用** をクリックします。CMC が自動的に冗長モジュールにフェールオーバーし、そのモジュールがアクティブになります。
- 5 デフォルトのシステム管理者ユーザー名 (**root**) およびパスワード (**calvin**) を使用してアクティブ CMC にログインします。必要に応じて、ユーザーアカウントの設定を復元します。既存のアカウントおよびパスワードは無効にならず、アクティブなままとなります。
- 6 忘れてしまったシステム管理者パスワードを新しく作成するなど、必要な管理操作を行います。
- 7 2 ピンジャンパを取り外し、ジャンパプラグを元に戻します。
  - a ハンドルに付いている CMC リリースラッチを押し、ハンドルを回してモジュールの前面パネルから離します。CMC モジュールをエンクロージャから引き出します。
  - b 2 ピンジャンパを取り外し、ジャンパプラグを元に戻します。
  - c CMC モジュールをエンクロージャの中に入れます。切断したケーブルをすべて再接続します。手順を繰り返して、手順 4 ジャンパを取り付けていない CMC モジュールをアクティブにします。

## シャーシ構成設定および資格情報の保存と復元

CMC GUI で **シャーシの概要** → **セットアップ** → **シャーシのバックアップ** に移動します。**シャーシのバックアップ** 画面が表示されます。

シャーシ構成のバックアップを保存するには、次の手順を実行します。

- 1 **シャーシのバックアップ** 画面で、**保存** をクリックします。
- 2 デフォルトのファイルパス（オプション）を上書きし、**OK** をクリックしてファイルを保存します。



**メモ**：デフォルトのバックアップファイル名には、シャーシサービスタグが含まれます。バックアップファイルは、後でそのシャーシ固有の設定資格情報を復元するために使用できます。

シャーシ設定を復元するには、次の手順を実行します。

- 1 **シャーシのバックアップ** 画面で、**参照** をクリックします。
- 2 バックアップファイルの場所まで移動するかまたはファイルパスを入力して、**開く** をクリックしてそのファイルを選択します。
- 3 **復元** をクリックします。



**メモ**：CMC 自体は設定の復元時にリセットすることはありませんが、CMC サービスに新しい（または変更された）構成内容が事実上反映されるまで、しばらく時間がかかることがあります。正常に終了したら、現在のすべてのセッションを閉じます。

## アラートのトラブルシューティング

CMC アラートのトラブルシューティングを行う際は、CMC ログおよびトレースログを使用します。E-メールまたは SNMP トラップの配信のすべての試み（成功または失敗）は、CMC ログに記録されます。特定のエラーに関する追加情報は、トレースログに記録されます。ただし、SNMP ではトラップの配信を確認できないため、ネットワークアナライザや Microsoft の **snmputil** などのツールを使って、管理下システム上のパケットをトレースすることをお勧めします。

ウェブインタフェースを使って SNMP アラートを設定できます。詳細については、**SNMP アラートの設定** を参照してください。



## 診断

LCD パネルは、シャーシ内のサーバーやモジュールの問題を診断する場合に役立ちます。シャーシまたはシャーシ内のサーバーやモジュールに問題やエラーがある場合は、LCD パネルの状態インジケータが橙色に点滅します。メインメニューで、サーバーまたはモジュール障害の原因となるメニューアイテム（サーバーまたはエンクロージャ）の横に背景が橙色のアイコンが表示されます。

LCD メニューシステムで橙色のアイコンをたどっていくと、問題のあるアイテムのステータス画面とエラーメッセージを表示できます。

LCD パネル上のエラーメッセージは、その問題の原因となっているモジュールやサーバーを取り外すと、エラーメッセージも削除されます。または、サーバーエラーの場合は、iDRAC 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を使ってそのサーバーのシステムイベントログ（SEL）を消去すると、LCD からそのサーバーエラーが削除されます。

## LCD パネルインタフェースの使用

LCD パネルを使用して設定と診断を実行したり、シャーシやそのコンテンツのステータス情報を取得したりできます。

## LCD のナビゲーション













LCD パネルを操作するには、LCD 画面の右側のボタンを使用します。上下左右の矢印ボタンは、画面で選択したメニュー項目やアイコンを変更します。選択されている項目は、青い背景または枠で表示されます。

中央のボタンは、選択した項目をアクティブにします。

LCD 画面に表示されたメッセージが画面の幅よりも長い場合は、左右の矢印ボタンを使ってテキストを左と右にスクロールします。

表 13-1 に示したアイコンは LCD 画面間の移動に使用します。

表 13-1 LCD パネルのナビゲーション用アイコン

標準アイコン	ハイライトアイコン	アイコン名および説明
		<b>戻る。</b> 前の画面に戻るには、中央のボタンをハイライトして押します。
		<b>適用 / はい。</b> 変更を適用して前の画面に戻るには、中央のボタンをハイライトして押します。
		<b>スキップ / 次へ。</b> 変更をスキップして次の画面に進むには、中央のボタンをハイライトして押します。
		<b>いいえ。</b> 変更を行わずに次の画面に進むには、中央のボタンをハイライトして押します。
		<b>回転。</b> シャーシの前面図と背面図を切り替えるには、中央のボタンをハイライトして押します。
		<b>メモ：</b> オレンジの背景は、前面または背面図にエラーがあることを示します。
		<b>コンポーネント識別。</b> コンポーネントの青い LED が点滅します。 <b>メモ：</b> コンポーネント識別 が有効になると、このアイコンを囲む青い長方形が点滅します。

## Main Menu (メインメニュー)

**メイン** メニューから以下のいずれかの画面に移動できます。

- **LCD 設定メニュー** — 使用する言語と、LCD を使用していないときに表示する LCD 画面を選択します。
  - **サーバー** — サーバーのステータス情報を表示します。
  - **エンクロージャ** — シャーシのステータス情報を表示します。
- 1 上下の矢印ボタンを使って項目をハイライトします。
  - 2 中央のボタンを押して選択項目をアクティブにします。



## LCD セットアップメニュー

**LCD 設定** メニューには、設定可能な項目のメニューが表示されます。

- **言語設定** — LCD 画面のテキストとメッセージに使用する言語を選択します。
  - **デフォルト画面** — LCD パネルにアクティビティがないときに表示される画面を選択します。
- 1 上下の矢印ボタンを使ってメニュー項目をハイライトするか、**メイン** メニューに戻る場合は **戻る** アイコンをハイライトします。
  - 2 中央のボタンを押して選択項目をアクティブにします。

### 言語設定画面

**言語設定** 画面では、LCD パネルのメッセージに使用する言語を選択します。現在アクティブな言語は、青色の背景でハイライトされています。

- 1 上下左右の矢印ボタンを使って任意の言語をハイライトします。
- 2 中央のボタンを押します。適用アイコンが表示されてハイライトされます。
- 3 中央のボタンを押して変更を確認します。**LCD 設定** メニューが表示されます。

### デフォルト画面

**デフォルト画面** では、パネルにアクティビティがないときに LCD パネルに表示される画面を変更できます。工場出荷時のデフォルト画面は **メインメニュー** です。以下から、表示する画面を選択できます。

- **Main Menu** (メインメニュー)
- **サーバーステータス** (シャーシの前面図)
- **モジュールステータス** (シャーシの背面図)
- **カスタム** (シャーシ名入りの Dell のロゴ)

現在アクティブなデフォルト画面は青でハイライトされます。

- 1 上下の矢印ボタンを使って、デフォルトに設定する画面をハイライトします。
- 2 中央のボタンを押します。**適用** アイコンがハイライトされます。
- 3 中央のボタンを再度押して変更を確認します。**デフォルト画面** が表示されます。

## グラフィカルサーバステータス画面

グラフィカルサーバステータス画面には、シャーシにインストールされている各サーバのアイコンが表示され、それぞれの正常性の状態が示されます。サーバの正常性は、以下のようにサーバアイコンの色で示されます。

- 灰色 — サーバがオフでエラーなし
- 緑色 — サーバがオンでエラーなし
- 橙色 — サーバに 1 つまたは複数の重大ではないエラーがある
- 赤色 — サーバに 1 つまたは複数の重大なエラーがある
- 黒色 — サーバが存在しない

サーバアイコンの周りで点滅する青い長方形は、サーバがハイライトされていることを示します。

グラフィカルモジュールステータス画面を表示するには

- 1 回転アイコンをハイライトします。
- 2 中央のボタンを押します。

サーバのステータス画面を表示するには

- 1 矢印ボタンを使って任意のサーバをハイライトします。
- 2 中央のボタンを押します。サーバステータス画面が表示されます。

メインメニューに戻るには

- 1 矢印ボタンを使って戻るアイコンをハイライトします。
- 2 中央のボタンを押します。

## グラフィカルモジュールステータス画面

グラフィカルモジュールステータス画面には、シャーシの後部にインストールされているモジュールがすべて表示され、各モジュールの正常性の情報が要約されています。モジュールの正常性は、以下のように各モジュールアイコンの色で示されます。

- グレー — モジュールがオフまたはスタンバイでエラーなし
- グリーン — モジュールがオンでエラーなし
- 橙色 — モジュールに 1 つまたは複数の重大ではないエラーがある
- 赤色 — サーバに 1 つまたは複数の重大なエラーがある
- 黒色 — モジュールが存在しない

モジュールアイコンの周りで点滅する青い長方形は、モジュールがハイライトされていることを示します。

**グラフィカルサーバーステータス** 画面を表示するには

- 1 回転アイコンをハイライトします。
- 2 中央のボタンを押します。

モジュールのステータス画面を表示するには

- 1 上下左右の矢印ボタンを使って任意のモジュールをハイライトします。
- 2 中央のボタンを押します。**モジュールステータス** 画面が表示されます。

**メインメニュー** に戻るには

- 1 矢印ボタンを使って **戻る** アイコンをハイライトします。
- 2 中央のボタンを押します。**メインメニュー** が表示されます。

## エンクロージャメニュー画面

この画面から以下の画面に移動できます。

- **モジュールステータス** 画面
  - **エンクロージャステータス** 画面
  - **IP サマリ** 画面
  - **Main Menu** (メインメニュー)
- 1 ナビゲーションボタンを使って任意の項目をハイライトします。(メインメニューに戻るには、**戻る** アイコンをハイライトします。)
  - 2 中央のボタンを押します。選択した画面が表示されます。

## モジュールステータス画面

**モジュールステータス** 画面には、モジュールに関する情報とエラーメッセージが表示されます。この画面に表示される可能性があるメッセージについては、424 ページの「LCD モジュールとサーバーステータス情報」と 417 ページの「LCD エラーメッセージ」を参照してください。

メッセージ間を移動するには、上下の矢印キーを使用します。画面をはみ出たメッセージは、左右の矢印キーを使ってスクロールします。

**グラフィカルモジュールステータス** 画面に戻るには、**戻る** アイコンをハイライトし、中央のボタンを押します。

## エンクロージャステータス画面

**エンクロージャステータス**画面には、エンクロージャに関する情報およびエラーメッセージを表示します。この画面に表示されるメッセージについては、417 ページの「LCD エラーメッセージ」を参照してください。

メッセージ間を移動するには、上下の矢印キーを使用します。画面をはみ出たメッセージは、左右の矢印キーを使ってスクロールします。

**エンクロージャステータス** 画面に戻るには、**戻る** アイコンをハイライトし、中央のボタンを押します。

## IP サマリ画面

**IP サマリ** 画面には、取り付けられている各サーバーの CMC と iDRAC の IP 情報が表示されます。

上下の矢印ボタンを使ってリストをスクロールできます。画面より長いメッセージを選択した場合は、左右の矢印ボタンを使ってスクロールします。

**エンクロージャ** メニューに戻るには、上下の矢印ボタンを使って **戻る** アイコンを選択し、中央のボタンを押します。

## 診断

LCD パネルは、シャーシ内のサーバーやモジュールの問題を診断する場合に役立ちます。シャーシまたはシャーシ内のサーバーやモジュールに問題やエラーがある場合は、LCD パネルの状態インジケータが橙色に点滅します。**メインメニュー** で、背景が橙色に点滅するアイコンがメニュー項目（サーバーまたはエンクロージャ）の横に表示される場合、サーバーまたはモジュールに障害があることを示します。

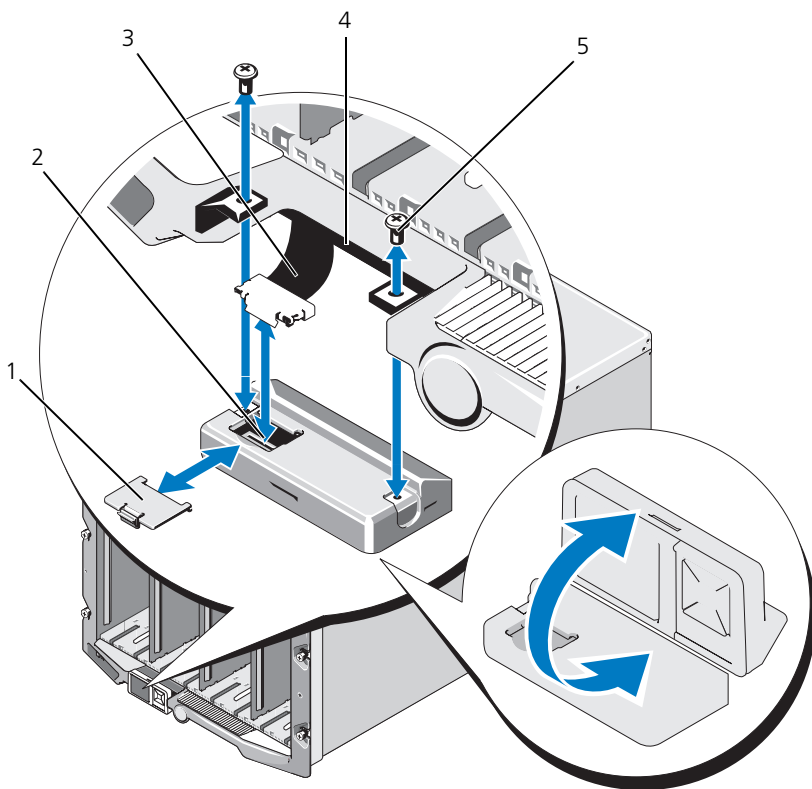
LCD メニューシステムで橙色の点滅アイコンをたどっていくと、問題のある項目のステータス画面とエラーメッセージを表示できます。

問題の原因となるモジュールやサーバーを取り外すか、モジュールまたはサーバーのハードウェアログをクリアすると、LCD パネルのエラーメッセージを削除できます。サーバーエラーの場合は、iDRAC 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を使用して、サーバーのシステムイベントログ (SEL) をクリアします。シャーシエラーの場合は、CMC 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を使用してハードウェアログをクリアします。

## LCD ハードウェアのトラブルシューティング

CMC の使用に関して LCD で何らかの問題に遭遇した場合は、次のハードウェアのトラブルシューティング項目を使用して、LCD ハードウェアまたは接続に問題がないか調べます。

図 13-1 LCD モジュールの取り外しと取り付け



- 1 ケーブルカバー
- 3 リボンケーブル
- 5 ネジ (2)

- 2 LCD モジュール
- 4 ヒンジ (2)

表 13-2 LCD ハードウェアのトラブルシューティング項目

現象	問題	回復処置
警告画面に CMC が応答しませんがのメッセージが表示され、LED が橙色に点滅する。	CMC から LCD 前面パネルへの通信の損失です。	CMC が起動していることを確認した上で、GUI または RACADM コマンドを使用して CMC をリセットします。
警告画面に CMC が応答しませんがのメッセージが表示され、LED が橙色に点灯、または消灯する。	CMC のフェールオーバーまたは再起動中に、LCD モジュールの通信が停止しました。	GUI または RACADM コマンドを使用してハードウェアログを確認します。Can not communicate with LCD controller. (LCD コントローラと通信できません。というメッセージを探してください。) LCD モジュールのリボンケーブルを抜き差しします。
画面のテキストが文字化けしている。	欠陥のある LCD 画面です。	LCD コントローラモジュールを交換します。
LED が消灯しており、LCD がオフになっている。	LCD ケーブルが正しく接続されていないかケーブルに欠陥がある、または LCD モジュールに欠陥があります。	GUI または RACADM コマンドを使用してハードウェアログを確認します。以下のメッセージを探します。 <ul style="list-style-type: none"> <li>• The LCD module cable is not connected, or is improperly connected. (LCD モジュールケーブルが接続されていないか、または正しく接続されていません。)</li> <li>• The control panel cable is not connected, or is improperly connected. (コントロールパネルケーブルが接続されていないか、または正しく接続されていません。)</li> </ul> ケーブルを接続し直します。
LCD 画面に CMC が見つかりませんがのメッセージが表示される。	シャーシに CMC が存在しません。	シャーシに CMC を挿入します。CMC が存在するのに機能していない場合は、既存の CMC を取り付け直します。

## 前面パネル LCD メッセージ

このセクションには 2 つのサブセクションがあり、前面パネル LCD に表示されるエラーとステータス情報をリストにします。

LCD のエラーメッセージの形式は、CLI またはウェブインタフェースで表示されるシステムイベントログ (SEL) に似ています。

エラーセクションの表には、さまざまな LCD 画面に表示されるエラーメッセージと警告メッセージ、および考えられる原因をリストにします。角かっこで囲まれたテキスト (< >) は、テキストにバリエーションがあることを示します。

LCD のステータス情報には、シャーシ内のモジュールに関する詳細説明が含まれています。このセクションの表では、各コンポーネントに表示される情報について説明します。

## LCD エラーメッセージ

表 13-3 CMC ステータス画面

重大度	メッセージ	原因
重要	CMC <番号> バッテリーが故障しました。	CMC CMOS バッテリーが存在しないか、電圧がありません。
重要	CMC <番号> LAN のハートビートが失われました。	CMC の NIC の接続が外されたか、または接続されていません。
警告	スロット <番号> の iDRAC と CMC との間でファームウェアまたはソフトウェアの互換性の不一致が検出されました。	1 つまたは複数の機能をサポートするためのファームウェアが、2 つのデバイス間で一致しません。
警告	スロット <番号> のシステム BIOS と CMC との間でファームウェアまたはソフトウェアの互換性の不一致が検出されました。	1 つまたは複数の機能をサポートするためのファームウェアが、2 つのデバイス間で一致しません。
警告	CMC 1 と CMC 2 との間でファームウェアまたはソフトウェアの互換性の不一致が検出されました。	1 つまたは複数の機能をサポートするためのファームウェアが、2 つのデバイス間で一致しません。

表 13-4 エンクロージャ/シャーシステータス画面

重大度	メッセージ	原因
重要	ファン < 番号 > が削除されました。	このファンはエンクロージャ/シャーシを正しく冷却するために必要です。
警告	電源冗長性が劣化しています。	1 個または複数の PSU が故障したか、取り出されたため、システムが完全な PSU 冗長性をサポートできなくなりました。
重要	電源冗長性が失われました。	1 個または複数の PSU が故障したか、取り出されたため、システムの冗長性がなくなりました。
重要	電源装置は非冗長です。正常な動作を維持するのに必要なリソースが不足しています。	1 個または複数の PSU が故障したか、取り出されたため、正常な動作を維持するのに必要な電力がシステムにありません。サーバーの電源が切れる可能性があります。
警告	コントロールパネルの周辺温度が、警告しきい値の上限を超えています。	シャーシ/エンクロージャの吸気温度が警告しきい値を超えました。
重要	コントロールパネルの周辺温度が、警告しきい値の上限を超えています。	シャーシ/エンクロージャの吸気温度が警告しきい値を超えました。
重要	CMC の冗長性が失われました。	CMC が冗長性がなくなりました。スタンバイの CMC が取り外された場合に発生します。
重要	すべてのイベントログが無効になりました。	シャーシ/エンクロージャは、イベントをログに保存できません。これは通常、コントロールパネルまたはコントロールパネルケーブルに問題があることを示します。
警告	ログが満杯です。	あと 1 つエントリを追加すると CEL (ハードウェアログ) が満杯になることを、シャーシが検出しました。
警告	ログがほとんど満杯です。	シャーシイベントログは 75% 満杯です。



表 13-5 ファンステータス画面

重大度	メッセージ	原因
重要	ファン<番号>の RPM が、重大なしきい値の下限を下回って稼働しています。	指定したファンの速度が遅いため、システムに十分な冷却を提供できません。
重要	ファン<番号>の RPM が、重大なしきい値の上限を上回って稼働しています。	指定されたファンの速度が速すぎます。これは通常、ファンのブレードが損傷したことが原因です。

表 13-6 IOM ステータス画面

重大度	メッセージ	原因
警告	I/O モジュール<番号>でファブリックの不一致が検出されました。	この I/O モジュールのファブリックが、サーバーまたは冗長 I/O モジュールのファブリックと一致しません。
警告	I/O モジュール<番号>でリンクチューニング障害が検出されました。	1 つまたは複数のサーバーの NIC を正しく使用するために、この I/O モジュールを設定することができませんでした。
重要	I/O モジュール<番号>で障害が検出されました。	I/O モジュールにエラーがあります。I/O モジュールがサーマルトリップした場合でも、同じエラーが起こることがあります。

表 13-7 iKVM ステータス画面

重大度	メッセージ	原因
警告	ローカル KVM 用にコンソールが使用できません。	ファームウェアの破損などの小さいエラー。
重要	ローカル KVM がどのホストにも見つかありません。	USB ホスト列挙エラーです。
重要	OSCAR (オンスクリーン表示) がローカル KVM で機能しません。	OSCAR の障害です。
リカバリ不可	ローカル KVM が機能せず、電源がオフになっています。	シリアル RIP エラーまたは USB ホストチップエラー。

**表 13-8 PSU ステータス画面**

重大度	メッセージ	原因
重要	電源装置 <番号> が故障しました。	PSU に障害が発生しました。
重要	電源装置 <番号> の電源入力が失われました。	AC 電源の喪失または AC コードが抜かれています。
警告	電源装置 <番号> が 110 ボルトで動作しており、ブレーカーの故障を引き起こす可能性があります。	電源装置が 110 ボルトの電源に接続されています。

**表 13-9 サーバステータス画面**

重大度	メッセージ	原因
警告	システムボードの周辺温度が、警告しきい値の下限を下回っています。	サーバー温度が低下しています。
重要	システムボードの周辺温度が、重大しきい値の下限を下回っています。	サーバー温度が低下しています。
警告	システム基板の周辺温度が、警告しきい値の上限を超えています。	サーバー温度が上昇しています。
重要	システム基板の周辺温度が、重大しきい値の上限を超えています。	サーバー温度が著しく上昇しています。
重要。	システム基板の電流ラッチの電流が許容範囲外です。	電流がエラーしきい値を超えました。
重要	システムボードのバッテリーに問題があります。	CMOS バッテリーが不在か、電圧がありません。
警告	ストレージバッテリーの残量が低下しています。	ROMB バッテリーの残量が低下しています。
重要	ストレージバッテリーに問題があります。	CMOS バッテリーが不在か、電圧がありません。
重要	CPU <番号> <電圧センサー名> 電圧が許容範囲外です。	
重要	システム基板 <電圧センサー名> 電圧が許容範囲外です。	
重要	メザニンカード <番号> <電圧センサー名> 電圧が許容範囲外です。	
重要	ストレージ <電圧センサー名> 電圧が許容範囲外です。	

表 13-9 サーバーステータス画面 (続き)

重大度	メッセージ	原因
重要	CPU < 番号 > で内部エラーが発生しました (IERR)。	CPU エラー。
重要	CPU < 番号 > でサーマルトリップ (過熱) イベントが発生しました。	CPU が過熱状態です。
重要	CPU < 番号 > の構成がサポートされません。	プロセッサの種類または搭載場所が間違っています。
重要	CPU < 番号 > が存在しません。	必要な CPU が見つからないか、不在です。
重要	メザニン B < スロット番号 > ステータス: メザニン B < スロット番号 > のアドインカードセンサー、取り付けエラーがアサートされました。	IO ファブリックに間違ったメザニンカードが取り付けられています。
重要	メザニン C < スロット番号 > ステータス: メザニン C < スロット番号 > のアドインカードセンサー、取り付けエラーがアサートされました。	IO ファブリックに間違ったメザニンカードが取り付けられています。
重要	ドライブ < 番号 > が取り外されました。	ストレージドライブが取り外されました。
重要	ドライブ < 番号 > で問題が検出されました。	ストレージドライブに障害が発生しました。
重要	システム基板のフェールセーフ電圧が許容範囲外です。	システム基板の電圧が異常レベルに達した場合に、このイベントが生成されます。
重要	ウォッチドッグタイマーが期限切れです。	iDRAC ウォッチドッグタイマーが期限切れですが、処置が設定されていません。
重要	ウォッチドッグタイマーがシステムをリセットします。	iDRAC ウォッチドッグは、システムのクラッシュ (ホストからの応答がないためのタイマー期限切れ) を検知し、再起動の処置が設定されています。

表 13-9 サーバステータス画面（続き）

重大度	メッセージ	原因
重要	ウォッチドッグタイマーがシステムの電源を切断しました。	iDRAC ウォッチドッグは、システムのクラッシュ（ホストからの応答がないためのタイマー期限切れ）を検知し、電源オフの処置が設定されています。
重要	ウォッチドッグタイマーがシステムの電源を切断し、再投入しました。	iDRAC ウォッチドッグは、システムのクラッシュ（ホストからの応答がないためのタイマー期限切れ）を検知し、電源入れ直しの処置が設定されています。
重要	ログが満杯です。	SEL デバイスは、SEL がいっぱいになる前に 1 つしかエントリを追加できないことを検出しました。
警告	<場所> のメモリデバイスで、訂正可能な永続的エラーが検出されました。	
警告	<場所> のメモリデバイスで、訂正可能な永続的エラーの発生率が増加しました。	修正可能な ECC エラーが重大な率に到達しました。
重要	<場所> のメモリデバイスで、マルチビットメモリエラーが検出されました。	訂正不能 ECC エラーが検知されました。
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、I/O チャンネルチェック NMI が検出されました。	I/O チャンネルに重要な割り込みが発生しています。
重要	スロット <番号> のコンポーネントで、I/O チャンネルチェック NMI が検出されました。	I/O チャンネルに重要な割り込みが発生しています。
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、PCI パリティエラーが検出されました。	PCI バスにパリティエラーが検知されました。
重要	スロット <番号> のコンポーネントで、PCI パリティエラーが検出されました。	PCI バスにパリティエラーが検知されました。

表 13-9 サーバーステータス画面（続き）

重大度	メッセージ	原因
重要	バス < 番号 > デバイス < 番号 > 機能 < 番号 > のコンポーネントで、PCI システムエラーが検出されました。	デバイスで PCI エラーが検出されました。
重要	スロット < 番号 > のコンポーネントで、PCI システムエラーが検出されました。	デバイスで PCI エラーが検出されました。
重要	< 場所 > のメモリデバイスで、訂正可能な永続的エラーのログインが無効になりました。	あるメモリデバイスについてログされるシングルビットエラーの数が過剰になった場合、シングルビットエラーのログが無効になります。
重要	すべてのイベントログが無効になりました。	
リカバリ不可	CPU プロトコルエラーが検出されました。	プロセッサプロトコルがリカバリ不可の状態になりました。
リカバリ不可	CPU バスパリティエラーが検出されました。	プロセッサバス PERR がリカバリ不可の状態になりました。
リカバリ不可	CPU 初期化エラーが検出されました。	プロセッサ初期化がリカバリ不可の状態になりました。
リカバリ不可	CPU マシンチェックが検出されました。	プロセッサマシンチェックがリカバリ不可の状態になりました。
重要	メモリの冗長性が失われました。	
重要	バス < 番号 > デバイス < 番号 > 機能 < 番号 > のコンポーネントで、バスの致命的なエラーが検出されました。	PCIe バスに致命的なエラーが検知されました。
重要	バス < 番号 > デバイス < 番号 > 機能 < 番号 > のコンポーネントで、ソフトウェア NMI が検出されました。	チップエラーが検出されました。
重要	バス < 番号 > デバイス < 番号 > 機能 < 番号 > のコンポーネントで、仮想 MAC アドレスのプログラムに失敗しました。	このデバイスにはフレックスアドレスをプログラムできます。

表 13-9 サーバーステータス画面（続き）

重大度	メッセージ	原因
重要	メザニンカード <番号> のデバイスオプション ROM が、リンクチューニングまたは FlexAddress のサポートに失敗しました。	オプション ROM がフレックスアドレスまたはリンクチューニングをサポートしていません。
重要	iDRAC からのリンクチューニングまたはフレックスアドレスデータの取得に失敗しました。	



**メモ：** その他のサーバー関連の LCD メッセージに関する情報は、『Server User Guide』を参照してください。

## LCD モジュールとサーバーステータス情報

このセクションの表では、シャーシ内のコンポーネントタイプごとにフロントパネル LCD に表示されるステータス項目について説明します。

表 13-10 CMC ステータス

項目	説明
例：CMC1、CMC2	名前 / 場所
エラーなし	何もエラーが発生していない場合は「エラーなし」が表示され、エラーがある場合はエラーメッセージのリストが表示されます。
ファームウェアバージョン	アクティブな CMC にのみ表示されます。スタンバイ CMC について <b>スタンバイ</b> と表示します。
IP4 <有効、無効>	現在の IPv4 の有効状態を表示します（アクティブな CMC にのみ表示）。
IP4 アドレス：<アドレス、取得中>	IPv4 が有効な場合のみ表示します（アクティブな CMC にのみ表示）。
IP6 <有効、無効>	現在の IPv6 の有効状態を表示します（アクティブな CMC にのみ表示）。
IP6 ローカルアドレス：<アドレス>	IPv6 が有効な場合のみ表示します（アクティブな CMC にのみ表示）。
IP6 グローバルアドレス：<アドレス>	IPv6 が有効な場合のみ表示します（アクティブな CMC にのみ表示）。

表 13-11 シャーシ/エンクロージャステータス

項目	説明
ユーザー定義名	例:「Dell ラックシステム」。これは CMC CLI または Web GUI から設定できます。
エラーメッセージ	エラーがない場合は、 <b>エラーなし</b> が表示されます。それ以外の場合は、エラーメッセージが重大、警告の順で表示されます。
モデル番号	例「PowerEdgeM1000」。
Power Consumption (電力消費)	現在の電力消費量 (ワット単位)。
ピーク電力	ピーク電力消費量 (ワット)。
最小電力	最小電力消費量 (ワット)。
周辺温度	現在の周辺温度 (摂氏)。
サービスタグ	出荷時に割り当てられたサービスタグ
CMC 冗長性モード	非冗長または冗長。
PSU 冗長性モード	非冗長、AC 冗長、または DC 冗長。

表 13-12 ファンスステータス

項目	説明
名前 / 場所	例: ファン 1、ファン 2 など
エラーメッセージ	エラーがない場合は、「エラーなし」が表示されます。それ以外の場合は、エラーメッセージが重大、警告の順で表示されます。
RPM	現在のファン速度 (RPM)。

表 13-13 PSU ステータス

項目	説明
名前 / 場所	例: PSU1、PSU2 など
エラーメッセージ	エラーがない場合は、「エラーなし」が表示されます。それ以外の場合は、エラーメッセージが重大、警告の順で表示されます。
状態	オフライン、オンライン、またはスタンバイ。
最大ワット数	PSU がシステムに供給できる最大ワット数。

**表 13-14 IOM ステータス**

項目	説明
名前 / 場所	例 : IOM A1、IOM B1。など
エラーメッセージ	エラーがない場合は、「エラーなし」が表示されます。それ以外の場合は、エラーメッセージが重大、警告の順で表示されます。
状態	オフまたはオン。
モデル	IOM のモデル。
ファブリックタイプ	ネットワークタイプ。
IP アドレス	IOM が オンの場合にのみ表示されます。パススルータイプ IOM の場合は、この値はゼロになります。
サービスタグ	出荷時に割り当てられたサービスタグ

**表 13-15 iKVM ステータス**

項目	説明
Name (名前)	iKVM。
エラーなし	エラーがない場合は、「 <b>エラーなし</b> 」が表示されます。それ以外の場合は、エラーメッセージがリスト表示されます。最初に重大なエラー、次に警告の順でリストされます。詳細については、「LCD エラーメッセージ」を参照してください。
状態	オフまたはオン。
モデル / メーカー	iKVM モデルの説明。
サービスタグ	出荷時に割り当てられたサービスタグ
パーツ番号	製造元のパーツ番号。
ファームウェアバージョン	iKVM ファームウェアバージョン。
ハードウェアバージョン	iKVM ハードウェアバージョン。
<b>メモ :</b> この情報は動的にアップデートされます	



表 13-16 サーバステータス

項目	説明
例：サーバー 1、サーバー 2、 など。	名前 / 場所
エラーなし	エラーがない場合は、「 <b>エラーなし</b> 」が表示されます。それ以外の場合は、エラーメッセージがリスト表示されます。最初に重大なエラー、次に警告の順でリストされます。詳細については、「LCD エラーメッセージ」を参照してください。
スロット名	シャーシスロット名。たとえば、 <b>SLOT-01</b> です。 <b>メモ</b> ：この表は、CMC CLI または Web GUI を使用して設定できます。
Name (名前)	サーバーの名前で、ユーザーが <b>Dell OpenManage</b> を使用して設定することが可能です。この名前は、iDRAC の起動が完了し、サーバーがこの機能をサポートする場合のみ表示されます。そうでない場合は、iDRAC のブートメッセージが表示されます。
モデル番号	iDRAC の起動が完了すると表示されます。
サービスタグ	iDRAC の起動が完了すると表示されます。
BIOS バージョン	サーバー BIOS ファームウェアのバージョン
最終の POST コード	最終のサーバー BIOS の POST コードのメッセージ文字列を表示します。
iDRAC ファームウェアバージョン	iDRAC の起動が完了すると表示されます。 <b>メモ</b> ：iDRAC バージョン 1.01 は 1.1 と表示されま す。iDRAC バージョン 1.10 はありません。
IP4 <有効、無効>	現在の IPv4 の有効状態を表示します。
IP4 アドレス：<アドレス、取得中>	IPv4 が有効な場合のみ表示します。
IP6 <有効、無効>	iDRAC が IPv6 をサポートする場合のみ表示します。 現在の IPv6 の有効状態を表示します。
IP6 ローカルアドレス：<アドレス>	iDRAC が IPv6 をサポートし、かつ IPv6 が有効な場合のみ表示します。
IP6 グローバルアドレス：<アドレス>	iDRAC が IPv6 をサポートし、かつ IPv6 が有効な場合のみ表示します。
ファブリック上で有効なフレックスアドレス	この機能がインストールされている場合に表示されます。このサーバーで有効なファブリックをリストします（例：A、B、C）

表 13-16 の情報は動的にアップデートされます。サーバーがこの機能をサポートしていない場合は、次の情報は表示されません。サポートしている場合は、サーバー管理者のオプションは次のとおりです。

- オプション「なし」= LCD にはいかなる文字列も表示されません。
- オプション「デフォルト」= 設定しても効果はありません。
- オプション「カスタム」= そのサーバーの名前を文字列で入力できます。

この情報は iDRAC の起動が完了した場合のみ表示されます。この機能の詳細については、『RACADM Command Line Reference Guide for iDRAC7 and CMC』を参照してください。

# 索引

## A

ACI, 329

Active Directory, 243

CMC へのアクセス設定, 254

CMC ユーザーの追加, 261

オブジェクト, 250

スキーマ拡張, 249

拡張スキーマ, 254

証明書の設定および管理, 157

標準スキーマでの使用, 244

## C

CMC

インストール, 29

セットアップ, 29

ファームウェアのダウンロード  
, 47

ログ, 391

機能セット, 19

冗長環境, 51

設定, 263

設定ファイルの作成, 91

CMC VLAN, 82

CMC のインストール, 29

CMC のセットアップ, 29

CMC の機能セット, 19

connect コマンド

CMC コマンドライン接続, 61

## D

DHCP の有効化または無効化  
, 80

## F

FlexAddress, 223

CLI を使用したステータス表示  
, 229

CLI を使用した設定, 228

Linux 設定, 229

Wake-On-LAN, 230

トラブルシューティング, 230

ライセンス契約, 235

無効化, 227

有効化, 224

有効化の検証, 225

FlexAddress Plus の使用, 242

FlexAddress Plus の有効化  
, 241

## I

I/O ファブリック, 353

iDRAC

ファームウェアの回復, 188

iKVM, 327

## L

LDC パネル  
CMC の設定, 47

## M

Microsoft Active  
Directory, 243

## O

OSCAR, 327

## R

RAC  
リモートアクセス接続を参照  
, 23

## RACADM

Linux 管理ステーションからの  
アンインストール, 36

racadm ユーティリティ  
ネットワークプロパティの設定  
, 77  
構文解析規則, 93

Red Hat Enterprise Linux  
シリアルコンソールリダイレク  
トの設定, 63

## S

SNMP アラート  
追加および設定, 370

SNMP アラートの設定, 370

## T

telnet コンソール  
使用, 56

## W

WS- 管理, 24

## Z

よくあるお問い合わせ  
CMC を Active Directory で  
使用, 267  
リモートシステムの管理と回復  
, 219, 239

アナログコンソールインタ  
フェース, 327

アラート  
トラブルシューティング, 407

ウェブインタフェース  
E- メールアラートの設定, 375  
アクセス, 99

ウェブブラウザ  
設定, 36  
対応ブラウザ, 24

コマンドラインコンソール  
特徴, 55

サーバー証明書  
アップロード, 171

- 表示, 172
- サービス
  - 設定, 173
- シリアルコンソール
  - 使用, 56
- シングルサインオン, 270
- スナップイン
  - Dell 拡張のインストール, 260
- スロット名
  - 編集, 123
  - 名前付けの規則, 123
- セキュアソケットレイヤ (SSL)
  - 説明, 167
- セキュリティ
  - SSL とデジタル証明書を使用した, 167
- ネットワーク LAN の設定, 78
- ネットワークプロパティ
  - racadm を使った設定, 77
  - 手動設定, 77
- ハードウェアログ, 388
- ハードウェア仕様, 22
- パスワード
  - ジャンパ位置のリセット, 405
  - 忘れたとき, 403
- ファームウェア
  - ダウンロード, 47
  - 管理, 181
  - 更新、CMC, 183
  - 更新、iKVM, 185
  - 更新、IOM 基盤デバイス, 186
  - 更新、サーバー iDRAC, 187
- ファブリック管理, 353
- プロキシサーバー, 37
- リモート RACADM
  - 設定, 46
- リモートアクセス接続 (RAC)
  - , 23
- ログ
  - CMC, 391
  - ハードウェア, 388
- 管理ステーション
  - 端末エミュレーションの設定, 59
- 管理下システム
  - ローカルシリアルポートを通じたアクセス, 56
- 機能カード, 225
- 現在の IPv4 ネットワーク設定の表示, 77
- 現在の IPv6 ネットワーク設定の表示, 77
- 構文解析規則, 93
- 仕様
  - ハードウェア, 22
- 証明書
  - Active Directory, 157
  - SSL とデジタル, 167
  - サーバー証明書のアップロード, 171
  - サーバー証明書の表示, 172
- 証明書署名要求 (CSR)
  - 新しい証明書の生成, 168
  - 説明, 167

冗長環境 , 51

設定

CMC リモート RACADM, 46

LCD パネルから CMC, 47

リモート RACADM, 46

電力バジェット , 47

設定ファイル

作成 , 91

節電 , 295

追加

SNMP アラート , 370

電力バジェット

設定 , 47

汎用 Lightweight Directory  
Access Protocol Services

の設定と管理 , 163

標準スキーマ

Active Directory との使用  
, 244