



# XClarity Controller 3

## ユーザーズ・ガイド



注：この情報を使用する前に、[177 ページの付録 B「注記」](#)に記載されている一般情報をお読みください。

第 1 版 (2024 年 10 月)

© Copyright Lenovo 2024.

制限付き権利に関する通知: データまたはソフトウェアが GSA (米国一般調達局) 契約に準じて提供される場合、使用、複製、または開示は契約番号 GS-35F-05925 に規定された制限に従うものとします。

# 目次

目次	i	セキュリティー・モード	37
第 1 章 概要	1	セキュリティー・モードの切り替え	41
XClarity Controller 標準および Premier レベルの機能	2	SSL の概要	41
XClarity Controller 標準レベルの機能	2	SSL 証明書の処理	42
XClarity Controller Premier レベルの機能	5	SSL 証明書管理	42
XClarity Controller のアップグレード	6	セキュア・シェル・サーバーの構成	43
Web ブラウザーとオペレーティング・システムの要件	6	キーボード・コントローラー・スタイル (KCS) 経由の IPMI のアクセス	43
複数言語サポート	7	システム・ファームウェアのレベル・ダウンの禁止	44
MIB 概要	7	セキュリティー鍵管理 (SKM) の構成	44
本書で使用される注記	8	Security password manager	44
第 2 章 XClarity Controller Web インターフェースの開始と使用	9	拡張監査ログ	44
XClarity Controller Web インターフェースへのアクセス	9	ユーザー・アカウントあたりの同時ログインの制限	45
XClarity Provisioning Manager による XClarity Controller のネットワーク接続のセットアップ	10	システム・ガード	45
XClarity Controller へのログイン	12	TLS バージョン・サポート	46
Web インターフェースでの XClarity Controller 機能の説明	13	BMC 構成のバックアップと復元	46
第 3 章 XClarity Controller の構成	17	BMC 構成のバックアップ	46
ユーザー・アカウント/LDAP の構成	17	BMC 構成の復元	47
ユーザー認証方式	17	BMC の出荷時のデフォルト値へのリセット	47
新しい役割の作成	18	XClarity Controller の再起動	48
新規ユーザー・アカウントの作成	19	第 4 章 サーバー状況の監視	49
ユーザー・アカウントの削除	21	ヘルス・サマリー/アクティブ・システム・イベントの表示	49
認証用にハッシュド・パスワードを使用	21	システム情報の表示	51
グローバル・ログイン設定の構成	23	システム使用率の表示	52
LDAP の構成	25	イベント・ログの表示	53
ネットワーク・プロトコルの構成	29	監査ログの表示	54
イーサネット設定の構成	29	メンテナンス履歴の表示	54
DNS の構成	31	アラート受信者の構成	55
DDNS の構成	32	第 5 章 サーバーの構成	57
Ethernet over USB の構成	32	アダプター情報および構成設定の表示	57
SNMP の構成	33	システムのブート・モードおよびブート順序の構成	57
IPMI ネットワーク・アクセスの有効化	34	一回限りのブートの構成	58
IPMI コマンドを使用したネットワーク設定の構成	34	サーバー電源の管理	58
サービスの有効化とポートの割り当て	35	電源の冗長性の構成	59
アクセス制限の構成	35	電源キャッピング・ポリシーの構成	59
前面パネル USB ポートから管理への構成	36	電源復元ポリシーの構成	60
セキュリティー設定の構成	37	電源操作	60
セキュリティー・ダッシュボード	37	IPMI コマンドを使用した電源消費量の管理および監視	61
		サービス・データ・ログのダウンロード	63
		サーバーのプロパティ	64
		ロケーションと連絡先の設定	64

サーバー・タイムアウトの設定	65
侵入警告メッセージ	65
ソリューション・サービス	65
XClarity Controller の日付と時刻の設定	65
D3 V2 シャーシの構成	66

## 第 6 章 . リモート・コンソール機能 . . . 69

リモート・コンソール機能の有効化	70
リモート電源制御	70
リモート・コンソールの画面キャプチャー	70
リモート・コンソールのキーボード・サポート	71
リモート・コンソールの画面モード	71
メディアのマウント方法	71
メディアのマウント・エラーに関する問題	75
リモート・コンソール・セッションの終了	76

## 第 7 章 . ストレージの構成 . . . . . 77

ストレージの詳細	77
RAID セットアップ	77
仮想ドライブの表示および構成	77
ストレージ・インベントリーの表示および構成	78

## 第 8 章 . サーバー・ファームウェアの更新 . . . . . 81

ファームウェア更新の概要	81
システム、アダプター、および PSU ファームウェア更新	82
リポジトリからの更新	82

## 第 9 章 . ライセンス管理 . . . . . 85

アクティベーション・キーのインストール	85
アクティベーション・キーの削除	86
アクティベーション・キーのエクスポート	86

## 第 10 章 . コマンド・ライン・インターフェース . . . . . 87

コマンド・ライン・インターフェースへのアクセス	87
コマンド・ライン・セッションへのログイン	87
Serial-to-SSH リダイレクトの構成	87
コマンド構文	88
機能および制限	88
アルファベット順のコマンド・リスト	89
ユーティリティー・コマンド	91
exit コマンド	91
help コマンド	91
history コマンド	91
モニター・コマンド	91
clearlog コマンド	92
fans コマンド	92
mhlog コマンド	92

led コマンド	93
readlog コマンド	95
servicelog コマンド	96
syshealth コマンド	97
temps コマンド	98
volts コマンド	99
vpd コマンド	99
サーバーの電源および再起動制御コマンド	100
power コマンド	100
reset コマンド	101
fuelg コマンド	102
pxeboot コマンド	103
構成コマンド	103
accseccfg コマンド	103
asu コマンド	104
backup コマンド	107
dhcpinfo コマンド	108
dns コマンド	108
encaps コマンド	109
ethtousb コマンド	110
firewall コマンド	110
hashpw コマンド	112
ifconfig コマンド	112
keycfg コマンド	114
ldap コマンド	115
ntp コマンド	117
portcontrol コマンド	117
ports コマンド	118
rdmount コマンド	119
restore コマンド	120
roles コマンド	120
rtd コマンド	121
seccfg コマンド	122
securityinfo コマンド	122
securitymode コマンド	123
set コマンド	123
snmp コマンド	123
snmpalerts コマンド	126
sshcfg コマンド	127
sslcfg コマンド	127
syslock コマンド	130
thermal コマンド	131
tls コマンド	132
trespass コマンド	132
uefipw コマンド	133
usbeth コマンド	133
users コマンド	134
IMM 制御コマンド	138
batch コマンド	138
clock コマンド	138

info コマンド . . . . .	139
sreset コマンド . . . . .	140
エージェントレス・コマンド . . . . .	140
storage コマンド . . . . .	140
adapter コマンド . . . . .	149
サポート・コマンド . . . . .	150
dbgshbmc コマンド . . . . .	151

## 第 11 章 . IPMI インターフェース . . . 153

IPMI を使用した XClarity Controller の管理 . . . . .	153
IPMItool の使用 . . . . .	153
OEM パラメーターを使用した IPMI コマンド . . . . .	154
LAN 構成パラメーターの取得 / 設定 . . . . .	154
OEM IPMI コマンド . . . . .	164

## 付録 A. ヘルプおよび技術サポートの 入手 . . . . . 173

依頼する前に . . . . .	173
サービス・データの収集 . . . . .	174
サポートへのお問い合わせ . . . . .	175

## 付録 B. 注記 . . . . . 177

商標 . . . . .	178
重要事項 . . . . .	178
粒子汚染 . . . . .	178
通信規制の注記 . . . . .	179
電波障害自主規制特記事項 . . . . .	179
台湾 BSMI RoHS 宣言 . . . . .	180
台湾の輸出入お問い合わせ先情報 . . . . .	180

## 索引 . . . . . 183



---

# 第 1 章 概要

Lenovo XClarity Controller 3 (XCC3) は、Lenovo ThinkSystem サーバー向けの次世代の管理コントローラーです。

このコントローラーは、サービス・プロセッサ機能、Super I/O、ビデオ・コントローラー、およびリモート・プレゼンス機能をサーバーのシステム・ボード上の単一のチップに一元化します。以下のような機能が提供されます。

- システム管理のための、専用あるいは共有のイーサネット接続の選択。
- HTML5 のサポート
- XClarity Mobile を経由したアクセスのサポート
- XClarity Provisioning Manager
- XClarity Essentials または XClarity Controller CLI を使用したリモート構成。
- アプリケーションおよびツールがローカルでもリモートでも XClarity Controller にアクセスできる機能。
- 拡張リモート・プレゼンス機能。
- 追加の Web 関連サービスおよびソフトウェア・アプリケーションにおける REST API (Redfish スキーマ) のサポート。

注：

- XClarity Controller は現在、Redfish スケーラブル・プラットフォーム管理 API 規格 1.16.0 およびスキーマ 2022.2 をサポートします
- XClarity Controller Web インターフェースで、BMC は、XCC を参照するのに使用されます。
- 一部の ThinkSystem サーバーでは、専用システム管理ネットワーク・ポートが使用できない場合があります。これらのサーバーでは、XClarity Controller へのアクセスはサーバーのオペレーティング・システムと共用するネットワーク・ポート経由のみで可能です。

この資料は、ThinkSystem サーバーに取り付けられている XClarity Controller の機能の使用方法を説明しています。XClarity Controller は XClarity Provisioning Manager および UEFI と連動して、ThinkSystem サーバーのシステム管理機能を提供します。

ファームウェア更新を確認するには、以下のステップを実行してください。

注：Support Portal に初めてアクセスする際、ご使用のサーバーの製品カテゴリー、製品ファミリー、および型式番号を選択する必要があります。次回、Support Portal にアクセスすると、最初に選択した製品が Web サイトによってプリロードされ、ご使用の製品用のリンクのみが表示されます。製品リストを変更するか、製品リストに追加するには、「**Manage my product lists (My プロダクト・リストの管理)**」リンクをクリックします。Web サイトは定期的に更新されます。ファームウェアと資料を検索する手順は、本書で説明する手順とは多少異なる場合があります。

1. <http://datacentersupport.lenovo.com> に進みます。
2. 「Support (サポート)」の下で、「Data Center (データセンター)」を選択します。
3. 内容がロードされたら、「Servers (サーバー)」を選択します。
4. 「Select Series (シリーズを選択)」の下で特定のサーバー・ハードウェア・シリーズを選択し、次に「Select SubSeries (サブシリーズを選択)」で特定のサーバー製品のサブシリーズを選択します。最後に、「Select Machine Type (マシンタイプを選択)」で特定のマシン・タイプを選択します。

---

## XClarity Controller 標準および Premier レベルの機能

XClarity Controller では、標準および Premier レベルの XClarity Controller 機能が提供されています。ご使用のサーバーに取り付けられている XClarity Controller のレベルについて詳しくは、ご使用のサーバーの資料を参照してください。以下の機能は、すべてのレベルで提供されます。

- ご使用のサーバーの 24 時間リモート・アクセスと管理
- 管理対象サーバーの状況に依存しないリモート管理
- ハードウェアおよびオペレーティング・システムのリモート制御

## XClarity Controller 標準レベルの機能

以下は、XClarity Controller 標準レベル機能のリストです。

### 業界標準管理インターフェース

- IPMI 2.0 インターフェース
- Redfish
- DCMI 1.5
- SNMPv3

### その他の管理インターフェース

- Web
- SSH CLI
- 前面パネル USB - モバイル・デバイス経由仮想オペレーター・パネル

### 電源/リセットの制御

- 電源オン
- ハード/ソフト・シャットダウン
- 電源制御のスケジューリング
- システム・リセット
- ブート順序制御

### イベント・ログ

- IPMI SEL
- 人間が読み取れるログ
- 監査ログ
- ミニ・ログ

### 環境監視

- エージェントなしの監視
- センサー監視
- ファンの制御
- LED 制御
- チップ・セット・エラー (Caterr、IERR など。)
- システム・ヘルス標識



- I/O アダプターの OOB パフォーマンス監視
- インベントリーの表示とエクスポート

## RAS

- 仮想 NMI
- 自動ファームウェア・リカバリー
- バックアップ・ファームウェアの自動プロモーション
- POST ウォッチドッグ
- OS ローター・ウォッチドッグ
- OS ウォッチドッグ
- ブルー・スクリーン・キャプチャー (OS 障害、FFDC 内)
- 組み込み診断ツール
- コール・ホーム

## ネットワーク構成

- IPv4
- IPv6
- IP アドレス、サブネット・マスク、ゲートウェイ
- IP アドレス割り当てモード
- ホスト名
- プログラマブル MAC アドレス
- デュアル MAC 選択 (サーバー・ハードウェアでサポートされている場合)
- ネットワーク・ポート再割り当て
- VLAN タグ付け

## ネットワーク・プロトコル

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SSL
- SSH
- SMTP
- LDAP クライアント
- NTP
- SSDP
- LLDP

## アラート

- PET Traps
- SNMP v1、v2c、および v3 トラップ

- メール
- Redfish 通知サブスクリプション

#### リモート・プレゼンス

- カード上のリモート・ディスク (RDOC)

#### シリアル・リダイレクト

- IPMI SOL
- シリアル・ポート構成 (権限と速度を含む)
- シリアル・コンソール・バッファ (120 秒)

#### セキュリティ

- 非ホスト・プロセッサ CRTM
- デジタル署名済みファームウェア更新
- 役割ベースのアクセス制御 (RBAC)
- ローカル・ユーザー・アカウント
- LDAP/AD ユーザー・アカウント
- ファームウェアのロールバックの保護
- NIST SP 800-131a
- シャーシ侵入検出 (サーバー・ハードウェアによりサポートされている場合)
- 有効になっているセキュアな暗号化プロトコルのみ
- 構成の変更とサーバー操作の監査ロギング
- 公開鍵 (PK) 認証
- システムのリタイア/再利用 (RTD/ERTD)
- PFR サポート
- FIPS 140-3
- セキュリティー・モードとセキュリティー・ダッシュボード
- セキュア・パスワード・ストレージ

#### 電源管理

- リアルタイム電源メーター

#### Features on Demand

- アクティベーション・キー・リポジトリ

#### デプロイメントと構成

- リモート構成
- OS パススルー
- 組み込みデプロイメントと構成ツールおよびドライバー・パック
- 構成のバックアップおよび復元
- 拡張 RDOC サイズ (MicroSD カード付き)
- 構成可能な温度プロファイル

#### ファームウェア更新

- エージェントを使用しない更新
- リモート更新

## XClarity Controller Premier レベルの機能

以下は、XClarity Controller Premier レベルの機能のリストです。

[2 ページの「XClarity Controller 標準レベルの機能」](#)のすべて。

### イベント・ログ

- コンポーネントの交換ログ

### RAS

- ブート・キャプチャー
- クラッシュ・ビデオ・キャプチャー

### アラート

- Syslog

### リモート・プレゼンス

- リモート KVM
- ローカル・クライアント ISO/IMG ファイルのマウント
- 品質/帯域幅制御
- リモート ISO/IMG ファイルの http、Samba、および NFS での仮想メディア・マウンティング

### シリアル・リダイレクト

- SSH-CLI 経由のシリアル・リダイレクト

### セキュリティ

- シングル・サインオン
- Security Key Lifecycle Manager (SKLM/KMIP)
- IP アドレスのブロックング
- エンタープライズ・ストリクト・セキュリティ・モード (CNSA 準拠)
- システム・ガード

### 電源管理

- 電源キャッピング
- OOB のパフォーマンスの監視 - システム・パフォーマンスのメトリック
- リアルタイム電源グラフィックス
- 温度グラフィックス

### デプロイメントと構成

- リモート OS デプロイメント

### ファームウェア更新

- リポジトリとの同期

- システム・パック・ファームウェア・バンドルの更新
- MicroSD カードのローカル・リポジトリからのファームウェア・ロールバック

## XClarity Controller のアップグレード

ご使用のサーバーに標準レベルの XClarity Controller ファームウェア機能が付属している場合は、サーバーの XClarity Controller 機能をアップグレードできる可能性があります。使用可能なアップグレード・レベルおよびオーダーの方法については、[85 ページの第 9 章「ライセンス管理」](#)を参照してください。

---

## Web ブラウザーとオペレーティング・システムの要件

サーバーでサポートされているブラウザー、暗号スイートおよびオペレーティング・システムのリストを表示するには、このトピックの情報を使用します。

XClarity Controller Web インターフェースには、次の Web ブラウザーのいずれか 1 つが必要です。

- Chrome 64.0 以上 (リモート・コンソールには 64.0 以上)
- Firefox ESR 78.0 以上
- Microsoft Edge 79.0 以上
- Safari 12.0 以上 (iOS 7 以上および OS X)

注：リモート・コンソール機能は、モバイル・デバイスのオペレーティング・システムのブラウザーからはサポートされていません。

前にリストしたブラウザーは、XClarity Controller ファームウェアで現在サポートされているものと一致します。XClarity Controller ファームウェアは定期的に拡張され、他のブラウザーのサポートが組み込まれる可能性があります。

XClarity Controller のファームウェアのバージョンに応じて、Web ブラウザーに対するサポートが、このセクションにリストしたブラウザーと異なる場合があります。現在 XClarity Controller 上にあるファームウェアでサポートされるブラウザーのリストを確認するには、XClarity Controller ログイン・ページの「サポートされているブラウザー」メニュー・リストをクリックします。

セキュリティを強化するため、HTTPS を使用する際は、強度の高い暗号のみが現在サポートされています。HTTPS を使用する場合、ご使用のクライアント・オペレーティング・システムとブラウザーの組み合わせが、以下のいずれかの暗号スイートをサポートしていなければなりません。

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256
- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_128\_CCM\_8\_SHA256
- TLS\_AES\_128\_CCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256

注：ご使用のインターネット・ブラウザのキャッシュには、後でロードが高速になるように、訪問した Web ページに関する情報が保管されます。XClarity Controller ファームウェアのフラッシュ更新後、ご使用のブラウザが情報を XClarity Controller から取得する代わりに、キャッシュからの情報を引き続き使用する可能性があります。XClarity Controller ファームウェアの更新後は、XClarity Controller から提供される Web ページが正しく表示されるように、ブラウザ・キャッシュを消去することをお勧めします。

---

## 複数言語サポート

XClarity Controller でサポートされる言語のリストを表示するには、このトピックの情報を使用します。

デフォルトでは XClarity Controller Web インターフェースで選択されている言語は英語です。インターフェースでは、複数言語を表示できます。以下のようなものがあります。

- フランス語
- ドイツ語
- イタリア語
- 日本語
- 韓国語
- ブラジル・ポルトガル語
- ロシア語
- 中国語 (簡体字)
- スペイン語 (インターナショナル)
- 中国語 (繁体字)

使用する言語を選択するには、現在選択されている言語の隣にある矢印をクリックします。ドロップダウン・メニューが表示され、優先言語を選択できます。

XClarity Controller ファームウェアで生成されるテキスト・ストリングは、ブラウザによって判別される言語で表示されます。ブラウザが上記リストにある翻訳済み言語のいずれか以外の言語を指定する場合、テキストは英語で表示されます。さらに、XClarity Controller ファームウェアによって表示されるが XClarity Controller によって生成されたものではないテキスト・ストリング (例: UEFI、PCIe アダプターなどによって生成されるメッセージ) は、英語で表示されます。

ログイン・メッセージなど、英語以外の言語固有のテキストの入力は、現在サポートされていません。英語で入力されたテキストのみサポートされます。

---

## MIB 概要

管理情報ベースにアクセスするには、このトピックの情報を使用します。

SNMP MIB は <https://support.lenovo.com/> からダウンロードできます (ポータルのマシン・タイプによる検索)。以下の 4 つの MIB が含まれます。

- SMI MIB は、Lenovo Data Center Group の管理情報の構造を記述します。

- **Product MIB** は、Lenovo 製品のオブジェクト識別子を記述します。
- **XCC MIB** は、Lenovo XClarity Controller のインベントリー情報および監視情報を提供します。
- **XCC Alert MIB** は、Lenovo XClarity Controller によって検出されたアラート状態のトラップを定義します。

注：4つのMIBのインポート順序は、**SMI MIB** → **Product MIB** → **XCC MIB** → **XCC Alert MIB** です。

---

## 本書で使用される注記

本書で使用される注記を理解するには、この情報を使用します。

本書では、以下の注意書きが使用されています。

- **注:** これらの注記には、注意事項、説明、助言が書かれています。
- **重要:** この注記には、不都合な、または問題のある状態を避けるために役立つ情報または助言が書かれています。
- **重要:** また、これらの注記は、プログラム、デバイス、またはデータに損傷を及ぼすおそれのあることを示します。「重要」の注記は、損傷を起こすおそれのある指示や状態の記述の直前に書かれています。

---

## 第 2 章 XClarity Controller Web インターフェースの開始と使用

このトピックでは、ログインの手順を説明し、XClarity Controller Web インターフェースから実行できる操作についても説明します。

XClarity Controller は、サービス・プロセッサ機能、ビデオ・コントローラー、およびリモート・プレゼンス機能を単一のチップにまとめています。リモートから XClarity Controller にアクセスするには、XClarity Controller Web インターフェースを使用して最初にログインする必要があります。この章では、ログインの手順を説明し、XClarity Controller Web インターフェースから実行できる操作についても説明します。

---

### XClarity Controller Web インターフェースへのアクセス

このトピックでは、XClarity Controller Web インターフェースにアクセスする方法を説明します。

XClarity Controller は、静的 IP アドレスおよび動的ホスト構成プロトコル (DHCP) による IPv4 アドレス指定をサポートします。XClarity Controller に割り当てられるデフォルトの静的 IPv4 アドレスは、192.168.70.125 です。XClarity Controller は、まず DHCP サーバーからのアドレスの取得を試行し、取得できない場合は静的 IPv4 アドレスを使用します。

XClarity Controller は IPv6 もサポートしますが、デフォルトで決められた静的 IPv6 IP アドレスがありません。IPv6 環境での XClarity Controller への最初のアクセスの場合、IPv4 IP アドレスまたは IPv6 リンク・ローカル・アドレスのどちらを使用することもできます。XClarity Controller は、IEEE 802 MAC アドレスを使用して一意のリンク・ローカル IPv6 アドレスを生成します。これには RFC4291 に従って 48 ビット MAC の中央に 16 進数値 0xFF および 0xFE を使用して 2 つのオクテットを挿入し、MAC アドレスの最初のオクテットの右から 2 番目のビットを反転させます。たとえば、MAC アドレスが 08-94-ef-2f-28-af の場合、リンク・ローカル・アドレスは、以下のとおりです。

```
fe80::0a94:eff:fe2f:28af
```

XClarity Controller にアクセスする際は、以下の IPv6 の状態がデフォルトで設定されます。

- IPv6 アドレスの自動構成は、有効です。
- IPv6 静的 IP アドレスの構成は、無効です。
- DHCPv6 は、有効です。
- ステートレス自動構成は、有効です。

XClarity Controller では、専用のシステム管理ネットワーク接続を使用する (該当する場合) か、サーバーと共有のシステム管理ネットワーク接続を使用するかを選択できます。ラック・マウント型のサーバーおよびタワー型のサーバーの場合、デフォルトの接続は専用のシステム管理ネットワーク・コネクタを使用します。

大部分のサーバーでは、専用システム管理ネットワーク接続は、個別の 1Gbit ネットワーク・インターフェース・コントローラーを使用して提供されます。ただし、一部のシステムでは、専用システム管理ネットワーク接続が複数のポート・ネットワーク・インターフェース・コントローラーのネットワーク・ポートの 1 つに対する Network Controller Sideband Interface (NCSI) を使用して提供される場合があります。この場合、専用システム管理ネットワーク接続は、側波帯インターフェースの 10/100 の速度に制限されます。システムへの管理ポートの実装にあたっての情報および制約事項については、システムの資料を参照してください。

**注：**専用システム管理ネットワーク・ポートは、ご使用のサーバーで使用できない場合があります。ご使用のハードウェアに専用のネットワーク・ポートがない場合、XClarity Controller の設定で使用可能なのは、共有の設定のみです。

# XClarity Provisioning Manager による XClarity Controller のネットワーク接続のセットアップ

XClarity Provisioning Manager による XClarity Controller のネットワーク接続のセットアップには、このトピックの情報を使用します。

サーバーを起動した後、XClarity Provisioning Manager を使用して XClarity Controller のネットワーク接続を構成できます。XClarity Controller ハードウェアを搭載したサーバーは、DHCP サーバーに接続するか、あるいはサーバー・ネットワークが複数のイベントのタイムスタンプが同じ場合に、静的 IP アドレスを使用するように構成されている必要があります。Setup ユーティリティーを使用して XClarity Controller ネットワーク接続をセットアップするには、以下のステップを実行します。

ステップ 1. サーバーの電源をオンにします。ThinkSystem のようこそ画面が表示されます。

注：サーバーが AC 電源に接続されてから電源制御ボタンがアクティブになるまでに、最長で 40 秒かかる場合があります。

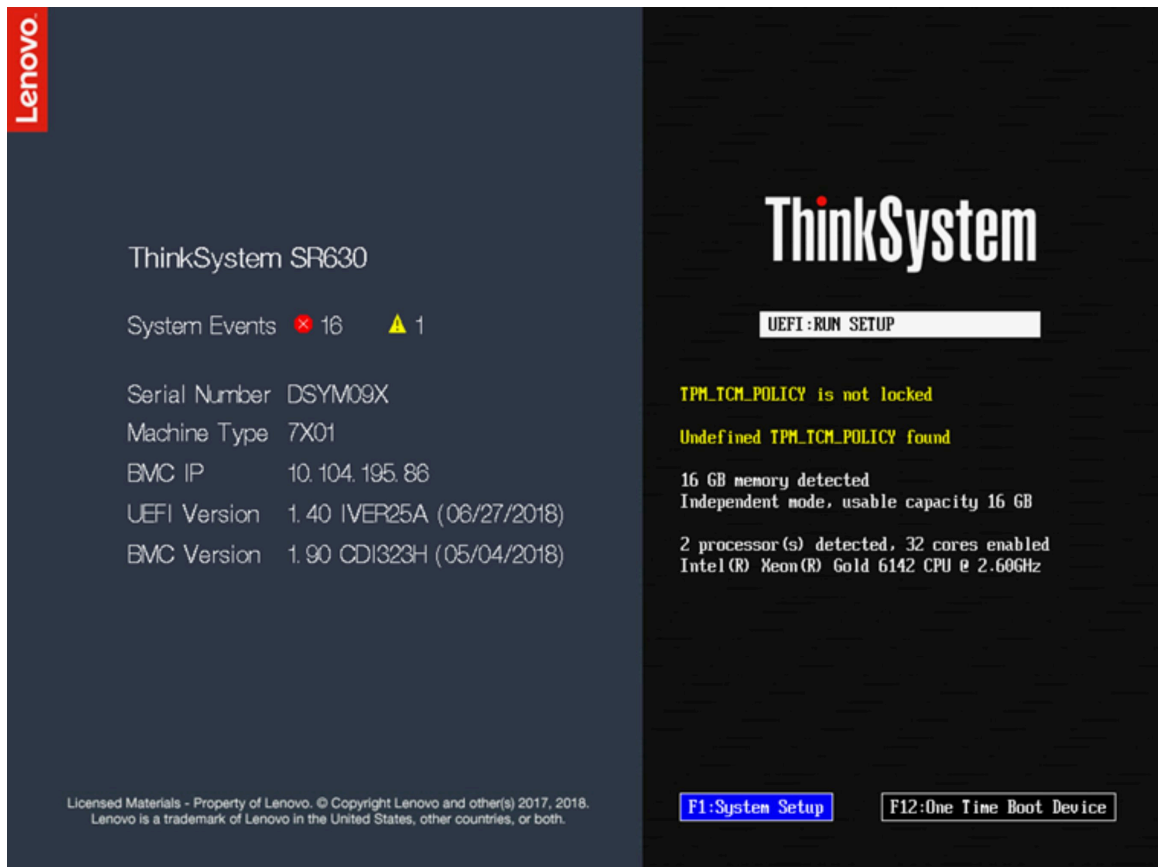


図 1. ThinkSystem のようこそ画面

ステップ 2. プロンプト「<F1> System Setup」が表示されたら、F1 を押します。始動パスワードと管理者パスワードの両方を設定している場合、XClarity Provisioning Manager にアクセスするには管理者パスワードを入力する必要があります。

ステップ 3. XClarity Provisioning Manager のメインメニューから「UEFI Setup」を選択します。

ステップ 4. 次の画面で「BMC Settings」を選択し、「Network Settings」をクリックします。



ステップ 5. 「DHCP Control」フィールドには、3つの XClarity Controller ネットワーク接続の選択項目があります。

- Static IP
- DHCP Enabled
- フォールバック対応の DHCP

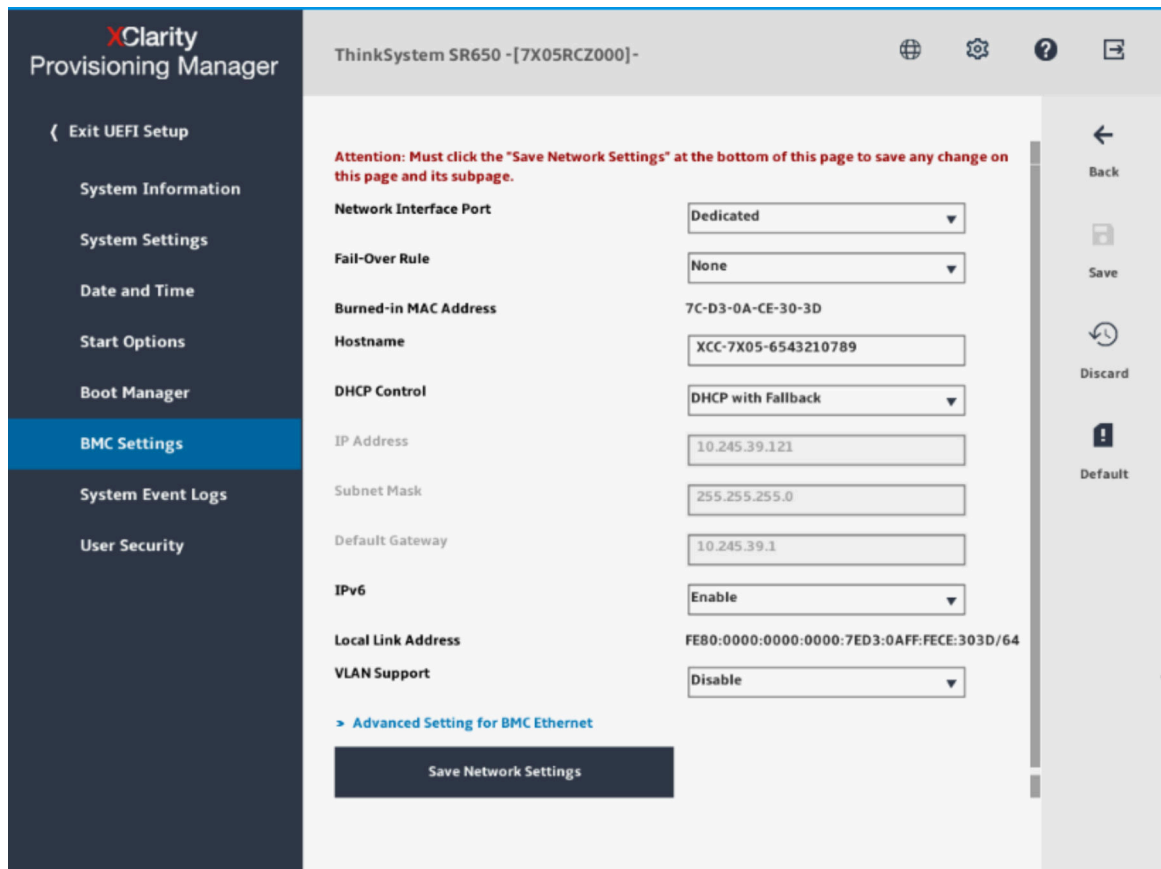


図2. ネットワーク接続設定

ステップ 6. ネットワーク接続の選択項目から 1つを選択します。

ステップ 7. 静的 IP アドレスの使用を選択した場合、IP アドレス、サブネット・マスク、およびデフォルト・ゲートウェイを指定する必要があります。

ステップ 8. また、Lenovo XClarity Controller Manager を使用して、専用のネットワーク接続 (ご使用のサーバーに専用ネットワーク・ポートがある場合)、または共有 XClarity Controller ネットワーク接続のどちらを使用するかを選択できます。

注：

- 専用のシステム管理ネットワーク・ポートは、ご使用のサーバーで使用できない場合があります。ご使用のハードウェアに専用のネットワーク・ポートがない場合、XClarity Controller の設定で使用可能なのは、共有の設定のみです。「Network Configuration」画面の「Network Interface Port」フィールドで、「Dedicated」(該当する場合)または「Shared」を選択します。
- XClarity Controller で使用するサーバー上のイーサネット・コネクタの位置を見つけるには、ご使用のサーバーに付属の資料を参照してください。

ステップ9. 「保存」をクリックします。

ステップ10.XClarity Provisioning Manager を終了します。

注：

- サーバー・ファームウェアが再度機能するには、変更が有効になるまで約1分間待つ必要があります。
- XClarity Controller Web インターフェースまたはコマンド・ライン・インターフェース (CLI) から、XClarity Controller ネットワーク接続を構成することもできます。XClarity Controller web インターフェースでは、ネットワーク接続は左ナビゲーション・パネルから「BMC 構成」をクリックし、「ネットワーク」を選択して構成できます。XClarity Controller CLI では、ご使用のインストール済み環境の構成に応じたいくつかのコマンドを使用して、ネットワーク接続が構成されます。

## XClarity Controller へのログイン

このトピックでは、XClarity Controller Web インターフェースを使用して XClarity Controller にアクセスする方法を説明します。

**重要：** XClarity Controller は、最初はユーザー名 USERID とパスワード PASSWORD (英字の O でなくゼロ) を使用して設定されます。このデフォルトのユーザー設定では、Supervisor アクセス権があります。拡張セキュリティを使用するには、初期構成時にこのユーザー名とパスワードを変更してください。変更を行った後、ログイン・パスワードとして再度 PASSWORD を設定することはできません。

XClarity Controller Web インターフェースを使用して XClarity Controller にアクセスするには、次のステップを実行します。

ステップ1. Web ブラウザーを開きます。「アドレス」または「URL」フィールドに、https:// の後に、接続する XClarity Controller の IP アドレスまたはホスト名を入力します。

ステップ2. 「言語」ドロップダウン・リストから、目的の言語を選択します。

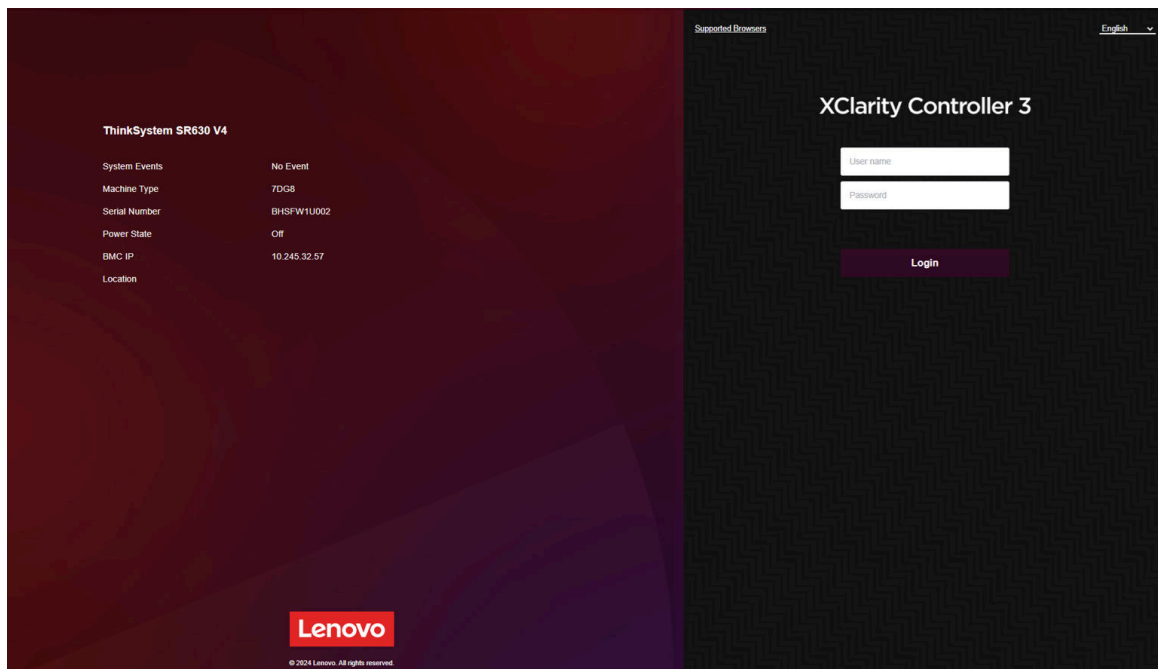


図3. ログイン・ページ

ステップ 3. XClarity Controller ログイン・ウィンドウでユーザー名とパスワードを入力します。XClarity Controller を初めて使用する場合、ユーザー名とパスワードはシステム管理者から入手できます。すべてのログイン試行はイベント・ログに記録されます。システム管理者がどのようにユーザー ID を構成したかに応じて、ログイン後に新規パスワードを入力する必要がある場合があります。

ステップ 4. 「ログイン」をクリックしてセッションを開始します。次の図に示すように、ブラウザーは XClarity Controller ホーム・ページを開きます。ホーム・ページには、XClarity Controller が管理するシステムに関する情報が、現在システム内に存在するクリティカル・エラー数 **1** および警告数 **▲** を示すアイコンとともに表示されます。

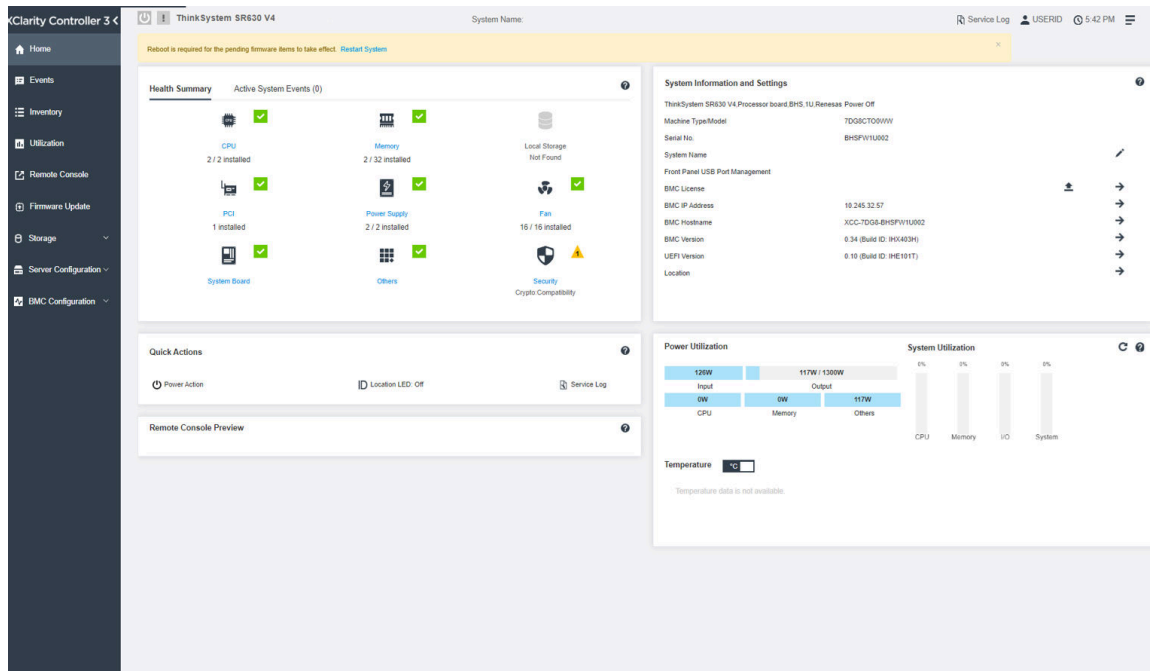


図 4. ホーム・ページ

ホーム・ページは基本的に 2 つのセクションに分けられます。最初のセクションは左のナビゲーション・パネルです。これは、次の操作を実行できる一連のトピックです。

- サーバー状況の監視
- サーバーの構成
- XClarity Controller または BMC の構成
- ファームウェアの更新

2 番目のセクションは、ナビゲーション・パネルの右に表示されるグラフィカルな情報です。モジュラー形式によって、サーバー状況の簡易ビューと実行できるクイック操作がいくつか表示されます。

## Web インターフェースでの XClarity Controller 機能の説明

このトピックの情報では、Web インターフェースでの XClarity Controller 機能について説明します。

以下は、左側のナビゲーション・パネルでの XClarity Controller の機能について説明する表です。

注：Web インターフェース使用時は、疑問符アイコンをクリックしてオンライン・ヘルプを表示することもできます。

タブ	選択	説明
ホーム	ヘルス・サマリー/アクティ ブ・システム・イベント	システム内のメジャーなハードウェア・コンポーネントの現在のステータスを表示します。
	システム情報と設定	一般的なシステム情報の要約を説明します。
	クイック操作	サーバーの電源およびロケーション LED を制御するためのクイック・リンク、およびサービス・データをダウンロードするボタンが用意されています。
	電力使用量	現在の電力使用量の簡単な概要を提供します。
	リモート・コンソール・プレ ビュー	オペレーティング・システム・レベルでサーバーを制御します。コンピューターからサーバー・コンソールを表示して操作できます。XClarity Controller ホーム・ページのリモート・コンソール・セクションには、画面イメージが起動ボタンとともに表示されます。
イベント	イベント・ログ	すべてのハードウェアおよび管理イベントの履歴が記録されています。
	監査ログ	ユーザー操作の履歴レコードを提供します。
	メンテナンス履歴	すべてのファームウェア更新、構成およびハードウェア交換の履歴が表示されます。
	アラート受信者  注：この機能は、今後のアップデートでサポートされる予定です。	システム・イベントの通知先を管理します。このページを使用して、各受信者を構成したり、すべてのイベント受信者に適用される設定を管理することができます。また、テスト・イベントを生成して、通知の構成設定を確認することもできます。
インベントリ	システム内のすべてのコンポーネントが、ステータスおよびキー情報とともに表示されます。デバイスをクリックすると、追加情報を表示できます。  注：ソリューションの電源ステータスについては、SMM3 Web インターフェースを参照してください。	
使用率	サーバーおよびそのコンポーネントの周囲温度/コンポーネント温度、電力使用率、電圧レベル、ファン速度情報をグラフィックス形式または表形式で表示します。	
リモート・コン ソール	リモート・コンソール機能にアクセスできます。仮想メディア機能を使用して、システム内、または CIFS、NFS、HTTPS、または SFTP を使用して BMC からアクセスできるネットワーク・ロケーションにある ISO または IMG ファイルをマウントできます。マウントされたディスクは、サーバーに接続されている USB ディスク・ドライブまたは DVD ROM として表示されます。	
ファームウェア更 新	<ul style="list-style-type: none"> <li>ファームウェア・レベルを表示します。</li> <li>XClarity Controller のファームウェアおよびサーバーのファームウェアを更新します。</li> <li>レポジトリから XClarity Controller のファームウェアを更新します。</li> </ul>	
ストレージ	詳細	ストレージ・デバイスの物理構造とストレージ構成が表示されます。
	RAID セットアップ	仮想ディスクおよび物理ストレージ・デバイスの情報を含む、現行の RAID 構成を表示または変更します。

タブ	選択	説明
サーバー構成	アダプター	インストールされているネットワーク・アダプターの情報および XClarity Controller から構成できる設定を表示します。
	ブート・オプション	<ul style="list-style-type: none"> <li>• 次回のサーバー再起動時に使用する一回限りブートするブート・デバイスを選択します。</li> <li>• ブート・モードおよびブート順序の設定を変更します。</li> </ul>
	電源ポリシー	<ul style="list-style-type: none"> <li>• パワー・サプライ障害のイベント時に、電源の冗長性を構成します。</li> <li>• 電源キャッピング・ポリシーを構成します。</li> <li>• 電源復元ポリシーを構成します。</li> </ul> <p>注：ソリューションの電源ステータスの詳細については、SMM3 Web インターフェースを参照してください。</p>
	サーバーのプロパティ	<ul style="list-style-type: none"> <li>• サーバーの各種プロパティ、状況条件、および設定を監視します。</li> <li>• サーバーの電源オフの遅延を管理します。</li> <li>• ログイン・メッセージの作成ログイン・メッセージは、ユーザーが XClarity Controller にログインするたび表示されるメッセージであり、お客様が作成できます。</li> </ul>
	シャーシ 注：この項目は、D3 V2 シャーシ互換ノードでのみ使用できます。	<ul style="list-style-type: none"> <li>• シャーシ情報を表示します。</li> <li>• ノードを再起動するか、物理ノードの再取り付けをシミュレートします。</li> <li>• シャーシ・ケアテイカー選択設定を表示します。</li> <li>• シャーシのメンテナンス履歴を表示します。</li> </ul>
BMC 構成	バックアップおよびリストア	XClarity Controller の構成の出荷時のデフォルト値へのリセット、現行構成のバックアップ、またはファイルからの元構成の復元を行います。
	ライセンス	オプションの XClarity Controller 機能のアクティベーション・キーを管理します。
	ネットワーク	XClarity Controller のネットワーク・プロパティ、ステータス、および設定を構成します。
	セキュリティ	XClarity Controller のセキュリティー・プロパティ、ステータス、および設定を構成します。
	ユーザー/LDAP	<ul style="list-style-type: none"> <li>• XClarity Controller のログイン・プロファイルおよびグローバル・ログイン設定を構成します。</li> <li>• 現在 XClarity Controller にログインしているユーザー・アカウントを表示します。</li> <li>• 「LDAP」タブでは、1つ以上の LDAP サーバーで使用するユーザー認証を構成します。LDAP セキュリティーを有効または無効に設定したり、LDAP セキュリティーの認証を管理することもできます。</li> </ul>
コール・ホーム 注：この機能は、今後のアップデートでサポートされる予定です。	システムに関する情報を収集して Lenovo にサービスの要請を送信するよう、コール・ホーム・オプションを構成します。	



---

## 第 3 章 XClarity Controller の構成

XClarity Controller の構成に使用できるオプションについて理解するには、この章の情報を使用します。

XClarity Controller を構成する際には、以下のキー・オプションを使用できます。

- バックアップおよびリストア
- ライセンス
- ネットワーク
- セキュリティー
- ユーザー/LDAP

---

### ユーザー・アカウント/LDAP の構成

ユーザー・アカウントの管理方法を理解するには、このトピックの情報を使用します。

「BMC 構成」の下にある「ユーザー/LDAP」をクリックしてユーザー・アカウントの作成、変更、表示、および LDAP 設定の構成を行います。

「ローカル・ユーザー」タブには、XClarity Controller 内に構成されたユーザー・アカウント、および現在誰が XClarity Controller にログインしているかが表示されます。

「LDAP」タブには、LDAP サーバーに保存されているユーザー・アカウントにアクセスするための LDAP 構成が表示されます。

### ユーザー認証方式

ログイン試行を認証するために XClarity Controller が使用できるモードを理解するには、このトピックの情報を使用します。

「ログオンを許可」の横にあるドロップダウン・メニューをクリックして、ユーザーのログイン試行の認証方法を選択します。以下のいずれかの認証方式を選択できます。

- **ローカルのみ:** ユーザーは XClarity Controller で構成されたローカル・ユーザー・アカウントの検索によって認証されます。ユーザー ID とパスワードが一致しない場合、アクセスは拒否されます。
- **LDAP のみ:** XClarity Controller は、LDAP サーバーに保持された資格情報を使用してユーザーの認証を試みます。この認証方式では、XClarity Controller 内のローカル・ユーザー・アカウントは検索されません。
- **最初にローカル、次に LDAP:** 最初にローカル認証が試みられます。ローカル認証が失敗すると、LDAP 認証が試みられます。
- **最初に LDAP、次にローカル・ユーザー:** 最初に LDAP 認証が試みられます。LDAP 認証が失敗すると、ローカル認証が試みられます。

注：

- ローカルで管理されているアカウントだけが、IPMI インターフェースと SNMP インターフェースで共有されます。これらのインターフェースは、LDAP 認証をサポートしていません。
- IPMI ユーザーおよび SNMP ユーザーは、「ログオンを許可」フィールドが「LDAP のみ」に設定されている場合でも、ローカルで管理されているアカウントを使用してログインすることができます。

## 新しい役割の作成

新しい役割を作成するには、このトピックの情報を使用します。

### 役割の作成

カスタムの役割を作成するには、「**役割**」タブをクリックし、「**作成**」をクリックします。

以下のフィールドに入力します。「**役割名**」および「**権限レベル**」。権限レベルの詳細については、以下のセクションを参照してください。

作成された役割は、ユーザー・セクションの「**役割**」ドロップダウン・メニューでユーザーに提供されます。

注：ユーザーとLDAPで使用されている役割については、役割名の編集および削除が許可されていません。ただし、対応するカスタム・アクセス権の変更にはアクセスできます。

### 権限レベル

カスタムの役割では、以下の権限の任意の組み合わせを有効にできます。

#### 構成 - ネットワーキングおよび BMC セキュリティー

ユーザーは、「**BMC セキュリティー**」および「**ネットワーク**」の各ページで構成パラメーターを変更できます。

#### ユーザー・アカウント管理

ユーザーは、ユーザーの追加、変更、または削除、およびグローバル・ログイン設定の変更が可能です。

#### リモート・コンソール・アクセス

ユーザーは、リモート・コンソールへアクセスすることができます。

#### リモート・コンソールおよびリモート・ディスクのアクセス

ユーザーはリモート・コンソールと仮想メディア機能の両方にアクセスできます。

#### リモート・サーバーの電源/再起動

ユーザーは、サーバーのパワーオン機能と再起動機能を実行できます。

#### 構成 - 基本

ユーザーは、「**サーバーのプロパティ**」および「**イベント**」の各ページで構成パラメーターを変更できます。

#### イベント・ログをクリアする権限

このユーザーはイベント・ログを消去することができます。イベント・ログは誰でも見ることができますが、ログを消去するには、この権限レベルが必要です。

#### 構成 - 拡張 (ファームウェア更新、BMC の再起動、構成の復元)

ユーザーは、XClarity Controller を構成するときに何も制約を受けません。さらに、このユーザーは XClarity Controller に対する管理アクセス権限があります。管理アクセス権限に含まれる拡張機能は、ファームウェア更新、PXE ネットワーク・ブート、XClarity Controller の出荷時デフォルト値の復元、構成ファイルに入っている XClarity Controller 設定の変更と復元、および XClarity Controller の再起動とリセットです。

#### 構成 - UEFI セキュリティー

ユーザーは「**UEFI セキュリティー**」設定を変更できます。

### 事前定義された役割

以下の役割は事前定義済みであり、編集または削除できません。

### 管理者



管理者の役割は一切の制限を受けず、すべての操作を実行できます。

#### 読み取り専用

読み取り専用の役割は、サーバー情報を表示できますが、システムの状態に影響を与える操作 (保存、変更、クリア、リブート、ファームウェアの更新など) は実行できません。

#### オペレーター

オペレーターの役割を持つユーザーには、以下の特権があります。

- 構成 - ネットワーキングおよび BMC セキュリティー
- リモート・サーバーの電源/再起動
- 構成 - 基本
- イベント・ログをクリアする権限
- 構成 - 拡張 (ファームウェア更新、BMC の再起動、構成の復元)

## 新規ユーザー・アカウントの作成

新規ローカル・ユーザーを作成するには、このトピックの情報を使用します。

#### ユーザーの作成

「ローカル・ユーザー」タブをクリックし、「作成」をクリックして新規ユーザー・アカウントを作成します。

「ユーザー名」、「パスワード」、「パスワードの確認」の各フィールドに入力し、ドロップダウン・メニューから「役割」を選択します。役割の詳細については、以下のセクションを参照してください。

#### 役割

以下の役割が事前定義されています。ユーザーのニーズに応じて新しいカスタムの役割を作成することもできます。

#### 管理者

管理者の役割は一切の制限を受けず、すべての操作を実行できます。

#### 読み取り専用

読み取り専用の役割は、サーバー情報を表示できますが、システムの状態に影響を与える操作 (保存、変更、クリア、リブート、ファームウェアの更新など) は実行できません。

#### オペレーター

オペレーターの役割を持つユーザーには、以下の特権があります。

- 構成 - ネットワーキングおよび BMC セキュリティー
- リモート・サーバーの電源/再起動
- 構成 - 基本
- イベント・ログをクリアする権限
- 構成 - 拡張 (ファームウェア更新、BMC の再起動、構成の復元)

## SNMPv3 設定

ユーザーの SNMPv3 アクセスを有効にするには、対応するユーザーの横にある「編集」ボタンをクリックし、「ユーザー・アクセス可能インターフェース」のドロップダウン・リストの下にある「SNMP」をオンにします。以下のユーザー・アクセス・オプションが表示されます。

#### アクセス・タイプ

「GET」操作のみがサポートされます。XClarity Controller では SNMPv3 SET 操作はサポートされません。SNMP3 は照会操作のみを実行できます。

### 認証プロトコル

このアルゴリズムは、SNMPv3 セキュリティー・モデルが認証に使用されます。以下のプロトコルがサポートされています。

- なし
- HMAC-SHA (デフォルト)
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512

### プライバシー・プロトコル

SNMP クライアントとエージェントの間のデータ転送は、暗号化を使用して保護することができます。次のメソッドがサポートされています。

- なし
- CBC-DES
- AES (デフォルト)
- AES192
- AES256
- AES192C
- AES256C

注：SNMPv3 ユーザーによってパスワードの文字列が繰り返し使用される場合でも、XClarity Controller に対するアクセスは依然として許可されます。参考のために、2つの例を示します。

- パスワードが「11111111」（8個の1）に設定されている場合、パスワードで8個を超える1を誤って入力した場合でも、ユーザーは依然としてXClarity Controller にアクセスできます。たとえば、パスワードとして「1111111111」（10個の1）を入力した場合、引き続きアクセスが許可されます。反復する文字列は、同じキーと見なされます。
- パスワードが「bertbert」に設定されている場合、ユーザーがパスワードとして誤って「bertbertbert」を入力しても、依然としてXClarity Controller にアクセスできます。両パスワードには、同じキーが含まれるものと見なされます。

詳しくは、インターネット標準 RFC 3414 文書 (<https://tools.ietf.org/html/rfc3414>) の「セキュリティの考慮事項」を参照してください。

### SSH 鍵

XClarity Controller は SSH 公開鍵認証 (RSA キー・タイプ) をサポートします。ローカル・ユーザー・アカウントに SSH 鍵を追加するには、対応するユーザーの横にある「編集」ボタンをクリックし、「ユーザー・アクセス可能インターフェース」のドロップダウン・リストの下にある「SSH 鍵」をオンにします。次の2つのオプションがあります。

#### 鍵ファイルを選択

サーバーから XClarity Controller にインポートする SSH 鍵ファイルを選択します。

#### テキスト・フィールドに鍵を入力

SSH 鍵からのデータをテキスト・フィールドに貼り付けまたは入力します。

注：



- サード・パーティーのパスワードが期限切れの場合、ユーザーのログイン・プロセス中に警告メッセージが表示されます。

## OneCLI 機能を使用したハッシュド・パスワードの設定

- 機能の有効化

```
$ sudo OneCli config set IMM.ThirdPartyPassword Enabled
```

- ハッシュド・パスワードの作成 (Salt なし) 次の例では、password123 パスワードを使用して、XClarity Controller にログインしています。

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
```

```
$ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

```
$ sudo OneCli config set IMM.Loginid.2 admin
```

```
$ sudo OneCli config set IMM.SHA256Password.2 $pwhash
```

```
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

- (Salt での) ハッシュド・パスワードによるユーザーの作成次の例では、password123 パスワードを使用して、XClarity Controller にログインしています。Salt=abc

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
```

```
$ echo $pwhash 292bcbcb41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
```

```
$ sudo OneCli config set IMM.Loginid.3 Admin
```

```
$ sudo OneCli config set IMM.SHA256Password.3 $pwhash
```

```
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
```

- ハッシュド・パスワードと salt の取得。

```
$ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled
```

```
$ sudo OneCli config show IMM.SHA256Password.3
```

```
$ sudo OneCli config show IMM.SHA256PasswordSalt.3
```

- ハッシュド・パスワードと salt の削除。

```
$ sudo OneCli config set IMM.SHA256Password.3 ""
```

```
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
```

- 既存のアカウントにハッシュド・パスワードを設定します。

```
$ sudo OneCli config set IMM.Loginid.2 admin
```

```
$ sudo OneCli config set IMM.Password.2 PasswOrd123abc
```

```
$ sudo OneCli config set IMM.SHA256Password.2 $pwhash
```

```
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

注：ハッシュド・パスワードの設定時に、このパスワードは直ちに有効になります。元の標準パスワードは無効になります。この例では、ハッシュド・パスワードを削除するまで、元の標準パスワード PasswOrd123abc は使用できなくなります。

## CLI 機能を使用したハッシュド・パスワードの設定

- 機能の有効化

```
> hashpw -sw enabled
```

- ハッシュド・パスワードの作成 (Salt なし) 次の例では、password123 パスワードを使用して、XClarity Controller にログインしています。

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
```

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

```
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

- (Salt での) ハッシュド・パスワードによるユーザーの作成次の例では、password123 パスワードを使用して、XClarity Controller にログインしています。Salt=abc

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}``
```

```
$ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
```

```
> users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt 'abc' -a super
```

- ハッシュド・パスワードと salt の取得。

```
> hashpw -re enabled
```

```
> users -3 -ghp -gsalt
```

- ハッシュド・パスワードと salt の削除。

```
> users -3 -shp "" -ssalt ""
```

- 既存のアカウントにハッシュド・パスワードを設定します。

```
> users -2 -n admin -p PasswOrd123abc -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

注：ハッシュド・パスワードの設定時に、このパスワードは直ちに有効になります。元の標準パスワードは無効になります。この例では、ハッシュド・パスワードを削除するまで、元の標準パスワード PasswOrd123abc は使用できなくなります。

ハッシュド・パスワードを設定した後、XClarity Controller へのログインにはこのパスワードを使用しないことに注意してください。ログイン時には、プレーン・テキストのパスワードを使用する必要があります。以下の例では、プレーン・テキスト・パスワードは「password123」です。

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}``
```

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

```
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

## グローバル・ログイン設定の構成

すべてのユーザーに適用するログインおよびパスワード・ポリシー設定を構成するには、このトピックの情報を 사용합니다。

### 非アクティブな Web セッションのタイムアウト

非アクティブな Web セッションのタイムアウト・オプションを設定するには、このトピックの情報を 사용합니다。

「非アクティブな Web セッションのタイムアウト」フィールドで、非アクティブな Web セッションを切断するまでの XClarity Controller の待ち時間を分単位で指定できます。最大待ち時間は 1,440 分です。0 に設定した場合、Web セッションは期限が切れません。

XClarity Controller ファームウェアは、最大 6 つの同時 Web セッションをサポートします。他のユーザーが使用できるようにセッションを解放するために、非アクティブ・タイムアウトでセッションが自動的にクローズされるのを待たず、作業が終了した時点で Web セッションからログアウトすることをお勧めします。

注：自動的に最新表示される XClarity Controller Web ページ上でブラウザーを開いたまま放置した場合、Web セッションが非アクティブでも自動的にクローズされません。

## アカウント・セキュリティ・ポリシーの設定

サーバーのアカウント・セキュリティ・ポリシーについて理解して設定するには、この情報を使用します。

セキュリティ設定の各フィールドの説明を以下に示します。

### 最初のアクセス時にパスワードを変更をユーザーに強制する

デフォルトのパスワードで新規ユーザーをセットアップした後、このチェック・ボックスを選択すると、そのユーザーは、最初にログインするときに自己のパスワードを変更するよう強制されます。このフィールドのデフォルト値はチェック・ボックスを有効に設定することです。

### 複雑なパスワードが必要

オプション・ボックスはデフォルトでチェックされています。複雑なパスワードは以下の規則に従っている必要があります。

- 以下の文字のみを含めることができます (空白文字は使用できません): A-z、a-z、0-9、~!@#\$%^&\*()-+={}[];'"<>?/\_
- 1つ以上の文字を含めなければならない
- 1つ以上の数字を含めなければならない
- 次の組み合わせのうち、少なくとも2つを使用する必要があります。
  - 1つ以上の大文字
  - 1つの小文字
  - 1つ以上の特殊文字
- 他の文字 (特にスペースまたは空白文字) は使用できない
- パスワードの中で同じ文字を3回以上続けることはできません (例えば、「aaa」)。
- パスワードをユーザー名とまったく同じにすることも、ユーザー名を1回以上繰り返すだけで作成することも、あるいはユーザー名の文字を逆順に並べて作成することもできません。
- パスワードは、8文字以上255文字以下の長さとする必要があります。

オプション・ボックスがオンになっていない場合、最小パスワード長に指定する数字は、0 ~ 255文字に設定できます。最小パスワード長が0に設定されている場合は、アカウント・パスワードを空白にできます。

### パスワードの有効期限までの期間 (日数)

このフィールドには、パスワードを変更せずに使用することが許可される、パスワードの最大使用日数が入ります。

### パスワード失効の警告期間 (日数)

このフィールドには、パスワードの有効期限が切れる前に、ユーザーが警告を受け取る日数を入力します。

### 最小パスワード長 (文字)

このフィールドには、パスワードの最小の長さが入ります。

### 最短パスワード再利用サイクル (回数)

このフィールドには、何回前までに使用したパスワードを再使用できないようにするかを指定する回数が入ります。

### 最短パスワード変更期間 (時間)

このフィールドには、パスワードの変更から次の変更までの必要な待ち時間が入ります。

### 最大ログイン失敗数 (回数)

このフィールドには、ログイン試行に何回失敗したら、一定期間ロックアウトされるかを指定する失敗回数が入ります。

### ログイン失敗が最大回数に達した後のロックアウト期間 (分)

このフィールドでは、最大ログイン失敗数に達した後、XClarity Controller サブシステムがリモート・ログインの試行に対して無効になる時間 (分) を指定します。

## LDAP の構成

XClarity Controller の LDAP 設定を表示または変更するには、このトピックの情報を使用します。

LDAP のサポートには以下が含まれます。

- LDAP プロトコル・バージョン 3 (RFC 2251) のサポート
- 標準 LDAP クライアント API (RFC 1823) をサポート
- 標準 LDAP 検索フィルター構文 (RFC 2254) のサポート
- Lightweight Directory Access Protocol (v3) Extension for Transport Layer Security (RFC-2830) のサポート

LDAP 実装では、以下の LDAP サーバーがサポートされます。

- Microsoft Active Directory (Windows 2003、Windows 2008、Windows 2012、Windows 2016、Windows 2019)
- Microsoft Active Directory Application Mode (Windows 2003、Windows 2008)
- Microsoft ライトウェイト・ディレクトリ・サービス (Windows 2008、Windows 2012、Windows 2016、Windows 2019)
- Novell eDirectory Server、バージョン 8.7 および 8.8
- OpenLDAP サーバー 2.1、2.2、2.3、2.4、2.5 および 2.6

XClarity Controller の LDAP 設定を表示または変更するには、「LDAP」タブをクリックします。

XClarity Controller は、XClarity Controller 自体に保存されたローカル・ユーザー・アカウントの代わりにまたはアカウントに追加で、中央 LDAP サーバーを介してユーザーのアクセスをリモートで認証できます。特権は、「ログイン許可属性」の値を使用して、ユーザー・アカウントごとに指定できます。また、LDAP サーバーを使用して、通常のユーザー (パスワード検査) 認証の他に、ユーザーをグループに割り当ててグループ認証を行うこともできます。たとえば、XClarity Controller を 1 つ以上のグループに関連付けることができ、ユーザーはこの XClarity Controller に関連付けられている少なくとも 1 つのグループに属している場合にのみ、グループ認証にパスします。

LDAP サーバーを構成するには、以下の手順を実行します。

1. 「LDAP サーバー情報」内で、項目リストから以下のオプションを使用できます。

- **認証のみに LDAP サーバーを使用する (ローカル承認):** この選択肢は、資格情報を LDAP サーバーへの認証にのみ使用し、グループ・メンバーシップ情報を取得するように XClarity Controller に指示します。グループ名と役割は、「ローカル承認用グループ」セクションで設定できます。
- **認証と承認に LDAP サーバーを使用する:** この選択肢は、資格情報を LDAP サーバーへの認証とユーザーのアクセス権限の識別の両方に使用するように XClarity Controller に指示します。

注：認証に使用する LDAP サーバーは、手動で構成することも DNS SRV レコード経由で動的に検出することも可能です。

- **事前構成済みのサーバーを使用する:** 各サーバーの IP アドレスまたはホスト名 (DNS が有効である場合) を入力して、最大 3 つの LDAP サーバーを構成できます。各サーバーのポート番号はオプションです。このフィールドを空白のまま残した場合、デフォルト値の 389 が、非セキュア LDAP 接続に使用されます。セキュア接続では、デフォルトのポート値は 636 です。少なくとも 1 つの LDAP サーバーが構成されている必要があります。

- **DNS を使用してサーバーを探す:** LDAP サーバーを動的に検出するように選択できます。RFC2782 (サービスのロケーションを指定する DNS RR) で説明されるメカニズムが LDAP サーバーの検索に使用されます。これは、DNS SRV と呼ばれています。DNS SRV 要求のドメイン名として使用する完全修飾ドメイン名 (FQDN) を指定する必要があります。
  - **AD フォレスト:** クロス・ドメインのユニバーサル・グループがある環境では、フォレスト名 (ドメインのセット) が、要求されたグローバル・カタログ (GC) を検出するように構成されている必要があります。ドメイン間グループ・メンバーシップが適用されない環境では、このフィールドは空白のままにしておきます。
  - **AD ドメイン:** DNS SRV 要求のドメイン名として使用する完全修飾ドメイン名 (FQDN) を指定する必要があります。

セキュア LDAP を有効にする場合は、「**セキュア LDAP を有効にする**」チェック・ボックスをクリックします。セキュア LDAP をサポートするには、有効な SSL 証明書が所定の場所にあり、少なくとも 1 つの SSL クライアント・トラステッド証明書が XClarity Controller にインポートされている必要があります。LDAP サーバーは、XClarity Controller セキュア LDAP クライアントとの互換性を持たせるために、トランスポート層セキュリティ (TLS) バージョン 1.2 をサポートする必要があります。証明書の処理について詳しくは、[42 ページの「SSL 証明書の処理」](#)を参照してください。

2. 「**追加のパラメーター**」の下に情報を入力します。パラメーターの説明を以下に示します。

#### LDAP タイプ

LDAP ベースの認証に使用する LDAP サーバーのタイプを選択します。以下のサーバー・タイプを使用できます。

- **OpenLDAP**  
OpenLDAP
- **Active Directory**  
ディレクトリー: Windows Active Directory
- **その他**  
ディレクトリー: Apache Directory、eDirectory など

#### バインディング方式

LDAP サーバーの検索または照会を行うには、事前にバインド要求を送信する必要があります。このフィールドにより、この LDAP サーバーへの初期バインドを実行する方法を制御します。以下のバインド方式が選択可能です。

- **構成済み資格情報を使用**  
構成済みの DN およびパスワードを使用してバインドするには、この方式を使用します。
- **ログイン資格情報を使用**  
ログイン・プロセスで提供された資格情報を使用してバインドするには、この方式を使用します。ユーザー ID は、DN、部分 DN、完全修飾ドメイン名を介して、または XClarity Controller 上で構成された UID 検索属性に一致するユーザー ID を介して提供できます。提示された資格情報が部分 DN (たとえば、cn=joe) と同様の場合、この部分 DN は、ユーザーの記録に一致する DN の作成を試行するときに、構成済みのルート DN の先頭に付けられます。バインド試行が失敗した場合、最後の試行は、ログイン資格情報の先頭に cn= を付けて試行されます。その後、その結果の文字列を構成済みのルート DN の先頭に追加します。

初期バインドが成功した場合は、ログインするユーザーに属する LDAP サーバーで項目の検索が実行されます。必要であれば 2 回目のバインド試行が実行されますが、ユーザーの LDAP レコードから取得された DN とログイン・プロセスで入力されたパスワードが使用されます。2 回目のバインド試行が失敗すると、ユーザーはアクセスを拒否されます。2 回目のバインドが実行されるのは、「**構成済み資格情報を使用**」のバインディング方式が使用されている場合のみです。

#### クライアント識別名



初期バインドに使用するクライアント識別名 (DN)。また、最大 300 文字に制限されています。

### クライアント・パスワード

この識別クライアントのパスワード。

### ルート DN

LDAP サーバー上のディレクトリー・ツリーのルート・エントリーの識別名 (DN) です (たとえば、dn=mycompany,dc=com)。この DN がすべての検索要求の基本オブジェクトとして使用されます。

### ユーザーのログイン名検索属性

バインド方式が「**構成済み資格情報を使用**」に設定されている場合、LDAP サーバーへの最初のバインドの後に、ユーザーの DN、ログイン権限、グループ・メンバーシップなど、ユーザーに関する特定の情報を取得する検索要求が続きます。この検索要求では、そのサーバー上でユーザー ID を表す属性名を指定する必要があります。この属性名は、このフィールドで構成されます。Active Directory サーバーでは、属性名は通常「CN」または「sAMAccountName」です。Novell eDirectory サーバーおよび OpenLDAP サーバーでは、この属性名は「uid」です。このフィールドを空白のままにした場合、デフォルトは「sAMAccountName」です。

### グループ・フィルター

「**グループ・フィルター**」フィールドは、グループ認証に使用されます。グループ認証は、ユーザーの資格情報が正常に確認された後に試行されます。グループ認証が失敗すると、ユーザーのログオン試行は拒否されます。グループ・フィルターが構成されている場合、XClarity Controller がどのグループに属しているかを指定するのに使用されます。つまり、成功するには、グループ認証向けに構成されたグループの少なくとも 1 つにユーザーが属する必要があります。「**グループ・フィルター**」フィールドが空白のまま残された場合、グループ認証は自動的に成功します。グループ・フィルターが構成されている場合は、リスト内のグループの少なくとも 1 つがユーザーが属しているグループと一致しているか、マッチングが試行されます。一致するグループがない場合、ユーザーは認証に失敗し、アクセスは拒否されます。少なくとも 1 つのグループが一致する場合は、グループ認証は成功します。この比較は大/小文字を区別します。フィルターは 511 文字が上限で、1 つ以上のグループ名から構成することができます。複数のグループ名を区切る場合は、コロン (:) 文字を使用する必要があります。先頭および末尾のスペースは無視されますが、それ以外のスペースはすべてグループ名の一部として処理されます。

注：ワイルドカード文字 (\*) はワイルドカードとして処理されなくなりました。機密漏れを防止するため、ワイルドカードの概念は廃止されました。グループ名は完全 DN として、または **cn** 部分のみを使用して指定できます。たとえば、DN が cn=adminGroup,dc=mycompany,dc=com であるグループは、実際の DN または adminGroup を使用して指定することができます。

### グループ・メンバーシップ検索属性

「**グループ検索属性**」フィールドは、ユーザーが属するグループを識別するために使用される属性名を指定します。Active Directory サーバーでは、通常、属性名は **memberOf** です。Novell eDirectory サーバーでは、属性名は **groupMembership** です。OpenLDAP サーバーでは、ユーザーは通常、objectClass が PosixGroup と等しいグループに割り当てられます。そのコンテキストでは、このフィールドは特定の PosixGroup のメンバーを識別するために使用する属性名を指定します。この属性名は「**memberUid**」です。このフィールドが空白のまま残されると、フィルターの属性名はデフォルトの **memberOf** になります。

### ログイン許可属性

ユーザーが LDAP サーバーを通じて正常に認証された場合、ユーザーのログイン許可を取り出す必要があります。ログイン許可を検索するには、サーバーに送信される検索フィルターでログイン許可に関連付けられている属性名を指定する必要があります。「**ログイン許可属性**」フィールドは、その属性名を指定します。認証と承認に LDAP サーバーを使用していて、このフィールドを空白のまま残した場合、ユーザーはアクセスを拒否されます。

LDAP サーバー検索から返される属性値は、13 個の連続した 0 または 1 として入力されたビット・ストリング、または合計 13 個の連続した 0 または 1 として入力されたビット・ストリングである必要があります。各ビットは、各機能の設定を表します。ビットは、その位置に応じて番号付けられています。左端のビットはビット位置 0 で、右端のビットはビット位置 12 です。ビット位置の値が 1 の場合、そのビット位置に関連付けられている関数が有効になります。あるビット位置の値が 0 の場合、そのビット位置に関連付けられた機能は無効になります。文字列 0100000000000 は有効な例であり、任意のフィールドに配置できるようにするために使用されます。使用する属性は、自由な形式のストリングが可能です。属性が正常に取り出された場合、LDAP サーバーから返された値は、以下の表の説明に従って解釈されます。

表 1. 許可ビット

ビット位置の説明を含む 3 列の表。

ビット位置	機能	説明
0	常に拒否	ユーザーは常に認証に失敗します。この機能は、特定のユーザーまたは特定のグループと関連付けられているユーザーをブロックするために使用されます。
1	スーパーバイザー・アクセス権	ユーザーに管理者特権が付与されます。ユーザーは、すべての機能に対して読み取り/書き込みアクセス権を持ちます。このビットを設定した場合、他のビットを個別に設定する必要はありません。
2	読み取り専用アクセス権	ユーザーは読み取り専用のアクセス権を持ち、保守手順(たとえば、再起動、リモート操作、またはファームウェア更新など)や変更操作(たとえば、保存、消去、または復元機能など)を行うことはできません。ビット位置 2 と他のすべてのビットは相互に排他的で、ビット位置 2 の優先順位が最下位です。他のいずれかのビットが設定されている場合、このビットは無視されます。
3	構成 - ネットワーキングおよび BMC セキュリティー	ユーザーは、「セキュリティ」、「ネットワーク・プロトコル」、「ネットワーク・インターフェース」、「ポート割り当て」、および「シリアル・ポート」の構成を変更できます。
4	ユーザー・アカウント管理	このユーザーは、ユーザーの追加、変更、または削除を行うことができ、「ログイン・プロファイル」ウィンドウで「グローバル・ログイン」設定を変更できます。
5	リモート・コンソール・アクセス	このユーザーは、リモート・サーバーのリモート・サーバー・コンソールにアクセスすることができます。
6	リモート・コンソールおよびリモート・ディスクのアクセス	このユーザーは、リモート・サーバーのリモート・サーバー・コンソールおよびリモート・ディスク機能にアクセスすることができます。
7	リモート・サーバー電源/再起動アクセス	ユーザーは、リモート・サーバーの電源オン機能と再起動機能にアクセスできます。
8	構成 - 基本	ユーザーは、「システム設定」ウィンドウおよび「アラート」ウィンドウで構成パラメーターを変更できます。
9	イベント・ログをクリアする権限	このユーザーはイベント・ログを消去することができます。 注：すべてのユーザーがイベント・ログを表示できますが、ログを消去するには、ユーザーにこのレベルの権限が必要です。
10	構成 - 拡張 (ファームウェア更新、BMC の再起動、構成の復元)	ユーザーは、XClarity Controller を構成するときに何も制約を受けません。さらに、ユーザーは XClarity Controller に対する管理アクセス権限を持ちます。ユーザーは、ファームウェア・アップグレード、PXE ネットワーク・ブート、アダプターの出荷時デフォルト値のリストア、構成ファイルに入っているアダプター構成の変更とリストア、およびアダプターの再始動とリセットなどの拡張機能を実行することができます。

表 1. 許可ビット (続き)

ビット位置	機能	説明
11	構成 - UEFI セキュリティー	ユーザーは UEFI セキュリティー関連設定を構成できますが、UEFI FI セキュリティー・セットアップ・ページから構成することもできます。
12	予約済み	将来の使用のために予約されており、現在は無視されています。

どのビットも設定されていない場合、ユーザーはアクセスを拒否されます

注：ユーザー・レコードから直接検索されるログイン許可には優先順位があることに注意してください。ユーザーのレコードにログイン許可属性が含まれていない場合、ユーザーが属しており、構成されていれば、グループ・フィルターに一致するグループから権限の取得が試行されます。この場合、ユーザーには、すべてのグループのすべてのビットの包含 OR が割り当てられます。同様に、「読み取り専用アクセス権」ビットはその他のビットがすべてゼロの場合にのみ設定されます。さらに、「常に拒否」ビットがいずれかのグループに設定されている場合、ユーザーはアクセスを拒否されるので注意してください。「常に拒否」ビットの優先順位は、常にその他のすべてのビットよりも高くなります。

**重要：**ユーザーに基本、ネットワーク、および/またはセキュリティ関連のアダプター構成パラメーターを変更する権限が付与する場合、そのユーザーに XClarity Controller を再起動する権限 (ビット位置 10) を付与することを検討してください。この権限がない場合、ユーザーはパラメーター (アダプターの IP アドレスなど) の変更はできても、そのパラメーターを有効にできない場合があります。

- 「認証のみに LDAP サーバーを使用する (ローカル承認)」モードを使用する場合は、「ローカル承認用グループ」を構成します。グループ名、グループ・ドメイン、および役割は、ユーザーのグループにローカル承認を提供するように構成されています。各グループには、ローカル・ユーザーの役割で構成されているのと同じ役割 (アクセス許可) を割り当てることができます。ユーザー・アカウントは、LDAP サーバー上の異なるグループに割り当てられます。ユーザー・アカウントには、BMC へのログイン後に、このユーザー・アカウントが属するグループの役割 (権限) が割り当てられます。グループ・ドメインは、識別名と同じ形式 (dc=mycompany,dc=com など) にする必要があります。これは、グループ検索の基本オブジェクトとして使用されます。フィールドを空白のままにすると、「ルート DN」フィールドと同じ値が使用されます。「+」アイコンをクリックしてグループを追加したり、「x」アイコンをクリックして削除したりできます。
- 「ユーザー名の表示に使用する属性を指定」ドロップダウン・メニューから、ユーザー名の表示に使用する属性を選択します。

## ネットワーク・プロトコルの構成

XClarity Controller のネットワーク設定を表示または確立するには、このトピックの情報を使用します。

## イーサネット設定の構成

XClarity Controller がイーサネット接続を使用して通信する方法を表示または変更するには、トピックの情報を使用します。

注：AMD サーバーは、イーサネット・フェイルオーバー機能をサポートしていません。

XClarity Controller は 2 つのネットワーク・コントローラーを使用します。1 つのネットワーク・コントローラーは専用管理ポートに接続され、もうひとつのネットワーク・コントローラーは共有ポートに接続されています。ネットワーク・コントローラーにはそれぞれ、独自の組み込み MAC アドレスが割り当てられています。XClarity Controller に IP アドレスを割り当てるために DHCP が使用されている場合、ユーザーがネットワーク・ポートを切り替えたり、専用ネットワーク・ポートから共有ネットワーク・ポート

へのフェイルオーバーが発生すると、別の IP アドレスが DHCP サーバーによって XClarity Controller に割り当てられる場合があります。DHCP を使用する場合は、XClarity Controller へのアクセスは IP アドレスよりもホスト名を使用することをお勧めします。XClarity Controller ネットワーク・ポートが変更されない場合でも、DHCP サーバーのリースが切れた場合や、XClarity Controller がリブートした場合に、DHCP サーバーによって別の IP アドレスが割り当てられる可能性があります。変更されない IP アドレスを使用して XClarity Controller にアクセスする必要がある場合は、DHCP ではなく静的 IP アドレスを使用するように XClarity Controller を構成する必要があります。

「BMC 構成」の下にある「ネットワーク」をクリックして XClarity Controller のイーサネット設定を変更します。

## XClarity Controller のホスト名の構成

XClarity Controller のデフォルトのホスト名は、文字列「XCC-」の後ろにサーバーのマシン・タイプとサーバーのシリアル番号が続く組み合わせで生成されます (例: 「XCC-7X03-1234567890」)。XClarity Controller のホスト名は、このフィールドに 63 文字以内を入力して変更できます。ホスト名にはピリオド (.) は使用できません。アルファベット、数字、ハイフンおよびアンダースコアのみを含めることができます。

## イーサネット・ポート

この設定は、管理コントローラーによって使用されるイーサネット・ポート (共有ポートや専用ポートなど) の有効化を制御します。

無効にすると、すべてのイーサネット・ポートに IPv4 や IPv6 のアドレスが割り当てられなくなり、イーサネット構成に対する変更は何もできなくなります。

注：この設定は、サーバーの前面にある USB LAN インターフェースまたは USB 管理ポートには影響しません。これらのインターフェースには、それぞれに独自の有効化設定があります。

## IPv4 ネットワーク設定の構成

IPv4 イーサネット接続を使用するには、以下のステップを実行します。

1. 「IPv4」オプションを有効にします。

注：イーサネット・インターフェースを無効にすることで、外部ネットワークから XClarity Controller へのアクセスを防ぐことができます。

2. 「メソッド」フィールドから、以下のいずれかのオプションを選択します。

- **DHCP から IP を取得する**: XClarity Controller は DHCP サーバーから IPv4 アドレスを取得します。
- **静的 IP アドレスを使用する**: XClarity Controller は、ユーザーがその IPv4 アドレスに指定した値を使用します。
- **最初に DHCP、次に静的 IP アドレス**: XClarity Controller は DHCP サーバーから IPv4 アドレスを取得しようと試みます。失敗した場合は、ユーザーがその IPv4 アドレスに指定した値を使用します。

3. 「静的 IPv4 アドレス」フィールドに、XClarity Controller に割り当てる IP アドレスを入力します。

注：この IP アドレスには 0 から 255 までの 4 つの整数がピリオドで区切られて入っている必要があり、スペースが含まれてはなりません。メソッドが「DHCP から IP を取得する」に設定されている場合は、このフィールドは構成できません。

4. 「ネットワーク・マスク」フィールドに、XClarity Controller が使用するサブネット・マスクを入力します。

注：このサブネット・マスクには 0 から 255 までの 4 つの整数がピリオドで区切られて入っている必要があり、スペースや連続したピリオドが含まれてはなりません。デフォルトの設定値は 255.255.255.0 です。メソッドが「DHCP から IP を取得する」に設定されている場合は、このフィールドは構成できません。

5. 「デフォルト・ゲートウェイ」フィールドに、使用するネットワーク・ゲートウェイ・ルーターを入力します。

注：このゲートウェイ・アドレスには0から255までの4つの整数がピリオドで区切られて入っている必要があり、スペースや連続したピリオドが含まれてはなりません。メソッドが「DHCP から IP を取得する」に設定されている場合は、このフィールドは構成できません。

### 拡張イーサネット設定の構成

イーサネットの追加設定を行うには、「拡張イーサネット」タブをクリックします。

仮想 LAN (VLAN) タギングを有効にするには、「VLAN を有効にする」チェック・ボックスを選択します。VLAN が有効になり、VLAN ID が構成されると、XClarity Controller は指定された VLAN ID のパケットのみを受け入れます。VLAN ID は、1 から 4094 の数値を使用して構成することができます。

「MAC アドレス」リストから、以下のいずれかの選択項目を選択します。

- **組み込み MAC アドレスを使用する**

出荷時書き込み MAC アドレス・オプションは、製造元によってこの XClarity Controller に割り当てられている固有な物理アドレスです。このアドレスは読み取り専用フィールドです。

- **カスタム MAC アドレスを使用する**

値を指定した場合は、ローカル管理アドレスが組み込み MAC アドレスをオーバーライドします。ローカル管理アドレスは、000000000000 から FFFFFFFF までの 16 進値である必要があります。この値は xx:xx:xx:xx:xx:xx 形式であり、x は 0 から 9 または a から f までの 16 進数の数字でなければなりません。XClarity Controller では、マルチキャスト・アドレスの使用はサポートされていません。マルチキャスト・アドレスの最初のバイトは奇数です (最下位ビットが 1 にセットされています)。したがって、最初のバイトは偶数でなければなりません。

「データ・レートと二重」フィールドで、「自動ネゴシエーション」または「カスタム」を選択して、データ・レートと二重を指定します。

「MTU (最大転送単位)」フィールドには、使用するネットワーク・インターフェースでのパケットの最大伝送単位 (バイト単位) を指定します。最大伝送単位範囲は 1,000 ～ 1,500 です。このフィールドのデフォルト値は 1,500 です。

### IPv6 ネットワーク設定の構成

1. 「IPv6」オプションを有効にします。
2. 以下のいずれかの割り当て方法を使用して、インターフェースに IPv6 アドレスを割り当てます。
  - ステートレス・アドレス自動構成を使用する
  - ステートフル・アドレス構成 (DHCPv6) を使用する
  - 静的に割り当てられた IP アドレスを使用する

注：「静的に割り当てられた IP アドレスを使用する」が選択されている場合は、以下の情報の入力を求められます。

- IPv6 アドレス
- 接頭部の長さ
- ゲートウェイ

### DNS の構成

XClarity Controller のドメイン・ネーム・システム (DNS) 設定を表示または変更するには、このトピックの情報を使用します。

「BMC 構成」の下にある「ネットワーク」をクリックして XClarity Controller の DNS 設定を表示または変更します。

「追加の DNS アドレス・サーバーを使用する」チェック・ボックスをクリックした場合は、ネットワーク上にある最大 3 台までのドメイン・ネーム・システム・サーバーの IP アドレスを指定します。各 IP アドレスは、0 から 255 までの整数をピリオドで区切って指定し、スペースを含めてはなりません。これらの DNS サーバー・アドレスは検索リストのトップに追加されるため、ホスト名検索は、これらのサーバー上で行われてから、DHCP サーバーによって自動的に割り当てられる DNS サーバー上で行われます。

「DNS を使用して Lenovo XClarity Administrator を検出する」チェック・ボックスをクリックした場合は、XClarity Manager を選択する必要があります。

## DDNS の構成

XClarity Controller の動的ドメイン・ネーム・システム (DDNS) プロトコルを有効または無効にするには、このトピックの情報を使用します。

「BMC 構成」の下にある「ネットワーク」をクリックして XClarity Controller の DDNS 設定を表示または変更します。

DDNS を有効にするには、「DDNS を有効にする」チェック・ボックスをクリックします。DDNS を有効にすると、XClarity Controller はドメイン・ネーム・サーバーに対して、XClarity Controller の構成済みのホスト名、アドレス、またはドメイン・ネーム・サーバーに保管されているその他の情報のアクティブなドメイン・ネーム・サーバー構成をリアルタイムに変更するように通知します。

項目リストからオプションを選択し、XClarity Controller のドメイン名の選択方法を決定します。

- **カスタムのドメイン名を使用する:** XClarity Controller が属するドメイン名を指定できます。
- **DHCP サーバーから取得したドメイン名を使用する:** XClarity Controller が属するドメイン名は、DHCP サーバーによって指定されます。

## Ethernet over USB の構成

サーバーと XClarity Controller 間のインバンド通信に使用する Ethernet over USB インターフェースを制御するには、このトピックの情報を使用します。

「BMC 構成」の下にある「ネットワーク」をクリックして XClarity Controller の Ethernet over USB 設定を表示または変更します。

Ethernet over USB は、XClarity Controller へのインバンド通信に使用されます。Ethernet over USB インターフェースを有効または無効にするには、チェック・ボックスをクリックします。

### 重要:

- **Ethernet Over USB を無効にすると、XClarity Essentials インバンド更新ユーティリティを使用する XClarity Controller ファームウェアまたはサーバー・ファームウェアのインバンド更新を実行できません。**ファームウェアを更新するには、XClarity Controller Web インターフェースの「ファームウェア更新」オプションまたは XClarity Essentials アウト・オブ・バンド更新ユーティリティを使用します。
- **USB インバンド・インターフェースが無効になっているときにサーバーが予期せず再起動しないように、ウォッチドッグ・タイムアウトを無効にすることが重要です。**
- **このインターフェースを使用するには、この機能をサポートするオペレーティング・システム・ドライバー (Windows の場合は RNDIS、Linux の場合は cdc\_ether および usbnet) がインストールされている必要があります。**XClarity Controller は、Windows が XClarity Controller USB デバイスを RNDIS デバイスとして認識できるようにする Windows 用の INF ファイルを提供します。

XClarity Controller が Ethernet over USB インターフェースのエンドポイントにアドレスを割り当てる方法を選択します。

- **Ethernet over USB に IPv6 リンク・ローカル・アドレスを使用する:** この方法は、Ethernet over USB インターフェースのエンドポイントに割り当てられた MAC アドレスに基づく IPv6 アドレスを使用します。通常、IPv6 リンク・ローカル・アドレスは、MAC アドレス (RFC 4862) を使用して生成されていますが、Windows 2008 および最新の 2016 オペレーティング・システムでは、インターフェースのホスト側で静的リンク・ローカル IPv6 アドレスをサポートしません。代わりに、デフォルトの Windows の動作では、実行中にランダムなリンク・ローカル・アドレスを再生成します。XClarity Controller Ethernet over USB インターフェースが IPv6 リンク・ローカル・アドレス・モードを使用するように構成されている場合、Windows がこのインターフェースに割り当てたアドレスが XClarity Controller 側でわからないため、このインターフェースを利用するさまざまな機能が動作しなくなります。サーバーで Windows を実行している場合は、他の Ethernet over USB アドレス構成方法を使用するか、コマンド `netsh interface ipv6 set global randomizeidentifiers=disabled` を使用してデフォルトの Windows の動作を無効にしてください
- **Ethernet over USB の IPv4 設定を構成する:** この方法では、XClarity Controller および Ethernet over USB インターフェースのサーバー側に割り当てる IP アドレスとネットワーク・マスクを指定します。

注：

- XClarity Controller の IP アドレス、OS の IP アドレス、およびネットワーク・マスクを構成した後、ローカル・オペレーティング・システムで Ethernet over USB インターフェースの IP アドレスを手動で構成する必要があります。
- OS の IP アドレス設定は、ウォッチドッグ・ステータス監視やインバンド・ファームウェア更新などの通信目的で、XClarity Controller に Ethernet over USB ネットワーク (オペレーティング・システム) の反対側を認識させるために使用されます。

外部イーサネット・ポート番号から USB 上のイーサネット・ポート番号へのマッピングを制御するには、「外部イーサネットから Ethernet over USB ポートへの転送を有効にする」チェック・ボックスをクリックして、管理ネットワーク・インターフェースからサーバーに転送するポートのマッピング情報を入力します。

## SNMP の構成

SNMP エージェントを構成するには、このトピックの情報を使用します。

XClarity Controller SNMP アラート設定を構成するには、以下のステップを実行します。

1. 「BMC 構成」の下にある「ネットワーク」をクリックします。
2. SNMPv3 エージェント、SNMPv1 トラップ、SNMPv2 トラップ、または SNMPv3 トラップを有効にするには、対応するチェック・ボックスにチェック・マークを付けます。

注：

- SNMPv3 エージェントを有効にするには、BMC の連絡先と場所を指定する必要があります。
  - SNMPv3 エージェントを有効にすると、XClarity Controller ユーザー・アカウントごとに SNMPv3 を構成できます。
  - トラップを受信するには、SNMP トラップと SNMPv3 エージェントの両方を有効にする必要があります
3. SNMPv1 トラップまたは SNMPv2 トラップを有効にした場合は、以下のフィールドに入力します。
    - a. 「コミュニティ名」フィールドに、コミュニティ名を入力します。コミュニティ名を空にすることはできません。
    - b. 「ホスト」フィールドに、ホスト・アドレスを入力します。
  4. SNMPv3 トラップを有効にした場合は、以下のフィールドに入力します。

- a. 「エンジン ID」フィールドに、エンジン ID を入力します。エンジン ID を空にすることはできません。
- b. 「トラップ・レシーバー・ポート」フィールドに、ポート番号を入力します。デフォルトのポート番号は 162 です。

5. SNMP トラップを有効にした場合は、アラートを受け取るイベント・タイプを以下から選択します。

- クリティカル
- 注意
- システム

注：各主要カテゴリーをクリックし、アラート対象のサブカテゴリー・イベント・タイプをさらに選択します。

6. 「SNMPv3 エージェント」を有効にする場合は、以下を実行します。
  - a. 「BMC 構成」の下にある「ユーザー/LDAP」をクリックします。
  - b. 対応するユーザーの横にある「編集」ボタンをクリックし、「ユーザー・アクセス可能インターフェース」のドロップダウン・リストの下にある「SNMP」をオンにします。

注：「テスト・トラップを送信」の横にある「送信」ボタンをクリックして、SNMP 設定を確認します。

## IPMI ネットワーク・アクセスの有効化

XClarity Controller への IPMI ネットワーク・アクセスを制御するには、このトピックの情報を使用します。

IPMI over LAN アクセスを有効にするには、次の手順を実行します。

1. 「BMC 構成」の下にある「ネットワーク」をクリックして XClarity Controller の IPMI 設定を表示または変更します。
2. 「サービスの有効化とポートの割り当て」の下にある「IPMI over LAN」スイッチをクリックして、XClarity Controller への IPMI ネットワーク・アクセスを有効にします。
3. 「BMC 構成」の下にある「ユーザー/LDAP」をクリックします。
4. 対応するユーザーの横にある「編集」ボタンをクリックし、「ユーザー・アクセス可能インターフェース」のドロップダウン・リストの下にある「IPMI over Lan」をオンにします。

**重要：**

- IPMI プロトコルを使用したネットワーク経由で XClarity Controller にアクセスするツールやアプリケーションを使用していない場合は、セキュリティ向上のために、IPMI ネットワーク・アクセスを無効にすることを強くお勧めします。
- XClarity Controller への IPMI over LAN アクセスは、デフォルトで無効になっています。

## IPMI コマンドを使用したネットワーク設定の構成

IPMI コマンドを使用したネットワーク設定を構成するには、このトピックの情報を使用します。

各 BMC ネットワーク設定は個別の IPMI 要求を使用して特定の順序はなく構成されるため、BMC が再起動され保留中のネットワークの変更が適用されるまでは、BMC にすべてのネットワーク設定が完全には表示されません。ネットワーク設定を変更する要求は、要求されたときに成功することもあります。後で追加の変更が要求されたときに無効と判断される場合があります。BMC の再起動時に保留中のネットワーク設定が BMC と互換性がない場合、その新規設定は適用されません。BMC を再起動した後、新しい設定を使用して BMC にアクセスしてみて、設定が想定どおりに適用されていることを確認してください。



## サービスの有効化とポートの割り当て

XClarity Controller の一部のサービスで使用するポート番号を表示または変更するには、このトピックの情報を参照します。

「BMC 構成」の下にある「ネットワーク」をクリックして XClarity Controller のポートの割り当てを表示または変更します。ポート割り当てを表示または変更するには、以下のフィールドに入力します。

### HTTPS (Web/Redfish)

この項目は常に有効です。このフィールドで、Web Over HTTPS のポート番号を指定します。デフォルト値は 443 です。

### Remote Presence

この項目は常に有効です。ポート番号は 443 です。

### IPMI over LAN

ポート番号は 623 です。このフィールドはユーザーが構成することはできません。

注：ユーザー/LDAP ページの対応するユーザーの「ユーザー・アクセス可能インターフェース」フィールドで「IPMI over LAN」が選択され、適用されていることを確認します。

### SSDP

ポート番号は 1900 です。このフィールドはユーザーが構成することはできません。

### SSH

このフィールドで、SSH プロトコルを介してコマンド・ライン・インターフェースにアクセスするために構成されたポート番号を指定します。デフォルト値は 22 です。

### SNMP Agent

このフィールドで、XClarity Controller 上で稼働する SNMP エージェントのポート番号を指定します。デフォルト値は 161 です。有効なポート番号の値は、1 から 65535 までです。

注：ユーザー/LDAP ページの対応するユーザーの「ユーザー・アクセス可能インターフェース」フィールドで「SNMP」が選択され、適用されていることを確認します。

## アクセス制限の構成

IP アドレスまたは MAC アドレスから XClarity Controller へのアクセスをブロックする設定を表示または変更するには、このトピックの情報を参照します。

「BMC 構成」の下にある「ネットワーク」をクリックして XClarity Controller のアクセス制御設定を表示または変更します。

### ブロック・リストと時間制限

これらのオプションを使用すると、特定の IP/Mac アドレスを特定の期間ブロックすることができます。

#### • ブロックされている IP アドレスのリスト

- XClarity Controller へのアクセスを許可しない IPv4 アドレスまたは範囲を最大 3 件、および IPv6 アドレスまたは範囲を 3 件、コマンドで区切って入力できます。以下の IPv4 の例を参照してください。
- 単一の IPv4 アドレスのサンプル: 192.168.1.1
- スーパーネット IPv4 アドレスのサンプル: 192.168.1.0/24
- IPv4 範囲のサンプル: 192.168.1.1-192.168.1.5

#### • ブロックされている MAC アドレスのリスト

- XClarity Controller へのアクセスを許可しない MAC アドレスを最大 3 件、コンマで区切って入力できます。例: 11:22:33:44:55:66。
- **アクセスが制限される場所 (1 回限り)**
  - XClarity Controller にアクセスできない 1 回限りの時間間隔をスケジュールできます。指定した時間間隔について:
    - 開始日時が現在の XCC 時刻よりも後でなければなりません。
    - 終了日時が開始時刻よりも後でなければなりません。
- **アクセスが制限される場所 (毎日)**
  - XClarity Controller にアクセスできない 1 回以上の時間間隔をスケジュールできます。指定した各時間間隔について:
    - 終了日時が開始時刻よりも後でなければなりません。

### 外部トリガー・ブロック・リスト

以下のオプションを使用すると、特定の IP アドレス (IPv4 および IPv6) の自動ブロックを設定し、クライアントが不正なユーザー名またはパスワードをさまざまに使用して XClarity Controller へのログイン試行を成功させるのを防ぐことができます。

自動ブロッキングは、特定の IP アドレスからログイン障害が過度に発生したことを動的に判断し、そのアドレスが XClarity Controller にアクセスするのを、事前に定義された時間だけブロックします。

- **特定の IP からの最大ログイン失敗数**
  - 最大回数とは、ユーザーがロックアウトされるまでに、特定の IP アドレスから誤ったパスワードを使用してログイン障害になることが許可された回数を言います。
  - 0 を設定すると、ログイン障害によって IP アドレスがロックされることはありません。
  - 特定の IP アドレスからのログイン障害の回数は、その IP アドレスから正常にログインした後、0 にリセットされます。
- **IP をブロックするロックアウト期間**
  - ユーザーがロックされた IP アドレスから再度ログインを試行できるようになるまでに必要な最短時間 (分単位)。
  - 0 を設定すると、管理者が明示的にロックを解除しない限り、ロックされた IP アドレスからのアクセスはブロックされたままになります。
- **ブロック・リスト**
  - ブロック・リストの表には、ロックされているすべての IP アドレスが表示されます。ブロック・リストから 1 つまたはすべての IP アドレスのロックを解除できます。

## 前面パネル USB ポートから管理への構成

XClarity Controller の前面パネル USB ポートから管理への構成を行うには、このトピックの情報を使用します。

XClarity Controller への接続は、主に Lenovo XClarity Mobile アプリを実行するモバイルデバイスと併せて使用します。モバイル・デバイスとサーバーの前面パネルが USB ケーブルで接続されている場合、デバイスで実行しているモバイル・アプリと XClarity Controller 間で Ethernet over USB 接続が確立されます。

一部のサーバーでは、前面パネル USB ポートを切り替えることで、サーバーまたは XClarity Controller に接続できます。

注：この機能は、今後のアップデートでサポートされる予定です。

---

## セキュリティ設定の構成

セキュリティ・プロトコルを構成するには、このトピックの情報を 사용합니다。

注：TLS の最低バージョンのデフォルト設定は TLS 1.2 ですが、ブラウザや管理アプリケーションが必要であれば、他の TLS バージョンを使用するように XClarity Controller を構成できます。詳しくは、[132 ページの「tls コマンド」](#)を参照してください。

「BMC 構成」の下の「セキュリティ」をクリックして、XClarity Controller のセキュリティのプロパティ、ステータス、および設定にアクセスし、構成します。

## セキュリティ・ダッシュボード

このトピックは、セキュリティ・ダッシュボードの概要です。

セキュリティ・ダッシュボードには、システムの全体的なセキュリティ評価とステータスが表示されます。

- **BMC セキュリティ・イベント**は、シャーシへの侵入、PFR により検出された破損、システム・ガードにより検出されたハードウェアの不整合、プレーナー上の開いたセキュリティ・ジャンパーなど、セキュリティの問題によってアサートされたイベントを報告します。
- 「**BMC セキュリティ・モード**」には、セキュリティ・モード・コンプライアンスの全体的なステータスが表示されます。
- 「**BMC サービスおよびポート**」は、有効になっているが現在のセキュリティ・モードに準拠していない、非セキュアなサービス/ポートがすべて列挙されます。
- 「**BMC 証明書**」には、XCC によって使用される非準拠の証明書がすべてリストされます。
- 「**BMC ユーザー・アカウント**」には、アカウントおよびパスワード管理のセキュリティを強化する方法に関する一般的な情報が表示されます。

注：XCC によってスキャンされたセキュリティ領域にリスクが生じた場合、ダッシュボードに警告アイコンが表示されます。各カテゴリー下の「**詳細**」リンクをクリックすると、ユーザーはセットアップ・ページに移動して問題を解決できます。

## セキュリティ・モード

このトピックは、セキュリティ・モードの概要です。

XCC 標準ライセンスを使用すると、ユーザーは2つのセキュリティ・モード (標準モードと互換性モード) でサーバーを構成することができます。これらはすべての V4 サーバーで使用できます。

Lenovo XClarity Controller 3 Premier アップグレード・ライセンスでは、3つ目のセキュリティ・モードであるエンタープライズ・ストリクト・モードを利用できます。このモードは、セキュリティ要件のレベルが高い場合に最も適しています。

注：デフォルトでは、XCC は ECDSA 自己署名証明書を使用し、ECDSA ベースのアルゴリズムのみ使用できます。RSA ベースの証明書を使用するには、CSR を生成し、内部または外部 CA で署名した後、署名された証明書を XCC にインポートします。

### エンタープライズ・ストリクト・セキュリティ・モード

- エンタープライズ・ストリクト・セキュリティ・モードが最もセキュアなモードです。
- BMC によって使用されるすべての暗号化アルゴリズムは CNSA 1.0 に準拠しています。
- BMC は FIPS 140-3 で検証されたモードで動作します。

- エンタープライズ・ストリクト・グレードの証明書が必要です。
- CNSA 1.0 暗号化をサポートするサービスのみを有効にできます。
- Feature on Demand キーを有効にする必要があります。

#### 標準セキュリティー・モード

- 標準モードはデフォルトのセキュリティー・モードです。
- BMC によって使用されるすべての暗号化アルゴリズムは FIPS 140-3 に準拠しています。
- すべての有効なサービスで FIPS 140-3 準拠の暗号化が使用されている場合、BMC は FIPS 140-3 検証済みモードで動作します。
- 標準グレードの証明書が必要です。
- FIPS 140-3 準拠の暗号化をサポートしない暗号化を必要とするサービスは、デフォルトでは無効になっています。

#### 互換性モード

- 互換性モードは、サービスおよびクライアントでエンタープライズ・ストリクト/標準準拠ではない暗号化が必要な場合に使用するモードです。
- より広範な暗号化アルゴリズムがサポートされています。
- このモードが有効になっている場合、BMC は標準検証済みモードで動作しません。
- すべてのサービスを有効にすることができます。

#### サポートされる TLS 暗号スイート

TLS 暗号化設定は、サポートされる TLS 暗号スイートを BMC サービスに対して制限するために使用されます。

TLS 暗号スイート	セキュリティー・モード	TLS バージョン
TLS_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• エンタープライズ・ストリクト</li> <li>• 標準*</li> <li>• 互換性*</li> </ul>	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	<ul style="list-style-type: none"> <li>• 互換性</li> </ul>	TLS 1.3
TLS_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>• 標準</li> <li>• 互換性</li> </ul>	TLS 1.3
TLS_AES_128_CCM_SHA256	<ul style="list-style-type: none"> <li>• 標準</li> <li>• 互換性</li> </ul>	TLS 1.3
TLS_AES_128_CCM_8_SHA256	<ul style="list-style-type: none"> <li>• 標準</li> <li>• 互換性</li> </ul>	TLS 1.3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• エンタープライズ・ストリクト</li> <li>• 標準*</li> <li>• 互換性*</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• エンタープライズ・ストリクト</li> <li>• 互換性*</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• エンタープライズ・ストリクト</li> </ul>	TLS 1.2

TLS 暗号スイート	セキュリティー・モード	TLS バージョン
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	<ul style="list-style-type: none"> <li>互換性</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305	<ul style="list-style-type: none"> <li>互換性</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>標準</li> <li>互換性</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>標準</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>標準</li> </ul>	TLS 1.2
TLS_RSA_WITH_AES_256_CBC_SHA256	<ul style="list-style-type: none"> <li>標準</li> </ul>	TLS 1.2
TLS_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>標準</li> </ul>	TLS 1.2

注：表にリストされているアスタリスク(\*)の付いたセキュリティー・モードでは、Lenovo XClarity Controller 3 Premier アップグレード・ライセンスが必要です。

### 3つのセキュリティー・モードのサービス・マトリックス

機能/サービス	暗号を使用	出荷時デフォルト状態	ストリクト・モードでサポートされる	標準モードでサポートされる	互換性モードでサポートされる
IPMI-over-KCS	いいえ	使用可能	はい	はい	はい
IPMI-over-LAN	はい	無効	いいえ	はい	はい

機能/サービス	暗号を使用	出荷時デフォルト状態	ストリクト・モードでサポートされる	標準モードでサポートされる	互換性モードでサポートされる
SNMPv1 トラップ	いいえ	構成なし	いいえ	はい	はい
SNMPv3 トラップ	はい	構成なし	いいえ	はい 有効な場合、FIPS 以外の暗号の使用が警告される	はい
SNMPv3 エージェント	はい	構成なし	いいえ	はい 有効な場合、FIPS 以外の暗号の使用が警告される	はい
メール・アラート	はい	構成なし	はい CRAM-MD5 認証によって有効にすることはできない	はい CRAM-MD5 が有効な場合、FIPS 以外の暗号の使用が警告される	はい
Syslog アラート	いいえ	構成なし	いいえ	はい	はい
TLS 1.2	はい	使用可能	はい	はい	はい
TLS 1.3	はい	使用可能	はい	はい	はい
Web over HTTPS	はい	使用可能	はい	はい	はい
Redfish over HTTPS	はい	使用可能	はい	はい	はい
SSDP	いいえ	使用可能	はい	はい	はい
SSH-CLI	はい	使用可能	はい	はい	はい
SFTP	はい	無効	はい	はい	はい
LDAP	いいえ	構成なし	いいえ	はい	はい
セキュア LDAP	はい	構成なし	はい	はい	はい
セキュリティー・キー管理	はい	構成なし	はい	はい	はい
リモート・コンソール	はい	使用可能	はい	はい	はい
仮想メディア - CIFS	はい	構成なし	いいえ	はい	はい
仮想メディア - NFS	いいえ	構成なし	いいえ	はい	はい
仮想メディア - HTTPFS	はい	構成なし	はい	はい	はい
RDOC - ローカル	はい	構成なし	はい	はい	はい
RDOC - CIFS	はい	構成なし	いいえ	はい	はい

機能/サービス	暗号を使用	出荷時デフォルト状態	ストリクト・モードでサポートされる	標準モードでサポートされる	互換性モードでサポートされる
RDOC - HTTP	いいえ	構成なし	いいえ	はい	はい
RDOC - HTTPS	はい	構成なし	はい	はい	はい
RDOC - FTP	いいえ	構成なし	いいえ	はい	はい
RDOC - SFTP	はい	構成なし	はい	はい	はい
FFDC アップロード (SFTP)	はい	使用可能	はい	はい	はい
FFDC アップロード (TFTP)	いいえ	使用可能	いいえ	はい	はい
リポジトリからの更新 - CIFS	はい	構成なし	いいえ	はい	はい
リポジトリからの更新 - NFS	いいえ	構成なし	いいえ	はい	はい
リポジトリからの更新 - HTTP	いいえ	構成なし	いいえ	はい	はい
リポジトリからの更新 - HTTPS	はい	構成なし	はい	はい	はい
コール・ホーム	はい	無効	はい	はい	はい
サード・パーティー・パスワード	はい	構成なし	いいえ	はい	はい
ポート転送	該当なし	無効	はい	はい	はい

## セキュリティー・モードの切り替え

セキュリティー・モードを切り替えて検証するには、このトピックの情報を使用します。

標準モードはデフォルトのセキュリティー・モードです。

通常、標準モードに準拠していない設定を XCC が検出した場合、XCC に通知が表示されますが、ユーザーに対してモードの変更は要求されません。この場合、XCC はオーバーライド (非準拠) によって標準セキュリティー・モードに入ります。

ユーザーは、ドロップダウン・メニューを開いて異なるモードを選択し、「**検証**」機能を使用して、XCC によって検出される非準拠項目の数を判別できます。

ユーザーが「**適用**」をクリックすると、XCC によって準拠項目も検証されます。

## SSL の概要

このトピックは、SSL セキュリティー・プロトコルの概要です。

SSL は、通信プライバシーを提供するセキュリティー・プロトコルです。SSL を使用すると、クライアント/サーバー・アプリケーションでは、盗聴、不正操作、およびメッセージの偽造が防止される方法で通信を行うことができます。セキュア Web サーバー (HTTPS)、セキュア LDAP 接続 (LDAPS)、CIM over

HTTPS、SSH サーバーなど、異なるタイプの接続に SSL サポートを使用し、SSL に必要な証明書を管理するように XClarity Controller を構成できます。

## SSL 証明書の処理

このトピックでは、SSL セキュリティー・プロトコルに使用できる証明書の管理について説明します。

WEB、Redfish、および LDAP クライアントは、同じ証明書構成を使用します。SSL 証明書の構成を変更する場合は、必ず SSL 接続を再確立する必要があります。SSL は、自己署名証明書またはサード・パーティーの認証局が署名した証明書のいずれかで使用できます。自己署名証明書の使用は、SSL を使用するための最も簡単な方法ですが、わずかにセキュリティ上のリスクがあります。このリスクは、SSL クライアントが、クライアントとサーバー間で最初に試行された接続の SSL サーバーの ID を検証する方法がないために発生します。悪意のある第三者がサーバーになりすまし、XClarity Controller とブラウザの間を流れるデータを傍受する可能性があります。ブラウザと XClarity Controller の間の初回接続時に、自己署名証明書がブラウザの証明書ストアにインポートされると、(初回接続で攻撃により暗号漏えいされなかったことを前提として) その後のすべての通信はそのブラウザではセキュアです。「SSL 証明書管理」ページを使用して鍵ペアと自己署名証明書を生成すると、SSL が有効になる場合があります。

セキュリティをより完全に行うには、認証局 (CA) によって署名された証明書を使用します。署名済み証明書を取得するには、以下の手順を実行します。

- 「SSL 証明書管理」の下の「生成」アイコンから「CSR (証明書署名要求) の生成」を選択します。
- 必須フィールドに入力し、「生成」を選択します。
- 自己署名証明書が生成されると、「SSL 証明書管理」に表示されます。
- 「ダウンロード」アイコンから「証明書署名要求 (CSR) のダウンロード」を選択して、署名済み証明書をダウンロードします。
- 署名済み証明書がダウンロードされたら、「CA 証明書管理」の下にある「署名済み証明書のインポート」アイコンを選択して、XClarity Controller にインポートします。

CA の機能は、XClarity Controller の ID を検査することです。証明書には、CA および BMC のデジタル署名が含まれています。既知の CA が証明書を発行する場合、または CA の証明書が既に Web ブラウザーにインポートされている場合、ブラウザは証明書を検証することができ、確実に BMC Web サーバーを識別できます。

SSL は、証明書内の XClarity Controller のホスト名 (または共通名) を、Web ブラウザーで表示されるホスト名と比較することに注意してください。

## SSL 証明書管理

このトピックでは、SSL セキュリティー・プロトコルを使用した証明書管理で選択できる操作の一部について説明します。

「BMC 構成」の下にある「セキュリティ」をクリックして、SSL 証明書管理を構成します。

XClarity Controller の証明書を管理する場合は、以下の操作が表示されます。

### 署名済み証明書のダウンロード

このリンクを使用して、現在インストールされている証明書のコピーをダウンロードします。証明書は PEM 形式または DER 形式でダウンロードできます。証明書の内容は、OpenSSL (<http://www.openssl.org>) などのサードパーティ・ツールを使用して表示できます。OpenSSL を使用して証明書の内容を表示するコマンド・ラインは、次の例に似たものになります。

```
openssl x509 -in cert.der -inform DER -text
```

### 証明書署名要求 (CSR) のダウンロード



このリンクを使用して、証明書署名要求のコピーをダウンロードします。CSR は PEM 形式または DER 形式でダウンロードできます。

### 署名済み証明書の生成

自己署名証明書を生成します。操作が完了すると、新しい証明書を使用して SSL が有効になる場合があります。

注：「署名済み証明書の生成」操作を実行すると、「HTTPS の自己署名証明書を生成」ウィンドウが開きます。必須フィールドとオプション・フィールドへの入力を促すプロンプトが出されます。必須フィールドには、**必ず**入力する必要があります。情報を入力したら、「生成」をクリックしてタスクを完了します。

### 証明書署名要求 (CSR) の生成

証明書署名要求 (CSR) の生成操作が完了すると、CSR ファイルがダウンロードされ、署名のために証明機関 (CA) に送信される場合があります。

注：「証明書署名要求 (CSR) の生成」操作を実行すると、「HTTPS の証明書署名要求を生成」ウィンドウが開きます。必須フィールドとオプション・フィールドへの入力を促すプロンプトが出されます。必須フィールドには、**必ず**入力する必要があります。情報を入力したら、「生成」をクリックしてタスクを完了します。

### 署名済み証明書のインポート

これを使用して署名済み証明書をインポートします。署名済み証明書を入手するには、まず証明書署名要求 (CSR) を生成して証明機関 (CA) に送信する必要があります。

## セキュア・シェル・サーバーの構成

SSH セキュリティー・プロトコルを理解して有効にするには、このトピックの情報を使用します。

「BMC 構成」の下にある「ネットワーク」をクリックして、セキュア・シェル・サーバーを構成します。

SSH プロトコルを使用するには、先に鍵を生成して SSH サーバーを有効にする必要があります。

注：

- このオプションを使用するのに、証明書管理は必要ありません。
- XClarity Controller は、最初に SSH サーバー鍵を作成します。新規の SSH サーバー鍵を生成する場合は、「BMC 構成」の下にある「ネットワーク」をクリックしてから、「SSH サーバー」の下にある「鍵の生成」をクリックします。
- 操作を完了した後、変更を有効にするために XClarity Controller を再起動する必要があります。

## キーボード・コントローラー・スタイル (KCS) 経由の IPMI のアクセス

XClarity Controller へのキーボード・コントローラー・スタイル (KCS) 経由の IPMI アクセスを制御するには、このトピックの情報を使用します。

XClarity Controller は、認証を必要としない KCS チャネル経由の IPMI インターフェースを提供します。

「BMC 構成」の下にある「セキュリティー」をクリックして、「IPMI over KCS アクセス」を有効または無効にします。

注：

- 設定を変更した後、変更を有効にするために XClarity Controller を再起動する必要があります。
- 「無効 (オンデマンドで有効)」に設定すると、ほとんどの場合 KCS チャネルは無効になりますが、システム・ファームウェア更新期間中に一部の Lenovo ツールが XClarity Controller と情報を交換でき

るようになります。これが発生すると、KCS チャンネルは数分間一時的に有効になり、完了時またはタイムアウト時に無効になります。

**重要：**IPMI プロトコル経由で XClarity Controller にアクセスするツールやアプリケーションをサーバーで実行していない場合は、セキュリティ向上のために、IPMI KCS アクセスを無効にすることを強くお勧めします。XClarity Essentials では、IPMI over KCS インターフェースを使用して XClarity Controller にアクセスします。IPMI over KCS インターフェースを無効にしている場合は、サーバーで XClarity Essentials を実行する前に、再度有効にしてください。完了後、インターフェースを無効にします。

## システム・ファームウェアのレベル・ダウンの禁止

システム・ファームウェアが古いファームウェア・レベルに変更されるのを防止するには、このトピックの情報を使用します。

この機能を使用すると、システム・ファームウェアを古いファームウェア・レベルに戻すことを許可するかどうかを決定できます。

「BMC 構成」の下にある「ネットワーク」をクリックして、「システム・ファームウェアのレベル・ダウンの禁止」を有効または無効にします。

加えられた変更は、XClarity Controller の再起動を必要とせずに即時に有効になります。

## セキュリティ鍵管理 (SKM) の構成

セキュリティ・キーを作成して管理するには、このトピックの情報を使用します。

この機能は、集中型鍵管理サーバーを使用してストレージ・ハードウェアのロックを解除するキーを提供し、ThinkSystem サーバーの SED に保管されているデータにアクセスできます。鍵管理サーバーには、SKLM - IBM SED 鍵管理サーバー、および Thales/Gemalto SED 鍵管理サーバー (KeySecure および CipherTrust) が含まれます。

注：この機能は、今後のアップデートでサポートされる予定です。

## Security password manager

サード・パーティー・パスワードを許可するには、このトピックの情報を使用します。

この機能を使用すると、サード・パーティー・パスワードの使用を許可するかどうかをユーザーが決定できます。

- **サード・パーティー・パスワード:** 有効にすると、ユーザーが指定したパスワード・ハッシュを BMC が認証に使用できるようになります。
- **サード・パーティー・パスワードの取得を許可する:** ユーザーは、BMC からのサード・パーティー・パスワード・ハッシュの取得を有効または無効にすることもできます。

## 拡張監査ログ

拡張監査ログを制御するには、このトピックの情報を使用します。

この機能により、LAN および KCS チャンネルからの IPMI set コマンド (raw データ) のログ項目を監査ログに含めるかどうかを決定することができます。

XCC Web の「BMC 構成」にある「セキュリティ」をクリックして、拡張監査ログを有効または無効にします。

注：IPMI set コマンドが LAN チャネルからの場合は、ユーザー名と送信元 IP アドレスがログ・メッセージに含まれます。また、機密のセキュリティー情報 (パスワードなど) を含むすべての IPMI コマンドは除外されます。

## ユーザー・アカウントあたりの同時ログインの制限

ユーザー・アカウントあたりの同時セッション数を制限するには、このトピックの情報を使用します。

この機能を使用すると、ユーザー・アカウントあたりに許可される同時セッション数をユーザーが決定できます。

- Web 同時セッションの数: 1 ~ 10 セッションの間で設定できます。
- コマンド・ライン同時セッションの数: 1 ~ 2 セッションの範囲で設定できます。
- Redfish 同時セッションの数: 1 ~ 16 セッションの間で設定できます。

注：合計セッション数が設定された数を超えた場合、ユーザーは新しいセッションを作成できなくなります。

## システム・ガード

このトピックでは、システム・ガードの概要を示します。

システム・ガード機能は、ハードウェア・コンポーネント・インベントリーのスナップショットをトラステッド参照として取得した後、参照スナップショットからの逸脱を監視します。逸脱が発生したら、イベントをユーザーに報告できます。オプションで、サーバーが OS からブートするのを抑制し、応答を求めるプロンプトをユーザーに表示することもできます。

機能が無効になっていても、ユーザーはいつでもスナップショットを取得できます。スナップショットの生成には約 1 分かかります。ユーザーは、適用するハードウェア・コンポーネントのサブセットを選択し、逸脱が検出された場合に実行する対応するアクションを選択できます。

注：逸脱の検出は、サーバーの電源オン (POST) またはシステム・リブート時に実行されます。たとえば、OS がまだ実行されているときに、ディスク・ドライブが引き出されてすぐに再挿入された場合、システム・ガードがイベントを記録したりアクションを実行したりすることはありません。引き出されたディスク・ドライブが次のリブートまで外したままの場合、システム・ガードが作動します。

注：AC 復元後の最初の電源オン時に、XCC は、以下の条件を満たしている場合、OS ブートを防ぐために UEFI に通知しないことがあります。

- システム・ガードが以下の設定で有効:
  - CPU または DIMM ハードウェアを選択
  - 「OS ブートを禁止する」オプションがオン
- 信頼されたスナップショットと一致しないハードウェア構成の変更。

XCC は POST 後に構成の不一致を報告します。この制限は、以降の OS リブートで保持されません。

## システム・ガードの有効化

システム・ガードを有効にするには、このトピックの情報を使用します。

システム・ガード機能は、デフォルトで無効になっています。エンド・ユーザーの要件に応じて出荷前に有効にされます。

XCC のデフォルトへのリセット・オプションを実行した場合も、システム・ガードが無効になり、スナップショット履歴を除く設定がクリアされます。

システム・ガードを有効にすると、ユーザーは、システム・ガード保護をオンにする前に、設定を確認するか、既存のトラステッド・スナップショットを使用するか、インベントリーを新しいトラステッド・スナップショットとしてキャプチャーするよう求められます。オンにすると、以下のようになります。

- システム電源がオフの場合、システム・ガードがハードウェア・インベントリーの取得をすぐに開始します。
- システム電源がオンの場合、システム・ガードはコンポーネントのインベントリー・データとトラステッド・スナップショットを比較します。

比較の結果、トラステッド・スナップショットから逸脱していることがわかった場合、「**ハードウェア構成が一致していないため準拠していません**」という警告が XCC に表示されます。不一致の詳細には、トラステッド・スナップショットと比較して、不足している/変更された/新しい各ハードウェア・コンポーネントが、場所/識別子/説明属性とともにリストされます。

ユーザーは、「スコープとアクション」パネルを通じて、システム・ガードのスコープとアクションを構成し、システムが非準拠になったときに実行するアクションを決定できます。

## TLS バージョン・サポート

さまざまなサポート対象の TLS バージョンを理解するには、このトピックの情報を使用します。

以下の TLS バージョンがサポートされています。

- TLS 1.2 以上
- TLS 1.3

サポートされている TLS 暗号スイートの完全なリストについては、[38 ページの「サポートされる TLS 暗号スイート」](#)を参照してください

---

## BMC 構成のバックアップと復元

このトピックでは、BMC 構成を復元または修正する方法について説明します。

「BMC 構成」の下にある「バックアップと復元」を選択して、以下の操作を実行します。

- 管理コントローラーの構成の要約の表示
- 管理コントローラーの構成のバックアップまたは復元
- バックアップまたは復元の状況表示
- 管理コントローラーの構成を工場出荷時の状態にリセット
- 管理コントローラーの初期セットアップ・ウィザードにアクセス

## BMC 構成のバックアップ

このトピックでは、BMC 構成をバックアップする方法について説明します。

「BMC 構成」の下にある「バックアップと復元」を選択します。一番上が「BMC 構成のバックアップ」セクションです。

以前にバックアップを行っている場合は、「最終バックアップ」フィールドに詳細が表示されます。

現在の BMC 構成をバックアップするには、以下に示されているステップを実行します。

1. BMC バックアップ・ファイルのパスワードを指定します。
2. ファイル全体を暗号化するか、機密データのみを暗号化するかを選択します。

3. 「バックアップを開始」をクリックして、バックアップ処理を開始します。処理中には、復元/リセット操作を実行できません。
4. 処理が完了すると、ファイルをダウンロードして保存するためのボタンが表示されます。

注：ユーザーが新しい XClarity Controller のユーザー/パスワードを設定し、構成のバックアップを実行すると、デフォルトのアカウント/パスワード (USERID/PASSWORD) も含まれます。次に、バックアップからデフォルトのアカウント/パスワードを削除すると、XClarity Controller アカウント/パスワードの復元でエラーが発生したことをユーザーに通知するメッセージがシステムで表示されます。ユーザーはこのメッセージは無視しても構いません。

## BMC 構成の復元

このトピックでは、BMC 構成を復元する方法について説明します。

「BMC 構成」の下にある「バックアップと復元」を選択します。「BMC 構成のバックアップ」の下に「構成ファイルからの BMC の復元」セクションがあります。

以前に保存された構成に BMC を復元するには、以下に示されている手順に従います。

1. 参照してバックアップ・ファイルを選択し、プロンプトが表示されたらパスワードを入力して、「次へ」をクリックします。
2. 「詳細の表示」をクリックして、ファイルを確認します。
3. 内容を確認した後、「復元を開始」をクリックします。

## BMC の出荷時のデフォルト値へのリセット

このトピックでは、BMC を出荷時のデフォルト設定にリセットする方法について説明します。

「BMC 構成」の下にある「バックアップと復元」を選択します。「構成ファイルからの BMC の復元」の下に「BMC を出荷時のデフォルト値にリセット」セクションがあります。

出荷時のデフォルト値に BMC をリセットするには、以下に示されている手順に従ってください。

1. 「BMC を出荷時のデフォルト値にリセット」をクリックします。

注：

- この操作は、スーパーバイザーのユーザー権限レベルのユーザーのみが実行できます。
- イーサネット接続が一時的に切断されます。リセット操作が完了した後、XClarity Controller Web インターフェースに再度ログインする必要があります。
- 「BMC を出荷時のデフォルト値にリセット」をクリックすると、確認ウィンドウがポップアップ表示され、チェック・ボックスを選択して以下の設定を保持できます。
  - ローカル・ユーザー設定の保持: 現在のユーザー/役割/グローバル設定がバックアップされます。コンテンツ CLI コマンド「users」/「roles」/「accesscfg」を復元します。例: ユーザー名/役割名/パスワードの有効期限の警告期間/パスワードの複雑さのルールが有効になっているなど。
  - ネットワーク設定の保持: 現在のネットワーク設定がバックアップされます。「ifconfig」CLI コマンドのネットワーク出力を復元します。例: ホスト名/IPv4 アドレス/IPv6 アドレス/ゲートウェイなど。
- 「OK」をクリックすると、保持を選択した構成を除き、以前の構成の変更がすべて失われます。
- BMC 構成を復元するときに LDAP を有効にする場合は、最初に信頼できるセキュリティ証明書をインポートしてから有効にする必要があります。
- BMC ローカル・システムから操作している場合、結果として TCP/IP 接続が失われます。接続を復元するには、BMC ネットワーク・インターフェースを再構成する必要があります。
- 処理が完了した後、XClarity Controller は再起動されます。

- BMC を出荷時のデフォルト値にリセットしても、リモート・コンソールの UEFI 設定およびアクセス・モード (シングル/マルチ・ユーザー) には影響しません (これはブラウザーの Cookie に保存されます)。

---

## XClarity Controller の再起動

このトピックでは、XClarity Controller を再起動する方法を説明します。

XClarity Controller を再起動する方法の詳細については、[60 ページの「電源操作」](#)を参照してください

---

## 第 4 章 サーバー状況の監視

アクセス先のサーバーの情報を表示および監視する方法を理解するには、このトピックの情報を使用します。

XClarity Controller にログインすると、システム・ステータス・ページが表示されます。このページから、サーバーのハードウェア・ステータス、イベント・ログと監査ログ、システム・ステータス、メンテナンス履歴、およびアラート受信者を表示できます。

---

### ヘルス・サマリー/アクティブ・システム・イベントの表示

ヘルス・サマリー/アクティブ・システム・イベントの表示方法を理解するには、このトピックの情報を使用します。

XClarity Controller のホーム・ページにアクセスすると、「ヘルス・サマリー」がデフォルトで表示されます。取り付けられているハードウェア数とそれぞれのヘルス・ステータスを表示するグラフィカル表現が提供されます。監視されるハードウェア・コンポーネントには、次のものがあります。















- CPU (プロセッサ)
- メモリー
- ローカル・ストレージ
- PCI アダプター
- パワー・サプライ
- ファン
- システム・ボード
- その他
- セキュリティー

注：シンプル・スワップ・バックプレーン構成のシステムでは、ローカル・ストレージの「ステータス」アイコンに「使用不可」と表示される場合があります。

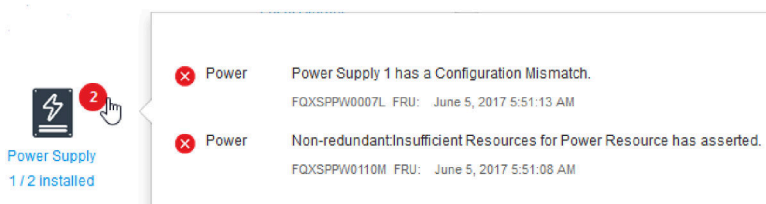
## Health Summary

Active System Events (0)



  <b>CPU</b> 1 / 2 installed	  <b>Memory</b> 1 / 32 installed	 <b>Local Storage</b> Not Found
 <b>PCI</b> Not Found	  <b>Power Supply</b> 2 / 2 installed	 <b>Fan</b> Not Found
  <b>System Board</b>	  <b>Others</b>	 <b>Security</b> Crypto:Standard

いずれかのハードウェア・コンポーネントが正常に動作していない場合、クリティカルまたは警告アイコンが付きます。クリティカルな状態は赤い円のアイコンによって示されます。警告状態は黄色の三角形のアイコンで示されます。クリティカルまたは警告マークの上にマウスを重ねることで、そのコンポーネントで現在アクティブなイベントが最大3つまで表示されます。



Power Supply  
1 / 2 installed

- Power: Power Supply 1 has a Configuration Mismatch.  
FQXSPW0007L FRU: June 5, 2017 5:51:13 AM
- Power: Non-redundant/insufficient resources for power resource has asserted.  
FQXSPW0110M FRU: June 5, 2017 5:51:08 AM

他のイベントを表示するには、「**アクティブなシステム・イベント**」タブをクリックします。システムで現在アクティブなイベントを表示するウィンドウが表示されます。イベント履歴全体を表示するには「**すべてのイベント・ログの表示**」をクリックします。

ハードウェア・コンポーネントに緑色のチェック・マークがついている場合は、正常に動作しており、アクティブなイベントはありません。

ハードウェア・コンポーネントの下のテキストは、取り付けられているコンポーネントの数を示します。テキスト(リンク)をクリックすると、「**システム一覧**」ページに移動します。

注：D3 V2 シャーシ互換ノードでは、「**パワー・サプライ**」リンクはケアテイカー・ノードでのみ使用できます。



## システム情報の表示

このトピックでは、一般的なサーバー情報の要約を取得する方法を説明します。

ホーム・ページの右にある「システム情報と設定」パネルには、以下を含む一般的なサーバー情報の要約が表示されます。

- マシン名、電源、およびオペレーティング・システムの状態
- マシン・タイプ/モデル
- シリアル番号
- システム名
- 前面パネル USB ポート管理

注：この機能は、今後のアップデートでサポートされる予定です。

- BMC ライセンス
- BMC IP アドレス
- BMC ホスト名
- アクティブ・シャーシ・ケアテイカー

注：この項目は、D3 V2 シャーシ互換ノードでのみ使用できます。

- BMC バージョン
- UEFI バージョン
- 位置

サーバーは、次の表にリストしたシステム状態のいずれかになります。

表 2. システム状態の説明

サーバーのシステム状況を示す見出しを持つ 2 列の表。

状態	説明
System power off/State unknown	サーバーの電源はオフです。
System on/starting UEFI	サーバーの電源はオンですが、UEFI は稼働していません。
System running in UEFI	サーバーの電源はオンで、UEFI が稼働しています。
オペレーティング・システムのブートまたはサポートされていないオペレーティング・システム (OS が ping に応答しない場合、システムはこの状態になっている可能性があります)	サーバーは、以下のいずれかの理由でこの状態になる場合があります。 <ul style="list-style-type: none"><li>• オペレーティング・システム・ローダーは起動したが、オペレーティング・システムが稼働していない</li><li>• BMC Ethernet over USB インターフェースが無効になっている。</li><li>• オペレーティング・システムに Ethernet over USB インターフェースをサポートするドライバーがロードされていない。</li></ul>
オペレーティング・システムがブート済み	サーバー・オペレーティング・システムは稼働しています。
メモリー・テストで実行されているシステム	サーバーの電源はオンで、メモリー診断ツールが稼働しています。

表 2. システム状態の説明 (続き)

状態	説明
システムがセットアップを実行中	サーバーの電源はオンでありシステムはブート済みでUEFI F1 セットアップ・メニューまたは LXPМ メニューに入りました。
システムは LXPМ 保守モードで実行中	サーバーの電源はオンでありシステムはブート済みで LXPМ 保守モードに入りました。このモードではユーザーは LXPМ メニュー内を移動できません。

システム名を変更する場合は、鉛筆アイコンをクリックします。使用するシステム名を入力して、緑色のチェック・マークをクリックします。

ご使用のサーバーに XClarity Controller Premier レベル・ライセンス以外のライセンスがある場合は、ライセンス・アップグレードを購入して拡張機能を有効にできる場合があります。アップグレード・ライセンスを取得した後、アップグレード・ライセンスをインストールするには、上向きの矢印アイコンをクリックします。

BMC License



ライセンスを追加、削除、エクスポートするには、右向きの矢印アイコンをクリックします。

BMC License



BMC の IP アドレス、BMC のホスト名、UEFI バージョン、BMC バージョンおよびロケーション項目に関連した設定を変更するには、右向きの矢印をクリックします。

- IP アドレスおよびホスト名の場合は、「ネットワーク」の下の「イーサネット構成」セクションに誘導されます。
- UEFI および BMC のバージョン項目の場合は、「ファームウェア更新」ページに誘導されます。
- ロケーション項目の場合は、「サーバー構成」ページの「サーバー・プロパティ」セクションに誘導されます。

BMC IP Address

10.245.32.57

BMC Hostname

XCC-7DG8-BHSFW1U002

BMC Version

0.34 (Build ID: IHX403H)

UEFI Version

0.10 (Build ID: IHE101T)

Location



## システム使用率の表示

左側のペインの「使用率」をクリックすると、一般的なサーバー使用率情報の概要が表示されます。

システム使用率は、システム、プロセッサ、メモリー、I/O サブシステムのリアルタイム使用率に基づく複合メトリックです。使用率データは、グラフィック・ビューまたはテーブル・ビューで表示できます。以下のデータが含まれます。

- 温度
  - リアルタイムの周囲温度および主要コンポーネントの温度が表示されます。
  - メモリー・モジュールの上にマウス・カーソルを置くと現在の温度が表示されます。

- **電力使用量**

- 現在の電力消費量の円グラフを表示します。
- 円グラフの上にマウス・カーソルを置くと現在の電力使用量が表示されます。
- 現在の電力消費量の円グラフは、4つのカテゴリ(CPU、メモリー、その他、スベア)で構成されます。「その他」とは、システムの合計電力消費量からCPUとメモリーの電力消費量を差し引いた値を意味します。「スベア」とは、合計割り振り電力からシステム電力使用量の合計を差し引いた値を意味します。
- 「電圧」タブには、ハードウェアによりサポートされているすべての電圧センサーの現在の電圧読み取り値およびステータスが表示されます。

- **システム使用率**

- システム、プロセッサ、メモリー、I/Oサブシステムの現在の使用率スナップショットが表示されます。

注：この機能は、今後のアップデートでサポートされる予定です。

- **ファン速度 (RPM)**

- ファン速度セクションには、ファン速度が最大速度のパーセンテージで表示されます。
- ユーザーは、歯車アイコンをクリックして、「**ファン速度ブースト**」オプションにアクセスできます。
- この設定では、周囲温度に応じてサーバーの冷却を追加できます。制御された温度アルゴリズムによって、通常の数値以上でファンを動作させることができます。ファンが既にフルスピードで動作している場合、変更はありません。

---

## イベント・ログの表示

イベント・ログには、すべてのハードウェアおよび管理イベントの履歴が記録されています。

「イベント」の「イベント・ログ」タブを選択すると、「イベント・ログ」ページが表示されます。ログ内のすべてのイベントには、XClarity Controllerの日付と時刻の設定を使用したタイム・スタンプが付いています。一部のイベントは、発生時にアラートも生成します(「アラート受信者」でそのように構成されている場合)。イベント・ログ内のイベントは、ソートしたりフィルターに掛けたりすることができます。

以下は、「イベント・ログ」ページで実行できる操作の説明です。

- **テーブルをカスタマイズ**: テーブルに表示する情報のタイプを選択するには、この操作項目を選択します。複数のイベントのタイムスタンプが同じ場合は、シーケンス番号を表示させてイベントの順番を判別できます。

注：一部のシーケンス番号はBMCの内部処理で使用されるため、イベントがシーケンス番号順にソートされた場合に隙間がある場合がありますが、これは正常です。

- **ログをクリア**: イベント・ログを削除するには、この操作項目を選択します。
- **最新表示**: ページが最後に表示された後で発生したイベント・ログ項目を表示されるためにディスプレイを更新するには、この操作項目を選択します。
- **タイプ**: 表示するイベントのタイプを選択します。イベント・タイプには以下のものがあります。



- ログ内のエラー・エントリを表示します



- ログ内の警告エントリを表示します



- ログ内の通知エントリーを表示します

表示されるエラーのタイプをオンまたはオフにするには、各アイコンをクリックします。アイコンをクリックすると、イベントの表示と非表示が連続して切り替わります。アイコンを囲む黒いボックスは、そのタイプのイベントが表示されることを示します。

- **ソース・タイプ・フィルター:** 表示するイベント・ログ項目のタイプが1つのみの場合は、ドロップダウン・メニューから項目を選択します。
- **時間フィルター:** 表示するイベントの間隔を指定するには、この操作項目を選択します。
- **検索:** 特定のイベントのタイプまたはキーワードを検索するには、拡大鏡アイコンをクリックして、「検索」ボックスに検索する語句を入力します。入力は大文字と小文字が区別されることに注意してください。

注：イベント・ログ記録の最大数は 1024 です。イベント・ログが満杯になると、新しいログ項目が最も古いログ項目を自動的に上書きします。

---

## 監査ログの表示

監査ログには、XClarity Controller へのログイン、新しいユーザーの作成、ユーザー・パスワードの変更など、ユーザー操作の履歴が記録されています。

監査ログを使用すると、認証、変更、システム操作を追跡および文書化できます。

イベント・ログおよび監査ログはどちらも同じような保守および表示操作をサポートします。監査ログ・ページ上で実行できる表示およびフィルタリング操作の説明を確認するには、[53 ページの「イベント・ログの表示」](#)を参照してください。

注：

- サーバーのオペレーティング・システムで Lenovo のツールを実行すると、知らないユーザー名 (ユーザー例「20luN4SB」) によって実行された操作として監査ログに記録されることがあります。一部のツールは、サーバーのオペレーティング・システムで実行されると、XClarity Controller にアクセスするために一時的なユーザー・アカウントを作成する場合があります。このアカウントはランダムなユーザー名とパスワードで作成され、内部 Ethernet over USB インターフェースの XClarity Controller にアクセスするためにのみ使用できます。このアカウントは、XClarity Controller Redfish インターフェースおよび SFTP インターフェースにアクセスするためにのみ使用できます。この一時アカウントの作成および削除は、その資格情報を使用してツールが実行したすべての操作とともに、監査ログに記録されます。
- 監査ログ記録の最大数は 1024 です。監査ログが満杯になると、新しいログ項目が最も古いログ項目を自動的に上書きします。

---

## メンテナンス履歴の表示

「メンテナンス履歴」ページには、ファームウェア更新、構成およびハードウェア交換の履歴に関する情報があります。

メンテナンス履歴の内容は、特定のイベントのタイプまたは特定の時間間隔でフィルターをかけて表示できます。

注：メンテナンス履歴記録の最大数は 250 です。メンテナンス履歴のログが満杯になると、新しいログ項目が最も古いログ項目を自動的に上書きします。

---

## アラート受信者の構成

メール通知および syslog 通知、または SNMP トラップの受信者を追加および変更するには、このトピックの情報を使用します。

注：この機能は、今後のアップデートでサポートされる予定です。



---

## 第 5 章 サーバーの構成

サーバーの構成に使用できるオプションについて理解するには、この章の情報を 사용합니다。

サーバーを構成する際は、以下のオプションを使用できます。

- アダプター
- ブート・オプション
- 電源ポリシー
- サーバーのプロパティ
- シャーシ

注：この項目は、D3 V2 シャーシ互換ノードでのみ使用できます。

---

### アダプター情報および構成設定の表示

サーバーに取り付けられているアダプターに関する情報を表示するには、このトピックの情報を 사용합니다。

サーバーに取り付けられているアダプターに関する情報を表示するには、「**サーバー構成**」の下にある「**アダプター**」をクリックします。

注：アダプターがステータス監視をサポートしていない場合、監視または構成では表示されません。取り付けられているすべての PCI アダプターのインベントリ関連情報については、「**システム一覧**」ページを参照してください。

---

### システムのブート・モードおよびブート順序の構成

システムのブート・モードおよび順序を構成するには、このトピックの情報を 사용합니다。

「**サーバー構成**」の下で「**ブート・オプション**」を選択すると、システムのブート順序を構成できます。

注：非認証のインバンド方式では、セキュリティー関連のシステム設定を変更することは許可されていません。たとえば、非認証のインバンド API を介して、OS または UEFI シェルからセキュア・ブートを構成できません。これには、インバンドで実行され、IPMI を使用して一時資格情報を取得する OneCLI や、セキュア・ブート、TPM、UEFI セットアップのパスワードに関する設定を構成するためのツールおよび API も含まれます。セキュリティーに関するすべての設定は、十分な権限を持つ適切な認証を必要とします。

システムのブート順序を構成するには、「**使用可能なデバイス**」のリストからデバイスを選択し、右矢印をクリックしてデバイスをブート順序に追加します。デバイスをブート順序から削除するには、ブート順序のリストからデバイスを選択し、左矢印をクリックしてデバイスを使用可能なデバイスのリストに戻します。ブート順序を変更するには、デバイスを選択し、上矢印または下矢印をクリックして優先順位内でデバイスを上下に移動させます。

ブート順序に変更を行った場合、その変更を適用する前に再起動オプションを選択する必要があります。使用可能なオプションは次のとおりです。

- **今すぐサーバーを再起動:** ブート順序の変更が保存され、サーバーはオペレーティング・システムをシャットダウンしないで即時に再起動します。
- **OS をシャットダウン後、サーバー再起動:** ブート順序の変更が保存され、オペレーティング・システムがシャットダウンされてからサーバーが再起動します。

- **後で手動で再起動:** ブート順序の変更は保存されますが、次にサーバーがリブートされるまで変更は有効になりません。

---

## 一回限りのブートの構成

一時的にブート設定を無視し、代わりに1回限り指定されたデバイスからブートするには、このトピックの情報を使用します。

「サーバー構成」の下にある「ブート・オプション」をクリックし、ドロップダウン・メニューからデバイスを選択して、次のサーバー再起動時に1回限りでシステムがブートするデバイスを構成します。以下の項目を選択できます。

### PXE ネットワーク

Preboot Execution Environment ネットワーク・ブートを試行するようにサーバーをセットアップします。

### 1次取り外し可能メディア

サーバーがデフォルト USB デバイスからブートされます。

### デフォルト CD/DVD

サーバーがデフォルト CD/DVD ドライブからブートされます。

### F1 システム・セットアップ

サーバーがブートして Lenovo XClarity Provisioning Manager に入ります。

### 診断パーティション

サーバーがブートして Lenovo XClarity Provisioning Manager の診断セクションに入ります。

### デフォルト・ハードディスク

サーバーがデフォルト・ディスク・ドライブからブートされます。

### 一次リモート・メディア

マウントされた仮想メディアからサーバーをブートします。

### マウント済み

構成済みのブート順序が使用されます。構成済みブート順序を1回限りのブートが上書きすることはありません。

### 一回限りでないブートの構成

構成済みのブート順序が使用されます。構成済みブート順序を1回限りのブートが上書きすることはありません。

ブート順序に1回限りの変更を選択した場合、その変更を適用する前に再起動オプションを選択する必要があります。

- **今すぐサーバーを再起動:** ブート順序の変更が保存され、サーバーはオペレーティング・システムをシャットダウンしないで即時に再起動します。
- **OS をシャットダウン後、サーバー再起動:** ブート順序の変更が保存され、オペレーティング・システムがシャットダウンされてからサーバーが再起動します。
- **後で手動で再起動:** ブート順序の変更は保存されますが、次にサーバーがリブートされるまで変更は有効になりません。

---

## サーバー電源の管理

電源管理に関する情報を表示し、電源管理機能を実行するには、このトピックの情報を使用します。

電源管理に関する情報を表示し、電源管理機能を実行するには、「サーバー構成」タブで「電源ポリシー」を選択します。



注：高密度サーバー・ノードを含むエンクロージャーでは、シャーシの冷却と電源は XClarity Controller ではなく SMM によって制御されます。ソリューションの電源ステータスの詳細については、SMM3 Web インターフェースを参照してください。

## 電源の冗長性の構成

電源の冗長性を構成するには、このトピックの情報を使用します。

注：

- AMD サーバーでは、電源ポリシー機能の構成はサポートされていません。
- パワー・サプライ・ユニットを 2 つ取り付ける場合、冗長性モードは「冗長 (N+N)」に設定されます。この 2 パワー・サプライ・ユニット構成では、いずれかのパワー・サプライ・ユニットで障害が発生したり、AC が失われたり、取り外されりした場合、XCC イベント・ログに冗長性消失イベントが報告されます。
- 配送後に取り付けるパワー・サプライ・ユニットが 1 つのみである場合、冗長性モードは自動的に非冗長モードに設定されます。

電源の冗長性セクションで使用可能なフィールドには、以下が含まれます。

- **冗長 (N+N):** システムに電力を同時に供給できる独立電源が 2 つ以上存在します。つまり、1 つ以上の電源に障害が発生した場合、中断することなく他の電源がシステムへの電力供給を継続できます。N+N の冗長性は、高いレベルのフォールト・トレランスを提供し、複数の障害が発生した場合でもシステムが稼働し続けます。
  - **ゼロ出力モード:** 冗長構成で有効にすると、一部の PSU は、負荷が軽い状態になったときに自動的にスタンバイ状態に入ります。この手法では、残りの PSU が電力負荷を全体的に提供して効率を向上させます。
- **冗長性なしモード:** 個のモードでは、1 つのパワー・サプライが失われた場合、サーバーが継続して稼働できない可能性があります。パワー・サプライに障害が発生すると、サーバーの稼働を継続させるため、サーバーのスロットルが行われる可能性があります。

構成の変更を行った後は「適用」をクリックします。

## 電源キャッピング・ポリシーの構成

電源キャッピング・ポリシーを構成するには、このトピックの情報を使用します。

注：

- AMD サーバーでは、電源キャッピング・ポリシー機能の構成はサポートされていません。
- 高密度サーバー・ノードを含むエンクロージャーでは、シャーシの冷却と電源は XClarity Controller ではなく SMM によって制御されます。ソリューションの電源ステータスの詳細については、SMM3 Web インターフェースを参照してください。

電源キャッピング機能を有効にするか無効にするかを選択できます。電源キャッピングを有効にすると、サーバーによって使用される電力量を制限する選択を行うことができます。電源キャッピングを無効にすると、サーバーが使用する最大電力は電源冗長性ポリシーによって決定されます。設定を変更するには、まず「リセット」をクリックします。目的の設定を選択して、「適用」をクリックします。

総電力容量は、電源の冗長化モードとシステムに取り付けられている PSU の数に基づいて計算されています。最大電力制限の手動設定は、実際の電力容量を超えることができます。

電源キャッピングが有効な場合、電力制限を維持するためにシステムがスロットルされる場合があります。

注：電源キャッピングが無効になっている場合でも、電源の障害、冷却の問題など、特定の障害状態でシステムがスロットルされる場合があります。

電源キャッピングは、入力測定または出力測定を使用して有効にできます。ドロップダウン・メニューから、電源キャッピングの制限を決定するために使用する計測タイプを選択します。測定値を切り替えると、それに応じてスライダの数字が変わります。

電源キャッピング値を変更するには、2つの方法があります。

- **方法 1:** スライダのマークを目的のワット数に移動させ、サーバー全体の電力制限を設定します。
- **方法 2:** 入力ボックスに値を入力します。スライダ・マークは、対応する位置に自動的に移動します。

構成の変更を行った後は「適用」をクリックします。変更はすぐに有効になります。

## 電源復元ポリシーの構成

電源喪失後に電源が復元したときにサーバーがどのように対応するかを構成するには、このトピックの情報を使用します。

電源復元ポリシーを構成する際には、以下の3つのオプションを使用できます。

### 常にオフ

電源が復元しても、サーバーは電源オフのままです。

### 復元

電源に障害が発生した際にサーバーの電源がオンであれば、電源が復旧した際にサーバーが自動的に電源オンになります。そうでない場合は、電源が復元しても、サーバーは電源オフのままです。

注：以下のチェック・ボックスを選択して、電源障害が発生する前にサーバーの電源がオンになっていた場合の電源オンのランダム遅延を1秒から15秒の間で設定します。

### 常にオン

電源が復元されるとサーバーの電源が自動的にオンになります。

構成の変更を行った後は「適用」をクリックします。

## 電源操作

サーバーに対して実行できる電源操作を理解するには、このトピックの情報を参照してください。

XClarity Controller ホーム・ページの「クイック操作」セクションで「電源操作」をクリックします。

次の表には、サーバーに対して実行できる電源操作と再起動操作の説明が記載されています。

表 3. 電源操作と説明

サーバーの電源および再起動操作を説明する2列の表です。

電源アクション	説明
サーバー電源オン	サーバーの電源をオンにし、オペレーティング・システムをブートするには、この操作を選択します。
OSをシャットダウン後、サーバー電源オフ	オペレーティング・システムをシャットダウンし、サーバーの電源をオフにするには、この操作項目を選択します。

表 3. 電源操作と説明 (続き)

電源アクション	説明
今すぐサーバーを電源オフ	先にオペレーティング・システムをシャットダウンせずにサーバーの電源をオフにするには、この操作項目を選択します。
OS をシャットダウン後、サーバーを再起動	オペレーティング・システムをシャットダウンし、サーバーの電源サイクルを実行するには、この操作項目を選択します。
今すぐサーバーを再起動	先にオペレーティング・システムをシャットダウンせずに、即時にサーバーの電源サイクルを実行するには、この操作項目を選択します。
サーバーをブートしてシステム・セットアップに入る	ブート中に F1 を押さずにサーバーを電源オンまたはリブートし自動的にシステム・セットアップに入るには、この項目を選択します。
NMI (マスク不能割り込み) をトリガー	「ハング」したシステムでマスク不能割り込み (NMI) を強制実行するには、この操作項目を選択します。この操作項目を選択すると、プラットフォームのオペレーティング・システムでメモリー・ダンプを行うことができ、これをシステムのハング状態をデバッグするために使用できます。F1 システム・セットアップ・メニューからの NMI での自動リブートの設定は、XClarity Controller が NMI 後にサーバーをリブートするかどうかを決定します。
スケジュール電源操作	サーバーの日次および週次の電源操作と再起動操作をスケジュールするには、この操作項目を選択します。
管理コントローラーを再起動	XClarity Controller を再起動するにはこの操作項目を選択します
サーバーの AC 電源サイクル	サーバーの電源サイクルを実行するには、この操作を選択します。
注：	<ul style="list-style-type: none"> <li>オペレーティング・システムのシャットダウンが試行されたときに、オペレーティング・システムがスクリーン・セーバー・モードまたはロック・モードにあると、XClarity Controller が正常なシャットダウンを開始できない場合があります。XClarity Controller は、オペレーティング・システムがまだ稼働中であっても、電源オフ遅延間隔が経過すると、ハード・リセットあるいはシャットダウンを実行します。</li> <li>前面パネルの電源 LED がすばやく点滅している場合、XClarity Controller は正常な電源オンの順番を開始できない可能性があります。XClarity Controller は、電源 LED がゆっくりと点滅し始めると、システムの電源をオンにすることができます。</li> </ul>

## IPMI コマンドを使用した電源消費量の管理および監視

IPMI コマンドを使用して電力使用量を管理および監視するには、このトピックの情報を使用します。

このトピックでは、Intel Intelligent Power Node Manager および Data Center Manageability Interface (DCMI) を使用して、Intelligent Platform Management Interface (IPMI) 電源管理コマンドを使用したサーバーの電源および熱の監視と、ポリシー・ベースの電源管理を行う方法について説明します。

Intel Node Manager SPS 3.0 を使用するサーバーの場合は、XClarity Controller のユーザーは Intel の Management Engine (ME) が提供する IPMI 電源管理コマンドを使用して、Node Manager 機能の制御およびサーバーの電力消費の監視を行うことができます。サーバーの電源管理は、DCMI 電源管理コマンドを使用して行うこともできます。Node Manager および DCMI 電源管理のコマンド例をこのトピックで示します。

## ノード・マネージャー・コマンドを使用したサーバー電源の管理

ノード・マネージャーを使用してサーバーの電源を管理するには、このトピックの情報を使用します。

Intel Node Manager のファームウェアには外部インターフェースがありません。そのため、Node Manager のコマンドはまず XClarity Controller で受信してから Intel Node Manager に送信される必要があります。XClarity Controller は、標準 IPMI ブリッジを使用した IPMI コマンドのリレーおよび転送デバイスとして機能します。

注：Node Manager IPMI コマンドを使用して Node manager のポリシーを変更すると、XClarity Controller の電源管理機能と競合を起こす場合があります。デフォルトでは、競合を回避するために Node Manager コマンドのブリッジは無効になっています。

XClarity Controller の代わりに Node Manager を使用してサーバーの電源の管理する場合は、(ネットワーク機能: 0x3A) および (コマンド: 0xC7) で構成される OEM IPMI コマンドが使用できます。

ネイティブの Node Manager IPMI コマンド・タイプを有効にするには: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x01`

ネイティブの Node Manager IPMI コマンド・タイプを無効にするには: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x00`

以下の情報は、Node Manager の電源管理コマンドの例です。

注：

- IPMI チャンネル 0 およびターゲット・アドレス 0x2c を指定することで、IPMITOOL を使用してコマンドを Intel Node Manager に送信して処理できます。要求メッセージは操作の開始に使用され、応答メッセージがリクエストに返されます。
- コマンドは、スペース上の制約のため、次の形式で表示されます。

Get Global System Power Statistics (コマンド・コード 0xC8) を使用した電源の監視: 要求: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC8 0x57 0x01 0x00 0x01 0x00 0x00` 応答: 57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Set Intel Node Manager Policy (コマンド・コード 0xC1) を使用した電源キャッピング: 要求: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00` 応答: 57 01 00

Set Intel Node Manager Policy (コマンド・コード 0xC1) を使用した電力の節約: 要求: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00`

Get Intel Management Engine Device ID を使用したデバイス ID 機能の取得: 要求: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x06 0x01` 応答: 50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

その他の Intel Node Manager コマンドについては、<https://businessportal.intel.com> の IPMI を使用した Intel インテリジェント電源ノード・マネージャー外部インターフェースの仕様の最新リリースを参照してください。

## DCMI コマンドを使用したサーバー電源の管理

DCMI コマンドを使用してサーバーの電源を管理するには、このトピックの情報を使用します。

DCMI は、標準的な管理ソフトウェア・インターフェースから表示できる監視および制御機能を提供します。サーバーの電源管理機能は、DCMI コマンドを使用して行うこともできます。

以下の情報は、よく使用される DCMI 電源管理機能およびコマンドの例です。要求メッセージは操作の開始に使用され、応答メッセージがリクエストに返されます。

注：コマンドは、スペース上の制約のため、次の形式で表示されます。

電源の測定値を取得: 要求:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x02 0xdc 0x01 0x00 0x00 応答:dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40

電源制限の設定: 要求:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03 応答:dc

電源キャッピング値の取得: 要求:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x03 0xdc 0x00 0x00 応答:dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00

電源制限のアクティブ化: 要求:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x01 0x00 0x00 応答:dc

電源制限の非アクティブ化: 要求:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x00 0x00 0x00 応答:dc

注：一部のサーバーでは「電源制限の設定」コマンドの例外操作がサポートされていない場合があります。たとえば、システムのハード電源オフを実行してイベントを SEL に記録するパラメーターはサポートされていない場合があります。

DCMI 仕様でサポートされるコマンドの完全なリストについては、<https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf> の Data Center Manageability Interface 仕様の最新リリースを参照してください。

---

## サービス・データ・ログのダウンロード

サーバーに関するサービス情報を収集するには、このトピックの情報を使用します。このプロセスは通常、サーバーの問題を解決するためにサービス担当者からの依頼でのみ実行されます。

XClarity Controller のホーム・ページで、「クイック操作」セクションの「サービス・ログ」オプションをクリックし、「サービス・データ・ログ」を選択します。

デフォルトでは、サービス・ログには、システム情報、システム・インベントリ、システム使用率、SMBIOS テーブル、センサー読み取り値、イベント・ログ、FOD キー、SLP キー、UEFI 構成、XClarity Controller 3 構成のデータが記録されます。

基本情報オプションの上にマウス・カーソルを置き、フローティング・ウィンドウをクリックすると、エクスポートされる実際のデータの一部が表示されます。

基本情報は必須ですが、次の情報もエクスポートできます。

- ネットワーク情報 (IP、ホスト名)
- テレメトリー (24 時間のデータ)
- 監査ログ (ユーザー名が含まれる)
- 最新の障害画面

「エクスポート」をクリックしてサービス・データ・ログをダウンロードします。

サービスおよびサポート・データを収集するプロセスは、完了までに数分かかることがあります。ファイルは、デフォルトのダウンロード・フォルダーに保存されます。サービス・データ・ファイルの命名規則は次の規則に従います。<machine type and model>\_<serial number>\_xcc3\_ServiceData\_<date>-<time>.zip

例: 7X2106Z01A\_2345678\_xcc3\_ServiceData\_240517-112857.zip。

.zip 形式のサービス・データに加えて、デバッグ・ログは「履歴の参照...」を通じて .tar.zst ファイル形式でダウンロードすることもできます。デバッグ・ログ・ファイルの命名規則は次の規則に従います。

<machine type and model>\_<serial number>\_xcc3\_DebugLog\_<date>-<time>.tar.zst

例: 7X2106Z01A\_2345678\_xcc3\_DebugLog\_240517-112857.zip。

注:

- 「履歴の参照...」では、最近エクスポートされたサービス・ログも保持されます。
- .tar.zst ファイル形式は、異なる圧縮アルゴリズムを使用し、パッケージ「zstd」で展開できます。例:  
tar --use-compress-program=unzstd -xvf <machine type and model>\_<serial number>\_xcc3\_DebugLog\_<date>-<time>.tar.zst

---

## サーバーのプロパティ

関連サーバー・プロパティを変更または表示するには、このトピックの情報を使用します。

### ロケーションと連絡先の設定

操作およびサポート担当者がシステムを識別するのに役立つさまざまなパラメーターを設定するには、このトピックの情報を使用します。

「サーバー構成」の下の「サーバー・プロパティ」を選択して「ロケーションと連絡先」情報を構成します。

#### 連絡先

システムに問題が発生した場合に、連絡を取る人の名前と電話番号を指定できます。

注: 注: このフィールドは SNMPv3 構成の「連絡先」フィールドと同じものであり、SNMPv3 を有効にする場合は必須です。

#### ラック名

サーバーのあるラックを指定することで、サーバーを見つけやすくなります。

#### 部屋番号

サーバーのある部屋を指定することで、サーバーを見つけやすくなります。

#### 建物

サーバーのある建物を指定することで、サーバーを見つけやすくなります。

#### 位置 (U):

ラック内の位置を指定することで、サーバーを見つけやすくなります。

#### 住所

サーバーがある場所の完全な郵便住所を指定できます。

注: 関連情報が入力された場合、SNMPv3 セクションおよび XClarity Controller ホーム・ページの「ロケーション」フィールドの単一行で表示されます。

## サーバー・タイムアウトの設定

サーバーのタイムアウトを設定するには、このトピックの情報を使用します。

これらのタイムアウトは、ハングしたサーバーの復元操作に使用されます。

「サーバー構成」の下にある「サーバー・プロパティ」を選択して、サーバー・タイムアウトを構成します。以下のサーバー・タイムアウトの選択肢があります。

### 電源オフ遅延を有効にする

このフィールドを使用して、BMC サブシステムがシステムの電源をオフにする前に、オペレーティング・システムのシャットダウンを待機する時間(分)を指定します。

電源オフ遅延タイムアウト値を設定するには、ドロップダウンから時間間隔を選択して「適用」をクリックします。XClarity Controller の強制電源オフを無効にするには、ドロップダウンの選択で「なし」を選択します。

### 侵入警告メッセージ

ユーザーが XClarity Controller にログインしたときに表示されるメッセージを作成するには、このトピックの情報を使用します。

「サーバー構成」の下にある「サーバー・プロパティ」を選択します。「ログイン・メッセージ」オプションを使用してユーザーに表示するメッセージを構成します。終わったら、「適用」をクリックします。

このメッセージ文は、ユーザーがログインしたときに XClarity Controller ログイン・ページのメッセージ領域に表示されます。

### ソリューション・サービス

ソリューション・サービスを有効または無効にするには、このトピックの情報を使用します。

注：この機能は、今後のアップデートでサポートされる予定です。

---

## XClarity Controller の日付と時刻の設定

XClarity Controller の日付と時刻の設定を理解するには、このトピックの情報を使用します。XClarity Controller の日付と時刻を構成するための手順が記載されています。XClarity Controller の日付と時刻は、イベント・ログに記録されるすべてのイベントおよび送信されるすべてのアラートにタイム・スタンプされます。

XClarity Controller の日付と時刻を表示または変更するには、XClarity Controller のホーム・ページで、右上の時計のアイコンをクリックします。XClarity Controller には、独自のリアルタイム・クロックはありません。日付と時刻を Network Time Protocol サーバーと同期するか、サーバーのリアルタイム・クロック・ハードウェアと同期するように、XClarity Controller を構成できます。

### NTP と同期

XClarity Controller のクロックを NTP サーバーと同期させるには、以下のステップを実行します。

- 「時刻を NTP と同期」を選択して NTP サーバー・アドレスを指定します。
- 「+」アイコンをクリックして追加の NTP サーバーを指定できます。
- XClarity Controller が NTP サーバーと同期する頻度を指定します。
- NTP サーバーから取得した時刻は、協定世界時 (UTC) 形式です。

- XClarity Controller を現地の日付と時刻に合わせて調整する場合は、ドロップダウン・メニューから現地のタイム・ゾーン時差を選択します。
- 現地が夏時間を採用している場合は、「夏時間 (DST) の自動調整」チェックボックスにチェックを入れます。
- 構成の変更が完了したら、「適用」をクリックします。

### ホストとの同期

サーバーのリアルタイム・クロック・ハードウェアに保持されている時刻は、協定世界時 (UTC) 形式の場合も、すでに現地時間形式に調整済みの場合もあります。UTC 形式でリアルタイム・クロックを保存しているオペレーティング・システムがあれば、現地時間で時刻を保存しているものもあります。サーバーのリアルタイム・クロックは、時刻がどの形式かを示しません。そのため、XClarity Controller をホストのリアルタイム・クロックと同期するように構成する場合は、リアルタイム・クロックから取得した日付と時刻を XClarity Controller がどのように使用するかを選択できます。

- ローカル (例: Windows): このモードでは、XClarity Controller はリアルタイム・クロックから取得した日付と時刻を、すでに適切なタイムゾーンと DST 時差が適用された現地時間として取り扱います。現地が夏時間を採用している場合は、「夏時間 (DST) の自動調整」チェック・ボックスにチェックを入れることもできます。
- UTC (例: Linux): このモードでは、XClarity Controller はリアルタイム・クロックから取得した日付と時刻を、タイムゾーンや DST 時差がまだ適用されていない協定世界時として取り扱います。このモードでは、ドロップダウン・メニューから現地のタイム・ゾーン時差を選択して、現地の日付と時刻に合わせて調整できます。現地が夏時間を採用している場合は、「夏時間 (DST) の自動調整」チェック・ボックスにチェックを入れることもできます。
- 構成の変更が完了したら、「適用」をクリックします。

注：夏時間になって時計が進められる際、飛ばされた時間の中に XClarity Controller が実行するようにスケジュールされていた操作は実行されません。たとえば、米国の夏時間の開始時刻が 3 月 12 日 2:00 am であり、電源アクションが 3 月 12 日の午前 2:10 am にスケジュールされていると、この操作は発生しません。時刻が 2:00 am になると、XClarity Controller はその時刻を 3:00 am として読み取ります。

---

## D3 V2 シャーシの構成

D3 V2 シャーシ設定を理解するには、このトピックの情報を使用します。

「サーバー構成」の下にある「シャーシ」をクリックして、D3 V2 シャーシに関する情報を表示します。

### シャーシ情報

このセクションには、UUID、シリアル番号、マシン・タイプ、ファームウェア・バージョンなどのシャーシ情報が表示されます。フォーム・ファクター、電源ステータス、IP アドレスなど、ノードの情報も表示されます。

注：

- 対応するノードの横にある「リセット/再取り付け」ボタンをクリックして、ノードを再起動するか、物理ノードの再取り付けをシミュレートします。
- 他のノードをリセットまたは再取り付けできるのは、ケアテイカー・ノードのみです。

### シャーシ・ケアテイカーの役割

このセクションには、シャーシ・ケアテイカーの選択設定が表示されます。

注：

- 「シャーシ・ケアテイカーの役割に参加する」を選択して、ケアテイカーの選出プロセスに参加するノードを有効にします。永続ケアテイカーとして指定されている別のノードがある場合は、そのノードが存在しない場合を除き、選択プロセスは実行されません。



- 1つのノードのみをケアテイカーにする場合は、「このノードを永続シャーシ・ケアテイカーとして指定する」を選択します。その場合、ケアテイカーの役割に対する高可用性はありません。永続ケアテイカー・ノードがシャーシに存在しない場合、次に適切なケアテイカーを選択するために、ケアテイカーの選出プロセスが実行されます。

#### シャーシのメンテナンス履歴

シャーシのメンテナンス履歴には、シャーシ内で追加または取り外されているノードの記録と、ノード間で変更されるケアテイカーの役割の記録が保持されます。



## 第 6 章 リモート・コンソール機能

サーバー・コンソールをリモートで表示および操作する方法を理解するには、このトピックの情報を使用します。

XClarity Controller Web インターフェースでリモート・コンソール機能を使用して、サーバー・コンソールの表示および操作を行うことができます。ディスク・イメージ (ISO または IMG ファイル) を仮想ドライブとしてサーバーに割り当てることができます。リモート・コンソール機能は、XClarity Controller Premier レベルの機能で使用でき、Web インターフェースからのみ使用できます。リモート・コンソール機能を使用するには、Supervisor アクセス権限またはリモート・コンソール・アクセス特権を持つユーザー ID を使用して XClarity Controller にログインする必要があります。XClarity Controller 標準レベルから XClarity Controller Premier レベルへのアップグレードについては、[6 ページの「XClarity Controller のアップグレード」](#)を参照してください。

リモート・コンソール機能は、以下の作業を行うために使用します。

- サーバーの状態に関係なく、最大 1920x1200 32bpp@60Hz のグラフィック解像度でビデオをリモートで表示します。
- リモート・クライアントからキーボードとマウスを使用して、リモート側でサーバーにアクセスできます。
- ローカル・システムまたはリモート・システム上の ISO および IMG ファイルを仮想ドライブとしてマウントして、サーバーで使用できるようにします。
- IMG または ISO イメージを XClarity Controller メモリーにアップロードし、これを仮想ドライブとしてサーバーにマウントします。合計サイズ 100 MB の最大 2 つのファイルを XClarity Controller のメモリーにアップロードできます。

注：

- リモート・コンソール機能がマルチユーザー・モードで開始された場合 (XClarity Controller Premier レベルの機能セットを備えた XClarity Controller は、最大 6 つの同時セッションをサポートします)、リモート・ディスク機能は一度に 1 つのセッションでのみ実行できます。
- リモート・コンソールで表示可能なのは、システム・ボード上のビデオ・コントローラーが生成したビデオのみです。別のビデオ・コントローラー・アダプターがインストールされ、システムのビデオ・コントローラーの代わりに使用されている場合、XClarity Controller リモート・コンソールでは、追加されたアダプターからのビデオの内容を表示することはできません。
- ネットワーク内にファイアウォールがある場合、リモート・コンソール機能をサポートするために、ネットワーク・ポートを開く必要があります。リモート・コンソール機能で使用されるネットワーク・ポート番号を表示または変更するには、[35 ページの「サービスの有効化とポートの割り当て」](#)を参照してください。
- リモート・コンソール機能は、HTML5 を使用してサーバー・ビデオを Web ページに表示します。この機能を使用するには、ブラウザーが HTML5 エレメントを使用したビデオ・コンテンツの表示をサポートしている必要があります。
- Internet Explorer ブラウザーを使用した BMC へのアクセスに自己署名証明書と IPv6 アドレスを使用している場合、証明書のエラーが原因でリモート・コンソール・セッションが開始できない場合があります。この問題を回避するには、自己署名証明書を Internet Explorer の信頼するルート証明機関に追加できます。
  - 「BMC 構成」の下にある「**セキュリティ**」を選択して、自己署名証明書をダウンロードします。
  - 証明書ファイルの拡張子を \*.cert に変更して、Web 証明書ファイルをダブルクリックします。
  - IE11 ブラウザーのキャッシュをクリアします。

- 「**証明書をインストールする**」をクリックして、証明書インポート・ウィザードの手順に従って証明書を証明書ストアにインストールします。

---

## リモート・コンソール機能の有効化

このトピックでは、リモート・コンソール機能について説明します。

XClarity Controller リモート・コンソール機能は、XClarity Controller Premier レベルの機能でのみ使用できます。リモート・コンソールを操作する特権がない場合は、ロック・アイコンが表示されます。

XClarity Controller Premier レベルのアップグレードのアクティベーション・キーを購入して入手した後、[85 ページの「アクティベーション・キーのインストール」](#)の手順を使用してインストールします。

リモート・コンソール機能を使用するには、XClarity Controller ホーム・ページまたはリモート・コンソール・プレビュー Web ページの「**リモート・コンソール・プレビュー**」セクションにある、白い斜め向きの矢印が付いた画像をクリックします。

---

## リモート電源制御

このトピックでは、リモート・コンソール・ウィンドウからサーバーの電源および再起動コマンドを送信する方法を説明します。

リモート・コンソール・ウィンドウからメイン Web ページに戻ることなく、サーバーに電源コマンドおよび再起動コマンドを送信できます。リモート・コンソールを使用してサーバーの電源を制御するには、「**電源**」をクリックし、次のコマンドのいずれかを選択します。

### サーバー電源オン

サーバーの電源をオンにし、オペレーティング・システムをブートするには、この操作を選択します。

### OS をシャットダウン後、サーバー電源オフ

オペレーティング・システムをシャットダウンし、サーバーの電源をオフにするには、この操作項目を選択します。

### 今すぐサーバーを電源オフ

先にオペレーティング・システムをシャットダウンせずにサーバーの電源をオフにするには、この操作項目を選択します。

### OS をシャットダウン後、サーバーを再起動

オペレーティング・システムをシャットダウンし、サーバーの電源サイクルを実行するには、この操作項目を選択します。

### 今すぐサーバーを再起動

先にオペレーティング・システムをシャットダウンせずに、即時にサーバーの電源サイクルを実行するには、この操作項目を選択します。

### サーバーをブートしてシステム・セットアップに入る

ブート中に F1 を押さずにサーバーを電源オンまたはリブートし自動的にシステム・セットアップに入るには、この項目を選択します。

---

## リモート・コンソールの画面キャプチャー

リモート・コンソールのスクリーン・キャプチャー機能の使用方法を理解するには、このトピックの情報を参照します。

リモート・コンソール・ウィンドウのスクリーン・キャプチャー機能は、サーバーのビデオ表示内容をキャプチャーします。画面イメージをキャプチャーおよび保存するには、以下のステップを実行します。

- ステップ1. リモート・コンソール・ウィンドウで、「**画面をキャプチャー**」をクリックします。
- ステップ2. ポップアップ・ウィンドウで、「**ファイルを保存**」をクリックして「**OK**」を押します。ファイルは `rpviewer.png` と命名され、デフォルトのダウンロード・フォルダーに保存されます。

注：スクリーン・キャプチャー・イメージは、JPG ファイル・タイプで保存されます。

---

## リモート・コンソールのキーボード・サポート

「**キーボード**」の下のリモート・コンソール・ウィンドウで、以下のオプション項目が表示されます。

- 仮想キーボードを起動するには「**仮想キーボード**」をクリックします。この機能は、物理キーボードがないタブレット・デバイスを使用する場合に便利です。以下のオプションを使用してサーバーに送信できるマクロやキーの組み合わせを作成できます。使用しているクライアント・システム上のオペレーティング・システムは、特定のキーの組み合わせ（たとえば、`Ctrl+Alt+Del`）をトラップし、それらをサーバーに伝送しない場合があります。F1 や Esc のようなその他のキーは、使用しているプログラムまたはブラウザによってインターセプトされる場合があります。マクロは、ユーザーが送信できないかもしれないキー・ストロークをサーバーに送信するメカニズムを提供します。
- サーバー定義マクロを使用するには「**サーバー・マクロ**」をクリックします。一部のサーバー・マクロは XClarity Controller ファームウェアによって事前定義されています。

---

## リモート・コンソールの画面モード

リモート・コンソールの画面モードを構成するには、このトピックの情報を使用します。

リモート・コンソールの画面モードを構成するには、「**画面モード**」をクリックします。

以下のメニュー・オプションが選択可能です。

### フルスクリーン

このモードは、クライアントのデスクトップにビデオ表示を全画面表示します。このモードで Esc キーを押すとフルスクリーン・モードを終了します。フルスクリーン・モードではリモート・コンソール・メニューが表示されないため、キーボード・マクロなどリモート・コンソール・メニューによって提供される機能を使用するには、フルスクリーン・モードを終了する必要があります。

### 画面に合わせる

これは、リモート・コンソール起動時のデフォルト設定です。この設定では、ターゲットのデスクトップがスクロール・バーなしで完全に表示されます。アスペクト比は維持されます。

---

## メディアのマウント方法

メディアのマウントの実行方法を理解するには、このトピックの情報を使用します。

仮想ドライブとして ISO および IMG ファイルをマウントするには、3つのメカニズムが提供されています。

- 仮想ドライブは、リモート・コンソール・セッションから「**メディア**」をクリックしてサーバーに追加できます。
- リモート・コンソール・セッションを確立しないで、リモート・コンソール Web ページから直接。
- スタンドアロン・ツール。

仮想メディア機能を使用するには、リモート・コンソールおよびリモート・ディスクのアクセス特権が必要です。

ファイルは、ローカル・システムまたはリモート・サーバーから仮想メディアとしてマウントして、ネットワーク経由でアクセスするか、RDOC 機能を使用して XClarity Controller メモリー内にアップロードできます。以下でメカニズムを説明します。

- ローカル・メディアは、XClarity Controller にアクセスするために使用しているシステムにある ISO または IMG ファイルです。このメカニズムは、リモート・コンソール・セッション経由でのみ使用できます。リモート・コンソール Web ページから直接使用することはできず、XClarity Controller Premier レベルの機能でのみ使用できます。ローカル・メディアをマウントするには、「**ローカル・メディア・ファイルのマウント**」セクションで「**すべてのローカル・メディアのマウント**」をクリックします。最大 4 ファイルまで同時にサーバーにマウントできます。
- リモート・システム上のファイルも、仮想メディアとしてマウントできます。4 つまでのファイルを仮想ドライブとして同時に取り付けることができます。XClarity Controller は、以下のファイル共有プロトコルをサポートします。

#### – CIFS - 共通インターネット・ファイル・システム:

- リモート・システム上のファイルがある URL を入力します。
- ファイルを読み取り専用仮想メディアとしてサーバーに表示する場合は、チェック・ボックスにチェックを入れます。
- XClarity Controller がリモート・システム上のファイルにアクセスするために必要な資格情報を入力します。

注：XClarity Controller では、ユーザー名、パスワード、または URL 内のスペースをサポートしません。CIFS サーバーに、空白が含まれたユーザー名またはパスワードを使用して構成されているログイン資格情報がないこと、および URL にスペースが含まれていないことを確認します。

- マウント・オプションは任意であり、CIFS プロトコルで定義されます。
- リモート・サーバーがサーバーのコレクションに属しており、セキュリティが一元処理されている場合、リモート・サーバーが属するドメイン名を入力します。

#### – NFS - ネットワーク・ファイル・システム:

- リモート・システム上のファイルがある URL を入力します。
- ファイルを読み取り専用仮想メディアとしてサーバーに表示する場合は、チェック・ボックスにチェックを入れます。
- マウント・オプションは任意であり、NFS プロトコルで定義されます。NFSv3 と NFSv4 の両方がサポートされます。たとえば、NFSv3 を使用するには、オプション「nfsvers=3」を指定する必要があります。NFS サーバーが AUTH\_SYS セキュリティー様式を使用して NFS 操作を認証する場合は、オプション「sec=sys」を指定する必要があります。

#### – HTTPFS - HTTP FUSE ベース・ファイル・システム:

- リモート・システム上のファイルがある URL を入力します
- ファイルを読み取り専用仮想メディアとしてサーバーに表示する場合は、チェック・ボックスにチェックを入れます。

注：Microsoft IIS で生成されたセキュリティ証明書のマウント処理中にエラーが発生することがあります。この状態が発生した場合は、[75 ページの「メディアのマウント・エラーに関する問題」](#)を参照してください。

「**すべてのリモート・メディアのマウント**」をクリックしてファイルを仮想メディアとしてマウントします。仮想メディアを削除するには、マウントされたメディアの右側にあるゴミ箱アイコンをクリックします。

- 2 つまでのファイルを XClarity Controller メモリーにアップロードして、XClarity Controller RDOC 機能を使用して仮想メディアとしてマウントできます。両方のファイルの合計サイズが 100 MB を超えてはなりません。これらのファイルは、リモート・コンソール・セッションが終了しても、削除され

るまで XClarity Controller メモリーに残ります。RDOC 機能はファイルをアップロードするときに以下のメカニズムをサポートします。

– CIFS - 共通インターネット・ファイル・システム: 詳細は上記の説明を参照。例:

IP アドレス 192.168.0.100 にある CIFS サーバーの backup\_2016 ディレクトリーにある account\_backup.iso という名前の ISO ファイルを読み取り専用仮想ドライブとしてサーバーにマウントするには、次の図に示されているようにフィールドに入力します。この例では、192.168.0.100 にあるサーバーは、ドメイン「accounting」の下にあるサーバーのコレクションのメンバーです。ドメイン名はオプションです。CIFS サーバーがドメインの一部でない場合、「ドメイン」フィールドは空白のままにします。ファイル名の大小文字の区別を無視するように CIFS サーバーに指示するため、この例では「マウント・オプション」フィールドに CIFS 「nocase」オプションが指定されています。「マウント・オプション」フィールドはオプションです。このフィールドにユーザーが入力した情報は BMC では使用されず、マウント要求が行われた際に単純に CIFS サーバーに渡されます。CIFS サーバーでサポートされているオプションを判別するには、CIFS サーバーを実装するためのドキュメントを参照してください。

Mount Media File from Network: 0 mounted

Mount an ISO or IMG image file from a file server to the host as a DVD or USB drive.  
Note: The client session could be closed without affecting mounted media.

CIFS Input URL: //192.168.0.100/backup\_2016/account\_backup.iso Read-only

User Name: mycifsname Password: \*\*\*\*\*

Mount Options: nocase Domain: accounting

Mount all remote media

BMC では、URL を指定する際のガイダンスを提供しています。入力された URL が有効ではない場合、マウント・ボタンがグレー表示になり、URL フィールドの下に URL の適切な形式を示す赤字のテキストが表示されます。

URL address in the form of //ipaddress/path/to/file or //domain-name/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '\_'. It must contain at least two domain items.

– NFS - ネットワーク・ファイル・システム: 詳細は上記の説明を参照。例:

IP アドレス 10.243.28.77 にある NFS サーバーの「personnel」ディレクトリーにある US\_team.iso という名前の ISO ファイルを読み取り専用仮想ドライブとしてサーバーにマウントするには、次の図に示されているようにフィールドに入力します。NFS 「port=2049」マウント・オプションは、データの転送にネットワーク・ポート 2049 を使用するように指定します。「マウント・オプション」フィールドはオプションです。このフィールドにユーザーが入力した情報は、マウント要求が行われた際に NFS サーバーに渡されます。NFS サーバーでサポートされているオプションを判別するには、NFS サーバーを実装するためのドキュメントを参照してください。

Mount Media File from Network: 0 mounted

Mount an ISO or IMG image file from a file server to the host as a DVD or USB drive.  
Note: The client session could be closed without affecting mounted media.

NFS Input URL: 10.243.28.77/personnel/US\_team.iso Read-only

Mount Options: port=2049

Mount all remote media

BMC では、URL を指定する際のガイダンスを提供しています。入力された URL が有効ではない場合、マウント・ボタンがグレー表示になり、URL フィールドの下に URL の適切な形式を示す赤字のテキストが表示されます。

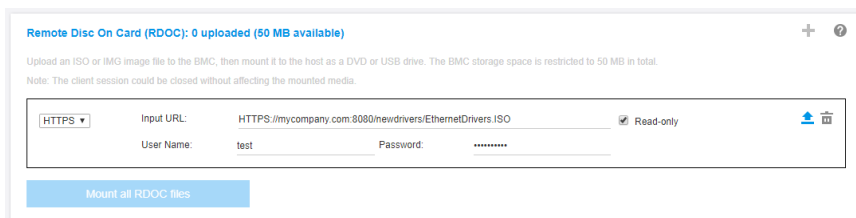
URL address in the form of ipaddress:/path/to/file or domain-name:/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '\_'. It must contain at least two domain items.

#### – HTTPS - Hypertext Transfer Protocol Secure:

- リモート・システム上のファイルがある URL を入力します。
- ファイルを読み取り専用仮想メディアとしてサーバーに表示する場合は、チェック・ボックスにチェックを入れます。
- XClarity Controller がリモート・システム上のファイルにアクセスするために必要な資格情報を入力します。

注：

- Microsoft IIS で生成されたセキュリティー証明書のマウント処理中にエラーが発生することがあります。この状態が発生した場合は、75 ページの「メディアのマウント・エラーに関する問題」を参照してください。
- XClarity Controller では、ユーザー名、パスワード、または URL 内のスペースをサポートしません。CIFS サーバーに、空白が含まれたユーザー名またはパスワードを使用して構成されているログイン資格情報がないこと、および URL にスペースが含まれていないことを確認します。例：ネットワーク・ポート 8080 を使用するドメイン名が「mycompany.com」の HTTPS サーバーの「newdrivers」ディレクトリーにある「EthernetDrivers.ISO」という名前の ISO ファイルを読み取り専用仮想ドライブとしてサーバーにマウントするには、次の図に示されているようにフィールドに入力します。



BMC では、URL を指定する際のガイダンスを提供しています。入力された URL が有効ではない場合、マウント・ボタンがグレー表示になり、URL フィールドの下に URL の適切な形式を示す赤字のテキストが表示されます。

URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '\_'. It must contain at least two domain items. The port number is optional

#### – SFTP - SSH ファイル転送プロトコル

- リモート・システム上のファイルがある URL を入力します。
- ファイルを読み取り専用仮想メディアとしてサーバーに表示する場合は、チェック・ボックスにチェックを入れます。
- XClarity Controller がリモート・システム上のファイルにアクセスするために必要な資格情報を入力します。



注：

- XClarity Controller では、ユーザー名、パスワード、または URL 内のスペースをサポートしません。CIFS サーバーに、空白が含まれたユーザー名またはパスワードを使用して構成されているログイン資格情報がないこと、および URL にスペースが含まれていないことを確認します。
- XClarity Controller が HTTPS サーバーに接続すると、HTTPS サーバーが使用するセキュリティー証明書の情報を表示するポップアップ・ウィンドウが表示されます。XClarity Controller では、セキュリティー証明書の認証を検証することはできません。
- ローカル - 共通インターネット・ファイル・システム
  - システムを参照してマウントする ISO または IMG ファイルを見つけます。
  - ファイルを読み取り専用仮想メディアとしてサーバーに表示する場合は、チェック・ボックスにチェックを入れます。

「すべての RDOC ファイルのマウント」をクリックしてファイルを仮想メディアとしてマウントします。仮想メディアを削除するには、マウントされたメディアの右側にあるゴミ箱アイコンをクリックします。

## スタンドアロン・ツール

XClarity Controller を使用してデバイスまたはイメージ (.iso/.img) をマウントする必要がある場合、ユーザーは OneCLI パッケージの一部である rdmount スタンドアロン・コードを使用できます。特に rdmount は、XClarity Controller への接続を開き、デバイスまたはイメージをホストにマウントします。

Rdmount の構文は次のとおりです。

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

iso ファイルをマウントする例:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

---

## メディアのマウント・エラーに関する問題

このトピックには、メディアのマウント・エラーに関する問題のトラブルシューティングのための情報が含まれています。

Microsoft IIS で生成されたセキュリティー証明書を使用すると、マウント処理中にエラーが発生することがあります。このような場合は、セキュリティー証明書を openssl によって生成された新しい証明書に置き換えてください。具体的には、新しく生成された pfx ファイルが Microsoft IIS サーバーにロードされます。

以下は、Linux オペレーティング・システムで openssl を使用して新しいセキュリティー証明書を生成する方法の例です。

```
$ openssl  
OpenSSL>
```

```
$ openssl genrsa 1024 > server.key  
Generating RSA private key, 1024 bit long modulus  
.....+*****  
.....+*****  
e is 65537 (0x10001)
```

```
$ openssl req -new -key server.key > server.csr  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank
```

For some fields there will be a default value,  
If you enter '.', the field will be left blank.

```
-----  
Country Name (2 letter code) [AU]:CN  
State or Province Name (full name) [Some-State]:BJ  
Locality Name (eg, city) []:HD  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo  
Organizational Unit Name (eg, section) []:Lenovo  
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66  
Email Address []:test@test.com
```

Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:LNV

```
$ ls  
server.csr server.key
```

```
$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.
```

```
-----  
Country Name (2 letter code) [AU]:CN  
State or Province Name (full name) [Some-State]:BJ  
Locality Name (eg, city) []:BJ  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV  
Organizational Unit Name (eg, section) []:LNV  
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66  
Email Address []:test@test.com
```

```
$ ls  
server.crt server.csr server.key
```

```
$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt  
Enter Export Password:  
Verifying - Enter Export Password:
```

```
$ ls  
server.crt server.csr server.key server.pfx
```

---

## リモート・コンソール・セッションの終了

このトピックでは、リモート・コンソール・セッションを終了する方法を説明します。

リモート・コンソール・セッションを終了するには、リモート・コンソールのウィンドウおよび仮想メディア・セッションのウィンドウを閉じます。

---

## 第 7 章 ストレージの構成

ストレージの構成に使用できるオプションについて理解するには、この章の情報を 사용합니다。

ストレージを構成する際に、以下のオプションを使用できます。

- ストレージの詳細
- RAID セットアップ

---

### ストレージの詳細

ストレージの詳細機能を使用するには、このトピックの情報を 사용합니다。

この機能は、ストレージ・デバイスの物理的な構造およびストレージ構成とともに、その場所、製造元、製品名、ステータス、容量、インターフェース、メディア、フォーム・ファクター、およびその他の情報などの詳細を表示します。

SSD ドライブの残量値がしきい値に達するか、それ以下になると、警告またはクリティカル・イベントがトリガーされます。警告イベントとクリティカル・イベントのデフォルトの残存寿命値は、それぞれ 8% と 4% です。「**ストレージの詳細**」の横にある歯車アイコンをクリックして、しきい値を設定します。

PCIe レーン x1 モードをサポートする SAS/SATA/NVMe (AnyBay) バックプレーンを構成するには、「**バックプレーン**」の横にある歯車アイコンをクリックします。次に、ドライブ・ベイ・グループを選択し、「**適用**」ボタンをクリックして構成を保存します。

---

### RAID セットアップ

RAID のセットアップ機能を実行するには、このトピックの情報を 사용합니다。

RAID アダプターのストレージ・プール、関連仮想ディスクおよびドライブを表示して構成するには、このトピックの情報を 사용합니다。システムの電源がオフの場合は、RAID 情報を表示するにはシステムの電源をオンにします。

### 仮想ドライブの表示および構成

仮想ドライブを表示および構成するには、このトピックの情報を 사용합니다。

「**サーバー構成**」の下で「**RAID セットアップ**」を選択すると、デフォルトで「**アレイ構成**」タブが選択され既存の仮想ディスクが表示されます。論理ドライブは、ディスク・アレイおよびコントローラ別にソートされます。仮想ディスクに関する詳細情報 (たとえば仮想ディスクのストリップ・サイズなど) とブート可能情報が表示されます。

RAID 設定を構成するには、「**編集モードを有効にする**」をクリックします。

編集モードで、コントローラの操作メニューをクリックして、現行の RAID 仮想ディスクを表示したり、新しい RAID 仮想ディスクを作成したりできます。

「**コントローラ操作**」メニューでは、以下の操作を実行できます。

#### RAID 構成のクリア

選択したコントローラのすべての構成およびデータをクリアします。

## 異種ドライブのインポート

検出された外部ドライブをインポートします。外部ドライブとは、別の RAID 構成から現行の RAID コントローラーに移動したドライブです

注：外部ドライブがない場合は通知されます。

## 外部構成の管理

検出された外部ドライブをインポートします。外部ドライブとは、別の RAID 構成から現行の RAID コントローラーに移動したドライブです

注：外部ドライブがない場合は通知されます。

特定のコントローラーの現行の RAID 仮想ディスクの情報はそれぞれの「仮想ディスク・カード」として表示されます。各カードには、仮想ディスクの名前、ステータス、容量、および操作などの情報が表示されます。鉛筆のアイコンは情報を編集できます。ゴミ箱のアイコンは「仮想ディスク・カード」を削除できます。

注：容量と RAID レベルは変更できません。

仮想ディスクの名前をクリックすると、仮想ディスクのプロパティ・ウィンドウが表示されます。

## 新しい RAID 仮想ディスクの作成

新しい RAID 仮想ディスクを作成するには、以下に示されている手順に従ってください。

注：ストレージ容量が残っていない場合は、新規仮想ディスクを作成できません。

### 1. ドライブまたはストレージ容量に空きがあるディスク・アレイを選択します

- a. 仮想ディスクを新規ディスク・アレイに作成する場合、RAID レベルを指定する必要があります。

注：選択したドライブが十分ではないまま「次へ」をクリックすると、RAID レベル・フィールドの下にエラー・メッセージが表示されます。

- b. 一部の RAID レベルでは、スパンが必要です。また、スパン内に必要なドライブの最小数があります。このような場合、「スパン番号」フィールドにスパン番号を指定し、ドライブの横にあるドロップダウン・メニューから「メンバー」または「ホット・スペア」を選択して、仮想ディスクの作成に使用するドライブの横にあるチェック・ボックスにチェックを入れます。
- c. 既存のディスク・アレイに仮想ディスクを作成するには、空き容量があるディスク・アレイを選択する必要があります。

### 2. 仮想ディスクの作成

- a. デフォルトでは、仮想ディスクを作成すると、すべてのストレージ容量が使用されます。すべてのストレージが使用されると「追加」アイコンは無効になります。鉛筆アイコンをクリックして、容量や他のプロパティを変更できます。
- b. 最初の仮想ディスクがストレージ容量の一部のみを使用するように編集すると、「追加」アイコンが有効になります。アイコンをクリックして「仮想ディスクを追加」ウィンドウを表示します。
- c. 「削除」アイコンをクリックして、仮想ディスクを削除します。このアイコンは仮想ディスクが 1 つしかない場合は表示されません。「削除」アイコンをクリックすると、選択された行は即時削除されます。仮想ディスクがまだ作成されていないため、確認ウィンドウはありません。
- d. 「作成を開始」をクリックして、プロセスを開始します。

注：コントローラーがサポートされていない場合、メッセージが表示されます。

## ストレージ・インベントリーの表示および構成

ストレージ・インベントリーを表示および構成するには、このトピックの情報を参照します。

「ストレージ・インベントリー」タブで、ディスク・アレイ、関連する仮想ドライブおよび RAID コントローラーのドライブを表示および構成できます。

• RAID 構成をサポートしているストレージ・デバイスの場合:

1. コントローラーに構成済みディスク・アレイが含まれている場合は、ディスク・アレイに基づいて取り付け済みドライブを表示します。以下でウィンドウに表示される項目について説明します。
  - **表のタイトル:** ディスク・アレイ ID、RAID レベルおよびドライブの合計数を表示します。
  - **表の内容:** ドライブ名、ドライブの状態、タイプ、製品、製造元、シリアル番号、アクションなどの基本的なプロパティをリストします。「システム一覧」ページで、XClarity Controller が検出可能なすべてのプロパティを表示できます。
  - **操作:** 以下は、実行できる操作項目です。一部の操作は、ドライブが異なる状態であるときは使用できません。
    - **ホット・スペアの割り当て:** ドライブをグローバル・ホット・スペアまたは専用ホット・スペアとして指定します。
    - **ホット・スペアを削除:** ドライブをホット・スペアから削除します。
    - **ディスク・ドライブをオフラインにする:** ドライブをオフラインに設定します。
    - **ディスク・ドライブをオンラインにする:** ドライブをオンラインに設定します。
    - **再構築の開始:** RAID を再構築します。
    - **ディスクドライブを再利用可能にする:** ドライブを再利用可能に設定します。
    - **ディスク・ドライブを欠落にする:** ドライブを欠落として設定します。
    - **単なるディスクの集まりに対してドライブを正常として設定する:** 単なるディスクの集まりディスク配置にドライブを追加します。
    - **未構成のドライブを正常として設定する:** ドライブをアレイに構成できるようにします。または緊急ホット・スペア用にします。
    - **未構成のドライブを不良として設定する:** ドライブを不良としてマークし、アレイ内や緊急ホット・スペア用には使用されないようにします。
    - **ディスク・ドライブを取り外し可能にする:** ドライブを取り外せるように設定します。
2. コントローラーにまだ構成されていないディスクが含まれている場合、そのドライブは「非 RAID ディスク・ドライブ」テーブルに表示されます。「単なるディスクの集まりを構成可能に変換」オプションをクリックすると、この操作項目をサポートするすべてのドライブを表示するウィンドウが開きます。1 つ以上のドライブを選択して変換できます。

RAID 構成をサポートしていないストレージ・デバイスの場合: XClarity Controller で一部のドライブのプロパティが検出できない場合があります。



---

## 第 8 章 サーバー・ファームウェアの更新

サーバー・ファームウェアを更新するには、このトピックの情報を 사용합니다。

---

### ファームウェア更新の概要

サーバー・ファームウェアの更新に関する一般情報。

左側のペインの「**ファームウェア更新**」をクリックすると、ファームウェア情報の概要が表示されます。

- **リポジトリからの更新:** サーバー・ファームウェアとリモート CIFS/NFS リポジトリを同期しバッチ更新を行います (82 ページの「**リポジトリからの更新**」を参照)。
- **システム・ファームウェア:** システム・ファームウェアのステータス、バージョン、およびシステム・ファームウェア更新の概要。

注: 「**自動同期**」をクリックして、「**バックアップする自動プロモート・プライマリー BMC**」を有効または無効にします。この設定を有効にすると、プライマリー・バンクが ISM (Image Stability Metric) 測定に合格した後、保留中のバックアップ・バンク・ファームウェアがプライマリー・バンクから同期されます。

- **アダプター・ファームウェア:** 取り付けられたアダプター・ファームウェア、ステータス、バージョン、およびアダプター・ファームウェア更新の概要。
- **パワー・サプライ・ユニットのファームウェア:** パワー・サプライ・ユニットのファームウェア・バージョンと PSU ファームウェアのアップデートの概要。
- **ドライブ・バックプレーン PSoc ファームウェア:** バックプレーン・ファームウェア・バージョンの概要。システム・ファームウェアの更新を実行します。

BMC、UEFI、LXPM、LXPM ドライバー、組み込み OS、FPGA、およびアダプターの現在のステータスとファームウェア・バージョン (BMC のプライマリー・バージョンとバックアップ・バージョンを含む) が表示されます。ファームウェア状況には、次の 3 つのカテゴリがあります。

- **アクティブ:** ファームウェアはアクティブです。
- **非アクティブ:** ファームウェアはアクティブではありません。
- **再起動保留中:** ファームウェア・イメージが更新されており、BMC のサーバーの再起動後に有効になります。
- **該当なし:** このコンポーネントにファームウェアがインストールされていませんでした。

注意:

- XCC および IMM は、UEFI を更新する前に最新バージョンに更新する必要があります。異なる順序で更新すると、正しく動作しない可能性があります。
- 誤ったファームウェア更新をインストールすると、サーバーが誤動作する可能性があります。ファームウェアまたはデバイス・ドライバの更新をインストールする前に、ダウンロードした更新に付属のすべての README および変更履歴ファイルをお読みください。これらのファイルには、更新に関する重要な情報および更新のインストール手順が記載されています。この手順には、以前のファームウェアまたはデバイス・ドライバのバージョンから最新のバージョンに更新するための特殊な手順も含まれます。Web ブラウザーに XCC キャッシュ・データが含まれている可能性があるため、XCC ファームウェアのアップグレード後に Web ページを再ロードすることをお勧めします。
- SATA M.2 アダプターを除き、AMD プロセッサ・サーバーはアウトオブバンドのアダプター・ファームウェアの更新をサポートしません。
- 一部のファームウェア更新では、システムの再起動が必要です。これにより、ファームウェアのアクティブ化または内部更新が実行されます。システムのブートのこのプロセスは、「システム保守

モード」と呼ばれ、ユーザーの電源操作を一時的に許可しません。このモードは、ファームウェア更新中も有効になっています。システムが保守モードに入ったときに、ユーザーは AC 電源を切り離してはなりません。

---

## システム、アダプター、および PSU ファームウェア更新

システム・ファームウェア、アダプター・ファームウェア、および PSU ファームウェアを更新する手順。

システム・ファームウェア、アダプター・ファームウェアおよび PSU ファームウェアの更新を手動で適用するには、次のステップを実行してください。

1. 各機能の**ファームウェアの更新**をクリックします。「サーバー・ファームウェアの更新」ウィンドウが開きます。
2. 「参照...」をクリックして、使用するファームウェア更新ファイルを選択します。
3. 選択したいファイルまでナビゲートし、「開く」をクリックします。選択したファイルが表示されている「サーバー・ファームウェアの更新」ウィンドウに戻ります。
4. 「次へ」をクリックして、選択したファイルに対するアップロードと検証のプロセスを開始します。ファイルがアップロードされて検証されている間、進行状況メーターが表示されます。この状況ウィンドウを表示して、更新のために選択したファイルが正しいファイルであることを確認できます。**システム・ファームウェア**では、状況ウィンドウに、BMC、UEFI、または LXPM など、更新されるファームウェア・ファイルのタイプに関する情報が示されます。ファームウェア・ファイルが正常にアップロードされて検証された後、「次へ」をクリックして更新するデバイスを選択します。
5. 「更新」をクリックして、ファームウェア更新を開始します。進行状況メーターによって更新の進行状況が示されます。ファームウェア更新が正常に完了したら、「完了」をクリックします。更新を有効にするために XClarity Controller の再起動が必要な場合は、警告メッセージが表示されます。XClarity Controller を再起動する方法の詳細については、[60 ページの「電源操作」](#)を参照してください。

---

## リポジトリからの更新

リモート・リポジトリからのサーバー・ファームウェアの更新

### 概要

注：CIFS/NFS/HTTPS/ オンボード・ファームウェア履歴機能には、XCC Premier ライセンスが必要です。

XCC には、更新バンドル(サービス・パック)パッケージを使用したサーバーでのファームウェアの更新が導入されました。この機能は、単一の API または Redfish クライアント・ツールを使用してシステム内のすべてのファームウェア (OOB ファームウェア・パッケージと IB ファームウェア・パッケージの両方を含む) を更新することによってプロセスを簡略化します。このプロセスでは、適用可能なファームウェア・パッケージの特定、リモート HTTP/HTTPS サーバーからのダウンロードと解凍、Web ブラウザーを介した BMC 内部ストレージへのアップロード、あるいは CIFS または NFS 共有ディレクトリからのマウントを行う必要があります。

メタデータ (JSON 形式) ファイルは、メタデータでファームウェア・ペイロードを指定した状態で CIFS または NFS マウントを使用する場合、ネットワーク共有ファイル・システムのルート・ディレクトリに配置する必要があります。サーバーの microSD デバイスには、ユーザーがファームウェア・レベルをロールバック可能にするため、履歴リポジトリを保存できます。

アウト・オブ・バンドのファームウェア更新をサポートしないペイロードがファームウェア・パッケージに含まれている場合、BMC は、サーバーを起動し、更新を実行する前に BMC にインストールされた組み込み OS イメージからブートするよう構成します。



## バンドルとメタデータの更新

更新バンドル(サービス・パック)は、ファームウェア・バンドルの圧縮ファイルです。このバンドルには、システム内のコンポーネント用の1つまたは複数のファームウェア・パッケージが含まれています。XCCの「リポジトリからの更新」機能では、更新バンドル・ファイルが使用されます。解凍されたバンドル・ファイルには、メタデータとペイロード・バイナリーが含まれています。JSONメタデータ・ファイルは、バンドル・ファイルに含まれているファームウェア・イメージの種類に関する情報をXCCに提供し、ペイロード・バイナリーはファームウェア・イメージを提供します。

## XCC内のファームウェア・リポジトリ

更新バンドルには複数のファームウェア・パッケージを含めることができ、XCCは新機能のためにフラッシュに2GBのスペースを予約します。XCCは、新しいバンドルを受信すると、古いデータをクリーンアップします。一部のプラットフォームでは、追加のストレージを提供するためにMicroSDカードが使用されています。XCCにより、最後の更新バンドルがSDカードの履歴リポジトリに移動されます。ファームウェア履歴リポジトリには、最大3つのバンドルを保存できます。ユーザーは、ファームウェア・ロールバック機能を使用して以前のバンドルに戻すことができます。



注：

- 更新バンドルに、システムが使用可能なOOBファームウェア・パッケージのみ含まれている場合、XCCはシステムの電源状態を変更しません。PCIデバイス・ファームウェアを更新するには、システムの電源がオンになっている必要があります。
- 更新バンドルに、システムが使用可能なIBファームウェア・パッケージが含まれている場合、XCCは更新前にシステムの電源状態を保存し、更新バンドルが更新されたら電源状態を復元します。更新プロセス中、XCCは組み込みOSにホストをリブートします。
- 更新バンドルにUEFIファームウェアの前提条件レベルが含まれているが、現在インストールされているUEFIバージョンがそのレベル以下である場合、XCCはシステムの電源をオフにし、まずUEFIファームウェア更新を実行します。
- 更新バンドルにXCCファームウェアの前提条件レベルが含まれているが、現在インストールされているXCCバージョンがそのレベル以下の場合、XCC自体のアップグレード後XCCが最初にリブートされます。

## WebGUIを使用した更新

リポジトリからの更新を使用すると、ユーザーは、サーバー・ファームウェアを内部ストレージと同期するようにXCCを構成できます。ファームウェア・リポジトリには、バイナリーおよびメタデータ・ファイル、更新バンドル・メタデータJSONおよび対応するバイナリー・ファイルなど、パッケージが含まれている必要があります。XCCはメタデータJSONファイルを解析し、この固有のシステム・ハードウェアのOOB更新をサポートするファームウェア・パッケージを取得してから、バッチ更新を開始します。

リポジトリから更新するには、以下のステップを実行します。

- 内部ストレージを使用する場合は、「**ファームウェア・パッケージのインポート**」をクリックし、ファームウェア・パッケージ(.tgzまたはzip形式)を参照します。
- 「**システムの更新**」をクリックして、バッチ更新を開始します。
- 「**詳細の表示**」をクリックして、更新ステータスを確認します。
  - 緑色のチェック・マーク** : ファームウェアのアップグレードが正常に完了しました。
  - 赤色Xマーク** : ファームウェアのアップグレードに失敗しました。
  - 更新中**: ファームウェアはアップグレードのプロセスを実行中です。
  - キャンセル**: ファームウェアのアップグレードが取り消されました。
  - 待機中**: ファームウェアのアップグレードがデプロイを待機中です。

注：「**更新の停止**」をクリックすると、現在のインストール・パッケージの更新が完了した後にキューにあるアップグレードが取り消されます。

4. CIFS または NFS を使用している場合は、「マウント解除」をクリックして、リモート・リポジトリから切断します。
5. 更新を有効にするために XClarity Controller の再起動が必要な場合は、警告メッセージが表示されます。XClarity Controller を再起動する方法の詳細については、[60 ページの「電源操作」](#)を参照してください。

注：システムに MicroSD カードが取り付けられている場合、更新バンドルの更新履歴を確認し、更新バンドルのインデックスを選択してファームウェア・ロールバックを実行できます。このプロセスは、過去の更新バンドルが MicroSD 内に配置されることを除き、リポジトリからの更新と似ています。

---

## 第9章 ライセンス管理

Lenovo XClarity Controller License Management を使用すると、オプションのサーバーおよびシステム管理機能をインストールして管理できます。

XClarity Controller ファームウェアの機能およびご使用のサーバーで使用可能なフィーチャーには、いくつかのレベルがあります。ご使用のサーバーにインストールされたファームウェア・フィーチャーのレベルは、ハードウェアのタイプによって異なります。

XClarity Controller の機能は、アクティベーション・キーを購入してインストールすることでアップグレードできます。

アクティベーション・キーを注文するには、販売担当員またはビジネス・パートナーにお問い合わせください。

XClarity Controller Web インターフェースまたは XClarity Controller CLI を使用して、アクティベーション・キーを手動でインストールします。これにより、購入したオプション・フィーチャーを使用できるようになります。キーをアクティブにする前に、以下のことを確認してください。

- アクティベーション・キーは、XClarity Controller へのログインに使用するシステム上に存在しなければなりません。
- ライセンス・キーの注文が完了し、その認証コードを郵送またはメールで受け取っていない限りなりません。

XClarity Controller Web インターフェースを使用してアクティベーション・キーを管理するには、[85 ページの「アクティベーション・キーのインストール」](#)、[86 ページの「アクティベーション・キーの削除」](#)、または [86 ページの「アクティベーション・キーのエクスポート」](#) を参照してください。XClarity Controller CLI を使用してアクティベーション・キーを管理するには、[114 ページの「keycfg コマンド」](#) を参照してください。

XClarity Controller ライセンスの管理で ID を登録するには、次のリンクをクリックしてください。

<https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome>

Lenovo サーバーのライセンス管理について詳しくは、以下の **Lenovo Press Web** サイトで入手できます。

<https://lenovopress.com/redp4895-using-lenovo-features-on-demand>

---

### アクティベーション・キーのインストール

サーバーにオプション・フィーチャーを追加するには、このトピックの情報を参照してください。

アクティベーション・キーをインストールするには、以下のステップを実行してください。

ステップ 1. 「**BMC 構成**」の下にある「**ライセンス**」をクリックします。

ステップ 2. 「**ライセンスのアップグレード**」をクリックします。

ステップ 3. 「**新規ライセンスの追加**」ウィンドウで「**参照**」をクリックします。次に「**ファイルのアップロード**」ウィンドウで追加するアクティベーション・キー・ファイルを選択し、「**開く**」をクリックしてそのファイルを追加します。キーの追加を完了するには、「**アクティベーション・キーの追加**」ウィンドウで「**インポート**」をクリックします。

注：アクティベーション・キーが無効である場合は、エラー・ウィンドウが表示されます。

---

## アクティベーション・キーの削除

サーバーからオプション・フィーチャーを削除するには、このトピックの情報を使用します。

アクティベーション・キーを削除するには、以下のステップを実行してください。

- ステップ 1. 「**BMC 構成**」の下にある「**ライセンス**」をクリックします。
- ステップ 2. 削除するアクティベーション・キーを選択して、「**削除**」をクリックします。
- ステップ 3. 「アクティベーション・キーの削除の確認」ウィンドウで、「**OK**」をクリックしてアクティベーション・キーの削除を確認します。選択したアクティベーション・キーがサーバーから削除され、「**ライセンス管理**」ページに表示されなくなります。

---

## アクティベーション・キーのエクスポート

サーバーからオプション・フィーチャーをエクスポートするには、このトピックの情報を使用します。

アクティベーション・キーをエクスポートするには、次のステップを実行します。

- ステップ 1. 「**BMC 構成**」の下にある「**ライセンス**」をクリックします。
- ステップ 2. 「**ライセンス管理**」ページから、エクスポートするアクティベーション・キーを選択して、「**エクスポート**」をクリックします。
- ステップ 3. 「**選択したライセンスをエクスポート**」ウィンドウで、「**エクスポート**」をクリックして、アクティベーション・キーのエクスポート要求を確認します。
- ステップ 4. ファイルを保存するディレクトリーを選択します。選択したアクティベーション・キーがサーバーからエクスポートされます。

---

## 第 10 章 コマンド・ライン・インターフェース

XClarity Controller Web インターフェースを使用せずに XClarity Controller を管理および監視するコマンドを入力するには、このトピックの情報を使用します。

XClarity Controller コマンド・ライン・インターフェース (CLI) を使用すると、Web インターフェースを使用せずに XClarity Controller にアクセスできます。このインターフェースは、Web インターフェースによって提供される管理機能のサブセットを提供します。

CLI には、SSH セッションからアクセスすることができます。CLI コマンドを発行するには、XClarity Controller に認証されている必要があります。

---

### コマンド・ライン・インターフェースへのアクセス

CLI にアクセスするには、このトピックの情報を使用します。

CLI にアクセスするには、XClarity Controller の IP アドレスに対して SSH セッションを開始します (詳しくは、[87 ページの「Serial-to-SSH リダイレクトの構成」](#)を参照)。

---

### コマンド・ライン・セッションへのログイン

コマンド・ライン・セッションにログインするには、このトピックの情報を使用します。

コマンド・ラインにログインするには、以下のステップを実行します。

ステップ 1. XClarity Controller との接続を確立します。

ステップ 2. ユーザー名プロンプトに、ユーザー ID を入力します。

ステップ 3. パスワードのプロンプトで、XClarity Controller へのログインに使用するパスワードを入力します。

注：コマンド・ライン・プロンプトは `system>` です。コマンド・ライン・セッションは、コマンド・ラインに `exit` と入力するまで続きます。ログオフされ、セッションは終了します。

---

### Serial-to-SSH リダイレクトの構成

このトピックでは、シリアル端末サーバーとしての XClarity Controller の使用について説明します。

Serial-to-SSH リダイレクトにより、システム管理者が XClarity Controller をシリアル端末サーバーとして使用できるようになります。シリアル・リダイレクトが有効な場合、SSH 接続からサーバーのシリアル・ポートにアクセスすることができます。

注：CLI の `console 1` コマンドを使用して、COM ポートとのシリアル・リダイレクト・セッションを開始することができます。

#### セッションの例

```
$ ssh USERID@10.240.1.12
```

```
Password:
```

```
system>
```

SSH セッションからのすべてのトラフィックは、COM2 へ経路指定されます。

ESC (

終了キー・シーケンスを入力して、CLIに戻ります。この例では、Escを押してから左括弧を入力します。CLIプロンプトが表示され、IMM CLIへ戻ることを示します。

system>

---

## コマンド構文

CLIにコマンドを入力する方法を理解するには、このトピックのガイドラインを確認します。

コマンドを使用する前に、以下のガイドラインをお読みください。

- 各コマンドは、次の形式をとります。  
`command [arguments] [-options]`
- コマンド構文には大/小文字の区別があります。
- コマンド名は、すべて小文字です。
- すべての引数は、コマンドの直後に置く必要があります。オプションは、引数の直後に置く必要があります。
- 各オプションの前には、必ずハイフン(-)を付けます。オプションには、短いオプション(単一の英字)と長いオプション(複数の英字)があります。
- オプションに引数がある場合は、その引数を必ず指定する必要があります。  
`ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`  
ここで、`ifconfig`はコマンドで、`eth0`は引数であり、`-i`、`-g`、および`-s`はオプションです。この例では、3つのオプションのすべてが引数を備えています。
- ブラケットは、引数またはオプションが省略可能であることを示しています。ブラケットは、入力するコマンドの一部ではありません。

---

## 機能および制限

このトピックでは、CLIの機能と制限事項について説明します。

CLIには、以下の機能と制限事項があります。

- 複数の並行CLIセッションはSSH経由で許可されます。
- 1行(スペースも含めて1,024文字が限度)につき1つのコマンドが許可されます。
- 長いコマンドに継続文字はありません。唯一の編集機能は、入力したばかりの文字を消去するBackspaceキーです。
- 上下の矢印キーを使用すると、最後の8つのコマンドを参照できます。`history`コマンドを使用すると最後の8つのコマンドが入ったリストが表示され、これをショートカットとして使用して、次の例のようにコマンドを実行できます。

```
system > history
0 ifconfig eth0
1 readlog
2 readlog
3 readlog
4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
```

```
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- CLI では、出力バッファの限度は 2 KB です。バッファリングはありません。個々のコマンドの出力は、2048 文字を超えることができません。この制限は、シリアル・リダイレクト・モードでは適用されません(シリアル・リダイレクトの間、データはバッファに格納されます)。

- コマンドの実行状況を表すために、次の例のように、単純なテキスト・メッセージが使用されます。

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- コマンド構文には大/小文字の区別があります。
- オプションとその引数の間には、少なくとも 1 つのスペースが存在する必要があります。たとえば、`ifconfig eth0 -i192.168.70.133` は誤った構文です。正しい構文は `ifconfig eth0 -i 192.168.70.133` です。
- すべてのコマンドに、構文のヘルプを表示する `-h`、`-help` および `?` オプションがあります。以下の例はすべて、同じ結果になります。

```
system> power -h
system> power -help
system> power ?
```

- 以下のセクションで説明しているコマンドの一部は、ご使用のシステム構成では使用できない場合があります。ご使用の構成でサポートされるコマンドのリストを参照するには、次の例に示すように、`help` または `?` オプションを使用します。

```
system> help
system> ?
```

---

## アルファベット順のコマンド・リスト

このトピックでは、CLI コマンドのリストをアルファベット順で表示します。各コマンドに対して、トピックへのリンクがあります。各コマンド・トピックでは、コマンド、その機能、構文、および使用方法について説明します。

すべての XClarity Controller CLI コマンドの完全なリスト (アルファベット順) は、次のとおりです。

- [103 ページの「accsecfg コマンド」](#)
- [149 ページの「adapter コマンド」](#)
- [104 ページの「asu コマンド」](#)
- [107 ページの「backup コマンド」](#)
- [138 ページの「batch コマンド」](#)
- [92 ページの「clearlog コマンド」](#)
- [138 ページの「clock コマンド」](#)
- [151 ページの「dbgshbmc コマンド」](#)
- [108 ページの「dhcpinfo コマンド」](#)
- [108 ページの「dns コマンド」](#)
- [109 ページの「encaps コマンド」](#)
- [110 ページの「ethtousb コマンド」](#)
- [91 ページの「exit コマンド」](#)

- 92 ページの 「fans コマンド」
- 110 ページの 「firewall コマンド」
- 102 ページの 「fuelg コマンド」
- 112 ページの 「hashpw コマンド」
- 91 ページの 「help コマンド」
- 91 ページの 「history コマンド」
- 112 ページの 「ifconfig コマンド」
- 139 ページの 「info コマンド」
- 114 ページの 「keycfg コマンド」
- 115 ページの 「ldap コマンド」
- 93 ページの 「led コマンド」
- 92 ページの 「mhlog コマンド」
- 117 ページの 「ntp コマンド」
- 117 ページの 「portcontrol コマンド」
- 118 ページの 「ports コマンド」
- 100 ページの 「power コマンド」
- 103 ページの 「pxeboot コマンド」
- 119 ページの 「rdmount コマンド」
- 95 ページの 「readlog コマンド」
- 101 ページの 「reset コマンド」
- 120 ページの 「restore コマンド」
- 120 ページの 「roles コマンド」
- 121 ページの 「rtd コマンド」
- 122 ページの 「seccfg コマンド」
- 122 ページの 「securityinfo コマンド」
- 123 ページの 「securitymode コマンド」
- 96 ページの 「servicelog コマンド」
- 123 ページの 「snmp コマンド」
- 126 ページの 「snmpalerts コマンド」
- 140 ページの 「spreset コマンド」
- 127 ページの 「sshcfg コマンド」
- 127 ページの 「sslcfg コマンド」
- 140 ページの 「storage コマンド」
- 97 ページの 「syshealth コマンド」
- 130 ページの 「syslock コマンド」
- 98 ページの 「temps コマンド」
- 131 ページの 「thermal コマンド」
- 132 ページの 「tls コマンド」
- 132 ページの 「trespass コマンド」
- 133 ページの 「uefipw コマンド」
- 133 ページの 「usbeth コマンド」



- [134 ページの「users コマンド」](#)
- [99 ページの「volts コマンド」](#)
- [99 ページの「vpd コマンド」](#)

---

## ユーティリティー・コマンド

このトピックでは、ユーティリティー CLI コマンドのアルファベット順リストを説明します。

ユーティリティー・コマンドは、現在 3 つあります。

### exit コマンド

CLI セッションをログオフするには、このコマンドを使用します。

exit コマンドは、CLI セッションをログオフし、終了するために使用します。

### help コマンド

このコマンドは、すべてのコマンドのリストを表示します。

help コマンドは、すべてのコマンドのリストを、コマンドの簡略説明を付けて表示するために使用します。コマンド・プロンプトで ? と入力することもできます。

### history コマンド

このコマンドは、以前に発行されたコマンドのリストを提供します。

history コマンドは、直前に発行された 8 つのコマンドのインデックス付きヒストリー・リストを表示するために使用します。その後、インデックスをショートカットとして (前に ! を付けて) 使用し、このヒストリー・リストからコマンドを再発行できます。

例:

```
system> history
0 ifconfig eth0
1 readlog
2 readlog
3 readlog
4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

---

## モニター・コマンド

このトピックでは、モニター CLI コマンドのアルファベット順リストを説明します。

モニター・コマンドは、現在 11 あります。

## clearlog コマンド

このコマンドは、IMM イベント・ログをクリアするために使用します。

**clearlog** コマンドを使用すると、IMM のイベント・ログをクリアします。このコマンドを使用するには、イベント・ログをクリアする権限を持っている必要があります。

注：このコマンドはサポート担当者のみが使用します。

構文:

```
clearlog [-options]
```

表 4. clearlog オプション

オプション	説明	値
-t	イベント・タイプ、クリアするイベントのタイプを選択します。指定しない場合、すべてのイベント・タイプが選択されます。	all、platform、audit <ul style="list-style-type: none"><li>• all: プラットフォーム・イベントと監査イベントを含む、すべてのイベント・タイプ。</li><li>• platform: プラットフォーム・イベント・タイプ。</li><li>• audit: 監査イベント・タイプ。</li></ul>

例:

```
system> clearlog
All event log cleared successfully
system>
system> clearlog -t all
All event log cleared successfully
system>
system> clearlog -t platform
Platform event log cleared successfully
system>
system> clearlog -t audit
Audit event log cleared successfully
system>
```

## fans コマンド

このコマンドは、サーバー・ファンの速度を表示するために使用します。

**fans** コマンドは、個々のサーバー・ファンの速度を表示するために使用します。

例:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

## mhlog コマンド

メンテナンス履歴のアクティビティ・ログ項目を表示するには、このコマンドを使用します。

構文:

mhlog [-options]

表 5. mhlog オプション

オプション	説明	値
-c	「count」項目数を表示	1 ~ 250
-i	インデックスで始まる項目を表示	1 ~ 250
-f	ログ・ファイルのリモート・ファイル名	ログ・ファイルのファイル名に有効なファイル名
-ip	tftp/sftp サーバーのアドレス	TFTP/SFTP サーバーの有効な IP アドレス
-pn	tftp/sftp サーバーのポート番号	TFTP/SFTP サーバーの有効なポート番号 (デフォルト 69/22)
-u	sftp サーバーのユーザー名	SFTP サーバーの有効なユーザー名
-pw	sftp サーバーのパスワード	SFTP サーバーの有効なパスワード

例:

```
system> mhlog
```

```
Type      Message                                     Time
-----
Hardware   SAS Backplane1(SN: XXXX9CE009L) is added.    05/08/2020,04:23:18
Hardware   CPU 1(SKU NO: 50844440) is added.            05/08/2020,04:23:22
Hardware   CPU 2(SKU NO: 50844440) is added.            05/08/2020,04:23:22
Hardware   M2 Card(SN: R1SH9AJ0037) is added.           05/08/2020,04:23:22
Firmware   Primary XCC firmware is updated to TGBT99T by XCC Web. 05/08/2020,06:40:37
Firmware   Primary XCC firmware is activated to TGBT99T. 05/08/2020,06:41:26
Hardware   PSU1(SN: D1D694C0075) is added.             05/08/2020,06:43:28
system>
```

## led コマンド

LED の状態を表示および設定するには、このコマンドを使用します。

led コマンドはサーバーの LED の状態を表示および設定します。

- オプションを指定せずに led コマンドを実行すると、前面パネル LED の状況が表示されます。
- led -d コマンド・オプションは、led -identify on コマンド・オプションと一緒に使用する必要があります。

次の表は、オプションの引数を示しています。

構文:

led [-options]

表 6. led オプション

オプション	説明	値
-l	システムおよびシステムのサブコンポーネントのすべての LED の状況の取得	
-identify	エンクロージャー識別 LED の状態の変更	off、on、blink
-d	識別 LED を指定された時間だけオンにする	時間 (秒)

例:

```
system> led
```

```

Fault      Off
Identify   On      Blue
Chklog     Off
Power      Off

```

```
system> led -l
```

```

Label      Location      State      Color
Battery    Planar        Off
BMC Heartbeat Planar      Blink     Green
BRD        Lightpath Card Off
Channel A   Planar        Off
Channel B   Planar        Off
Channel C   Planar        Off
Channel D   Planar        Off
Channel E   Planar        Off
Chklog      Front Panel   Off
CNFG       Lightpath Card Off
CPU        Lightpath Card Off
CPU 1      Planar        Off
CPU 2      Planar        Off
DASD       Lightpath Card Off
DIMM       Lightpath Card Off
DIMM 1     Planar        Off
DIMM 10    Planar        Off
DIMM 11    Planar        Off
DIMM 12    Planar        Off
DIMM 13    Planar        Off
DIMM 14    Planar        Off
DIMM 15    Planar        Off
DIMM 16    Planar        Off
DIMM 2     Planar        Off
DIMM 3     Planar        Off
DIMM 4     Planar        Off
DIMM 5     Planar        Off
DIMM 6     Planar        Off
DIMM 7     Planar        Off
DIMM 8     Planar        Off
DIMM 9     Planar        Off
FAN        Lightpath Card Off
FAN 1     Planar        Off
FAN 2     Planar        Off
FAN 3     Planar        Off
Fault      Front Panel (+) Off
Identify   Front Panel (+) On      Blue
LINK       Lightpath Card Off
LOG        Lightpath Card Off
NMI        Lightpath Card Off
OVER SPEC  Lightpath Card Off
PCI 1     FRU          Off
PCI 2     FRU          Off
PCI 3     FRU          Off
PCI 4     FRU          Off
Planar     Planar        Off
Power      Front Panel (+) Off
PS        Lightpath Card Off
RAID      Lightpath Card Off
Riser 1   Planar        Off
Riser 2   Planar        Off
SAS ERR   FRU          Off
SAS MISSING Planar        Off
SP        Lightpath Card Off

```

```
TEMP          Lightpath Card    Off
VRM           Lightpath Card    Off
system>
```

## readlog コマンド

このコマンドは、IMM のイベント・ログを表示します。

**readlog** コマンドは、IMM イベント・ログ項目を表示するために使用します。一度に5つのイベント・ログが表示されます。項目は、最も新しいものから最も古いものへという順序で表示されます。

注：

- R - 無効
- I - 情報
- W - 警告
- E - クリティカル

構文:

```
readlog [-options]
```

表 7. readlog オプション

オプション	説明	値
-a	イベント・ログのすべてのエントリを、最新のものから順に表示します。	
-f	カウンターをリセットし、イベント・ログ内の最初の5項目を、最も新しいものから順に表示します。	
-date	指定した日付のイベント・ログ項目を表示します	mm/dd/yyyy の形式を使用します。
-sev	指定した重大度レベルのイベント・ログ項目を表示します。	R、I、W、E
-i	イベント・ログが保存される TFTP または SFTP サーバの IPv4 または IPv6 IP アドレスを設定します。-i および -I コマンド・オプションは一緒に使用され、ロケーションを指定します。	有効な IP アドレス
-l	イベント・ログ・ファイルのファイル名を設定します。-i および -I コマンド・オプションは一緒に使用され、ロケーションを指定します。	有効なファイル名
-pn	TFTP または SFTP サーバのポート番号を表示または設定します。	有効なポート番号 (デフォルト 69/22)
-u	SFTP サーバーのユーザー名を指定します。	有効なユーザー名
-pw	SFTP サーバーのパスワードを指定します。	有効なパスワード
-di	監査ログ機能の拡張	none、ipmi

例:

```
system> readlog -f
```

```

1 I 2017-06-17T09:31:59.217 Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685 Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581 Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174 Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5 I 2017-06-16T10:40:14.352 Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>

```

## servicelog コマンド

このコマンドは、新規サービス・データ・ファイルを生成するために使用します。

注：このコマンドは、以前は `ffdc` コマンドでした。

`servicelog` コマンドを使用して、サービス・データを生成し、サポートに転送します。

`servicelog` コマンドと一緒に使用するコマンドのリストを次に示します。

次の表は、オプションの引数を示しています。

構文:

```
servicelog [subset_command] [-options]
```

表 8. `servicelog` サブセット・コマンド

オプション	説明
<code>generate</code>	新しいサービス・データ・ファイルを作成する
<code>status</code>	サービス・データ・ファイルの状況をチェックする
<code>copy</code>	既存のサービス・データをコピーする
<code>delete</code>	既存のサービス・データを削除する

表 9. `servicelog` オプション

オプション	説明	値
<code>-t</code>	サービス・ログ・タイプ	1, 2, 3 <ul style="list-style-type: none"> <li>1: デバッグ・ログ (FFDC、デフォルト)</li> <li>2: サービス・データ・ログ</li> <li>3: サービス・データ・ログ結合デバッグ・ログ (ログ・ファイルをコピーする場合にのみ有効)</li> </ul>
コマンド生成のための追加オプション		
<code>-c</code>	ダンプ・データ・カテゴリーの選択。このオプションで指定されていない場合、データ・カテゴリーは含まれません。	<ul style="list-style-type: none"> <li>タイプ 1 (<code>ffdc</code>) の場合: <code>corefile</code></li> <li>タイプ 2 (サービス・データ・ログ) の場合: <code>network</code>、<code>audit</code>、<code>telemetry</code>、<code>osscreen</code></li> </ul>

表 9. servicelog オプション (続き)

オプション	説明	値
コマンドの生成およびコピーのための追加オプション		
-f	リモート・ファイル名または sftp ターゲット・ディレクトリ。	sftp の場合は、ディレクトリ名 (~ / または /tmp/) に絶対パスまたは後書きの / を使用します。デフォルト値は、システムが生成した名前です。
-ip	tftp/sftp サーバーのアドレス。	有効な IP アドレス
-pn	tftp/sftp サーバーのポート番号。	有効なポート番号 (デフォルト 69/22)
-u	sftp サーバーのユーザー名。	有効なユーザー名
-pw	sftp サーバーのパスワード。	有効なパスワード
-timeout	フォアグラウンド・コピーを許可する分数。	1 ~ 5 (デフォルトは 1)

例:

```
system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz
```

```
system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -ip 192.168.70.230
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

## syshealth コマンド

このコマンドは、正常性またはアクティブ・イベントの要約を提供します。

**syshealth** コマンドは、サーバーのヘルスの要約やアクティブ・イベントを表示するために使用します。電源状態、システム状態、ハードウェア状態 (ファン、パワー・サプライ、ストレージ、プロセッサ、メモリーを含む)、再起動カウント、および IMM ソフトウェア・ステータスが表示されます。

構文:

```
syshealth [arguments]
```

表 10. syshealth 引数

引数	説明
summary	システムの正常性の概要を表示します。
activeevents	アクティブなイベントを表示します。
cooling	冷却装置のヘルス・ステータスを表示します。
power	電源モジュールのヘルス・ステータスを表示します。
storage	ローカル・ストレージのヘルス・ステータスを表示します。
processors	プロセッサのヘルス・ステータスを表示します。
memory	メモリーのヘルス・ステータスを表示します。

例:

```
system> syshealth summary
Power On
State OS booted
Restarts 29
```

```
system> syshealth activeevents
No Active Event Available!
```

## temps コマンド

このコマンドは、すべての温度および温度しきい値の情報を表示します。

**temps** コマンドは、すべての温度と温度しきい値を表示するために使用します。Web インターフェースの場合と同じ温度セットが表示されます。

構文:

```
temps
```

例:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
  WR   W  T   SS   HS
-----
Ambient Temp 109.40/43  N/A  78.80/26.00  109.40/43.00  122.00/50.00
Exhaust Temp N/A     N/A  32.00/0.00  116.60/47.00  N/A
system>
```

注:

- 出力には、次の列見出しがあります。
  - WR: 警告リセット (正方向しきい値ヒステリシス値)
  - W: 警告 (上段非クリティカルしきい値)
  - T: 温度 (現行値)
  - SS: ソフト・シャットダウン (上段クリティカルしきい値)
  - HS: ハード・シャットダウン (上段リカバリー不能しきい値)
- 温度値は、すべて華氏/摂氏となっています。
- N/A は該当なしを意味します。



## volts コマンド

サーバーの電圧情報を表示するには、このコマンドを使用します。

**volts** コマンドは、すべての電圧と電圧しきい値を表示するために使用します。Web インターフェースの場合と同じ電圧セットが表示されます。

構文:

```
volts
```

例:

```
system> volts
      HSL SSL WL  WRL V  WRH WH  SSH HSH
-----
CMOS Battery N/A 2.25 2.39 0.03 3.12 0.03 N/A N/A N/A
system>
```

注：出力には、次の列見出しがあります。

HSL: ハード・シャットダウン低 (下段リカバリー不能しきい値)

SSL: ソフト・シャットダウン低 (下段クリティカルしきい値)

WL: 警告低 (下段非クリティカルしきい値)

WRL: 警告リセット低 (負方向しきい値ヒステリシス値)

V: 電圧 (現行値)

WRH: 警告リセット高 (正方向しきい値ヒステリシス値)

WH: 警告高 (上段非クリティカルしきい値)

SSH: ソフト・シャットダウン高 (上段クリティカルしきい値)

HSH: ハード・シャットダウン高 (上段リカバリー不能しきい値)

## vpd コマンド

このコマンドは、サーバーのハードウェアおよびソフトウェアに関連する構成および情報データ (重要プロダクト・データ) を表示します。

**vpd** コマンドは、システム (sys)、IMM (bmc)、サーバー BIOS (uefi)、Lenovo XClarity Provisioning Manager (lxpm)、サーバー・ファームウェア (fw)、サーバー・コンポーネント (comp)、および PCIe デバイス (pcie) の重要プロダクト・データを表示します。Web インターフェースの場合と同じ情報が表示されます。

構文:

```
vpd [arguments]
```

表 11. vpd 引数

引数	説明
vpd sys	システムの重要プロダクト・データを表示します。
vpd bmc	管理コントローラーの重要プロダクト・データを表示します。
vpd uefi	システム BIOS の重要プロダクト・データを表示します。
vpd lxpm	システム LXPM の重要プロダクト・データを表示します。
vpd fw	システム・ファームウェアの重要プロダクト・データを表示します。

表 11. vpd 引数 (続き)

引数	説明
vpd comp	システム・コンポーネントの重要プロダクト・データを表示します。
vpd pcie	PCIe デバイスの重要プロダクト・データを表示します。

例:

```
system> vpd bmc
Type      Status  Version  Build   ReleaseDate
-----
BMC (Primary) Active   0.00    DVI399T  2017/06/06
BMC (Backup) Inactive 1.00    TEI305J  2017/04/13
system>
```

## サーバーの電源および再起動制御コマンド

このトピックでは、電源および再起動 CLI コマンドのアルファベット順リストを説明します。

サーバーの電源および再起動コマンドは、現在 4 つあります。

### power コマンド

このコマンドは、サーバーの電源の制御方法を説明します。

**power** コマンドは、サーバーの電源を制御するために使用します。**power** コマンドを発行するには、リモート・サーバーの電源/再起動アクセスの権限レベルが必要です。

構文:

```
power on [-options]
power off [-options]
power cycle [-options]
power uefi
power state
```

表 12. power コマンド

コマンド	説明
power on	このコマンドは、サーバーの電源をオンにするのに使用します。
power off	サーバーの電源をオフにするには、このコマンドを使用します。
power cycle	サーバーの電源をいったんオフにしてから、再びオンにするには、このコマンドを使用します。
power uefi	このコマンドを使用して、UEFI の F1 セットアップに入ります。
power state	サーバーの電源の状態と、サーバーの現在の状態を表示するには、このコマンドを使用します。

表 13. power options

オプション	説明	値
-s	このオプションは、サーバーの電源をオフにする前に、オペレーティング・システムをシャットダウンするのに使用します。 注：power off コマンドおよび power cycle コマンドに -every オプションを使用すると、-s オプションが暗黙指定されます。	
-every	このオプションは、サーバーの電源を制御するために power on、power off、および power cycle の各コマンドで使用します。ご使用のサーバーの電源オン、電源オフ、および電源サイクルを行う日付、時間、および頻度 (1 日に 1 回、または週に 1 回) をセットアップすることができます。	Sun、Mon、Tue、Wed、Thu、Fri、Sat、Day、clear
-t	このオプションは、サーバーの電源オン、オペレーティング・システムのシャットダウン、およびサーバーの電源オフまたは再起動を行う時刻を、時間および分の単位で指定するのに使用します。	hh:mm の形式を使用します。
-d	このオプションは、サーバーの電源をオンにする日付を指定するのに使用します。これは、power on コマンドの追加オプションです。 注：-d オプションと -every オプションは、同一のコマンド上で一緒に使用することはできません。	mm/dd/yyyy の形式を使用します。
-clear	このオプションは、電源をオンにするスケジュール済みの日付をクリアするのに使用します。これは、power on コマンドの追加オプションです。	

次の情報は、power コマンドの例です。

オペレーティング・システムのシャットダウンとサーバーの電源オフを、毎週日曜日の 1:30 に行うには、次のコマンドを入力します。

```
system> power off -every Sun -t 01:30
```

オペレーティング・システムのシャットダウンとサーバーの再起動を、毎日 1:30 に行うには、次のコマンドを入力します。

```
system> power cycle -every Day -t 01:30
```

サーバーの電源オンを毎週月曜日の 1:30 に行うには、次のコマンドを入力します。

```
system> power on -every Mon -t 1:30
```

サーバーの電源オンを 2013 年 12 月 31 日午後 11:30 に行うには、次のコマンドを入力します。

```
system> power on -d 12/31/2013 -t 23:30
```

週に 1 回の電源サイクルをクリアするには、次のコマンドを入力します。

```
system> power cycle -every clear
```

## reset コマンド

このコマンドは、サーバーのリセット方法を説明します。

reset コマンドは、サーバーを再起動するために使用します。このコマンドを使用するには、電源および再起動アクセス権限を持っている必要があります。

構文:  
reset [-options]

表 14. リセット・オプション

オプション	説明	値
-s	サーバーをリセットする前に、オペレーティング・システムをシャットダウンします。	
-d	リセットの実行を、指定した秒数だけ遅らせます。	0 - 120
-nmi	サーバー上でマスク不可能割り込み (NMI) を生成します。	

## fuelg コマンド

このコマンドは、サーバーの電源についての情報を表示します。

**fuelg** コマンドは、サーバーの電力使用量に関する情報を表示し、サーバーの電源管理を構成します。このコマンドは、電源の冗長性を失った場合のポリシーも構成します。

構文:  
fuelg [-options]

表 15. fuelg オプション

オプション	説明	値
-pme	サーバー上の電源管理および電源キャッピングを有効または無効にします。	on、off
-pcapmode	サーバーの電源キャッピング・モードを設定します。	output、input
-pcap	ターゲット上でオプションを指定せずに fuelg コマンドを実行すると表示される電源キャッピング値の範囲内の数値。	ワット数の数値
-history	電力消費量またはパフォーマンス履歴を表示します。	pc、perf
-period	履歴を表示する数値。	1、6、12、24 時間
-pm	冗長電源を失った場合のポリシー・モードを設定します。	<ul style="list-style-type: none"><li>• <b>bt</b>- スロットルあり基本</li><li>• <b>rt</b>- スロットルあり冗長 (デフォルト)</li></ul>
-zm	ゼロ出力モードを有効または無効にします。この設定は、ポリシー・モードが「スロットルあり冗長」に設定されている場合にのみ設定できます。	on、off
-perf	現在のコンピューティング使用率 (システム、プロセッサ、メモリー・モジュール、I/O など) を表示します。	
-pc	現在の電力消費量を表示します	<ul style="list-style-type: none"><li>• <b>output</b>- システム、プロセッサ、メモリー・モジュール、およびその他のコンポーネントの現在の出力電力消費量を表示します。</li><li>• <b>input</b> - システムの電力消費を含む、現在の入力電力消費量を表示します。</li></ul>

表 15. fuelg オプション (続き)

オプション	説明	値
		注：AMD サーバーの場合、現在の出力電力消費量では一部のコンポーネントが表示されません。

## pxeboot コマンド

このコマンドは、Preboot eXecution Environment の状態を表示および設定します。

構文:

pxeboot [-options]

表 16. pxeboot オプション

オプション	説明	値
-en	次回のシステム再起動の際の Preboot eXecution Environment の状態を設定します。	enabled、disabled

## 構成コマンド

このトピックでは、構成 CLI コマンドのアルファベット順リストを説明します。

構成コマンドは、現在 41 あります。

## accseccfg コマンド

アカウント・セキュリティ設定を表示および構成するには、このコマンドを使用します。

構文:

accseccfg [-options]

表 17. accseccfg オプション

オプション	説明	値
-am	ユーザー認証方式を設定します。	local、ldap、localldap、ldaplocal
-lp	ログイン失敗が最大回数に達した後のロックアウト期間 (分)。	0 ~ 2880、0 = ロックアウトの期限切れなし
-pe	パスワード有効期限の期間 (日)。	0 ~ 365、0 = 期限切れなし
-pew	パスワード失効の警告期間 注：パスワード失効の警告期間は、パスワード有効期限の期間より短くする必要があります。	0 ~ 30、0 = 警告なし
-pc	パスワードの複雑性の規則が有効です。	on、off
-pl	パスワードの長さ。	パスワードの複雑性の規則が有効になっている場合、パスワードの長さは 8 から 32 の範囲です。そうでない場合は、0 から 32 の範囲です。

表 17. accseccfg オプション (続き)

オプション	説明	値
-ci	最短パスワード変更期間 (時間)。	0 ~ 240、0 = 直ちに変更
-lf	最大ログイン失敗数。	0 ~ 10、0 = ロックしない
-chgnew	初回ログイン後の新規ユーザー・パスワードの変更。	on、off
-rc	パスワード再利用サイクル。	0 ~ 10、0 = 直ちに再使用
-wt	Web およびセキュア・シェルの非アクティブ・セッションのタイムアウト (分)。	0 ~ 1440

例:

```
system> accseccfg
-am: local
-lp: 60
-pe: none
-pew: 0
-pc: on
-pl: 10
-ci: 0
-lf: 5
-chgnew: on
-rc: 5
-wt: 20
system>
```

## asu コマンド

このコマンドは、UEFI 設定の構成に使用されます。

詳細設定ユーティリティー・コマンド (ASU) は、UEFI 設定を構成するために使用します。UEFI 設定の変更を有効にするには、ホスト・システムをリブートする必要があります。

構文:

```
asu [subset_command]
```

表 18. ASU サブセット・コマンド

コマンド	説明	値
help	1 つ以上の設定のヘルプ情報を表示するには、このコマンドを使用します。	setting_name
set	設定の値を変更するには、このコマンドを使用します。UEFI 設定を、入力された値に設定します。 注： <ul style="list-style-type: none"> <li>設定/値のペアを 1 つ以上設定します。</li> <li>設定には、単一文字に展開されるワイルドカードを含めることができます。</li> <li>値は、スペースを含む場合は引用符で囲む必要があります。</li> <li>順序リストの値は、等号(=)で区切ります。例: set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network"</li> </ul>	setting_name=value

表 18. ASU サブセット・コマンド (続き)

コマンド	説明	値
show	1つ以上の設定の現行値を表示するには、このコマンドを使用します。	setting_name
showvalues	1つ以上の設定について、指定できるすべての値を表示するには、このコマンドを使用します。 注： <ul style="list-style-type: none"> <li>このコマンドは、その設定の許容値に関する情報を表示します。</li> <li>その設定に許容されるインスタンス数の最小値と最大値が表示されます。</li> <li>デフォルト値があれば、それも表示されます。</li> <li>デフォルト値は、開く不等号括弧と閉じる不等号括弧 (&lt;と&gt;) で囲まれます。</li> <li>テキスト値では、最小と最大の長さ、および正規表現が表示されます。</li> </ul>	setting_name
showgroups	選択可能な設定グループを表示するには、このコマンドを使用します。このコマンドは、既知のグループの名前を表示します。グループ名は、取り付けられたデバイスによって異なる場合があります。	
注： <ul style="list-style-type: none"> <li>コマンド構文の中で、<b>setting_name</b> は表示または変更する設定の名前を示し、<b>value</b> は設定に指定する値を示しています。</li> <li><b>setting_name</b> は複数の名前にすることができます (<b>set</b> コマンドを使用する場合は除く)。</li> <li><b>setting_name</b> には、アスタリスク (*) や疑問符 (?) などのワイルドカードを含めることができます。</li> <li><b>setting_name</b> には、グループ、設定名、または <b>all</b> を指定できます。</li> </ul>		

例:

- asu コマンドのすべてのオプションを表示するには、`asu help` と入力します。
- あるコマンドのヘルプを表示するには、「`asu help setting_name`」を入力します。
- 値を変更するには、「`asu set setting_name=value`」を入力します。
- 現行値を表示するには、「`asu show setting_name`」を入力します。
- 設定で指定できるすべての値を表示するには、「`asu showvalues setting_name`」を入力します。show values コマンドの例:  

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```
- 使用可能な設定グループを表示するには、「`asu showgroups`」を入力します。

次の表は、オプションの引数を示しています。

表 19. asu オプション

次の表は、オプション、オプションの説明、そのオプションに該当する値で構成される複数行 3 列の表です。

表 19. asu オプション (続き)

オプション	説明	値
-b	バッチ形式で表示します。	
-help <sup>1</sup>	コマンドの使用法とオプションを表示します。-help オプションは、たとえば <b>asu -help show</b> のように、コマンドの前に置きます。	
-l	長形式の設定名 (構成セットを含む)。	
-m	混合形式の設定名 (構成 ID を使用)。	
-v <sup>2</sup>	詳細な出力。	
1. -help オプションは、すべてのコマンドに使用できます。 2. -v オプションは、 <b>asu</b> とコマンドの間にだけ使用します。		

構文:

**asu** [-options] command [cmdopts]

options:

- v verbose output
- help display main help

cmdopts:

- help help for the command

注：他のコマンド・オプションについては、個々のコマンドの項を参照してください。

asu トランザクション・コマンドは、複数の UEFI 設定を設定し、バッチ・モード・コマンドを作成および実行するために使用します。**tropen** コマンドおよび **trset** コマンドは、適用する複数の設定が入っている トランザクション・ファイルを作成するために使用します。所定の ID を持つ トランザクションは、**tropen** コマンドを使用してオープンします。設定は、**trset** コマンドを使用して設定されます。完了した トランザクションは、**trcommit** コマンドを使用してコミットされます。トランザクションを終了したら、**trrm** コマンドで トランザクションを削除できます。

注：UEFI 設定の復元操作では、ランダムな 3 桁の数値を使用した ID を持つ トランザクションが作成されます。

次の表には、**asu** コマンドと一緒に使用できる トランザクション・コマンドが記載されています。

表 20. asu トランザクション・コマンド

次の表は、トランザクション・コマンド、コマンドの説明、そのコマンドに該当する値で構成される複数行 3 列の表です。

コマンド	説明	値
<b>tropen id</b>	このコマンドは、設定するいくつかの設定が入っている新規 トランザクション・ファイルを作成します。	<b>Id</b> は識別文字列で、1 文字から 3 文字の英数字です。
<b>trset id</b>	このコマンドは、1 つ以上の設定と値のペアを トランザクションに追加します。	<b>Id</b> は識別文字列で、1 文字から 3 文字の英数字です。
<b>trlist id</b>	このコマンドは、トランザクション・ファイルの内容を最初に表示します。これは、トランザクション・ファイルが CLI シェルで作成される場合に便利です。	<b>Id</b> は識別文字列で、1 文字から 3 文字の英数字です。



表 20. asu トランザクション・コマンド (続き)

コマンド	説明	値
trcommit id	このコマンドは、トランザクション・ファイルの内容をコミットおよび実行します。実行の結果とエラー (ある場合) が表示されます。	Id は識別ストリングで、1 文字から 3 文字の英数字です。
trrm id	このコマンドは、コミットが済んだトランザクション・ファイルを削除します。	Id は識別ストリングで、1 文字から 3 文字の英数字です。

複数の UEFI 設定を確立する例:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

## backup コマンド

システム・セキュリティーの現行設定を含むバックアップ・ファイルを作成するには、このコマンドを使用します。

構文:

```
backup [-options]
```

表 21. バックアップ・オプション

オプション	説明	値
-f	バックアップ・ファイルのファイル名	有効なファイル名
-pp	バックアップ・ファイルの内部でパスワードを暗号化するのに使用するパスワードまたは引用符で区切られたパスフレーズ	有効なパスワードまたは引用符で区切られたパスフレーズ
-ip	TFTP/SFTP サーバーの IP アドレス	有効な IP アドレス
-pn	TFTP/SFTP サーバーのポート番号	有効なポート番号 (デフォルト 69/22)
-u	SFTP サーバーのユーザー名	有効なユーザー名
-pw	SFTP サーバーのパスワード	有効なパスワード
-fd	バックアップ CLI コマンドの XML 記述のためのファイル名	有効なファイル名

例:

```
system> backup -f xcc-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

## dhcpcfg コマンド

DHCP サーバーに割り当てられた eth0 の IP 構成を表示するには、このコマンドを使用します。

**dhcpcfg** コマンドは、インターフェースが DHCP サーバーによって自動的に構成される場合に、DHCP サーバーが eth0 に割り当てた IP 構成を表示するために使用します。**ifconfig** コマンドを使用して、DHCP を有効または無効にすることができます。

構文:

```
dhcpcfg [ethernet_number]
```

例:

```
dhcpcfg eth1
```

次の表は、上記の例からの出力を説明したものです。

表 22. dhcpcfg の出力

フィールド	説明
-server	この構成を割り当てた DHCP サーバー
-n	割り当てられたホスト名
-i	割り当てられた IPv4 アドレス
-i6	割り当てられた IPv6 アドレス
-g	割り当てられたゲートウェイ・アドレス
-s	割り当てられたサブネット・マスク
-d	割り当てられた IPv4 ドメイン名
-d6	割り当てられた IPv6 ドメイン名
-dns1	1 次 IPv4 DNS サーバーの IP アドレス
-dns2	2 次 IPv4 DNS の IP アドレス
-dns3	3 次 IPv4 DNS サーバーの IP アドレス
-i6	IPv6 アドレス
-d6	IPv6 ドメイン名
-dns61	1 次 IPv6 DNS サーバーの IP アドレス
-dns62	2 次 IPv6 DNS の IP アドレス
-dns63	3 次 IPv6 DNS サーバーの IP アドレス

## dns コマンド

IMM の DNS 構成を表示および設定するには、このコマンドを使用します。

構文:

```
dns [-options]
```

表 23. dns オプション

オプション	説明	値
-state	DNS の状態	on、off
-i1	1 次 IPv4 DNS サーバーの IP アドレス	IP アドレス (小数点付き 10 進数形式)

表 23. dns オプション (続き)

オプション	説明	値
-i2	2次 IPv4 DNS の IP アドレス	IP アドレス (小数点付き 10 進数形式)
-i3	3次 IPv4 DNS サーバーの IP アドレス	IP アドレス (小数点付き 10 進数形式)
-i61	1次 IPv6 DNS サーバーの IP アドレス	IP アドレス (IPv6 形式)
-i62	2次 IPv6 DNS の IP アドレス	IP アドレス (IPv6 形式)
-i63	3次 IPv6 DNS サーバーの IP アドレス	IP アドレス (IPv6 形式)
-ddns	DDNS の状態	enabled、disabled
-dnsrc	優先 DDNS ドメイン名	DHCP、手動
-ddn	手動で指定した DDN	
-ddncur	現在の DDN (読み取り専用)	
-p	優先 DNS サーバー (ipv4、ipv6)	ipv4、ipv6
-dscvry	LXCA アドレスの検出	enabled、disabled
-dsclist	DNS SRV の LXCA リスト	
-dscxm	XClarity Manager の構成	

以下の例では、DNS が無効にされた場合の IMM 構成を示しています。

```
system> dns
  -state : disabled
  -i1    : 0.0.0.0
  -i2    : 0.0.0.0
  -i3    : 0.0.0.0
  -i61   : ::
  -i62   : ::
  -i63   : ::
  -ddns  : enabled
  -dnsrc : DHCP
  -ddn   :
  -ddncur : labs.lenovo.com
  -p     : ipv6
  -dscvry : enabled
system>
```

## encaps コマンド

BMC に encapsulation モードを終了させるには、このコマンドを使用します。

構文:

```
encaps [arguments]
```

表 24. encaps 引数

引数	説明
lite off	BMC が encapsulation モードを終了し、すべてのユーザーにグローバル・アクセスを開きます

## ethtousb コマンド

**ethtousb** コマンドは、イーサネットから Ethernet-over-USB ポートへのマッピングを表示および構成するのに使用します。

このコマンドを使用すると、外部イーサネット・ポート番号を Ethernet-over-USB の異なるポート番号にマップすることができます。

構文:

```
ethtousb [-options]
```

表 25. *ethtousb* コマンド

オプション	説明	値
-en	Ethernet-over-USB の状態。	enabled、disabled 注：Ethernet over USB インターフェースを <usbeth> を介して有効にし、ポート・マッピングを有効にします。
-m[x] port1:port2	インデックス <b>x</b> のポート・マッピングを構成します。	ここで、それぞれ以下の意味があります。 <ul style="list-style-type: none"><li>• ポートのインデックス番号 <b>x</b> は、コマンド・オプションで 1 から 10 の整数として指定されます。</li><li>• ポート・ペアの <b>port1</b> は、外部イーサネットのポート番号です。</li><li>• ポート・ペアの <b>port2</b> は、Ethernet-over-USB のポート番号です。</li></ul>
-rm map_index	指定されたインデックスのポート・マッピングを削除します。	ポートのインデックス番号 <b>map_index</b> は、コマンド・オプションで 1 から 10 までの整数として指定します。 注：ポート・マップのインデックスは、オプションを指定せずに <b>ethtousb</b> コマンドを使用すると表示されます。

例:

```
system> ethtousb -en enabled -m1 100:200 -m2 101:201
system> ethtousb
  ethtousb : On
  =====
  1: 100: 200
  2: 101: 201
system>
```

## firewall コマンド

特定のアドレスからのアクセスを制限し、オプションでアクセス・タイム・フレームを制限するようにファイアウォールを構成するには、このコマンドを使用します。オプションを指定しない場合は、現在の設定が表示されます。

構文:

```
firewall [-options]
```

表 26. firewall オプション

オプション	説明	値
次のオプションは、IP アドレスのホワイトリスト用です		
-wips	ホワイトリストの IP アドレスを表示/設定します。	<p>&lt;有効な IP アドレス&gt;, clr</p> <ul style="list-style-type: none"> <li>有効な IP アドレス: 1 から 3 個の IP アドレスを許可します (コンマ区切り、CIDR または範囲)</li> </ul> <p>注: IPv4 および IPv6 アドレスは CIDR 形式を使用してアドレスの範囲をブロックできます。</p> <ul style="list-style-type: none"> <li>-clr: ホワイトリストをクリアします</li> </ul>
次のオプションは、ブロック・リストと時間制限用です		
-bips	1 ~ 3 個の IP アドレスをブロック (コンマ区切り、CIDR または範囲)	<p>有効な IP アドレス</p> <p>注: IPv4 および IPv6 アドレスは CIDR 形式を使用してアドレスの範囲をブロックできます。</p>
-bmacs	1 ~ 3 個の MAC アドレスをブロックする (コンマ区切り)	<p>有効な MAC アドレス</p> <p>注: MAC アドレス・フィルタリングは、特定のアドレスでのみ機能します。</p>
-bbt	ブロック開始時刻、現在時刻より後である必要があります	<YYYY-MM-DD HH:MM> 形式の時刻
-bet	ブロック終了時刻、開始時刻より後である必要があります	<YYYY-MM-DD HH:MM> 形式の時刻
-bti	1 ~ 3 つの時間間隔をブロックする (コンマ区切り)	<HH:MM-HH:MM> 形式の時間範囲
	たとえば、 <code>firewall -bti 01:00-02:00,05:05-10:30</code> は、01:00 ~ 02:00 および 05:05 ~ 10:30 の間、アクセスを毎日ブロックします。	
-clr	指定したタイプのファイアウォール規則をクリアする	ip, mac, datetime, interval, all
IP アドレスのブロックについては、以下のオプションがあります		
-iplp	IP アドレスのロックアウト期間 (分)。	0 から 2880 の間の数値。0 = 無期限
-iplf	IP アドレスがロックアウトされるまでの最大ログイン失敗数。	0 から 32 の間の数値。0 = ロックしない 注: この値が 0 ではない場合は、<accseccfg -lf> で設定された <最大ログイン失敗数> 以上である必要があります
-ipbl	ロックアウトされている IP アドレスのリストを表示または構成します。	<p>del, clrall, show</p> <ul style="list-style-type: none"> <li>-del: IPv4 または IPv6 アドレスをブロック・リストから削除します。</li> <li>-clrall: ブロック中のすべての IP をクリアします。</li> <li>-show: ブロック中のすべての IP を表示します。</li> </ul>

firewall コマンドの構文の例を、次のリストに示します。

- すべてのオプションの値と IP アドレスのブロック・リストを表示するには、「firewall」を入力します。
- 複数の IP からのアクセスをブロックするには、「firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5」を入力します。
- 毎日 01:00-02:00、05:05-10:30、14:15-20:00 の間にすべてのアクセスをブロックするには、「firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00」を入力します。
- ブロック・リストと時間制限のすべてのルールをクリアするには、「firewall -clr all」を入力します。
- IP アドレスのロックアウト期間を 60 分に設定するには、「firewall -iplp 60」を入力します。
- ログイン失敗の最大回数を 5 回に設定するには、「firewall -iplf 5」を入力します。
- IP アドレスのブロック・リストから 192.168.100.1 を削除するには、「firewall -ipbl -del 192.168.100.1」を入力します。
- IP アドレスのブロック・リストから 3fcc:1234::2 を削除するには、「firewall -ipbl -del 3fcc:1234::2」を入力します。
- ブロックしているすべての IP アドレスを削除するには、「firewall -ipbl -clral」を入力します。
- ブロックしているすべての IP アドレスを表示するには、「firewall -ipbl -show」を入力します。

## hashpw コマンド

このコマンドを `-sw` オプションとともに使用して、サード・パーティーのパスワード機能を有効または無効にするか、または `-re` オプションとともに使用して、サード・パーティーのパスワードの取得許可を有効または無効にします。

構文:

hashpw [-options]

表 27. hashpw オプション

オプション	説明	値
-sw	サード・パーティー・パスワードのスイッチ・ステータス	enabled、disabled
-re	サード・パーティー・パスワードの読み取りステータス  注：スイッチが有効になっている場合は、読み取りを設定できます。	enabled、disabled

例:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafef771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f - r Administrator
system> users -5 ghp
ef92b778bafef771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account  Login ID  Advanced Attribute  Role  Password Expires
-----  -
1        USERID   Native              Administrator  Password doesn't expire
5        guest5    Third-party Password Administrator  90 day(s)
```

## ifconfig コマンド

イーサネット・インターフェースを構成するには、このコマンドを使用します。

`ifconfig` コマンドを使用して、現在のイーサネット・インターフェース構成を表示します。イーサネット・インターフェース構成を変更するには、オプションと、それに続けて値を入力します。インター

フェース構成を変更するには、少なくとも「アダプター・ネットワークおよびセキュリティー構成」の権限を持っている必要があります。

構文:

```
ifconfig [ethernet_number] [-options]
```

例:

```
dhcpcinfo eth1 -b
```

表 28. ifconfig オプション

オプション	説明	値
-state	インターフェースの状態	disabled、enabled
-c	構成方式	dhcp、static、dthens (dthens は、Web インターフェースの <b>try dhcp server, if it fails use static config</b> オプションに対応します。)
-ghn	DHCP からホスト名を取得する	disabled、enabled
-i	静的 IP アドレス	有効な形式のアドレス。
-g	ゲートウェイ・アドレス	有効な形式のアドレス。
-s	サブネット・マスク	有効な形式のアドレス。
-n	ホスト名	63 文字以内のストリング。このストリングには、英字、数字、ピリオド、アンダースコア、およびハイフンを含めることができます。
-auto	データ転送速度および二重ネットワークの設定が構成可能かどうかを決定する、自動ネゴシエーションの設定	true、false
-vlan	VLAN タグ付けを有効または無効にする	enabled、disabled
-vlanid	VLAN ID	1 から 4094 までの数値。
-r	Data rate	10, 100, 1000
-d	二重モード	フル、ハーフ
-m	MTU	60 から 1500 までの数値。
-l	LAA	MAC アドレス・フォーマット。マルチキャスト・アドレスは許容されません(最初のバイトは偶数である必要があります)。
-b	組み込み MAC アドレス (読み取り専用)	
-dn	ドメイン名 (読み取り専用)	
-ipv6	IPv6 の状態	disabled、enabled
-ipv6static	静的 IPv6 の状態	disabled、enabled
-i6	静的 IP アドレス	イーサネット・チャンネル 0 の静的 IP アドレス (IPv6 形式)
-p6	アドレスのプレフィックスの長さ	1 から 128 までの数値。
-g6	ゲートウェイまたはデフォルト経路	イーサネット・チャンネル 0 のゲートウェイまたはデフォルト経路の IP アドレス (IPv6)。
-dhcp6	IPv6 DHCP モード	enabled、disabled

表 28. ifconfig オプション (続き)

オプション	説明	値
-sa6	IPv6 ステートレス・モード	enabled、disabled
-lla	リンクローカル・アドレス (読み取り専用)	
-ncsi	NCSI NIC ポートの選択	nic[x]:port[y] 注：設定が2つ以上ある場合は、区切り文字としてコンマを使用します。
-nic	スイッチ NIC モード <sup>1</sup>	shared、dedicated、shared:nic[x] <sup>2</sup>
-failover <sup>2</sup>	フェイルオーバー・モード	none、shared、shared:nic[x]
-nssync <sup>3</sup>	ネットワーク設定の同期	enabled、disabled
-address_table	自動生成された IPv6 アドレスとそのプレフィックス長の表 (読み取り専用) 注：このオプションは、IPv6 およびステートレス自動構成が有効な場合にのみ表示されます。	

注：

- nic は nic のステータスも示します。[active] は、現在どの nic XCC が使用されているかを示します。  
例：  
-nic: shared:nic3  
nic1: dedicate  
nic2: ext card slot #3  
nic3: ext card slot 5 [active]  
nic3 は共有モードでスロット 5 に存在し、nic2 はスロット 3 に存在し、nic1 は XCC 専用ポートであり、XCC は nic3 を使用していることを示します。
- shared:nic[x] 値は、オプションのメザニン・ネットワーク・カードを取り付けてあるサーバー上で使用できません。IMM は、このメザニン・ネットワーク・カードを使用できません。
- IMM が専用の管理ネットワーク・ポートを使用するように構成されている場合、-failover オプションは、専用ポートが切断された場合に共用ネットワーク・ポートに切り替えるよう IMM に指示します。
- フェイルオーバー・モードが有効の場合、-nssync オプションは、専用の管理ネットワーク・ポートで 사용되는のと同じネットワーク設定を共用ネットワーク・ポートに使用するよう IMM に指示します。

例：

```
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

## keycfg コマンド

アクティベーション・キーを表示、追加、または削除するには、このコマンドを使用します。

アクティベーション・キーは、IMM のオプション機能へのアクセスを制御します。

注：

- ファイル転送を介して新規アクティベーション・キーを追加します。
- キーの番号またはキーのタイプを指定して、古いキーを削除します。タイプ別にキーを削除する場合、指定されたタイプの最初のキーが削除されます。

構文：

```
keycfg [-options]
```



表 29. keycfg オプション

オプション	説明	値
-add	アクティベーション・キーの追加	ip、pn、u、pw、f <ul style="list-style-type: none"> <li>• <b>-ip</b>: 追加するアクティベーションキーを持つ TFTP/SFTP サーバーの IP アドレス</li> <li>• <b>-pn</b>: 追加するアクティベーションキーを持つ TFTP/SFTP サーバーのポート番号 (デフォルトは 69/22)</li> <li>• <b>-u</b>: 追加するアクティベーション・キーがある SFTP サーバーのユーザー名</li> <li>• <b>-pw</b>: 追加するアクティベーション・キーを持つ SFTP サーバーのパスワード</li> <li>• <b>-f</b>: 追加するアクティベーション・キーのファイル名</li> </ul>
-del	インデックス番号によるアクティベーション・キーの削除	keycfg リストにある、有効なアクティベーション・キーのインデックス番号
-deltype	キー・タイプによるアクティベーション・キーの削除	有効なキー・タイプの値

オプションを指定せずに **keycfg** コマンドを実行すると、インストールされているアクティベーション・キーのリストが表示されます。表示されるキーの情報には、各アクティベーション・キーのインデックス番号、アクティベーション・キーのタイプ、キーが有効になる日付、残りの使用回数、キーの状況、およびキーの説明などがあります。

例:

```
system> keycfg
ID Type Valid      Uses      Status  Description
1  4  10/10/2010    5        "valid"  "IMM remote presence"
2  3  10/20/2010    2        "valid"  "IMM feature"
3  32796 NO CONSTRAINTS NO CONSTRAINTS "valid"  "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

注：ID 番号 3 の「説明」フィールドは、スペース上の制約により、別の行に表示されます。

## ldap コマンド

LDAP プロトコル構成パラメーターを表示および構成するには、このコマンドを使用します。

構文:

```
ldap [-options]
```

表 30. ldap オプション

オプション	説明	値
-aom	Active Directory ユーザーの認証専用モード	enabled、disabled
-a	ユーザー認証方式	<ul style="list-style-type: none"> <li>• <b>loc</b>: ローカルのみ</li> <li>• <b>ldap</b>: LDAP のみ</li> <li>• <b>locl</b>: 最初にローカル、次に LDAP</li> <li>• <b>ldloc</b>: 最初に LDAP、次にローカル</li> </ul>

表 30. ldap オプション (続き)

オプション	説明	値
-b	バイインディング方式	<ul style="list-style-type: none"> <li>• anon: 匿名</li> <li>• client: ClientDN とパスワードを使用したバインド</li> <li>• login: ログイン資格情報を使用したバインド</li> </ul>
-c	クライアント識別名	client_dn の最大 127 文字のストリング
-d	検索ドメイン	search_domain の最大 63 文字のストリング
-fn	フォレスト名	Active Directory 環境用。127 文字以内のストリング。
-f	グループ・フィルター	group_filter の最大 127 文字のストリング
-g	グループ検索属性	group_search_attr の最大 63 文字のストリング
-l	ログイン許可属性	string の最大 63 文字のストリング
-p	クライアント・パスワード	client_pw の最大 15 文字のストリング
-pc	クライアント・パスワードの確認	confirm_pw の最大 15 文字のストリング コマンドの使用方法: ldap -p client_pw -pc confirm_pw  このオプションは、クライアント・パスワードを変更する場合に必要です。このオプションは confirm_pw 引数と client_pw 引数を比較します。引数が一致しない場合、コマンドは失敗します。
-r	root エントリー識別名 (DN)	root_dn の最大 127 文字のストリング
-s1ip	サーバー 1 のホスト名/IP アドレス	host name/ip_addr の最大 127 文字のストリングまたは IP アドレス
-s2ip	サーバー 2 のホスト名/IP アドレス	host name/ip_addr の最大 127 文字のストリングまたは IP アドレス
-s3ip	サーバー 3 のホスト名/IP アドレス	host name/ip_addr の最大 127 文字のストリングまたは IP アドレス
-s4ip	サーバー 4 のホスト名/IP アドレス	host name/ip_addr の最大 127 文字のストリングまたは IP アドレス
-s1pn	サーバー 1 のポート番号	port_number の最大 5 桁のポート番号
-s2pn	サーバー 2 のポート番号	port_number の最大 5 桁のポート番号
-s3pn	サーバー 3 のポート番号	port_number の最大 5 桁のポート番号
-s4pn	サーバー 4 のポート番号	port_number の最大 5 桁のポート番号
-u	ユーザーのログイン名検索属性	search_attr の最大 63 文字のストリング
-v	DNS を使用した LDAP サーバー・アドレスの取得	off、on
-h	コマンドの使用方法およびオプションの表示	

例:  
 system> ldap  
 -aom enable

```

-a loclld
-b client
-c cn=admin,dc=lenovo,dc=com
-d
-fn
-f example.com
-g cn
-l XCC3RBSPermissions
-r
-s1ip 10.241.99.94
-s2ip
-s3ip
-s4ip
-s1pn 389
-s2pn 389
-s3pn 389
-s4pn 389
-u uid
-v off
system>

```

## ntp コマンド

Network Time Protocol (NTP) を表示および構成するには、このコマンドを使用します。

構文:

```
ntp [-options]
```

表 31. ntp コマンド

オプション	説明	値
-en	Network Time Protocol を有効または無効にします。	enabled、disabled
-i[x]	インデックス x の Network Time Protocol サーバーの名前または IP アドレス。	クロック同期には NTP サーバーの名前を使用しません。NTP サーバーのインデックス番号の範囲は、-i1 から -i4 までです。 注：-i は i1 と同じです。
-f	IMM クロックを Network Time Protocol サーバーと同期する頻度 (分単位)。	3 から 1440 分
-synch	Network Time Protocol サーバーとの即時同期の要求。	このパラメーターには値を使用しません。

例:

```

system> ntp
-en: disabled
-f: 3 minutes
-i: not set

```

## portcontrol コマンド

ネットワーク・サービス・ポートをオンまたはオフにするには、このコマンドを使用します。

構文:

```
portcontrol [-options]
```

表 32. portcontrol オプション

オプション	説明	値
-ipmi	LAN 経由の IPMI アクセスを有効または無効にする	on、off
-ipmi-kcs	サーバーからの ipmi アクセスをオンデマンドで有効、有効、または無効にする	auto、on、off
-rest	REST ディスカバリーを有効または無効にする	on、off
-snmp	SNMP ディスカバリーを有効または無効にする	on、off
-ssdp	SSDP ディスカバリーを有効または無効にする	on、off
-cli	CLI ディスカバリーを有効または無効にする	on、off
-web	WEB ディスカバリーを有効または無効にする	on、off
-all	すべてのインターフェースおよび検出プロトコルを有効または無効に設定する	on、off

例:

```
system> portcontrol
ipmi : on
ipmi-kcs : on
rest : on
snmp : off
ssdp : on
cli : on
web : on
system>
```

## ports コマンド

IMM ポートを表示および構成するには、このコマンドを使用します。

構文:

```
ports [-options]
```

表 33. ports オプション

オプション	説明	値
-open	開いているポートの表示 (読み取り専用)	
-reset	ポートをデフォルト設定にリセット (読み取り専用)	
-http	HTTP ポート番号	デフォルトのポート番号: 80
-https	HTTPS ポート番号	デフォルトのポート番号: 443
-ssh	SSH のレガシー CLI ポート番号	デフォルトのポート番号: 22
-snmpa	SNMP エージェントのポート番号	デフォルトのポート番号: 161

表 33. ports オプション (続き)

オプション	説明	値
-snmpt	SNMP トラップのポート番号	デフォルトのポート番号: 162
-rp	リモート・プレゼンスのポート番号	デフォルトのポート番号: 3900

例:

```
system> ports
  -http 80
  -https 443
  -rp 3900
  -snmpa 161
  -snmpt 162
  -ssh 22
system>
```

## rdmount コマンド

リモート・ディスク・イメージまたはネットワーク共有をマウントするには、このコマンドを使用します。

注:

- 2つまでのファイルを XClarity Controller メモリーにアップロードして、XClarity Controller RDOC 機能を使用して仮想メディアとしてマウントできます。両方のファイルの合計サイズが 50 MB を超えてはなりません。-rw オプションを使用しない限り、アップロードされたイメージは読み取り専用です。
- イメージをマウントまたはマップするために HTTP、SFTP、または FTP プロトコルを使用する場合、すべてのイメージの合計サイズが 50 MB を超えないことが必要です。NFS または SAMBA プロトコルを使用する場合、サイズに制限はありません。

構文:

```
rdmount [-options]
```

表 34. rdmount オプション

オプション	説明
-r	rdoc 操作 (使用時には、最初のオプションであることが必要です) -r -map: RDOC イメージをマウントします  -r -unmap<filename>: マウントされた RDOC イメージをアンマウントします  -r -maplist: XClarity Controller Web ブラウザーおよび CLI インターフェースによりマウントされた RDOC イメージを表示します
-map	-t <samba nfs http sftp ftp> ファイル・システム・タイプ  -ro 読み取り専用  -rw read-write  -u ユーザー  -p password  -l ファイル・ロケーション (URL 形式)

表 34. rdmount オプション (続き)

オプション	説明
	-o オプション (Samba および NFS マウント用の追加オプション・ 文字列)  -d ドメイン (Samba マウント用ドメイン)
-maplist	マップされたイメージを表示します
-unmap	<id fname> は id とネットワーク・イメージ、ファイル名と rdoc を 使用します
-mount	マップされたイメージをマウントします
-unmount	マウントされたイメージをアンマウントします

## restore コマンド

バックアップ・ファイルからシステム設定を復元するには、このコマンドを使用します。

構文:

```
restore [-options]
```

表 35. restore オプション

オプション	説明	値
-f	バックアップ・ファイル名	有効なファイル名
-pp	バックアップ・ファイルの内部でパ スワードを暗号化するのに使用する パスワードまたはパスフレーズ	有効なパスワードまたは引用符で区切られたパスフレーズ
-ip	TFTP/SFTP サーバーの IP アドレス	有効な IP アドレス
-pn	TFTP/SFTP サーバーのポート番号	有効なポート番号 (デフォルト 69/22)
-u	SFTP サーバーのユーザー名	有効なユーザー名
-pw	SFTP サーバーのパスワード	有効なパスワード

例:

```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

## roles コマンド

役割を表示または構成するには、このコマンドを使用します。

構文:

```
roles role_account[3-31] [-options]
```

表 36. roles オプション

オプション	説明	値
-n	役割名	32 文字に制限される
-p	特権の設定	custom:am、rca、rcvma、pr、cel、bc、nsc、ac、us <ul style="list-style-type: none"> <li>• am: ユーザー・アカウント管理アクセス</li> <li>• rca: リモート・コンソール・アクセス</li> <li>• rcvma: リモート・コンソールおよびリモート・ディスク (仮想メディア) アクセス</li> <li>• pr: リモート・サーバー電源/再起動アクセス</li> <li>• cel: イベント・ログを消去する機能</li> <li>• bc: アダプター構成 (基本)</li> <li>• nsc: アダプター構成 (ネットワークおよびセキュリティ)</li> <li>• ac: アダプター構成 (拡張)</li> <li>• us: UEFI セキュリティー</li> </ul> 注: 上記のカスタム許可フラグは、どの組み合わせでも使用できます
-d	行を削除する	

例:

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok
```

```
system> roles
```

Account	Role	Privilege	Assigned To
0	Administrator	all	USERID
1	ReadOnly	none	
2	Operator	custom:pr cel bc nsc	
3	test1	custom:am rca rcvma	

## rtd コマンド

BMC のすべての設定を出荷時のデフォルト値に復元するには、このコマンドを使用します。

注: このコマンドは、以前は `restoredefaults` および `clearcfg` コマンドでした。

構文:

```
rtd [-options]
```

表 37. rtd オプション

オプション	説明
-all	すべての BMC 設定を出荷時のデフォルトにリセットします。
-eu	ユーザー設定を除くすべての BMC 設定を出荷時のデフォルトにリセットします

表 37. rtd オプション (続き)

オプション	説明
-en	ネットワーク設定を除くすべての BMC 設定を出荷時のデフォルトにリセットします。
-eun	ユーザー設定とネットワーク設定を除くすべての BMC 設定を出荷時のデフォルトにリセットします。

例:

```
system> rtd -all
```

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result. You will need to reconfigure the IMM network interface to restore connectivity. After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)

Y

Restoring defaults

## seccfg コマンド

ファームウェアのロールバックを実行するには、このコマンドを使用します。

構文:

```
seccfg [-options]
```

表 38. seccfg オプション

オプション	説明	値
-fwrb	ファームウェアを以前のバージョンにロールバックすることを許可します。	enabled、disabled
-aubp	バックアップからプライマリーへの自動プロモーション機能を有効または無効にします。	enabled、disabled

## securityinfo コマンド

このコマンドは、セキュリティー関連の情報を表示するために使用されます。

構文:

```
securityinfo [-options]
```

表 39. securityinfo オプション

オプション	説明
-event	セキュリティー・イベントを表示します。
-cryptomode	セキュリティー暗号モードのステータスを表示します。
-service	サービスとポートのセキュリティー・ステータスを表示します。
-cert	証明書のセキュリティー・ステータスを表示します。
-account	ユーザー・アカウントのセキュリティー・ステータスを表示します。



## securitymode コマンド

このコマンドは、新規サービス・データ・ファイルを生成するために使用します。

構文:

```
securitymode [-options]
```

表 40. securitymode オプション

オプション	説明	値
-mode	セキュリティー・モードを選択します。 <ul style="list-style-type: none"><li>• CNSA - エンタープライズ・ストリクト</li><li>• FIPS - 標準</li><li>• COMPAT- 互換性</li></ul>	CNSA、FIPS、COMPAT <ul style="list-style-type: none"><li>• <b>CNSA</b>: エンタープライズ・ストリクト・レベルの暗号化をサポートするサービスのみが許可されます。Feature on Demand キーを有効にする必要があります。</li><li>• <b>FIPS</b>: 標準レベルの暗号化をサポートしない暗号化を必要とするサービスは、デフォルトでは無効になっています。</li><li>• <b>COMPAT</b>: このモードが有効な場合、XCC は標準検証済みモードで動作しません。すべてのサービスを有効にすることができます。</li></ul>
-h	使用法とオプションを一覧表示します。	

## set コマンド

IMM の一部の設定を変更するには、このコマンドを使用します。

- 一部の IMM 設定は、シンプルな **set** コマンドを使用して変更できます。
- このような一部の設定 (環境変数など) は、CLI によって使用されます。

次の表は、オプションの引数を示しています。

表 41. set コマンド

次の表は、このコマンドの説明と関連情報で構成される 1 行 3 列の表です。

オプション	説明	値
値	指定されたパスまたは設定の値を設定	指定されたパスまたは設定の適切な値。

構文:

```
set [-options]
option:
  value
```

## snmp コマンド

SNMP インターフェースの情報を表示および構成するには、このコマンドを使用します。

構文:

```
snmp [-options]
```

表 42. snmp オプション

オプション	説明	値
-a3	SNMPv3 エージェント	on、off 注：SNMPv3 エージェントを有効にするには、次の基準を満たす必要があります。 <ul style="list-style-type: none"> <li>• IMM の連絡先が、-cn コマンド・オプションを使用して指定されている。</li> <li>• IMM のロケーションが、-l コマンド・オプションを使用して指定されている。</li> </ul>
-t	SNMPv3 トラップ	on、off
-tn	SNMPv3 トラップのユーザー名	有効なユーザー名
-tauth	SNMPv3 トラップ認証プロトコル	none、HMAC-SHA
-tapw	SNMPv3 トラップ認証パスワード	有効なパスワード
-tpriv	SNMPv3 トラップのプライバシー・プロトコル	none、CBC-DES、AES
-tppw	SNMPv3 トラップのプライバシー・パスワード	有効なパスワード
-tix	コミュニティ IP アドレスまたはホスト名 x	有効な IP アドレスまたはホスト名 (63 文字に制限、x は 1 から 3 までの範囲)。 注： <ul style="list-style-type: none"> <li>• IP アドレスまたはホスト名に含めることができるのは、ドット、アンダースコア、負符号 (-)、文字、および数字です。組み込みスペースまたは連続したピリオドは許可されません。</li> <li>• 引数を指定しないと、コミュニティの IP アドレスまたはホスト名がクリアされます。</li> </ul>
-l	IMM ロケーション	ストリング (47 文字の制限)。 注： <ul style="list-style-type: none"> <li>• スペースが含まれている引き数は引用符で囲む必要があります。引き数の先頭または末尾にスペースは使用できません。</li> <li>• 引数を指定しないか、引数として空ストリングを指定 (" " など) すると、IMM のロケーションがクリアされます。</li> </ul>
-cn	IMM の連絡先名	ストリング (47 文字の制限)。 注： <ul style="list-style-type: none"> <li>• スペースが含まれている引き数は引用符で囲む必要があります。引き数の先頭または末尾にスペースは使用できません。</li> <li>• 引数を指定しないか、引数として空ストリングを指定 (" " など) すると、IMM の連絡先名がクリアされます。</li> </ul>
-tl	SNMPv1 トラップ	on、off
-c	SNMP コミュニティ名	ストリング (15 文字の制限)。 注： <ul style="list-style-type: none"> <li>• スペースが含まれている引き数は引用符で囲む必要があります。引き数の先頭または末尾にスペースは使用できません。</li> <li>• 引数を指定しないか、引数として空ストリングを指定 (" " など) すると、SNMP コミュニティ名がクリアされます。</li> </ul>

表 42. snmp オプション (続き)

オプション	説明	値
-ci	コミュニティの IP アドレス/ホスト名 1	有効な IP アドレスまたはホスト名 (63 文字の制限)。 注： <ul style="list-style-type: none"> <li>IP アドレスまたはホスト名に含めることができるのは、ドット、アンダースコア、負符号 (-)、文字、および数字です。組み込みスペースまたは連続したピリオドは許可されません。</li> <li>引数を指定しないと、コミュニティの IP アドレスまたはホスト名がクリアされます。</li> </ul>
-cliy	コミュニティの IP アドレス/ホスト名 y	有効な IP アドレスまたはホスト名 (63 文字に制限、y は 2 または 3 の範囲)。 注： <ul style="list-style-type: none"> <li>IP アドレスまたはホスト名に含めることができるのは、ドット、アンダースコア、負符号 (-)、文字、および数字です。組み込みスペースまたは連続したピリオドは許可されません。</li> <li>引数を指定しないと、コミュニティの IP アドレスまたはホスト名がクリアされます。</li> </ul>
-t2	SNMPv2 トラップ	on、off
-ct	SNMPv2 トラップのコミュニティ名	ストリング (15 文字の制限)。 注： <ul style="list-style-type: none"> <li>スペースが含まれている引き数は引用符で囲む必要があります。引き数の先頭または末尾にスペースは使用できません。</li> <li>引数を指定しないか、引数として空ストリングを指定 (「」など) すると、IMM の連絡先名がクリアされます。</li> </ul>
-cti	SNMPv2 トラップのコミュニティ IP アドレス/ホスト名 1	有効な IP アドレスまたはホスト名 (63 文字の制限)。 注： <ul style="list-style-type: none"> <li>IP アドレスまたはホスト名に含めることができるのは、ドット、アンダースコア、負符号 (-)、文字、および数字です。組み込みスペースまたは連続したピリオドは許可されません。</li> <li>引数を指定しないと、SNMP コミュニティの IP アドレスまたはホスト名がクリアされます。</li> </ul>
-eid	SNMP エンジン ID	ストリング (1 から 27 文字の制限)
-send	テスト・トラップ情報の送信	

例:

```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

## snmpalerts コマンド

SNMP 経由で送信されるアラートを管理するには、このコマンドを使用します。

構文:

snmpalerts [-options]

表 43. snmpalerts オプション

オプション	説明	値
-status	SNMP アラートの状況	on、off
-crt	アラートを送信するクリティカル・イベントを設定	all、none、custom:te vo po di fa cp me in re ot pc カスタムのクリティカル・アラート設定は、値をパイプで区切られたリストにして、 <b>snmpalerts -crt custom:te vo</b> の形式で指定します。ここで、カスタム値は以下のとおりです。 <ul style="list-style-type: none"> <li>te: クリティカルな温度しきい値超過</li> <li>vo: クリティカルな電圧しきい値超過</li> <li>po: クリティカルな電源障害</li> <li>di: ハードディスク・ドライブ障害</li> <li>fa: ファン障害</li> <li>cp: マイクロプロセッサ障害</li> <li>me: メモリー障害</li> <li>in: ハードウェアの互換性なし</li> <li>re: 電源の冗長性の障害</li> <li>ot: その他すべてのクリティカル・イベント</li> <li>pc: PCIe クリティカル・イベント</li> </ul>
-wrn	アラートを送信する警告イベントを設定	all、none、custom:rp te vo po fa cp me ot pw カスタムの警告アラート設定は、値をパイプで区切られたリストにして、 <b>snmpalerts -wrn custom:rp te</b> の形式で指定します。ここで、カスタム値は以下のとおりです。 <ul style="list-style-type: none"> <li>rp: 電源の冗長性の警告</li> <li>te: 警告の温度しきい値超過</li> <li>vo: 警告の電圧しきい値超過</li> <li>po: 警告の電力しきい値超過</li> <li>fa: クリティカルではないファン・イベント</li> <li>cp: マイクロプロセッサが機能低下状態</li> <li>me: メモリーの警告</li> <li>ot: その他すべての警告イベント</li> <li>pw: PCIe 警告イベント</li> </ul>
-sys	アラートを送信するルーチン・イベントを設定	all、none、custom:lo tio ot po bf til pf el ne nl dh oa カスタムのルーチン・アラート設定は、値をパイプで区切られたリストにして、 <b>snmpalerts -sys custom:lo tio</b> の形式で指定します。ここで、カスタム値は以下のとおりです。 <ul style="list-style-type: none"> <li>lo: 正常なりモード・ログイン</li> <li>tio: オペレーティング・システムのタイムアウト</li> <li>ot: その他すべての通知イベントおよびシステム・イベント</li> <li>po: システムの電源オン/オフ</li> <li>bf: オペレーティング・システムのブート障害</li> </ul>

表 43. *snmpalerts* オプション (続き)

オプション	説明	値
		<ul style="list-style-type: none"> <li>オペレーティング・システム・ローダーのウォッチドッグ・タイムアウト</li> <li>pf: 予知された障害 (PFA)</li> <li>el: イベント・ログ 75% フル</li> <li>ne: ネットワーク変更</li> <li>nl: ホスト NIC リンクのダウン/アップ</li> <li>dh: ドライブ・ホットプラグ</li> <li>oa: その他すべての監査イベント</li> </ul>

## ssshcfg コマンド

SSH パラメーターを表示および構成するには、このコマンドを使用します。

構文:

ssshcfg [-options]

表 44. *ssshcfg* オプション

オプション	説明	値
-cstatus	SSH CLI の状態	enabled、disabled
-hk	サーバー・キー	gen、all <ul style="list-style-type: none"> <li><b>gen</b>: SSH サーバーの秘密鍵を生成</li> <li><b>all</b>: サーバーの公開鍵を表示</li> </ul>

例:

```
system> ssshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

## sslcfg コマンド

IMM の SSL を表示および構成し、証明書を管理するには、このコマンドを使用します。

sslcfg コマンドは、新規の暗号鍵と自己署名証明書、または証明書署名要求 (CSR) を生成するために使用します。

構文:

sslcfg [-options]

表 45. *sslcfg* オプション

オプション	説明	値
-server	Web over HTTPS のステータス	enabled、disabled 注： <ul style="list-style-type: none"> <li>Web over HTTPS は、証明書が設定されている場合にのみ有効にできます。</li> <li>証明書を完全に無効にするには、<b>-rm</b> を使用します。</li> </ul>
-client	セキュア LDAP ステータス	enabled、disabled 注：SSL クライアントは、有効なサーバーまたはクライアントの証明書が提供されている場合にのみ有効にすることができます。
-cert	自己署名証明書の生成	server、client、sysdir、storekey 注： <ul style="list-style-type: none"> <li>自己署名証明書を生成する際には、<b>-c</b>、<b>-sp</b>、<b>-cl</b>、<b>-on</b>、および <b>-hn</b> コマンド・オプションの値は必須です。</li> <li>自己署名証明書を生成する際には、<b>-cp</b>、<b>-ea</b>、<b>-ou</b>、<b>-s</b>、<b>-gn</b>、<b>-in</b>、および <b>-dq</b> コマンド・オプションの値はオプションです。</li> </ul>
-csr	CSR の生成	server、client、sysdir、storekey 注： <ul style="list-style-type: none"> <li>CSR を生成する際には、<b>-c</b>、<b>-sp</b>、<b>-cl</b>、<b>-on</b>、および <b>-hn</b> コマンド・オプションの値は必須です。</li> <li>CSR を生成する際には、<b>-cp</b>、<b>-ea</b>、<b>-ou</b>、<b>-s</b>、<b>-gn</b>、<b>-in</b>、<b>-dq</b>、<b>-cpwd</b>、および <b>-un</b> コマンド・オプションの値はオプションです。</li> </ul>
-form	エクスポートされる CSR または証明書の形式。	der、pem (デフォルト pem)
-algo	CSR アルゴリズム	p256、p384、rsa2048、rsa3072、rsa4096 注：-algo オプションがない場合、デフォルト値 (p256) が設定されます。
-rm	証明書の削除	server、storekey 注：デフォルトの自己署名証明書 (サーバー) は、現在の証明書が削除された後に自動的に生成されます。
-i	TFTP/SFTP サーバーの IP アドレス	有効な IP アドレス 注：証明書のアップロード、または証明書あるいは CSR のダウンロードの際には、TFTP または SFTP サーバーの IP アドレスを指定する必要があります。
-pn	TFTP/SFTP サーバーのポート番号	有効なポート番号 (デフォルト 69/22)
-u	SFTP サーバーのユーザー名	有効なユーザー名
-pw	SFTP サーバーのパスワード	有効なパスワード
-l	証明書ファイル名	有効なファイル名 注：証明書または CSR をダウンロードあるいはアップロードする際には、ファイル名は必須です。ダウンロードを行う場合にファイル名が指定されないと、ファイルのデフォルト名が使用され、表示されます。
-dnld	リモート・ホストへの指定したファイルのエクスポート	このオプションでは引数を使用せず、 <b>-cert</b> または <b>-csr</b> と、 <b>-i</b> および <b>-l</b> コマンド・オプションとともに使用する必要があります。
-upld	証明書ファイルのインポート	このオプションには引数を使用しませんが、 <b>-cert</b> 、 <b>-i</b> 、および <b>-l</b> コマンド・オプションは指定する必要があります。

表 45. sslcfg オプション (続き)

オプション	説明	値
-tcx	SSL クライアントのトラステッド証明書 x	import、download、remove 注：トラステッド証明書の番号 x は、コマンド・オプションで 1 から 4 の整数として指定されます。
自己署名証明書または CSR を生成するために必要なオプション 注：自己署名証明書または CSR を生成する際には必須です。		
-c	国	国別コード (2 文字)
-sp	都道府県/州	引用符で区切ったストリング (最大 60 文字)
-cl	市区町村または地方	引用符で区切ったストリング (最大 50 文字)
-on	組織名	引用符で区切ったストリング (最大 60 文字)
-hn	BMC ホスト名	ストリング (最大 60 文字)
自己署名証明書または CSR を生成するための任意のオプション 注：自己署名証明書または CSR を生成する際にはオプションです。		
-cp	連絡先担当者	引用符で区切ったストリング (最大 60 文字)
-ea	連絡先担当者のメール・アドレス	有効なメール・アドレス (最大 60 文字)
-ou	組織単位	引用符で区切ったストリング (最大 60 文字)
-s	姓	引用符で区切ったストリング (最大 60 文字)
-gn	名	引用符で区切ったストリング (最大 60 文字)
-in	イニシャル	引用符で区切ったストリング (最大 20 文字)
-dq	ドメイン名の修飾子	引用符で区切ったストリング (最大 60 文字)
CSR を生成するための任意のオプション 注：CSR を生成する際にはオプションです。		
-cpwd	チャレンジ・パスワード	ストリング (最小 6 文字、最大 30 文字)
-un	非構造化名	引用符で区切ったストリング (最大 60 文字)

例:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
A self-signed certificate is installed
SSL Client Certificate status:
A self-signed certificate is installed
SSL Client Trusted Certificate status:
Trusted Certificate 1: Not available
Trusted Certificate 2: Not available
Trusted Certificate 3: Not available
Trusted Certificate 4: Not available
```

クライアント証明書の例:

- ストレージ・キー用の CSR を生成するには、次のコマンドを入力します。

```
system> sslcfg -csr storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou ""
ok
```

- IMM から別のサーバーに証明書をダウンロードするには、次のコマンドを入力します:

```
system> sslcfg -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
ok
```

- 証明機関 (CA) によって処理された証明書をアップロードするには、次のコマンドを入力します。

```
system> sslcfg -cert storekey -upld -i 192.168.70.230 -l tkkm.der
```

- 自己署名証明書を生成するには、次のコマンドを入力します。

```
system> sslcfg -cert storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou ""
ok
```

SKLM サーバー証明書の例:

- SKLM サーバー証明書をインポートするには、次のコマンドを入力します。

```
system> storekeycfg -add -ip 192.168.70.200 -f tkkm-server.der
ok
```

## syslock コマンド

このコマンドを使用して、システム・ロックダウン設定を表示および構成します。

構文:

```
syslock [-options]
```

表 46. syslock オプション

オプション	説明	値
-en	システム構成ロック機能を有効または無効にします。 注: -e オプションを指定して有効にすると、現在のインベントリーをトラステッド・スナップショットとしてプロモートできます。	enabled、disabled
-e	システム構成のロック設定を、現在のインベントリーをトラステッド・スナップショットに強制するかどうかを指定して有効にします。 注: -e オプションがない場合、デフォルト値が設定されます。	enabled、disabled
-l [x]	インデックス x にある特定のスナップショットのインベントリーをリストします。	インデックス番号 x は、コマンド・オプションで整数として指定します。
-m	手動スナップショットを作成します。	
-d	手動スナップショットの説明。	32 文字以内のストリング。
-c	トラステッド・スナップショットとのインベントリーの相違点をリストします。	



表 46. syslock オプション (続き)

オプション	説明	値
-po	ロックダウン・ポリシーを設定します。 注：このアクションにより、システム・ガードが非準拠ステータスの場合にサーバーがブートできなくなります。	none、osboot、pperm
-cpu	cpu ロックダウンを設定します。	on、off
-dimm	dimm ロックダウンを設定します。	on、off
-pci	pci ロックダウンを設定します。	on、off
-drive	drive ロックダウンを設定します。	on、off
-riser	riser ロックダウンを設定します。	on、off
-bp	bp ロックダウンを設定します。	on、off

## thermal コマンド

ホスト・システムのサーマル・モード・ポリシーを表示および構成するには、このコマンドを使用します。

オプションを指定せずに **thermal** コマンドを実行すると、サーマル・モード・ポリシーが表示されます。次の表は、オプションの引数を示しています。

構文:

thermal [-options]

表 47. thermal オプション

オプション	説明	値
-mode	温度モード・ポリシーの表示およびホスト・システムの温度テーブルの構成 (読み取り専用)	<ul style="list-style-type: none"> <li>• 一般コンピューティング - 電力効率</li> <li>• 一般コンピューティング - ピーク周波数</li> <li>• 一般コンピューティング - 最大パフォーマンス</li> <li>• 仮想化 - 電力効率</li> <li>• 仮想化 - 最大パフォーマンス</li> <li>• データベース - トランザクション処理</li> <li>• 低遅延</li> <li>• 高パフォーマンス・コンピューティング</li> <li>• カスタム</li> <li>• 不明</li> </ul>
-table table_number	table_number は、使用する代替温度テーブルを指定します。	<p>1 = 低: ファン速度がわずかに上昇</p> <p>2 = 中: ファン速度がある程度上昇</p> <p>3 = 高: ファン速度が大きく上昇</p> <p>0 = 正常: ファン速度の上昇なし</p>

例:

```
system> thermal
```

```
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

## tls コマンド

TLS の最小レベルを設定するには、このコマンドを使用します。

構文:  
tls [-options]

表 48. tls オプション

オプション	説明	値
-min	TLS の最小レベルを選択します。	1.2, 1.3 注：暗号化モードを「NIST-800-131A Compliance Mode」に設定する場合は、TLS バージョンを 1.2 に設定する必要があります。
-h	使用方法およびオプションをリストします。	

注：

1. 暗号化モードを「NIST-800-131A Compliance Mode」に設定する場合は、TLS バージョンを 1.2 に設定する必要があります。

例:

tls コマンドの使用法を表示するには、次のコマンドを発行します。

```
system> tls
-h
system>
```

現在の tls バージョンを表示するには、次のコマンドを発行します。

```
system> tls
-min 1.2
system>
```

現在の tls バージョンを 1.2 に変更するには、次のコマンドを発行します。

```
system> tls -min 1.2
ok
system>
```

## trespass コマンド

侵入警告メッセージを構成および表示するには、このコマンドを使用します。

**trespass** コマンドを使用して、侵入警告メッセージを構成および表示することができます。侵入警告メッセージは、WEB または CLI インターフェースを使用してログインしているすべてのユーザーに表示されます。

構文:  
trespass [-options]

表 49. *trespass* オプション

オプション	説明
-s	侵入警告メッセージの構成
-h	使用方法およびオプションのリスト

例:

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage
system>
system> trespass -s "testing message"
ok
system> trespass
testing message
system>
```

## uefipw コマンド

UEFI 管理パスワードを構成するには、このコマンドを使用します。パスワードは書き込み専用です。

**Uefipw** コマンドを「-p」オプションと一緒に使用して、XCC の UEFI 管理パスワードを構成したり、「-ep」オプションと一緒に使用して、LXCA の UEFI 管理パスワードを CLI インターフェースによって構成したりできます。パスワードは書き込み専用です。

構文:

```
uefipw [-options]
```

表 50. *uefipw* オプション

オプション	説明
-cp	現在のパスワード (20 文字に制限)
-p	新しいパスワード (20 文字に制限)

## usbeth コマンド

インバンド LAN over USB インターフェースを有効または無効にするには、このコマンドを使用します。

注:

- OS IP 構成設定は、Ethernet Over USB インターフェースの OS IP アドレスの設定には使用されず、Ethernet over USB の OS IP アドレスが変更されたことを BMC に通知するために使用されます。
- Ethernet over USB の 3 つの IP 設定を構成する前に、ローカル・オペレーティング・システムで Ethernet over USB インターフェースの OS IP アドレスを手動で構成する必要があります。

構文:

```
usbeth [-options]
```

表 51. *usbeth* オプション

オプション	説明	値
-en	インバンド (Ethernet over USB) インターフェースを有効または無効にします。	enabled、disabled
-am	アドレス・モードとして IPv4 または IPv6 LLA を選択します。	ipv4、ipv6lla
注：-ip、-sn、および -ipos オプションは、-am ipv4 モードが選択されている場合にのみ有効です		
-ip	BMC の Ethernet over USB インターフェースの IP アドレス。	有効な IP アドレス
-sn	BMC の Ethernet over USB インターフェース・サブネット・マスク。	有効な IP アドレス
-ipos	OS の Ethernet over USB インターフェースの IP アドレス。	有効な IP アドレス

例:

```
system> usbeth
-en : disabled
system> usbeth -en enabled
ok
system> usbeth
-en : disabled
system>
```

## users コマンド

すべてのユーザー・アカウントとその権限レベルにアクセスするには、このコマンドを使用します。

また、**users** コマンドは、新規ユーザー・アカウントの作成、および既存のアカウントの変更を行うためにも使用します。オプションを指定せずに **users** コマンドを実行すると、ユーザーと、ユーザーの一部の基本情報のリストが表示されます。

構文:

```
users [-user_index] [-options]
```

表 52. *users* オプション

オプション	説明	値
-user_index	ユーザー・アカウントのインデックス番号。	ここで <b>user_index</b> は 1 ~ 12、またはすべてのユーザーの場合は <b>all</b> です。
-l	パスワードの有効期限の日数を表示	
-n	ユーザー・アカウント名	数字、文字、ピリオド、およびアンダースコアのみを含む固有の文字列。最小で 4 文字、最大で 16 文字です。
-p	ユーザー・アカウントのパスワード	少なくとも 1 文字の英字と 1 文字の英字以外の文字を含む文字列。最小で 6 文字、最大で 255 文字です。NULL は、初回ログイン時にユーザーが設定する必要がある、パスワードなしのアカウントを作成します。
-shp	ハッシュ・パスワードの設定	合計 64 文字
-ssalt	salt の設定	64 文字に制限されます

表 52. users オプション (続き)

オプション	説明	値
-ghp	ハッシュパスワードを取得	
-gsalt	salt を取得	
-ep	暗号化パスワード (バックアップ/復元用)	有効なパスワード
-esalt	暗号化されたパスワードの salt	バックアップまたは復元のみ
-r	役割名	管理者、オペレーター、読み取り専用。120 ページの「roles コマンド」コマンドに記載の通り。
-clear	指定されたユーザー・アカウントの削除	削除するユーザー・アカウントのインデックス番号を、以下の形式で指定する必要があります。 <code>users -clear -user_index</code> 注：許可されている場合は、現在ログインしている自分のアカウントまたは他のユーザーのアカウントであっても削除できます。ただし、ユーザー・アカウント管理権限を持つアカウントが他に残っている場合に限りです。ユーザー・アカウントが削除されたときに既に進行しているセッションは、自動的に終了されません。
-curr	現在ログイン中のユーザーの表示	
-ai	ユーザー・アクセス可能インターフェース	web, ssh, redfish, ipmi, snmp, all 注：デフォルト値 (web ssh redfish) は、-ai オプションがない場合に設定されます。
-sauth	SNMPv3 認証プロトコル	None, HMAC_MD5, HMAC_SHA96, HMAC128_SHA224, HMAC192_SHA256, HMAC256_SHA384, HMAC384_SHA512
-spriv	SNMPv3 プライバシー・プロトコル	None, CBC_DES, CFB128_AES128, AES192, AES256, AES192C, AES256C
-spw	SNMPv3 プライバシー・パスワード	有効なパスワード
-sepw	SNMPv3 プライバシー・パスワード (暗号化)	有効なパスワード
-sacc	SNMPv3 アクセス・タイプ	get
-strap1	SNMPv3 トラップ・ホスト名 1	有効なホスト名
-strap2	SNMPv3 トラップ・ホスト名 2	有効なホスト名
-strap3	SNMPv3 トラップ・ホスト名 3	有効なホスト名
-pk	ユーザーの SSH 公開鍵の表示	ユーザー・アカウントのインデックス番号。 注： <ul style="list-style-type: none"> <li>該当するユーザーに割り当てられている各 SSH 鍵が、識別するための鍵のインデックス番号と一緒に表示されます。</li> <li>SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー・インデックス (-userindex オプション) の後に、<code>users -2 -pk</code> の形式で使用する必要があります。</li> <li>すべての鍵は、OpenSSH フォーマットです。</li> </ul>

表 52. users オプション (続き)

オプション	説明	値
以下のオプションは -pk と一緒に使用します		
-e	OpenSSH フォーマットで、 全体の SSH 鍵を表示 (SSH 公開鍵オプション)	このオプションでは引数を使用せず、他のすべての users -pk オプションと同時に使用することはできません。 注：SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー・インデックス (-userindex オプション) の後に、users -2 -pk -e の形式で使用する必要があります。
-remove	SSH 公開鍵のユーザーからの削除 (SSH 公開鍵オプション)	削除する公開鍵のインデックス番号は、該当するユーザーに割り当てられているすべての鍵で、固有の -key_index または -all として指定する必要があります。 注：SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー・インデックス (-userindex オプション) の後に、users -2 -pk -remove -1 の形式で使用する必要があります。
-add	ユーザーの SSH 公開鍵の追加 (SSH 公開鍵オプション)	OpenSSH フォーマットの引用符で区切られた鍵 注： <ul style="list-style-type: none"> <li>-add オプションは、他のすべての users -pk コマンド・オプションと同時に使用することはできません。</li> <li>SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー・インデックス (-userindex オプション) の後に、次の形式で使用する必要があります。users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEAfnTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaNOy400ICEKcKjKEhrYymtAoVtFKApvY39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKHj46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBL3SAAtMucUsTkYjLXcqex10Qz4+N50R6MbNcwlSx+mTEAvvcPjhuga70UNPGhLJML6k7jeJiQ&amp;Xd2p Xb0ZQ=="</li> </ul>
-upld	OpenSSH または RFC4716 形式の SSH 公開鍵のアップロード (SSH 公開鍵オプション)	鍵のロケーションを指定するには、-i および -l オプションが必要です。 注： <ul style="list-style-type: none"> <li>-upld オプションは、他のすべての users -pk コマンド・オプションと同時に使用することはできません (-i および -l を除く)。</li> <li>鍵を新しい鍵と置き換えるには、-key_index を指定する必要があります。現行の鍵のリストの最後に鍵を追加する場合は、鍵のインデックスを指定しないでください。</li> <li>SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー・インデックス (-userindex オプション) の後に、users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key の形式で使用する必要があります。</li> </ul>

表 52. users オプション (続き)

オプション	説明	値
-dnld	指定した SSH 公開鍵を TFTP/SFTP サーバにダウンロード (SSH 公開鍵オプション)	ダウンロードする鍵を指定するには <code>-key_index</code> オプションが必要で、TFTP サーバを稼働している別のコンピュータ上のダウンロード・ロケーションを指定するには <code>-i</code> および <code>-l</code> オプションが必要です。 注： <ul style="list-style-type: none"> <li><code>-dnld</code> オプションは、他のすべての <code>users -pk</code> コマンド・オプションと同時に使用することはできません (<code>-i</code>、<code>-l</code>、および <code>-key_index</code> を除く)。</li> <li>SSH 公開鍵のオプションを使用する場合、<code>-pk</code> オプションはユーザー・インデックス (<code>-userindex</code> オプション) の後に、<code>users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key</code> の形式で使用する必要があります。</li> </ul>
-i	鍵ファイルをアップロードまたはダウンロードするための TFTP/SFTP サーバの IP アドレス (SSH 公開鍵オプション)	有効な IP アドレス 注： <code>-i</code> オプションは、 <code>users -pk -upld</code> および <code>users -pk -dnld</code> コマンド・オプションで必要です。
-pn	TFTP/SFTP サーバのポート番号 (SSH 公開鍵オプション)	有効なポート番号 (デフォルト 69/22) 注： <code>users -pk -upld</code> および <code>users -pk -dnld</code> コマンド・オプションのオプション・パラメーター。
-u	SFTP サーバのユーザー名 (SSH 公開鍵オプション)	有効なユーザー名 注： <code>users -pk -upld</code> および <code>users -pk -dnld</code> コマンド・オプションのオプション・パラメーター。
-pw	SFTP サーバのパスワード (SSH 公開鍵オプション)	有効なパスワード 注： <code>users -pk -upld</code> および <code>users -pk -dnld</code> コマンド・オプションのオプション・パラメーター。
-l	TFTP または SFTP 経由で鍵ファイルをアップロードまたはダウンロードするためのファイル名 (SSH 公開鍵オプション)	有効なファイル名 注： <code>-l</code> オプションは、 <code>users -pk -upld</code> および <code>users -pk -dnld</code> コマンド・オプションで必要です。
-af	ホストからの接続を受け入れる (SSH 公開鍵オプション)	ホスト名および IP アドレスのコンマ区切りリスト (最大で 511 文字)。有効な文字には、英数字、コンマ、アスタリスク、疑問符 (?)、感嘆符、ピリオド、ハイフン、コロン、および % 記号があります。
-cm	コメント (SSH 公開鍵オプション)	最大 255 文字の、引用符で区切ったストリング。 注：SSH 公開鍵のオプションを使用する場合、 <code>-pk</code> オプションはユーザー・インデックス ( <code>-userindex</code> オプション) の後に、 <code>users -2 -pk -cm "This is my comment."</code> の形式で使用する必要があります。

例:

```
system> users
Login ID   Name      Advanced Attribute  Role          Password Expires
-----
1         USERID   Native             Administrator  89 day(s)
system> users -2 -n sptest -p Passw0rd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
Login ID   Name      Advanced Attribute  Role          Password Expires
-----
```

```

1  USERID      Native  Administrator  90 day(s)
2  sptest      Native  Administrator  Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -r Administrator
system> users -5 ghp
292bc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system>

```

---

## IMM 制御コマンド

このトピックでは、IMM 制御 CLI コマンドのアルファベット順リストを説明します。

IMM 制御コマンドは、現在 7 つあります。

### batch コマンド

同一のファイルに含まれている 1 つ以上の CLI コマンドを実行するには、このコマンドを使用します。

注：

- バッチ・ファイルのコメント行は、# で始まります。
- バッチ・ファイルを実行する際、失敗したコマンドは、失敗の戻りコードとともに返されます。
- 認識されないコマンド・オプションを含むバッチ・ファイル・コマンドでは、警告が生成される場合があります。

構文:

```
batch [-options]
```

表 53. バッチ・オプション

オプション	説明	値
-f	バッチ・ファイル名	有効なファイル名
-ip	TFTP/SFTP サーバーの IP アドレス	有効な IP アドレス
-pn	TFTP/SFTP サーバーのポート番号	有効なポート番号 (デフォルト 69/22)
-u	SFTP サーバーのユーザー名	有効なユーザー名
-pw	SFTP サーバーのパスワード	有効なパスワード

例:

```

system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>

```

### clock コマンド

現在の日付と時刻を表示するには、このコマンドを使用します。UTC オフセットおよび夏時間調整の設定値を設定できます。

構文:

```
clock [-options]
```



表 54. 時計オプション

オプション	説明	値
-u	UTC オフセット	+2、-7、-6、-5、-4、および-3のUTC時差では、特殊な夏時間の設定が必要です。 <ul style="list-style-type: none"> <li>• +2の場合、夏時間オプションには、off、ee(東欧)、tky(トルコ)、bei(ペイルート)、amm(アンマン)、jem(エルサレム)があります。</li> <li>• -7の場合、夏時間の設定には、off、mtn(山岳部標準時)、maz(マサトラン)があります。</li> <li>• -6の場合、夏時間の設定には、off、mex(メキシコ)、cna(中央/北アメリカ)があります。</li> <li>• -5の場合、夏時間の設定には、off、cub(キューバ)、ena(アメリカ北東部)があります。</li> <li>• -4の場合、夏時間の設定には、off、asu(アスンシオン)、cui(クイアバ)、san(サンティアゴ)、cat(カナダ-大西洋岸)があります。</li> <li>• -3の場合、夏時間の設定には、off、gtb(ゴットホープ)、bre(ブラジル-東部)があります。</li> </ul>
-dst	夏時間	on、off、special case
-host	ホストから取得した時刻の形式(デフォルト: utc)	ローカル、UTC 注: Windows システムは現地時刻を使用し、Linux は utc を使用します

注:

- BMC はホスト・サーバーまたはNTPサーバーから時刻を取得します。
- ホストから取得した時刻は現地時間であることもUTC時間であることもあります。NTPを使用せずホストがUTC形式を使用している場合、ホスト・オプションをUTCに設定する必要があります。
- UTC時差は、正の時差の場合には+0200、+2:00、+2、または2という形式、負の時差の場合には-0500、-5:00または-5という形式にすることができます。
- UTC時差および夏時間は、NTPを使用する場合またはホスト・モードがUTCの場合に使用されます。

例:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

## info コマンド

BMCに関する情報を表示および構成するには、このコマンドを使用します。

構文:

```
info [-options]
```

表 55. info オプション

オプション	説明	値
-name	BMCの名前	ストリング
-contact	BMCの連絡先担当者の名前	ストリング
-location	BMCのロケーション	ストリング
-postal	BMCの完全な郵便住所	ストリング

表 55. info オプション (続き)

オプション	説明	値
-room	BMC のルーム ID	ストリング
-rack	BMC のラック ID	ストリング
-rup	ラック内での BMC の位置	ストリング

例:

```
system> info
-name: BMCName
-location: location
-contact: contact
-rack: rack
-room: room
-postal: postal
-rup: 1
system>
```

## sreset コマンド

IMM を再起動するには、このコマンドを使用します。

このコマンドを発行するには、少なくとも「拡張アダプター構成」の権限を持っている必要があります。

構文:

```
sreset
```

## エージェントレス・コマンド

このトピックでは、エージェントレス・コマンドのアルファベット順リストを説明します。

エージェントレス・コマンドは、現在 3 つあります。

## storage コマンド

(プラットフォームでサポートされている場合) IMM によって管理されているサーバーのストレージ・デバイスに関する情報を表示および構成するには、このコマンドを使用します。

構文:

```
storage [-options]
```

表 56. storage オプション

オプション	説明	値
-list	IMM によって管理されているストレージ・ターゲットをリストします。	<b>controllers pools volumes drives</b> <ul style="list-style-type: none"> <li>• controllers: サポートされている RAID コントローラーをリストします<sup>1</sup></li> <li>• pools: RAID コントローラーに関連したストレージ・プールをリストします<sup>1</sup></li> <li>• volumes: RAID コントローラーに関連したストレージ・ボリュームをリストします<sup>1</sup></li> </ul>

表 56. storage オプション (続き)

オプション	説明	値
		<ul style="list-style-type: none"> <li>drives: RAID コントローラーに関連したストレージ・ドライブをリストします<sup>1</sup></li> </ul>
-list storage targets -target target_id	IMM によって管理されているストレージ・ターゲットを、target_id に従ってリストします。	<p>pools volumes drives および ctrl[x] pool[x] ここでストレージ・ターゲットおよび target_id は次のとおりです。</p> <ul style="list-style-type: none"> <li>pools および ctrl[x]: target_id に基づいて、RAID コントローラーに関連したストレージ・プールをリストします<sup>1</sup></li> <li>volumes および ctrl[x] pool[x]: target_id に基づいて、RAID コントローラーに関連したストレージ・ボリュームをリストします<sup>1</sup></li> <li>drives および ctrl[x] pool[x]: target_id に基づいて、RAID コントローラーに関連したストレージ・ドライブをリストします<sup>1</sup></li> </ul>
-list devices	IMM によって管理されているすべてのディスクのステータスを表示します。	
-show target_id	IMM によって管理されている選択済みターゲットに関する情報を表示します。	ここで target_id は ctrl[x] vol[x] disk[x] pool[x] です <sup>3</sup>
-show target_id info	IMM によって管理されている選択済みターゲットに関する詳細情報を表示します。	ここで target_id は ctrl[x] vol[x] disk[x] pool[x] です <sup>3</sup>
-show target_id firmware <sup>3</sup>	IMM によって管理されている選択済みターゲットに関するファームウェア情報を表示します。	ここで target_id は ctrl[x] disk[x] です <sup>2</sup>
-showinfo nvme	Nvme ディスクのファームウェア情報を表示します。	
-wthre show	重大および警告の SSD 装着しきい値を表示します。	しきい値 (1 ~ 99)
-wthre -ct しきい値	SSD 装着クリティカルしきい値を設定します。	しきい値 (1 ~ 99)
-wthre -wt しきい値	SSD 装着警告しきい値を設定します。	しきい値 (1 ~ 99) 注: 警告値は、重大値より大きくする必要があります。
-config ctrl -scanforgn -target target_id <sup>3</sup>	外部 RAID 構成を検出します。	ここで target_id は ctrl[x] <sup>5</sup> です
-config ctrl -imptforgn -target target_id <sup>3</sup>	外部 RAID 構成をインポートします。	ここで target_id は ctrl[x] <sup>5</sup> です
-config ctrl -clrforgn -target target_id <sup>3</sup>	外部 RAID 構成をクリアします。	ここで target_id は ctrl[x] <sup>5</sup> です
-config ctrl -clrcfg -target target_id <sup>3</sup>	RAID 構成をクリアします。	ここで target_id は ctrl[x] <sup>5</sup> です
-config ctrl -bootdevice -vd volume -target target_id	ブート・デバイスをボリュームごと設定します。	ここで target_id は ctrl[x] で、volume は "list volumes" 出力の最初の列の値です。

表 56. storage オプション (続き)

オプション	説明	値
-config ctrl -bootdevice -pd drive -target target_id	ドライブごとに起動デバイスを設定します。	ここで target_id は ctrl[x] で、drive は "list drives" 出力の最初の列の値です。
-config ctrl -bootdevice -index index -target target_id	起動デバイスをインデックスで設定します。	ここで target_id は ctrl[x] で、index は "display" オプションの出力である "[]" の値です。
-config ctrl -bootdevice -display -target target_id	起動可能デバイスを表示します。	
-config drv -mkoffline -target target_id <sup>3</sup>	オンラインからオフラインにドライブ状態を変更します。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -mkonline -target target_id <sup>3</sup>	オフラインからオンラインにドライブ状態を変更します。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -mkmissing -target target_id <sup>3</sup>	オフラインのドライブを未構成の正常ドライブとしてマークします。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -prprm -target target_id <sup>3</sup>	未構成の正常ドライブを削除する準備をします。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -undoprprm -target target_id <sup>3</sup>	未構成の正常ドライブの削除操作の準備をキャンセルします。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -mkbad -target target_id <sup>3</sup>	未構成の正常ドライブを未構成の不良ドライブに変更します。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -mkgood -target target_id <sup>3</sup>	未構成の不良ドライブを未構成の正常ドライブに変更します。 または 単なるディスクの集まりドライブを未構成の正常ドライブに変換します。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -mkjbod -target target_id <sup>3</sup>	未構成の正常を単なるディスクの集まりにします。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -rebuild -target target_id <sup>3</sup>	ドライブの再構築を開始します。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -addhsp -target target_id <sup>3</sup>	選択したドライブをホット・スペアとして1つのコントローラーまたは既存のストレージ・プールに割り当てます。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -dedicated pools -target target_id <sup>3</sup>	ドライブを専用ホットスペアとして選択したストレージ・プールに割り当てます。	ここで target_id は disk[x] <sup>5</sup> です
-config drv -rmhsp -target target_id <sup>3</sup>	ホット・スペアを削除します。	ここで target_id は disk[x] <sup>5</sup> です
-config vol -remove -targettarget_id <sup>3</sup>	1つのボリュームを削除します。	ここで target_id は vol[x] <sup>5</sup> です

表 56. storage オプション (続き)

オプション	説明	値
-config vol -set [-N] [-w] [-r ] [-i] [-a] [-d] [-b] -target target_id <sup>5</sup>	1つのボリュームのプロパティを変更します。	<ul style="list-style-type: none"> <li>• [-N volume_name] はボリュームの名前です</li> <li>• [-w &lt;0 1 2 3&gt;] はキャッシュの書き込みポリシーです。                         <ul style="list-style-type: none"> <li>- ライト・スルー・ポリシーの場合は 0 を入力します</li> <li>- 保護されたライト・バック・ポリシーの場合は 1 を入力します</li> <li>- 保護されていないライト・バック・ポリシーの場合は 2 を入力します</li> <li>- ポリシーなしの場合は 3 を入力します</li> </ul> </li> <li>• [-r &lt;0 1&gt;] はキャッシュの読み取りポリシーです。                         <ul style="list-style-type: none"> <li>- 先読みなしポリシーの場合は 0 を入力します</li> <li>- 先読みポリシーの場合は 1 を入力します</li> </ul> </li> <li>• [-i &lt;0 1&gt;] はキャッシュの I/O ポリシーです。                         <ul style="list-style-type: none"> <li>- ダイレクト I/O ポリシーの場合は 0 を入力します</li> <li>- キャッシュ I/O ポリシーの場合は 1 を入力します</li> </ul> </li> <li>• [-a &lt;0 2 3&gt;] はアクセス・ポリシーです。                         <ul style="list-style-type: none"> <li>- 読み取り/書き込みポリシーの場合は 0 を入力します</li> <li>- 読み取り専用ポリシーの場合は 2 を入力します</li> <li>- ブロック・ポリシーの場合は 3 を入力します</li> </ul> </li> <li>• [-d &lt;0 1 2&gt;] はディスクのキャッシュ・ポリシーです。                         <ul style="list-style-type: none"> <li>- ポリシーを変更しない場合は 0 を入力します</li> <li>- ポリシーを有効にするには 1 を入力します<sup>6</sup></li> <li>- ポリシーを無効にするには 2 を入力します</li> </ul> </li> <li>• [-b &lt;0 1&gt;] はバックグラウンドの初期化です。                         <ul style="list-style-type: none"> <li>- 初期化を有効にするには 0 を入力します</li> <li>- 初期化を無効にするには 1 を入力します</li> </ul> </li> <li>• -target_id は vol[x]<sup>5</sup> です</li> </ul>

表 56. storage オプション (続き)

オプション	説明	値
<p>-config vol -add [-R] [-D disk] [-H disk] [-l hole] [-N] [-w] [-r]<sup>3,7</sup></p>	<p>ターゲットがコントローラーの場合、新規ストレージ・プールに対して1つのボリュームを作成します。</p> <p>または</p> <p>ターゲットがストレージ・プールの場合、既存のストレージ・プールで1つのボリュームを作成します。</p>	<ul style="list-style-type: none"> <li>• [-R &lt;0 1 5 1E 6 10 50 60 00&gt;] このオプションは RAID レベルを定義し、新規ストレージ・プールにのみ使用されます</li> <li>• [-D disk [id1]:disk[id2]:..disk[id21]:disk[id22]:..] このオプションは、ドライブ・グループ (スパンを含む) を定義し、新規ストレージ・プールにのみ使用されます</li> <li>• [-H disk [id1]:disk[id2]:..] このオプションは、ホット・スペア・グループを定義し、新規ストレージ・プールにのみ使用されます</li> <li>• [-l hole] このオプションは既存のストレージ・プールの空きホール・スペースのインデックス番号を定義します</li> <li>• [-N volume_name] はボリュームの名前です</li> <li>• [-w &lt;0 1 2 3&gt;] はキャッシュの書き込みポリシーです。 <ul style="list-style-type: none"> <li>- ライト・スルー・ポリシーの場合は <b>0</b> を入力します</li> <li>- 保護されたライト・バック・ポリシーの場合は <b>1</b> を入力します</li> <li>- 保護されていないライト・バック・ポリシーの場合は <b>2</b> を入力します</li> <li>- ポリシーなしの場合は <b>3</b> を入力します</li> </ul> </li> <li>• [-r &lt;0 1&gt;] はキャッシュの読み取りポリシーです。 <ul style="list-style-type: none"> <li>- 先読みなしポリシーの場合は <b>0</b> を入力します</li> <li>- 先読みポリシーの場合は <b>1</b> を入力します</li> </ul> </li> </ul>
<p>-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target target_id<sup>3</sup></p>	<p>ターゲットがコントローラーの場合、新規ストレージ・プールに対して1つのボリュームを作成します。</p> <p>または</p> <p>ターゲットがストレージ・プールの場合、既存のストレージ・プールで1つのボリュームを作成します。</p>	<ul style="list-style-type: none"> <li>• [-i &lt;0 1&gt;] はキャッシュの I/O ポリシーです。 <ul style="list-style-type: none"> <li>- ダイレクト I/O ポリシーの場合は <b>0</b> を入力します</li> <li>- キャッシュ I/O ポリシーの場合は <b>1</b> を入力します</li> </ul> </li> <li>• [-a &lt;0 2 3&gt;] はアクセス・ポリシーです。 <ul style="list-style-type: none"> <li>- 読み取り/書き込みポリシーの場合は <b>0</b> を入力します</li> <li>- 読み取り専用ポリシーの場合は <b>2</b> を入力します</li> <li>- ブロック・ポリシーの場合は <b>3</b> を入力します</li> </ul> </li> <li>• [-d &lt;0 1 2&gt;] はディスクのキャッシュ・ポリシーです。 <ul style="list-style-type: none"> <li>- ポリシーを変更しない場合は <b>0</b> を入力します</li> <li>- ポリシーを有効にするには <b>1</b> を入力します<sup>6</sup></li> <li>- ポリシーを無効にするには <b>2</b> を入力します</li> </ul> </li> <li>• [-f &lt;0 1 2&gt;] は初期化のタイプです。 <ul style="list-style-type: none"> <li>- 初期化なしの場合は <b>0</b> を入力します</li> </ul> </li> </ul>

表 56. storage オプション (続き)

オプション	説明	値
		<ul style="list-style-type: none"> <li>- クイック初期化の場合は 1 を入力します</li> <li>- 完全初期化の場合は 2 を入力します</li> <li>• [-S volume_size] は新規ボリュームのサイズ (MB) です</li> <li>• [-P strip_size] は、ボリュームのストリップ・サイズ (512B、4K、128K、1M など) です</li> <li>• -target target_id は:               <ul style="list-style-type: none"> <li>- ctrl[x] (新規ストレージ・プール)<sup>5</sup></li> <li>- pool[x] (既存のストレージ・プール)<sup>5</sup></li> </ul> </li> </ul>
-config vol -getfreecap [-R] [-D disk] [-H disk] -target target_id <sup>3</sup>	ドライブ・グループの空き容量を取得します。	<ul style="list-style-type: none"> <li>• [-R &lt;0 1 5 1E 6 10 50 60 00&gt;] このオプションは RAID レベルを定義し、新規ストレージ・プールにのみ使用されます</li> <li>• [-D disk [id11]:[id12]:..[id21]:[id22]:...] このオプションは、ドライブ・グループ (スパンを含む) を定義し、新規ストレージ・プールにのみ使用されます</li> <li>• [-H disk [id1]:[id2]:...] このオプションは、ホット・スペア・グループを定義し、新規ストレージ・プールにのみ使用されます</li> <li>• -target target_id is ctrl[x]<sup>5</sup></li> </ul>
-fgi vol[idx]	指定したボリュームを高速初期化する	ここで vol[idx] は vol[id1],vol[id2]:.. です
-help	コマンドの使用法とオプションを表示します。	
<p>注：</p> <ol style="list-style-type: none"> <li>1. このコマンドは、IMM が RAID コントローラーにアクセスできるサーバーでのみサポートされます。</li> <li>2. ファームウェア情報は、関連したコントローラー、ディスク、およびフラッシュ DIMM についてのみ表示されます。関連したプールとボリュームに関するファームウェア情報は表示されません。</li> <li>3. 情報は、スペース上の制約のため、複数の行に表示されます。</li> <li>4. このコマンドは、RAID ログをサポートするサーバーでのみサポートされます。</li> <li>5. このコマンドは、RAID 構成をサポートするサーバーでのみサポートされます。</li> <li>6. <b>Enable</b> 値は RAID レベル 1 構成をサポートしません。</li> <li>7. 使用可能なオプションの一部をここにリストします。storage -config vol -add コマンドの残りのオプションは以下の行にリストされます。</li> </ol>		

例:

```

system> storage -config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage -config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage -config drv -addhsp -dedicated pool[0-1] -target disk[0-0]

```

```

ok
system>
system> storage -config drv -addhsp -target disk[0-0]
ok
system>
system> storage -config drv -mkbad -target disk[0-0]
ok
system>
system> storage -config drv -mkgood -target disk[0-0]
ok
system>
system> storage -config drv -mkmissing -target disk[0-0]
ok
system>
system> storage -config drv -mkoffline -target disk[0-0]
ok
system>
system> storage -config drv -mkonline -target disk[0-0]
ok
system>
system> storage -config drv -prprm -target disk[0-0]
ok
system>
system> storage -config drv -rmhsp -target disk[0-0]
ok
system>
system> storage -config drv -undoprprm -target disk[0-0]
ok
system>
system> storage -config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage -config vol -add -R 1 -D
disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage -config vol -getfreecap -R 1 -D
disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage -config vol -remove -target vol[0-1]
ok
system>
system> storage -config vol -set -N LD_volume
-w 0 -target vol[0-0]
ok
system>
system> storage -list controllers
ctrl[0] ServerRAID M5110e(Slot No. 0)
ctrl[1] ServerRAID M5110f(Slot No. 1)
system>
system> storage -list drives
disk[0-0] Drive 0
disk[0-1] Drive 1
disk[0-2] Drive 2
system>
system> storage -list pools
pool[0-0] Storage Pool 0
pool[0-1] Storage Pool 1
system>

```



```

system> storage -list volumes
vol[0-0] Volume 0
vol[0-1] Volume 1
Vol[0-2] Volume 2
system>
system> storage -list drives -target ctrl[0]
disk[0-0] Drive 0
disk[0-1] Drive 1
disk[0-2] Drive 2
system>
system> storage -list drives -target pool[0-0]
disk[0-0] Drive 0
disk[0-1] Drive 1
system>
system> storage -list pools -target ctrl[0]
pool[0-0] Storage Pool 0
system>
system> storage -list volumes -target ctrl[0]
vol[0-0] Volume 0
vol[0-1] Volume 1
system>
system> storage -list volumes -target pool[0-0]
vol[0-0] Volume 0
vol[0-1] Volume 1
system>
system> storage -show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manufacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage -show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0] Storage Pool 0
pool[0-1] Storage Pool 1
Drives: 3

```

```

disk[0-0] Drive 0
disk[0-1] Drive 1
disk[0-2] Drive 2
system>
system> storage -show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage -show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclosure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage -show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0] Drive 0
disk[0-1] Drive 1
Volumes: 2
vol[0-0] Volume 0
vol[0-1] Volume 1
system>
system> storage -show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1] Drive 1
disk[0-2] Drive 2

Volume: 1
vol[0-1] LD_volume
system>
system> storage -show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>

```

```

system> storage -show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>

```

## adapter コマンド

このコマンドは、PCIe アダプターのインベントリ情報を表示するために使用します。

構文:

```
adapter [-options]
```

表 57. adapter オプション

オプション	説明	値
-list	サーバー内のすべての PCIe アダプターをリストします。	
-show target_id	ターゲット PCIe アダプターの詳細情報を表示します。	<b>target_id [info firmware ports]</b> ここで、それぞれ以下の意味があります。 <ul style="list-style-type: none"> <li>• <b>info</b>: アダプターのハードウェア情報を表示する</li> <li>• <b>firmware</b>: アダプターのすべてのファームウェア情報を表示する</li> <li>• <b>ports</b>: アダプターのすべてのイーサネット・ポート情報を表示する</li> </ul>

**adapter** コマンドがサポートされていない場合、コマンドが発行されると、サーバーは以下のメッセージで応答します。

```
Your platform does not support this command.
```

注：アダプターの取り外し、交換、または構成を行ったときは、サーバーを (少なくとも 1 回) 再起動して、更新されたアダプター情報を表示する必要があります。

例:

```

system> adapter -list
ob-1 Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2 GPU Card 1
slot-1 Raid Controller 1
slot-2 Adapter 01:02:03
system>

system> adapter -show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2
Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949

```

Device Number: 1334  
Function Number: 21  
Vendor Id: 12  
Device Id: 33  
Revision Id: 1  
Class Code: 2  
Sub Vendor: 334  
Sub Device: 223  
Slot Description: a slot  
Slot Type: 23  
Slot Data Bus Width: 0  
Hot Plug: 12  
PCI Type: 11  
Blade Slot Port: xxx  
UUID: 39302938485  
Manufacturer: IBM  
Serial Number: 998AAGG  
Part Number: ADB233  
Model: 345  
Function Sku: 221  
Fod Uid: 2355  
Required Daughter: 0  
Max Data Width: 0  
Connector Layout: pci x  
Package Type: dci  
Function Name: xxx nVidia xx component2  
Segment Number: 2348  
Bus Number: 23949  
Device Number: 1334  
Function Number: 21  
Vendor Id: 12  
Device Id: 33  
Revision Id: 1  
Class Code: 2  
Sub Vendor: 334  
Sub Device: 223  
Slot Description: a slot  
Slot Type: 23  
Slot Data Bus Width: 0  
Hot Plug: 12  
PCI Type: 11  
Blade Slot Port: xxx  
UUID: 39302938485  
Manufacturer: IBM  
Serial Number: 998AAGG  
Part Number: ADB233  
Model: 345  
Function Sku: 221  
Fod Uid: 2355  
Required Daughter: 0  
Max Data Width: 0  
Connector Layout: pci x  
Package Type: dci  
system>

---

## サポート・コマンド

このトピックでは、サポート・コマンドのアルファベット順リストを説明します。

サポート・コマンドは [151 ページ](#) の「[dbgshbmc コマンド](#)」の1つのみです。

## dbgshbmc コマンド

セキュア・デバッグ・シェルへのネットワーク・アクセスをロック解除するには、このコマンドを使用します。

注：このコマンドは、以前は **dbgshimm** コマンドでした。

重要：このコマンドはサポート担当者のみが使用します。

次の表は、オプションの引数を示しています。

構文:

```
dbgshbmc [subset_command]
```

表 58. *dbgshbmc* サブセット・コマンド

オプション	説明
status	ステータスを表示します
enable	デバッグ・アクセスを有効にします (オプションを指定しない場合のデフォルト)
disable	デバッグ・アクセスを無効にします



---

## 第 11 章 IPMI インターフェース

この章では、XClarity Controller によってサポートされる IPMI インターフェースについて説明します。

標準の ipmi コマンドの詳細については、Intelligent Platform Management Interface (ipmi) の仕様書 (バージョン 2.0 以降) を参照してください。この資料では、XClarity Controller のファームウェアでサポートされている標準の IPMI および OEM IPMI コマンドとともに使用される OEM パラメーターについて説明します。

---

### IPMI を使用した XClarity Controller の管理

Intelligent Platform Management Interface (IPMI) を使用して XClarity Controller を管理するには、このトピックの情報を使用します。

XClarity Controller は、ユーザー ID がユーザー名 USERID、パスワード PASSWORD (英字の O でなくゼロ) に初期設定されています。このユーザーには、Supervisor アクセス権限があります。

**重要：**拡張セキュリティーを使用するには、初期構成時にこのユーザー名とパスワードを変更してください。

Flex System では、ユーザーは、XClarity Controller IPMI ユーザー・アカウントを集中管理するように Flex System CMM を構成できます。この環境では、CMM で IPMI ユーザー ID を構成するまでは、IPMI を使用して XClarity Controller にアクセスできない場合があります。

注：CMM で構成されたユーザー ID の資格情報は、上記の USERID/PASSWORD の組み合わせとは異なる場合があります。IPMI ユーザー ID が CMM で構成されていない場合、IPMI プロトコルに関連付けられたネットワーク・ポートは終了します。

XClarity Controller は、以下の IPMI リモート・サーバー管理機能も提供します。

#### IPMI コマンド・ライン・インターフェース

IPMI コマンド・ライン・インターフェースにより、IPMI 2.0 プロトコルを介してサーバー管理機能に直接アクセスできます。IPMITool を使用して、サーバー電源の制御、サーバー情報の表示、およびサーバーの識別を行うためのコマンドを発行することができます。IPMITool の詳細については、[153 ページの「IPMITool の使用」](#)を参照してください。

#### Serial over LAN

リモート・ロケーションからサーバーを管理するには、IPMITool を使用して、Serial over LAN (SOL) 接続を確立します。IPMITool の詳細については、[153 ページの「IPMITool の使用」](#)を参照してください。

---

### IPMITool の使用

IPMITool に関する情報にアクセスするには、このトピックの情報を使用します。

IPMITool は、IPMI システムを管理および構成するのに使用できるさまざまなツールを提供します。IPMITool をインバンドまたはアウト・オブ・バンドで使用して、XClarity Controller を管理および構成できます。

IPMITool の詳細について、あるいは IPMITool をダウンロードするには、<https://github.com/ipmitool/ipmitool> にアクセスしてください。

## OEM パラメーターを使用した IPMI コマンド

### LAN 構成パラメーターの取得 / 設定

一部のネットワーク設定について、XCC によって提供される機能を反映するために、一部のパラメーター・データの値は次に示すように定義されます。

#### DHCP

IP アドレスを取得する通常の方法に加えて、XCC には、指定された期間、DHCP サーバーから IP アドレスを取得することを試みるモードがあり、それが失敗した場合には静的 IP アドレスの使用にフェイルオーバーします。

次の表は、オプション、オプションの説明、そのオプションに該当する値で構成される複数行 3 列の表です。

パラメーター	#	パラメーター・データ
IP アドレスのソース	4	<p><u>データ 1</u></p> <p>[7:4] – 予約済み</p> <p>[3:0] – アドレスのソース</p> <p>0h = 未指定</p> <p>1h = 静的アドレス (手動構成)</p> <p>2h = XCC 実行中の DHCP によるアドレスの取得</p> <p>3h = BIOS またはシステム・ソフトウェアにより取得されたアドレス</p> <p>4h = 他のアドレス割り当てプロトコルを実行している XCC により取得されたアドレス。</p> <p>XCC は、値 4h を使用して、静的にフェイルオーバーする DHCP のアドレス・モードを示します。</p>

#### イーサネット・インターフェースの選択

XCC ハードウェアには、RMII インターフェースを使用したデュアル 10/100 イーサネット MAC が含まれています。XCC ハードウェアには、RGMII インターフェースを使用したデュアル 1Gbps イーサネット MAC も含まれています。いずれかの MAC は、通常共有サーバー NIC に接続されており、もう一方の MAC は専用システム管理ポートとして使用されます。サーバー上のイーサネット・ポートは、一度に 1 つだけアクティブになります。両方のポートを同時に有効にすることはできません。

一部のサーバーでは、システム・デザイナーは、いずれかのイーサネット・インターフェースの 1 つのみをシステム平面上に接続することを選択できます。そのようなシステムでは、平面に接続されているイーサネット・インターフェースのみが XCC でサポートされます。未接続ポートの使用要求には、CCh 完了コードが返されます。

すべてのオプションのネットワーク・カードのパッケージ ID には、次のように番号が付けられています。

- オプションのカード #1、パッケージ ID = 03h (eth2)、
- オプションのカード #2、パッケージ ID = 04h (eth3)、



次の表は、オプション、オプションの説明、そのオプションに該当する値で構成される複数行 3 列の表です。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>このパラメーター番号は、使用可能なイーサネット・ポート(論理パッケージ)のうちのどれを使用すべきかを示すために XCC により使用されます。</p> <p>LAN 構成パラメーターの取得/設定コマンドのこのパラメーターは、セット・セレクターまたはブロック・セレクターを使用していないため、これらのフィールドは 00h に設定する必要があります。</p> <p>応答データは 3 バイトを返します。またはデバイスが NCSI パッケージにある場合は 4 バイトを返します。</p> <p>バイト 1 = 完了コード</p> <p>バイト 2 = リビジョン</p> <p>バイト 3 = eth0 の場合は 00h、eth1 の場合は 01h など。</p> <p>バイト 4 = (オプション) チャネル番号 (デバイスが NCSI パッケージの場合)</p>	C0h	<p><u>data1</u></p> <p>00h = eth0</p> <p>01h = eth1</p> <p>02h = eth2</p> <p>etc...</p> <p>FFh = すべての外部ネットワーク・ポートを無効にする)</p> <p>XCC は、パッケージ内のどのチャネルを使用するかを指定するために、2 番目のオプション・データ・バイトをサポートします</p> <p><u>data2</u></p> <p>00h = チャネル 0</p> <p>01h = チャネル 1</p> <p>etc...</p> <p>要求で data2 が指定されていない場合、チャネル 0 が想定されます</p>

data1 のバイトは、論理パッケージを指定するために使用されます。これは、サーバーと共有される NIC への、専用システム管理 NIC または NCSI インターフェースである場合があります。

data2 のバイトは、パッケージが NCSI デバイスの場合は、論理パッケージのチャネルを指定するために使用されます。要求で data2 が指定されておらず、論理パッケージが NCSI デバイスの場合は、チャネル 0 が想定されます。要求で data2 が指定されているものの、論理パッケージが NCSI デバイスではない場合は、チャネル情報は無視されます。

例:

付録 A. 平面 (パッケージ ID = 0, eth0) 上の共有 NIC のチャネル 2 を管理ポートとして使用する場合、入力データは次のようになります。0xC0 0x00 0x02

付録 B. 最初のネットワーク・メザニン・カードの最初のチャネルを使用する場合、入力データは次のようになります。0xC0 0x02 0x0

### Ethernet Over USB を有効または無効にする

以下のパラメーターは、XCC インバンド・インターフェースを有効または無効にするために使用されます。

次の表は、オプション、オプションの説明、そのオプションに該当する値で構成される複数行 3 列の表です。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>(このパラメーター番号は、Ethernet Over USB インターフェースを有効または無効にするために XCC によって使用されます。)</p> <p>LAN 構成パラメーターの取得/設定コマンドのこのパラメーターは、セット・セレクターまたはブロック・セレクターを使用しないため、これらのフィールドは 00h に設定する必要があります。</p> <p>応答データは 3 バイトを返します。</p> <p>バイト 1 = 完了コード            バイト 2 = リビジョン            バイト 3 = 00h (無効)、または 01h (有効)</p>	C1h	<p>データ 1</p> <p>0x00 = 無効            0x01 = 有効</p>

data1 のバイトは、論理パッケージを指定するために使用されます。これは、サーバーと共有される NIC への、専用システム管理 NIC または NCSI インターフェースである場合があります。

data2 のバイトは、パッケージが NCSI デバイスの場合は、論理パッケージのチャンネルを指定するために使用されます。要求で data2 が指定されておらず、論理パッケージが NCSI デバイスの場合は、チャンネル 0 が想定されます。要求で data2 が指定されているものの、論理パッケージが NCSI デバイスではない場合は、チャンネル情報は無視されます。

例:

付録 A。平面 (パッケージ ID = 0, eth0) 上の共有 NIC のチャンネル 2 を管理ポートとして使用する場合、入力データは次のようになります。0xC0 0x00 0x02

付録 B。最初のネットワーク・メザニン・カードの最初のチャンネルを使用する場合、入力データは次のようになります。0xC0 0x02 0x0

## DUID-LLT を取得するための IPMI オプション

IPMI 経由で保護されていない状態にする必要のある追加の読み取り専用値は、DUID です。RFC3315 によれば、この DUID の形式は、Link Layer Address Plus Time に基づいています。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>(このパラメーター番号は、Ethernet Over USB インターフェースを有効または無効にするために XCC によって使用されます。)</p> <p>LAN 構成パラメーターの取得/設定コマンドのこのパラメーターは、セット・セレクターまたはブロック・セレクターを使用しな</p>	C2h	

パラメーター	#	パラメーター・データ
<p>いため、これらのフィールドは 00h に設定する必要があります。</p> <p>応答データは 3 バイトを返します。</p> <p>    バイト 1 = 完了コード</p> <p>    バイト 2 = パラメーターのリビジョン (IPMI 仕様と同じ)</p> <p>    バイト 3 = 後続のデータ・バイトの長さ (現在は 16 バイト)</p> <p>    バイト 4-n DUID_LL</p>		

### イーサネット構成パラメーター

以下のパラメーターを使用して、特定のイーサネット設定を構成することができます。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>(このパラメーター番号は、イーサネット・インターフェースの自動ネゴシエーション設定を有効または無効にするために XCC によって使用されます。)</p> <p>応答データは 3 バイトを返します。</p> <p>    バイト 1 = 完了コード</p> <p>    バイト 2 = リビジョン</p> <p>    バイト 3 = 00h (無効)、または 01h (有効)</p>	C3h	<p>データ 1</p> <p>0x00 = 無効</p> <p>0x01 = 有効</p> <p>注: Flex および ThinkSystem D2 エンクロージャー (ThinkSystem SD530 計算ノード) システムでは、CMM および SMM を経由するネットワーク通信パスが切断される可能性があるため、オートネゴシエーション設定は変更できません。</p>
<p>OEM パラメーター</p> <p>(このパラメーター番号は、イーサネット・インターフェースのデータ・レートを取得または設定するために XCC によって使用されます。)</p> <p>応答データは 3 バイトを返します。</p> <p>    バイト 1 = 完了コード</p> <p>    バイト 2 = リビジョン</p> <p>    バイト 3 = 00h (10Mb)、または 01h (100Mb)</p>	C4h	<p>データ 1</p> <p>0x00 = 10Mbit</p> <p>0x01 = 100Mbit</p>

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>(このパラメーター番号は、イーサネット・インターフェースの二重化設定を取得または設定するために XCC によって使用されます。)</p> <p>応答データは 3 バイトを返します。</p> <p>バイト 1 = 完了コード            バイト 2 = リビジョン            バイト 3 = 00h (半二重)、または 01h (全二重)</p>	C5h	<p><u>データ 1</u></p> <p>0x00 = 半二重            0x01 = 全二重</p>
<p>OEM パラメーター</p> <p>(このパラメーター番号は、イーサネット・インターフェースの最大転送単位 (MTU) を取得または設定するために XCC によって使用されます。)</p> <p>応答データは 3 バイトを返します。</p> <p>バイト 1 = 完了コード            バイト 2 = リビジョン            バイト 3-4 = MTU のサイズ</p>	C6h	<p><u>データ 1</u></p> <p>MTU のサイズ</p>
<p>OEM パラメーター</p> <p>(このパラメーター番号は、ローカル管理対象 MAC アドレスを取得または設定するために XCC によって使用されます。)</p> <p>応答データは 3 バイトを返します。</p> <p>バイト 1 = 完了コード            バイト 2 = リビジョン            バイト 3-8 = MAC アドレス</p>	C7h	<p><u>データ 1-6</u></p> <p>MAC アドレス</p>

### リンク・ローカル・アドレスを取得するための IPMI オプション

これは、IPV6 リンク・ローカル・アドレスを取得するための読み取り専用のパラメーターです。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>このパラメーターは、XCC のリンク・ローカル・アドレスを取得するために使用されます。</p> <p>応答データは以下を返します。</p> <p>    バイト 1 = 完了コード</p> <p>    バイト 2 = パラメーターのリビジョン (IPMI 仕様と同じ)</p> <p>    バイト 3 = IPV6 アドレスのプレフィックスの長さ</p> <p>    バイナリ形式のバイト 4-19 のローカル・リンク・アドレス</p>	C8h	

### IPv6 を有効/無効にするための IPMI オプション

これは、XCC で IPV6 を有効/無効にする読み取り/書き込みパラメーターです。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>このパラメーターは、XCC で IPv6 を有効/無効にするために使用されます。</p> <p>応答データは以下を返します。</p> <p>    バイト 1 = 完了コード</p> <p>    バイト 2 = パラメーターのリビジョン (IPMI 仕様と同じ)</p> <p>    バイト 3 = 00h (無効)、または 01h (有効)</p>	C9h	<p><u>データ 1</u></p> <p>0x00 = 無効</p> <p>0x01 = 有効</p>

### 外部ネットワークへの Ethernet Over USB パススルー

以下のパラメーターは、外部イーサネット・パススルーへの Ethernet-over-USB を構成するために使用されます。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>LAN 構成パラメーターの取得/設定コマンドのこのパラメーターは、セット・セレクターまたはブロック・セレクターを使用していないため、これらのフィールドは 00h に設定する必要があります。</p> <p>「取得」応答データは以下を返します。</p> <p>    バイト 1 = 完了コード</p>	CAh	<p>LAN 構成パラメーターの設定:</p> <p><u>データ 1</u></p> <p>予約済み (= 00h)</p> <p><u>データ 2:3</u></p> <p>Ethernet-over-USB ポート番号、LSByte から</p> <p><u>データ 4:5</u></p> <p>外部イーサネット・ポート番号、LSByte から</p>

パラメーター	#	パラメーター・データ
<p>バイト 2 = リビジョン            バイト 3 = 予約済み (00h)            バイト 4:5 = Ethernet-over-USB ポート番号 (LSByte から)            バイト 6:7 = 外部イーサネット・ポート番号 (LSByte から)</p> <p>後続のバイト数は、アドレス指定モードに応じて異なる場合があります (1、4、または 16 バイト)。</p> <ul style="list-style-type: none"> <li>バイト 8 = 事前定義済みのモード:               <ul style="list-style-type: none"> <li>00h = パススルーが無効になりました</li> <li>01h = CMM の IP アドレスが使用されています</li> </ul> </li> </ul> <p>バイト 8:11 = IPv4 外部ネットワーク IP アドレス (バイナリ形式)            バイト 8:23 = IPv6 外部ネットワーク IP アドレス (バイナリ形式)</p> <p>完了コード:</p> <p>00h - 成功</p> <p>80h - パラメーターがサポートされていません</p> <p>C1h - コマンドがサポートされていません</p> <p>C7h - リクエスト・データの長さが無効です</p>		<p>後続のバイト数は、アドレス指定モードに応じて異なる場合があります (1、4、または 16 バイト)。</p> <p><u>データ 6</u></p> <p>00h = パススルーを無効にする</p> <p>01h = CMM の IP アドレスを使用する</p> <p><u>データ 6:9</u></p> <p>IPv4 外部ネットワーク IP アドレス (バイナリ形式)</p> <p><u>データ 6:21</u></p> <p>IPv6 外部ネットワーク IP アドレス (バイナリ形式)</p>
<p>OEM パラメーター</p> <p>このパラメーターは、LAN over USB の IP アドレスと XCC のネットマスクを設定および取得するために使用されます。</p> <p>応答データは以下を返します。</p> <p>バイト 1 = 完了コード            バイト 2 = パラメーターのリビジョン (IPMI 仕様と同じ)</p> <p>バイト 3:10 = 最初に IP アドレスおよびネットマスク値 (MS バイト)</p>	CBh	<p><u>データ 1:4</u></p> <p>XCC 側の LAN over USB インターフェースの IP アドレス。</p> <p><u>データ 5:8</u></p> <p>XCC 側の LAN over USB インターフェースのネットマスク</p>
<p>OEM パラメーター</p> <p>このパラメーターは、ホスト OS の LAN over USB IP アドレスを設定および取得するために使用されます。</p> <p>応答データは以下を返します。</p>	CCh	<p><u>データ 1:4</u></p> <p>ホスト側の LAN over USB インターフェースの IP アドレス。</p>

パラメーター	#	パラメーター・データ
バイト1=完了コード バイト2=パラメーターのリビジョン (IPMI仕様と同じ) バイト3:6=最初にIPアドレス (MSバイト)		

### 論理パッケージ・インベントリの照会

以下のパラメーターは、NCSIパッケージ・インベントリを照会するために使用されます。

パラメーター	#	パラメーター・データ
OEMパラメーター LAN構成パラメーターの取得/設定コマンドのこのパラメーターは、セット・セクターまたはブロック・セクターを使用していないため、これらのフィールドは00hに設定する必要があります。 パッケージ・インベントリ操作の照会 照会パッケージ情報の操作は、D3hパラメーター番号以外に2つの0x00データ・バイトを使用して要求を発行することにより実行されます。 パッケージ・インベントリの照会 --> 0x0C 0x02 0x00 0xD3 0x00 0x00 XCCの応答には、存在する各パッケージの情報のバイトが含まれています。 ビット7:4=パッケージ内のNCSIチャンネルの番号 ビット3:0=論理パッケージ番号 応答 --> 0x00 0x00 0x40 0x01 0x32 3つの論理パッケージが存在することを示します。 パッケージ0には4つのNCSIチャンネルがあります パッケージ1はNCSI NICではないため、NCSIチャンネルをサポートしていません	D3h	LAN構成パラメーターを取得/設定。

パラメーター	#	パラメーター・データ
パッケージ2には3つのNCSIチャンネルがあります		

### 論理パッケージ・データの取得/設定

以下のパラメーターは、各パッケージに割り当てられた優先順位の読み取りと設定のために使用されます。

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>LAN 構成パラメーターの取得/設定コマンドのこのパラメーターは、セット・セレクターまたはブロック・セレクターを使用していないため、これらのフィールドは00hに設定する必要があります。</p> <p>そのコマンドは、2つの操作のみをサポートします。</p> <ul style="list-style-type: none"> <li>• パッケージの優先順位の読み取り</li> <li>• パッケージの優先順位の設定</li> </ul> <p>パッケージの優先操作の読み取り</p> <p>読み取りパッケージの優先操作は、D4hパラメーター番号以外に2つの0x00データ・バイトを使用して要求を発行することにより実行されます。</p> <p>パッケージの優先順位の読み取り</p> <p>--&gt; 0x0C 0x02 0x01 0xD4 0x00 0x00</p> <p>応答</p> <p>--&gt; 0x00 0x00 0x00 0x12 0x23</p> <p>論理パッケージ0 = 優先順位0          論理パッケージ2 = 優先順位1          論理パッケージ3 = 優先順位2</p> <p>パッケージの優先操作の設定</p> <p>パッケージの優先操作の設定は、D4hパラメーター番号以外に1つまたは複数のパラメーターを使用して要求を発行することにより実行されます。</p> <p>パッケージの優先順位の設定</p>	D4	<p>LAN 構成パラメーターの取得/設定:</p> <p>ビット [7-4] = 論理パッケージの優先順位 (1 = 最高、15 = 最低)</p> <p>ビット [3:0] = 論理パッケージ番号</p>



パラメーター	#	パラメーター・データ
--> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 論理パッケージ 0 に設定 = 優先順位 0 論理パッケージ 2 に設定 = 優先順位 1 論理パッケージ 3 に設定 = 優先順位 2 応答: 完了コードのみ、追加データなし		

### XCC ネットワークの同期ステータスの取得/設定

パラメーター	#	パラメーター・データ
OEM パラメーター バイトを使用して、専用および共有の nic モード間でネットワーク設定を同期するよう構成します。 LAN 構成パラメーターの取得/設定コマンドのこのパラメーターは、セット・セレクターまたはブロック・セレクターを使用しないため、これらのフィールドは 00h に設定する必要があります。 応答データは 3 バイトを返します。 バイト 1 = 完了コード バイト 2 = リビジョン バイト 3 = 00h (有効)、または 01h (無効)	D5h	データ 1 0x00 = 同期 0x01 = 独立

バイトを使用して、専用の nic モードと共有 NIC モードとの間でネットワーク設定を同期するよう構成します。ここで、デフォルト値は 0h でした。それは、XCC がモード変更間でネットワーク設定を自動的に更新し、共有 nic (ボード上) 主な参照値として使用することを意味します。1h として設定した場合には各ネットワーク設定は「独立」となり、専用モードでは VLAN を有効とし、共有 NIC モードでは VLAN を無効とするなど、モード間で異なるネットワーク設定を構成することができます。

### XCC ネットワーキング・モードを取得/設定

パラメーター	#	パラメーター・データ
<p>OEM パラメーター</p> <p>このパラメーターは、XCC 管理 NIC のネットワーク・モードを取得/設定するために使用されます。</p> <p>応答データは 4 バイトを返します。</p> <p>バイト 1 = 完了コード            バイト 2 = リビジョン            バイト 3 = 適用済み/指定されたネットモード            バイト 4 = 適用されたネットモードのパッケージ ID            バイト 5 = 適用されたネットモードのチャンネル ID</p>	D6h	<p>LAN 構成パラメーターの設定:</p> <p><u>データ 1</u></p> <p>設定すべきネットモード</p> <p>LAN 構成パラメーターの取得:</p> <p><u>データ 1</u></p> <p>取得すべきネットモード。これはオプションのデータで、デフォルトでは現在のネットモードを照会します。</p>

## OEM IPMI コマンド

XCC は、以下の IPMI OEM コマンドをサポートします。各コマンドは、以下に示すように異なるレベルの特権を必要とします。

コード	Netfn 0x2E コマンド	特権
0xCC	XCC をデフォルトにリセット	PRIV_USR

コード	Netfn 0x3A コマンド	特権
0x00	ファームウェア・バージョンの照会	PRIV_USR
0x0D	ボード情報	PRIV_USR
0x1E	シャーシの電源復元遅延オプション	PRIV_USR
0x38	NMI およびリセット	PRIV_USR
0x49	データ収集の開始	PRIV_USR
0x4A	ファイルのプッシュ	PRIV_USR
0x4D	データ収集のステータス	PRIV_USR
0x50	Build 情報の取得	PRIV_USR
0x55	ホスト名の取得/設定	PRIV_USR
0x6B	FPGA ファームウェアのリビジョン・レベルの照会	PRIV_USR
0x6C	ボード・ハードウェアのリビジョン・レベルの照会	PRIV_USR

コード	Netfn 0x3A コマンド	特権
0x6D	PSoC ファームウェアのリビジョン・レベルの照会	PRIV_USR
0x98	FP USB ポートの制御	PRIV_USR
0xC7	ネイティブ NM IPMI スイッチ	PRIV_ADM

### XCC をデフォルト・コマンドにリセット

このコマンドは、XCC 構成設定をデフォルト値にリセットします。

ネット関数 = 0x2E			
コード	コマンド	要求、応答データ	説明
0xCC	XCC をデフォルトにリセット	<b>要求:</b> バイト 1 – 0x5EByte 2 – 0x2B  バイト 3 – 0x00  バイト 4 – 0x0AByte 5 – 0x01  バイト 6 – 0xFF  バイト 7 – 0x00Byte 8 – 0x00  バイト 9 – 0x00  <b>応答:</b> バイト 1 – Completion CodeByte 2 – 0x5EByte 3 – 0x2B  バイト 4 – 0x00  バイト 5 – 0x0AByte 6 – 0x01  バイト 7 – 応答データ 0 = 成功 0 以外 = 失敗	このコマンドは、XCC 構成設定をデフォルト値にリセットします。

### ボード / ファームウェア情報コマンド

このセクションでは、ボードとファームウェアの情報を照会するためのコマンドを記載します。

ネット関数 = 0x3A			
コード	コマンド	要求、応答データ	説明
0x00	ファームウェア・バージョンの照会	<b>要求:</b> リクエストされているデータはありません  <b>応答:</b> バイト1-完了コード バイト2-メジャー・バージョン バイト3-マイナー・バージョン	このコマンドは、ファームウェアのメジャーおよびマイナーバージョン番号を返します。オプションの1バイトの要求データを使用してコマンドを実行すると、XCCの応答はバージョンの3番目のフィールド(リビジョン)も返します。  (メジャー、マイナー、リビジョン)
0x0D	ボード情報の照会	<b>要求:</b> 該当なし  <b>応答:</b> バイト1-システム ID バイト2-ボードのリビジョン	このコマンドは、ボード ID および平面のリビジョンを返します。
0x50	ビルド情報の照会	<b>要求:</b> 該当なし  <b>応答:</b> バイト1-完了コード バイト2:10-ASCII Build 名 バイト11:23-ASCII Build の日付 バイト24:31-ASCII Build の時刻	このコマンドは、ビルド名、ビルドの日付、およびビルドの時刻を返します。ビルド名およびビルドの日付の文字列の最後はゼロです。  ビルドの日付の形式は YYYY-MM-DD です。  例: 「ZUBT99A」 “2005-03-07” “23:59:59”
0x6B	FPGA ファームウェアのリビジョン・レベルの照会	<b>要求:</b> バイト1-FPGA デバイスのタイプ*  FPGA デバイスのタイプ 0=ローカル(アクティブ・レベル) 1=CPU カード1(アクティブ・レベル) 2=CPU カード2(アクティブ・レベル) 3=CPU カード3(アクティブ・レベル) 4=CPU カード4(アクティブ・レベル) 5=ローカル・プライマリ ROM 6=ローカル・リカバリー ROM	このコマンドは、FPGA ファームウェアのリビジョン・レベルを返します。  バイト1が省略されている場合、ローカル(アクティブ・レベル)が選択されます。

ネット関数 = 0x3A			
コード	コマンド	要求、応答データ	説明
		<b>応答:</b> バイト1-完了コード バイト2-メジャー・リビジョン・レベル バイト3-マイナー・リビジョン・レベル バイト4-サブマイナー・リビジョン・レベル (XCC プラットフォームでのテスト・バイト)	
0x6C	ボード・ハードウェアのリビジョン・レベルの照会	<b>要求:</b> データはありません。 <b>応答:</b> バイト1-完了コード バイト2-リビジョン・レベル	このコマンドは、FPGA が常駐するボード・ハードウェアのリビジョン・レベルを返します。
0x6D	PSoC ファームウェアのリビジョン・レベルの照会	<b>要求:</b> なし <b>応答:</b> バイト1-完了コード バイト2-ピン番号 バイト3-APID バイト4-リビジョン バイト5-6-FRU ID バイト6: N-検出された PSoC ごとに、バイト2-6を繰り返します	このコマンドは、検出されたすべての PSoC デバイスのリビジョン・レベルを返します。 注: ピン番号は物理的な位置を示します。詳細については、システム仕様を参照してください。

## システム制御コマンド

IPMI 仕様は、基本的な電源およびリセット制御を提供します。Lenovo は、追加の制御機能を提供します。

ネット関数 = 0x2E							
コード	コマンド	要求、応答データ	説明				
0x1E	シャーシの電源復元遅延オプション	<p><b>要求:</b></p> <table border="1"> <tr> <td>バイト 1</td> <td>           要求のタイプ:            0x00 = 遅延設定オプション            0x01 = 遅延オプションの照会         </td> </tr> <tr> <td>バイト 2</td> <td>           (バイト 1 = 0x00 の場合)            0x00 = 無効 (デフォルト)            0x01 = ランダム            0x02 - 予約済みの 0xFF         </td> </tr> </table> <p><b>応答:</b></p> <p>バイト 1 - 完了コード</p> <p>バイト 2 - 遅延オプション (照会要求のみ)</p>	バイト 1	要求のタイプ: 0x00 = 遅延設定オプション 0x01 = 遅延オプションの照会	バイト 2	(バイト 1 = 0x00 の場合) 0x00 = 無効 (デフォルト) 0x01 = ランダム 0x02 - 予約済みの 0xFF	<p>この設定は、シャーシ電源復元ポリシーが常に電源オンまたは (以前に電源がオンになっていた場合) 電源オンに復元するよう設定されている場合、AC が適用された後、または戻った後に使用されます。オプションは、無効 (デフォルト設定、電源オン時の遅延なし) およびランダムの 2 つです。ランダム遅延設定は、AC が適用されるか戻った後に、サーバーの電源が自動的にオンになってから、1 から 15 秒の間でランダム遅延を提供します。</p> <p>このコマンドは、ラック・サーバーの XCC でのみサポートされています。</p>
バイト 1	要求のタイプ: 0x00 = 遅延設定オプション 0x01 = 遅延オプションの照会						
バイト 2	(バイト 1 = 0x00 の場合) 0x00 = 無効 (デフォルト) 0x01 = ランダム 0x02 - 予約済みの 0xFF						
0x38	NMI およびリセット	<p><b>要求:</b></p> <p>バイト 1 - 秒数 0 = NMI のみ</p> <p>バイト 2 - リセットのタイプ 0 = ソフト・リセット 1 = 電源サイクル</p> <p><b>応答:</b></p> <p>バイト 1 - 完了コード</p>	<p>このコマンドは、システム NMI を実行するために使用されます。任意で、NMI の後にシステムをリセット (リブート) したり電源を入れ直したりすることができます。</p> <p>「秒数」フィールドが 0 ではない場合は、指定された秒数経過後にシステムがリセットされるか、電源が入れ直されます。</p> <p>要求のバイト 2 はオプションです。バイト 2 が指定されていない場合、または値が 0x00 の場合は、ソフト・リセットが実行されます。バイト 2 が 0x01 の場合は、システムの電源が入れ直されます。</p>				

## その他のコマンド

このセクションでは、他のセクションに適合しないコマンドについて説明します。

ネット関数 = 0x3A											
コード	コマンド	要求、応答データ	説明								
0x55	ホスト名の取得/設定	<p>要求の長さ = 0: リクエスト・データがありません</p> <p>応答:</p> <table border="1"> <tr> <td>バイト 1</td> <td>完了コード</td> </tr> <tr> <td>バイト 2-65</td> <td>現在のホスト名。  ASCIIZ、Null 終了文字列。</td> </tr> </table> <p>要求の長さ 1-64:</p> <table border="1"> <tr> <td>バイト 1-64</td> <td>DHCP のホスト名  00h を使用した ASCIIZ の終了</td> </tr> </table>	バイト 1	完了コード	バイト 2-65	現在のホスト名。  ASCIIZ、Null 終了文字列。	バイト 1-64	DHCP のホスト名  00h を使用した ASCIIZ の終了	<p>ホスト名を取得/設定するには、このコマンドを使用します。</p> <p>ホスト名を設定するときは、希望する値を 00h で終了する必要があります。ホスト名は、63 文字に null を加算したものに限定されます。</p>		
バイト 1	完了コード										
バイト 2-65	現在のホスト名。  ASCIIZ、Null 終了文字列。										
バイト 1-64	DHCP のホスト名  00h を使用した ASCIIZ の終了										
0x98	FP USB ポートの制御	<p>要求:</p> <p>バイト 1</p> <table border="1"> <tr> <td>01h:</td> <td>前面パネル USB ポートの現在のオーナーを取得します</td> </tr> </table> <p>応答:</p> <p>バイト 1 - 完了コード</p> <p>バイト 2</p> <table border="1"> <tr> <td>00h:</td> <td>ホストによる所有</td> </tr> <tr> <td>01h:</td> <td>BMC による所有</td> </tr> </table> <p>要求:</p> <p>バイト 1</p> <table border="1"> <tr> <td>02h:</td> <td>前面パネル USB ポートの構成を取得します</td> </tr> </table> <p>応答:</p>	01h:	前面パネル USB ポートの現在のオーナーを取得します	00h:	ホストによる所有	01h:	BMC による所有	02h:	前面パネル USB ポートの構成を取得します	<p>このコマンドは、FP USB ポートのステータス/構成の照会、FP USB ポートのモード/タイムアウトの構成、および USB ポートのオーナーの切り替え (ホストと BMC 間で) に使用します。</p> <p>構成では、FP USB には、ホスト専用、BMC のみによる所有、オーナーをホストと BMC との間で切り替えることができる共用モードという、3つのモードがあります。</p> <p>共用モードが有効になっている場合、USB ポートは、サーバーの電源がオフになっているときには BMC に接続され、サーバーの電源がオンになっているときにサーバーに接続されます。</p> <p>共用モードが有効になっていて、サーバーの電源がオンになっている場合、構成で非アクティブ・タイムアウトが発生すると、BMC はサーバーに USB ポートを戻します。</p> <p>サーバーに ID ボタンがある場合、ユーザーは、ID ボタンを有効にし、ID ボタンを 3 秒以上押し続けることにより FP USB ポートのオーナーを切り替えられるようになります。</p>
01h:	前面パネル USB ポートの現在のオーナーを取得します										
00h:	ホストによる所有										
01h:	BMC による所有										
02h:	前面パネル USB ポートの構成を取得します										

ネット関数 = 0x3A																							
コード	コマンド	要求、応答データ	説明																				
		バイト1-完了コード バイト2 <table border="1" data-bbox="652 405 1024 543"> <tr> <td>00h:</td> <td>ホスト専用</td> </tr> <tr> <td>01h:</td> <td>BMC 専用</td> </tr> <tr> <td>02h:</td> <td>共用モード</td> </tr> </table> バイト3:4-非アクティブ・セッションのタイムアウト(分)(MSBが最初) バイト5-IDの有効化ボタン <table border="1" data-bbox="652 743 1024 835"> <tr> <td>00h:</td> <td>無効</td> </tr> <tr> <td>01h:</td> <td>使用可能</td> </tr> </table> バイト6-ヒステリシス(オプション)(秒単位) <b>要求:</b> バイト1 03h: 前面パネル USB ポートの構成を設定します バイト2 <table border="1" data-bbox="652 1205 1024 1344"> <tr> <td>00h:</td> <td>ホスト専用</td> </tr> <tr> <td>01h:</td> <td>BMC 専用</td> </tr> <tr> <td>02h:</td> <td>共用モード</td> </tr> </table> バイト3:4-非アクティブ・セッションのタイムアウト(分)(MSBが最初) バイト5-IDの有効化ボタン <table border="1" data-bbox="652 1543 1024 1635"> <tr> <td>00h:</td> <td>無効</td> </tr> <tr> <td>01h:</td> <td>使用可能</td> </tr> </table> バイト6-ヒステリシス(オプション)(秒単位) <b>応答:</b> バイト1-完了コードバイト2	00h:	ホスト専用	01h:	BMC 専用	02h:	共用モード	00h:	無効	01h:	使用可能	00h:	ホスト専用	01h:	BMC 専用	02h:	共用モード	00h:	無効	01h:	使用可能	<p>電源サイクル中にポートを自動的に切り替える場合は、秒単位のヒステリシスが設定されます。これはオプションのパラメーターです。</p> <p>SD530 サーバー</p> <p>SD530 プラットフォームでは、ポートはオプションであり、存在する場合は XCC に直接有線で、XCC のみに接続されています。ポートをホストに切り替えることはできません。</p> <ul style="list-style-type: none"> <li>• バイト1=1でコマンドが発行された場合、XCC は常に、ポートが BMC によって所有されていると応答します。</li> <li>• バイト1=2でコマンドが発行された場合、XCC は常に、ポートが BMC 専用であると応答します。</li> <li>• コマンドがバイト1=3またはバイト1=4で発行された場合、XCC は完了コード D6h を使用して応答します。</li> </ul> <p>非 SD530 サーバー</p> <p>非 SD530 プラットフォームでは、「ホストのみ」モードに切り替えることで、XCC の前面パネル USB ポートの使用を無効にすることができます。</p> <p>コマンドがバイト1=5またはバイト1=6で発行された場合、XCC は完了コード D6h を使用して応答します。</p>
00h:	ホスト専用																						
01h:	BMC 専用																						
02h:	共用モード																						
00h:	無効																						
01h:	使用可能																						
00h:	ホスト専用																						
01h:	BMC 専用																						
02h:	共用モード																						
00h:	無効																						
01h:	使用可能																						



ネット関数 = 0x3A															
コード	コマンド	要求、応答データ	説明												
		<table border="1"> <tr> <td>00h:</td> <td>ホストへの切り替え</td> </tr> <tr> <td>01h:</td> <td>BMC への切り替え</td> </tr> </table> <p>応答:</p> <p>バイト 1-完了コード</p> <p>バイト 1</p> <table border="1"> <tr> <td>05h:</td> <td>前面パネル USB ポートを有効/無効にする</td> </tr> </table> <p>バイト 2</p> <table border="1"> <tr> <td>00h:</td> <td>無効にする</td> </tr> <tr> <td>01h:</td> <td>有効にする</td> </tr> </table> <p>応答:</p> <p>バイト 1-完了コード</p> <p>要求:</p> <p>バイト 1</p> <table border="1"> <tr> <td>06h:</td> <td>前面パネル USB ポートの有効/無効状態を確認します</td> </tr> </table> <p>応答:</p> <p>バイト 1-完了コード</p> <p>バイト 2</p>	00h:	ホストへの切り替え	01h:	BMC への切り替え	05h:	前面パネル USB ポートを有効/無効にする	00h:	無効にする	01h:	有効にする	06h:	前面パネル USB ポートの有効/無効状態を確認します	
00h:	ホストへの切り替え														
01h:	BMC への切り替え														
05h:	前面パネル USB ポートを有効/無効にする														
00h:	無効にする														
01h:	有効にする														
06h:	前面パネル USB ポートの有効/無効状態を確認します														
0xC7	ネイティブ NM IPMI スイッチ	<p>要求の長さ = 0:</p> <p>リクエスト・データがありません</p> <p>応答:</p> <table border="1"> <tr> <td>バイト 1</td> <td>完了コード</td> </tr> <tr> <td>バイト 2</td> <td>現在の有効/無効ステータス</td> </tr> </table> <p>要求の長さ = 1:</p>	バイト 1	完了コード	バイト 2	現在の有効/無効ステータス	このコマンドは、ネイティブ Intel IPMI コマンドの XCC のブリッジング機能を有効または無効にするために使用されます。								
バイト 1	完了コード														
バイト 2	現在の有効/無効ステータス														

ネット関数 = 0x3A									
コード	コマンド	要求、応答データ	説明						
		<table border="1"> <tr> <td>バイト 1</td> <td>           ネイティブ            NM IPMI イン            ターフェース            の有効/無効属            性             00h – 無効             01h – 有効         </td> </tr> <tr> <td colspan="2">応答:</td> </tr> <tr> <td>バイト 1</td> <td>完了コード</td> </tr> </table>	バイト 1	ネイティブ NM IPMI イン ターフェース の有効/無効属 性  00h – 無効  01h – 有効	応答:		バイト 1	完了コード	
バイト 1	ネイティブ NM IPMI イン ターフェース の有効/無効属 性  00h – 無効  01h – 有効								
応答:									
バイト 1	完了コード								

---

## 付録 A ヘルプおよび技術サポートの入手

ヘルプ、サービス、技術サポート、または Lenovo 製品に関する詳しい情報が必要な場合は、Lenovo がさまざまな形で提供しているサポートをご利用いただけます。

WWW 上の以下の Web サイトで、Lenovo システム、オプション・デバイス、サービス、およびサポートについての最新情報が提供されています。

<http://datacentersupport.lenovo.com>

注：このセクションには、IBM Web サイトへの言及、およびサービスの取得に関する情報が含まれていません。IBM は、ThinkSystem に対する Lenovo の優先サービス・プロバイダーです。

---

### 依頼する前に

連絡する前に、以下の手順を実行してお客様自身で問題の解決を試みてください。サポートを受けるために連絡が必要と判断した場合、問題を迅速に解決するためにサービス技術員が必要とする情報を収集します。

#### お客様自身での問題の解決

多くの問題は、Lenovo がオンライン・ヘルプまたは Lenovo 製品資料で提供するトラブルシューティング手順を実行することで、外部の支援なしに解決することができます。Lenovo 製品資料にも、お客様が実行できる診断テストについての説明が記載されています。ほとんどのシステム、オペレーティング・システムおよびプログラムの資料には、トラブルシューティングの手順とエラー・メッセージやエラー・コードに関する説明が記載されています。ソフトウェアの問題だと考えられる場合は、オペレーティング・システムまたはプログラムの資料を参照してください。

ThinkSystem 製品については、以下の場所で製品ドキュメントが見つかります。

<https://pubs.lenovo.com/>

以下の手順を実行してお客様自身で問題の解決を試みることができます。

- ケーブルがすべて接続されていることを確認します。
- 電源スイッチをチェックして、システムおよびすべてのオプション・デバイスの電源がオンになっていることを確認します。
- ご使用の Lenovo 製品用に更新されたソフトウェア、ファームウェア、およびオペレーティング・システム・デバイス・ドライバーがないかを確認します。Lenovo 保証規定には、Lenovo 製品の所有者であるお客様の責任で、製品のソフトウェアおよびファームウェアの保守および更新を行う必要があることが明記されています (追加の保守契約によって保証されていない場合)。お客様のサービス技術員は、問題の解決策がソフトウェアのアップグレードで文書化されている場合、ソフトウェアおよびファームウェアをアップグレードすることを要求します。
- ご使用の環境で新しいハードウェアを取り付けたり、新しいソフトウェアをインストールした場合、<http://www.lenovo.com/serverproven/> でそのハードウェアおよびソフトウェアがご使用の製品によってサポートされていることを確認してください。
- <http://datacentersupport.lenovo.com> にアクセスして、問題の解決に役立つ情報があるか確認してください。
  - 同様の問題が発生した他のユーザーがいるかどうかを調べるには、[https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv\\_eg](https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg) の Lenovo Forums (Lenovo フォーラム) を確認してください。

多くの問題は、Lenovo がオンライン・ヘルプまたは Lenovo 製品資料で提供するトラブルシューティング手順を実行することで、外部の支援なしに解決することができます。Lenovo 製品資料にも、お客様

が実行できる診断テストについての説明が記載されています。ほとんどのシステム、オペレーティング・システムおよびプログラムの資料には、トラブルシューティングの手順とエラー・メッセージやエラー・コードに関する説明が記載されています。ソフトウェアの問題だと考えられる場合は、オペレーティング・システムまたはプログラムの資料を参照してください。

### サポートへの連絡に必要な情報の収集

ご使用の Lenovo 製品に保証サービスが必要であると思われる場合は、連絡される前に準備をしていただくと、サービス技術員がより効果的にお客様を支援することができます。または製品の保証について詳しくは <http://datacentersupport.lenovo.com/warrantylookup> で参照できます。

サービス技術員に提供するために、次の情報を収集します。このデータは、サービス技術員が問題の解決策を迅速に提供する上で役立ち、お客様が契約された可能性があるレベルのサービスを確実に受けられるようにします。

- ハードウェアおよびソフトウェアの保守契約番号 (該当する場合)
- マシン・タイプ番号 (Lenovo の 4 桁のマシン識別番号)
- 型式番号
- シリアル番号
- 現行のシステム UEFI およびファームウェアのレベル
- エラー・メッセージやログなど、その他関連情報

Lenovo サポートに連絡する代わりに、<https://www-947.ibm.com/support/servicerequest/Home.action> にアクセスして Electronic Service Request を送信することもできます。Electronic Service Request を送信すると、お客様の問題に関する情報をサービス技術員が迅速に入手できるようになり、問題の解決策を判別するプロセスが開始されます。Lenovo サービス技術員は、お客様が Electronic Service Request を完了および送信するとすぐに、解決策の作業を開始します。

---

## サービス・データの収集

サーバーの問題の根本原因をはっきり特定するため、または Lenovo サポートの依頼によって、詳細な分析に使用できるサービス・データを収集する必要がある場合があります。サービス・データには、イベント・ログやハードウェア・インベントリなどの情報が含まれます。

サービス・データは以下のツールを使用して収集できます。

- **Lenovo XClarity Controller**

Lenovo XClarity Controller Web インターフェースまたは CLI を使用してサーバーのサービス・データを収集できます。ファイルは保存でき、Lenovo サポートに送信できます。

- Web インターフェースを使用したサービス・データの収集について詳しくは、[https://pubs.lenovo.com/xcc3/nnlia\\_c\\_servicesandsupport.html](https://pubs.lenovo.com/xcc3/nnlia_c_servicesandsupport.html) を参照してください。
- CLI を使用したサービス・データの収集について詳しくは、[https://pubs.lenovo.com/xcc3/nnlia\\_r\\_ffdcommand.html](https://pubs.lenovo.com/xcc3/nnlia_r_ffdcommand.html) を参照してください。

- **Lenovo XClarity Administrator**

一定の保守可能イベントが Lenovo XClarity Administrator および管理対象エンドポイントで発生した場合に、診断ファイルを収集し自動的に Lenovo サポートに送信するように Lenovo XClarity Administrator をセットアップできます。Call Home を使用して診断ファイルを Lenovo サポートに送信するか、SFTP を使用して別のサービス・プロバイダーに送信するかを選択できます。また、手動で診断ファイルを収集したり、問題レコードを開いたり、診断ファイルを Lenovo サポート・センターに送信したりもできます。

Lenovo XClarity Administrator 内での自動問題通知のセットアップに関する詳細情報は [https://pubs.lenovo.com/lxca/admin\\_setupcallhome.html](https://pubs.lenovo.com/lxca/admin_setupcallhome.html) で参照できます。

- **Lenovo XClarity Provisioning Manager**

Lenovo XClarity Provisioning Manager のサービス・データの収集機能を使用して、システム・サービス・データを収集します。既存のシステム・ログ・データを収集するか、新しい診断を実行して新規データを収集できます。

- **Lenovo XClarity Essentials**

Lenovo XClarity Essentials はオペレーティング・システムからインバンドで実行できます。Lenovo XClarity Essentials では、ハードウェア・サービス・データに加えて、オペレーティング・システム・イベント・ログなどオペレーティング・システムに関する情報を収集できます。

サービス・データを取得するには、`getinfor` コマンドを実行できます。getinfor の実行についての詳細は、[https://pubs.lenovo.com/lxce-onecli/onecli\\_r\\_getinfor\\_command.html](https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html) を参照してください。

---

## サポートへのお問い合わせ

サポートに問い合わせで問題に関するヘルプを入手できます。

ハードウェアの保守は、Lenovo 認定サービス・プロバイダーを通じて受けることができます。保証サービスを提供する Lenovo 認定サービス・プロバイダーを見つけるには、<https://datacentersupport.lenovo.com/us/en/serviceprovider> にアクセスし、フィルターを使用して国別で検索します。Lenovo サポートの電話番号については、<https://datacentersupport.lenovo.com/us/en/supportphonenumber> で地域のサポートの詳細を参照してください。



---

## 付録 B 注記

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、Lenovo の営業担当員にお尋ねください。

本書で Lenovo 製品、プログラム、またはサービスに言及していても、その Lenovo 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、Lenovo の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、他の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

Lenovo は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、いかなる特許出願においても実施権を許諾することを意味するものではありません。お問い合わせは、書面にて下記宛先にお送りください。

**Lenovo (United States), Inc.**  
1009 Think Place  
Morrisville, NC 27560  
U.S.A.  
Attention: Lenovo VP of Intellectual Property

LENOVO は、本書を特定物として「現存するままの状態」で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。Lenovo は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、Lenovo 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書の内容は、Lenovo またはサード・パーティーの知的所有権のもとで明示または黙示のライセンスまたは損害補償として機能するものではありません。本書に記載されている情報はすべて特定の環境で得られたものであり、例として提示されるものです。他の操作環境で得られた結果は、異なる可能性があります。

Lenovo は、お客様が提供するいかなる情報も、お客様に対してなら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本書において Lenovo 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この Lenovo 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのもと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

---

## 商標

Lenovo、Lenovo ロゴ、ThinkSystem、Flex System、System x、NeXtScale System、および x Architecture は、Lenovo の米国およびその他の国における商標です。

インテル、および Intel Xeon は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Internet Explorer、Microsoft、および Windows は、Microsoft Corporation の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

---

## 重要事項

プロセッサの速度とは、マイクロプロセッサの内蔵クロックの速度を意味しますが、他の要因もアプリケーション・パフォーマンスに影響します。

CD または DVD ドライブの速度は、変わる可能性のある読み取り速度を記載しています。実際の速度は記載された速度と異なる場合があります、最大可能な速度よりも遅いことがあります。

主記憶装置、実記憶域と仮想記憶域、またはチャネル転送量を表す場合、KB は 1,024 バイト、MB は 1,048,576 バイト、GB は 1,073,741,824 バイトを意味します。

ハードディスク・ドライブの容量、または通信ボリュームを表すとき、MB は 1,000,000 バイトを意味し、GB は 1,000,000,000 バイトを意味します。ユーザーがアクセス可能な総容量は、オペレーティング環境によって異なる可能性があります。

内蔵ハードディスク・ドライブの最大容量は、Lenovo から入手可能な現在サポートされている最大のドライブを標準ハードディスク・ドライブの代わりに使用し、すべてのハードディスク・ドライブ・ベイに取り付けることを想定しています。

最大メモリーは標準メモリーをオプション・メモリー・モジュールと取り替える必要があることもあります。

各ソリッド・ステート・メモリー・セルには、そのセルが耐えられる固有の有限数の組み込みサイクルがあります。したがって、ソリッド・ステート・デバイスには、可能な書き込みサイクルの最大数が決められています。これを **total bytes written (TBW)** と呼びます。この制限を超えたデバイスは、システム生成コマンドに 응답できなくなる可能性があり、また書き込み不能になる可能性があります。Lenovo は、正式に公開された仕様に文書化されているプログラム/消去のサイクルの最大保証回数を超えたデバイスについては責任を負いません。

Lenovo は、他社製品に関して一切の保証責任を負いません。他社製品のサポートがある場合は、Lenovo ではなく第三者によって提供されます。

いくつかのソフトウェアは、その小売り版 (利用可能である場合) とは異なる場合があります、ユーザー・マニュアルまたはすべてのプログラム機能が含まれていない場合があります。

---

## 粒子汚染

注意: 浮遊微小粒子 (金属片や微粒子を含む) や反応性ガスは、単独で、あるいは湿気や気温など他の環境要因と組み合わせられることで、本書に記載されているデバイスにリスクをもたらす可能性があります。



過度のレベルの微粒子や高濃度の有害ガスによって発生するリスクの中には、デバイスの誤動作や完全な機能停止の原因となり得る損傷も含まれます。以下の仕様では、このような損傷を防止するために設定された微粒子とガスの制限について説明しています。以下の制限を、絶対的な制限として見なしたり、あるいは使用したりしてはなりません。温度や大気中の湿気など他の多くの要因が、粒子や環境腐食性およびガス状の汚染物質移動のインパクトに影響することがあるからです。本書で説明されている特定の制限が無い場合は、人体の健康と安全の保護に合致するよう、微粒子やガスのレベル維持のための慣例を実施する必要があります。お客様の環境の微粒子あるいはガスのレベルがデバイス損傷の原因であると Lenovo が判断した場合、Lenovo は、デバイスまたは部品の修理あるいは交換の条件として、かかる環境汚染を改善する適切な是正措置の実施を求めます。かかる是正措置は、お客様の責任で実施していただきます。

表 59. 微粒子およびガスの制限

汚染物質	制限
微粒子	<ul style="list-style-type: none"> <li>室内の空気は、ASHRAE Standard 52.2<sup>1</sup> に従い、大気塵埃が 40% のスポット効率で継続してフィルタリングされなければならない (MERV 9 準拠)。</li> <li>データ・センターに取り入れる空気は、MIL-STD-282 に準拠する HEPA フィルターを使用し、99.97% 以上の粒子捕集率効果のあるフィルタリングが実施されなければならない。</li> <li>粒子汚染の潮解相対湿度は、60% を超えていなければならない<sup>2</sup>。</li> <li>室内には、亜鉛ウィスカーのような導電性汚染があってはならない。</li> </ul>
ガス	<ul style="list-style-type: none"> <li>銅: ANSI/ISA 71.04-1985 準拠の Class G1<sup>3</sup></li> <li>銀: 腐食率は 30 日間で 300 Å 未満</li> </ul>

<sup>1</sup> ASHRAE 52.2-2008 - 「一般的な換気および空気清浄機器について、微粒子の大きさごとの除去効率をテストする方法」。アトランタ: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

<sup>2</sup> 粒子汚染の潮解相対湿度とは、水分を吸収した塵埃が、十分に濡れてイオン導電性を持つようになる湿度のことです。

<sup>3</sup> ANSI/ISA-71.04-1985。 「プロセス計測およびシステム制御のための環境条件: 気中浮遊汚染物質」。 Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

## 通信規制の注記

本製品は、お客様の国で、いかなる方法においても公衆通信ネットワークのインターフェースへの接続について認定されていない可能性があります。このような接続を行う前に、法律による追加の認定が必要な場合があります。ご不明な点がある場合は、Lenovo 担当員または販売店にお問い合わせください。

## 電波障害自主規制特記事項

このデバイスにモニターを接続する場合は、モニターに付属の指定のモニター・ケーブルおよび電波障害抑制デバイスを使用してください。

その他の電波障害自主規制特記事項は以下に掲載されています。

<https://pubs.lenovo.com/>

## 台湾 BSMI RoHS 宣言

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr <sup>6+</sup> )	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合作件	-	○	○	○	○	○
空氣傳動設備	-	○	○	○	○	○
冷卻組合作件	-	○	○	○	○	○
內存模塊	-	○	○	○	○	○
處理器模塊	-	○	○	○	○	○
鍵盤	-	○	○	○	○	○
調製解調器	-	○	○	○	○	○
監視器	-	○	○	○	○	○
滑鼠	-	○	○	○	○	○
電纜組合作件	-	○	○	○	○	○
電源	-	○	○	○	○	○
儲備設備	-	○	○	○	○	○
電池匣組合作件	-	○	○	○	○	○
有mech的電路卡	-	○	○	○	○	○
無mech的電路卡	-	○	○	○	○	○
雷射器	-	○	○	○	○	○
<p>備考1. “超出0.1 wt %” 及 “超出0.01 wt %” 係指限用物質之百分比含量超出百分比含量基準值。            Note1: “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.</p> <p>備考2. “○” 係指該項限用物質之百分比含量未超出百分比含量基準值。            Note2: “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.</p> <p>備考3. “-” 係指該項限用物質為排除項目。            Note3: The “-” indicates that the restricted substance corresponds to the exemption.</p>						

## 台湾の輸出入お問い合わせ先情報

台湾の輸出入情報に関する連絡先を入手できます。

委製商/進口商名稱: 台灣聯想環球科技股份有限公司  
進口商地址: 台北市南港區三重路 66 號 8 樓  
進口商電話: 0800-000-702



# 索引

## a

accsecfg コマンド 103  
Active Directory ユーザー  
LDAP 134  
adapter コマンド 149  
asu コマンド 104

## b

backup コマンド 107  
batch コマンド 138  
BIOS (基本入出力システム) 1  
BMC

構成のリセット 121  
デフォルト構成 121

BMC 管理

BMC 構成  
BMC 構成の復元 47  
BMC 構成のバックアップ 46  
BMC 構成のバックアップおよび復元 46  
出荷時のデフォルト値へのリセット 47

## C

CIM over HTTP ポート  
設定 118  
CIM over HTTPS  
証明書管理 127  
セキュリティ 127  
CIM over HTTPS ポート  
設定 118  
clearlog コマンド 92  
clock コマンド 138

## d

D3 V2 シャーシ、XClarity Controller  
設定 66  
dbgshbmc コマンド 151  
dcmi  
関数およびコマンド 62  
電源管理 62  
DDNS  
DHCP サーバーが指定したドメイン名 108  
カスタムのドメイン名 108  
管理 108  
構成 108  
ドメイン名のソース 108  
dhepinfo コマンド 108  
DNS  
IPv4 アドレッシング 108  
IPv6 アドレッシング 108  
LDAP サーバー 115  
構成 108

サーバー・アドレッシング 108  
dns コマンド 108

## e

encaps コマンド 109  
Ethernet over USB  
構成 110  
ポート転送 110  
ethtousb コマンド 110  
exit コマンド 91

## f

fans コマンド 92  
Features on Demand  
管理 114  
フィーチャーのインストール 114  
フィーチャーの除去 114  
firewall コマンド 110  
Flex System 1  
Flex サーバー 1  
FoD  
管理 114  
フィーチャーのインストール 114  
フィーチャーの除去 114  
fuelg コマンド 102

## h

hashpw コマンド 112  
help コマンド 91  
history コマンド 91  
HTTP ポート  
設定 118  
HTTPS サーバー  
証明書管理 127  
セキュリティ 127  
HTTPS ポート  
設定 118

## i

ifconfig コマンド 112  
IMM  
reset 140  
sreset 140  
構成の復元 120  
IMM 制御コマンド 138  
info コマンド 139  
IP アドレス  
IPv4 9  
IPv6 9  
LDAP サーバー 115

- 構成 9
- IP アドレス、デフォルトの静的 10
- IPMI
  - 構成 34
  - リモート・サーバー管理 153
- IPMI over KCS アクセス
  - 構成 43
- IPMI インターフェース
  - 説明 153
- IPMI コマンド
  - 電力使用量 61
- IPMI ブリッジ
  - XClarity Controller 経由 62
  - 電源管理 62
- IPMItool 153
- IPv4
  - 構成 112
- IPv4 アドレッシング
  - DNS 108
- IPv6 9
  - 構成 112
- IPv6 アドレッシング
  - DNS 108

## k

- keycfg コマンド 114

## l

- LDAP
  - Active Directory ユーザー 134
  - 拡張役割ベース・セキュリティ 134
  - グループ検索属性 115
  - グループ・フィルター 115
  - 構成 17, 115
  - サーバーのターゲット名 115
  - 証明書管理 127
  - セキュリティ 127
  - 役割ベース・セキュリティ、拡張 134
  - ログイン許可属性 115
- ldap コマンド 115
- LDAP サーバー
  - DNS 115
  - IP アドレス 115
  - UID 検索属性 115
  - クライアント識別名 115
  - 検索ドメイン 115
  - 構成 115
  - 事前構成 115
  - バインディング方式 115
  - パスワード 115
  - ホスト名 115
  - ポート番号 115
  - ルート識別名 115
- LDAP サーバー・ポート
  - 設定 115
- led コマンド 93

## m

- MAC アドレス
  - 管理 112
- mhlog コマンド 92
- MIB 概要 7
- MTU
  - 設定 112

## n

- ntp コマンド 117

## O

- OEM IPMI コマンド 164
- OneCLI 1

## p

- portcontrol コマンド 117
- ports
  - オープンの表示 118
- ports コマンド 118
- power コマンド 100
- pxeboot コマンド 103

## r

- RAID セットアップ
  - サーバー構成 77
- rdmount コマンド 119
- readlog コマンド 95
- reset
  - IMM 140
- reset コマンド 101
- restore コマンド 120
- restoredefaults コマンド 121
- roles コマンド 120

## S

- seccfg コマンド 122
- security password manager
  - security password manager 44
  - 構成 44
- securityinfo コマンド 122
- securitymode コマンド 123
- Serial over LAN 153
- Serial-to-SSH リダイレクト 87
- servicelog コマンド 96
- set コマンド 123
- SKM
  - オプション 44
- SNMP TRAP 受信者 55
- SNMP エージェント・ポート
  - 設定 118

- snmp コマンド 123
  - SNMP トラップ・ポート 設定 118
- snmpalerts コマンド 126
- SNMPv1
  - 構成 123
- SNMPv1 コミュニティー 管理 123
- SNMPv1 トラップ
  - 構成 123
- SNMPv1 の連絡先 設定 123
- SNMPv3 設定
  - ユーザー 134
- SNMPv3 の連絡先 設定 123
- SNMPv3 のユーザー・アカウント 構成 134
- sreset コマンド 140
- SSH 鍵
  - ユーザー 134
- SSH CLI ポート 設定 118
- SSH サーバー
  - 証明書管理 127
- SSH サーバー
  - セキュリティ 127
- sshcfg コマンド 127
- SSL
  - 証明書管理 42
  - 証明書の処理 42
- sslcfg コマンド 127
- storage
  - 構成オプション 77
- storage コマンド 140
  - ストレージ・デバイス 140
- syshealth コマンド 97
- syslock コマンド 130

## t

- temps コマンド 98
- thermal コマンド 131
- ThinkSystem サーバー・ファームウェア 説明 1
- TLS
  - 最小レベル 132
- TLS コマンド 132
- TLS バージョン・サポート
  - TLS バージョン・サポート 46
- trespass コマンド 132

## u

- uefipw コマンド 133
- UID 検索属性
  - LDAP サーバー 115
- USB
  - 構成 110
- usbeth コマンド 133

- users コマンド 134

## V

- volts コマンド 99
- vpd コマンド 99

## W

- Web インターフェース
  - Web インターフェースへのログイン 12
- Web インターフェースの開始および使用 9
- Web の非アクティブ・タイムアウト 設定 103
- Web ブラウザーの要件 6

## X

- XClarity Controller
  - IPMI ブリッジ 62
  - Web インターフェース 9
  - XClarity Controller プラチナ・レベル 2
  - XClarity Controller 標準レベル 2
    - 機能 2
    - 構成オプション 17
    - シリアル・リダイレクト 87
    - 新機能 1
    - 説明 1
    - ネットワーク接続 10
    - ネットワーク・プロトコルの構成 29
  - XClarity Controller の再起動 48
  - XClarity Controller の構成
    - 構成のオプション
      - XClarity Controller 17
    - XClarity Controller の機能 2
      - Web インターフェースで 13
      - 標準レベル 2
  - XClarity Controller の管理
    - LDAP の構成 17
    - XClarity Controller のプロパティ
      - D3 V2 シャーシ 66
      - 日付と時刻 65
      - 新しい役割の作成 18
      - 新規ローカル・ユーザーの作成 19
      - セキュリティ設定 37
      - ユーザー・アカウントの削除 21
      - ユーザー・アカウントの構成 17
  - XClarity Controller の機能 プラチナ・レベルの機能
    - プラチナ・レベル 5
  - XClarity Controller へのログイン 12
  - XClarity Provisioning Manager
    - Setup Utility 10

## あ

- アクティブ・システム・イベント 概要 49
- アクティベーション・キー エクスポート 86

- 管理 114
  - 取り付け 85, 114
  - 取り外し 86, 114
- アダプター情報
  - サーバー構成 57
- 新しい役割
  - 作成 18
- アルファベット順のコマンド・リスト 89
- 暗号鍵
  - 集中管理 44

## い

- 一回限り
  - セットアップ 58
- イベント・ウィンドウ
  - log 53-54
- イベント・ログ 53
- イーサネット
  - 構成 112

## え

- エクスポート
  - アクティベーション・キー 86
- エージェントレス・コマンド 140

## お

- オプション
  - SKM 44
- オペレーティング・システム要件 6
- オペレーティング・システムのスクリーン・キャプチャー 70
- 汚染、微粒子およびガス 179
- オンライン資料
  - エラー・コード情報 1
  - 資料更新情報 1
  - ファームウェア更新情報 1
- オープン・ポートの表示 118

## か

- 概要 49
  - ssl 41
    - システム・ガード 45
    - セキュリティ・ダッシュボード 37
    - セキュリティ・モード 37
- 拡張イーサネット
  - 設定 154
  - 設定 29
- 拡張監査ログ
  - 拡張監査ログ 44
- 拡張管理モジュール 1
- 拡張役割ベース・セキュリティ
  - LDAP 134
- ガス汚染 179
- カスタム・サポート Web ページ 173
- 仮想ドライブの表示および構成 77
- 監査ログ 54

- 関数およびコマンド
  - dcmi 62
    - ノード・マネージャー 62

- 管理
  - DDNS 108
  - Features on Demand 114
  - FoD 114
  - MAC アドレス 112
  - SNMPv1 コミュニティー 123
  - アクティベーション・キー 114
  - ユーザー 134

- 管理、電源
  - IPMI コマンドを使用した 61

## く

- クライアント識別名
  - LDAP サーバー 115
- グループ検索属性
  - LDAP 115
- グループ・フィルター
  - LDAP 115
- グローバル・ログイン
  - 設定 23
- グローバル・ログイン設定
  - アカウント・セキュリティ・ポリシーの設定 24

## け

- 現在の表示
  - ユーザー 134
- 検索ドメイン
  - LDAP サーバー 115

## こ

- 構成
  - DDNS 108
  - DDNS 設定 32
  - DNS 108
  - DNS 設定 32
  - Ethernet over USB 110
  - Ethernet over USB 設定 32
  - IPMI 34
  - IPMI over KCS アクセス 43
  - IPv4 112
  - IPv6 112
  - LDAP 115
  - LDAP 設定 25
  - LDAP サーバー 115
  - ports 118
  - security password manager 44
  - Serial-to-SSH リダイレクト 87
  - SNMPv1 123
  - SNMPv1 トラップ 123
  - SNMPv3 アラート設定 33
  - SNMPv3 のユーザー・アカウント 134
  - SSH サーバー 43
  - USB 110
  - イーサネット 112



- イーサネット設定 29, 154
- グローバル・ログイン設定 23
- システム・ガード 45
- システム・ファームウェアの下位レベルの禁止 44
- セキュリティ設定 37
- 前面パネル USB ポートから管理へ 36
- ネットワーク・サービス・ポート 117
- ネットワーク・プロトコル 29
- ブロック・リストと時間制限 35
- ポート割り当て 35
- ユーザー・アカウントあたりの同時ログインの制限 45
- ユーザー・アカウント・セキュリティ・レベル 103
- 構成コマンド 103
- 構成の復元
  - IMM 120
- 構成のリセット
  - BMC 121
- 個別設定したサポート Web ページの作成 173
- コマンド
  - accseccfg 103
  - adapter 149
  - asu 104
  - backup 107
  - batch 138
  - clearlog 92
  - clock 138
  - dbgshbmc 151
  - dhcpinfo 108
  - dns 108
  - encaps 109
  - ethtousb 110
  - exit 91
  - fans 92
  - firewall 110
  - fuelg 102
  - hashpw 112
  - help 91
  - history 91
  - ifconfig 112
  - info 139
  - keycfg 114
  - ldap 115
  - led 93
  - mhlog 92
  - ntp 117
  - portcontrol 117
  - ports 118
  - power 100
  - pxeboot 103
  - rdmout 119
  - readlog 95
  - reset 101
  - restore 120
  - restoredefaults 121
  - roles 120
  - seccfg 122
  - securityinfo 122
  - securitymode 123
  - servicelog 96
  - set 123

- snmp 123
- snmpalerts 126
- sreset 140
- sshcfg 127
- sslcfg 127
- storage 140
- syshealth 97
- syslock 130
- temps 98
- thermal 131
- TLS 132
- trespass 132
- uefipw 133
- usbeth 133
- users 134
- volts 99
- vpd 99
- コマンド、アルファベット順リスト 89
- コマンド、タイプ
  - IMM 制御 138
  - エージェントレス 140
  - 構成 103
  - サポート 150
  - サーバーの電源および再起動 100
  - モニター 92
  - ユーティリティ 91
- コマンド・ライン・インターフェース (CLI)
  - アクセス 87
  - 機能および制限 88
  - コマンド構文 88
  - 説明 87
  - ログイン 87

## さ

- 最小、レベル
  - TLS 132
- 最大伝送単位
  - 設定 112
- 作業
  - イベント・ログのイベント 53
  - 監査ログのイベント 54
- 削除
  - ユーザー 134
- 作成
  - ユーザー・アカウント 134
- サポート Web ページ、カスタム 173
- サポート・コマンド 150
- サーバー
  - 構成オプション 57
- サーバー状況
  - 監視 49
- サーバー管理
  - 一回限り 58
  - サーバー・タイムアウト、設定 65
  - サーバー・ファームウェア 81-82
  - システムのブート順序 57
  - システムのブート・モード 57
- サーバー構成
  - RAID セットアップ 77

- アダプター情報 57
- サーバーのプロパティ 64
  - ストレージの詳細 77
- サーバー状況の監視 49
  - 「サーバー管理」タブ
  - 電源管理オプション 58
- サーバーの構成
  - 構成のオプション
    - サーバー 57
- サーバーのターゲット名
  - LDAP 115
- サーバーの電源および再起動
  - コマンド 100
- サーバーのプロパティ
  - サーバー構成 64
    - ロケーションと連絡先の設定 64
- サーバー・アドレッシング
  - DNS 108
- サーバー・タイムアウト
  - 選択 65
- サーバー・タイムアウトの設定 65
- サーバー・ファームウェア
  - 更新 81-82
- サービスおよびサポート
  - 依頼する前に 173
  - ソフトウェア 175
  - ハードウェア 175
- サービス・データ 174
- サービス・データの収集 174
- サービス・データ・ログ
  - 収集 63
    - ダウンロード 63
- サービス・データ・ログの収集 63

## し

- 識別名、クライアント
  - LDAP サーバー 115
- 識別名、ルート
  - LDAP サーバー 115
- 事項、重要 178
- 時刻
  - 設定 138
- システム使用率 52
  - 表示 52
- システム情報 51
  - 表示 51
- システム・ガード
  - システム・ガード 45
    - 設定 45
- システム・ファームウェアの下位レベルの禁止
  - 構成 44
- 事前構成
  - LDAP サーバー 115
- 自動ネゴシエーション
  - 設定 112
- 集中管理
  - 暗号鍵 44
- 重要な注意事項 178
- 使用

- リモート・コンソール機能 69
- 商標 178
- 証明書管理
  - CIM over HTTPS 127
  - HTTPS サーバー 127
  - LDAP 127
  - SSH サーバー 127
- 新規ローカル・アカウント
  - 作成 19
- 侵入警告メッセージ・オプション 65

## す

- スイッチ
  - セキュリティ・モード 41
- ストレージの構成
  - 構成のオプション
    - ストレージ 77
- ストレージの詳細
  - サーバー構成 77
- ストレージ・インベントリ 79
- ストレージ・デバイス
  - storage コマンド 140

## せ

- 静的 IP アドレス、デフォルト 10
- セキュリティ
  - CIM over HTTPS 127
  - HTTPS サーバー 127
  - LDAP 127
  - SSH サーバー 43, 127
  - SSL 証明書管理 42
  - SSL 証明書の処理 42
  - SSL の概要 41
  - システム・ガードの概要 45
  - セキュリティ・ダッシュボードの概要 37
  - セキュリティ・モードの概要 37
  - セキュリティ・モードの切り替え 41
- セキュリティ・オプション
  - ドライブ・アクセス・タブ 44
- 設定
  - CIM over HTTP ポート 118
  - CIM over HTTPS ポート 118
  - DDNS 32
  - DNS 32
  - Ethernet over USB 32
  - HTTP ポート 118
  - HTTPS ポート 118
  - LDAP 25
  - LDAP サーバー・ポート 115
  - MTU 112
  - SNMP アラート 33
  - SNMP エージェント・ポート 118
  - SNMP トラップ・ポート 118
  - SNMPv1 の連絡先 123
  - SNMPv3 の連絡先 123
  - SSH CLI ポート 118
  - SSH サーバー 43

- Web の非アクティブ・タイムアウト 103
- XClarity Controller の日付と時刻 65
- イーサネット 29
- イーサネット 154
- グローバル・ログイン 23
  - アカウント・セキュリティ・ポリシーの設定 24
- 最大伝送単位 112
- 時刻 138
- システム・ガード 45
- 自動ネゴシエーション 112
- 詳細 29, 45, 154
- セキュリティ 37
- 日付 138
- ブロック・リストと時間制限 35
- ホスト名 112
- ポート割り当て 35
- ユーザー認証方式 103
- リモート・コンソール・ポート 118
- 設定、ポート番号 118

## そ

- ソフトウェアのサービスおよびサポートの電話番号 175
- ソリューション・サービス 65

## た

- 台湾 BSMI RoHS 宣言 180
- 台湾の輸出入お問い合わせ先情報 181
- ターゲット名、サーバー
  - LDAP 115

## ち

- 注記 8, 177

## つ

- 通信規制の注記 179
- ツール
  - IPMItool 153

## て

- デフォルト構成
  - BMC 121
- デフォルトの静的 IP アドレス 10
- 電源
  - IPMI コマンドを使用した監視 61
  - IPMI コマンドを使用した管理 61
- 電源管理
  - dcmi 62
  - IPMI ブリッジ 62
- 電源管理オプション
  - 「サーバー管理」タブ 58
  - 電源キャッピング・ポリシー 59
  - 電源操作 60
  - 電源の冗長性 59

- 電源復元ポリシー 60
- 電源の監視
  - IPMI コマンドを使用した 61
- 電力使用量
  - IPMI コマンド 61
- 電話番号 175

## と

- ドメイン名、DHCP サーバーが指定
  - DDNS 108
- ドメイン名、カスタム
  - DDNS 108
- ドメイン名のソース
  - DDNS 108
- ドライブ・アクセス・タブ
  - セキュリティ・オプション 44
- 取り付け
  - アクティベーション・キー 85, 114
- 取り外し
  - アクティベーション・キー 86, 114

## ね

- ネットワーク接続 10
  - IP アドレス、デフォルトの静的 10
  - 静的 IP アドレス、デフォルト 10
  - デフォルトの静的 IP アドレス 10
- ネットワーク設定
  - IPMI コマンド 34
- ネットワーク・サービス・ポート
  - 構成 117
- ネットワーク・プロトコルのプロパティ
  - DDNS 32
  - DNS 32
  - Ethernet over USB 32
  - IPMI 34
  - IPMI over KCS アクセス 43
  - SNMP アラート設定 33
  - イーサネット設定 29, 154
  - システム・ファームウェアの下位レベルの禁止 44
  - ブロック・リストと時間制限 35
  - ポート割り当て 35

## の

- ノード・マネージャー
  - 関数およびコマンド 62

## は

- バインディング方式
  - LDAP サーバー 115
- パスワード
  - LDAP サーバー 115
  - ユーザー 134
- ハッシュ・パスワード 21
- ハードウェアのサービスおよびサポートの電話番号 175
- ハードウェア・ヘルス 49

## ひ

- 非アクティブな Web セッションのタイムアウト 23
- 日付
  - 設定 138
- 日付と時刻、XClarity Controller
  - 設定 65
- ビデオ・ビューアー
  - スクリーン・キャプチャー 70
  - 電源および再起動コマンド 70
  - ビデオ・カラー・モード 71
- 標準レベル機能 2

## ふ

- ファームウェア
  - 表示、サーバー 99
- ファームウェア、サーバー
  - 更新 81-82
- ファームウェア情報の表示
  - サーバー 99
- フィーチャーのインストール
  - Features on Demand 114
  - FoD 114
- フィーチャーの除去
  - Features on Demand 114
  - FoD 114
- 複数言語サポート 7
- 複数言語のサポート 7
- ブラウザの要件 6
- ブルー・スクリーン・キャプチャー 70
- ブロック・リストと時間制限
  - 設定 35

## へ

- ヘルプ 173
- ヘルプの入手 173
- ベースボード管理コントローラー (BMC) 1

## ほ

- ホスト名
  - LDAP サーバー 115
  - 設定 112
- ポート
  - 構成 118
  - 番号の設定 118
- ポート転送
  - Ethernet over USB 110
- ポート番号
  - LDAP サーバー 115
  - 設定 118
- ポート割り当て
  - 構成 35
  - 設定 35

## め

- メディアのマウント方法 71

- メディアのマウント・エラーに関する問題 75
- メンテナンス履歴 54
- メールおよび syslog 通知 55

## も

- モニター・コマンド 92

## や

- 役割ベース・セキュリティー、拡張
  - LDAP 134

## ゆ

- ユーザー
  - SNMPv3 設定 134
  - SSH 鍵 134
    - 管理 134
    - 現在の表示 134
    - 削除 134
    - パスワード 134
  - ユーザー認証方式 17
    - 設定 103
  - ユーザー・アカウント
    - 削除 21
    - 作成 134
  - ユーザー・アカウントあたりの同時ログインの制限
    - 構成 45
    - ユーザー・アカウントあたりの同時ログインの制限 45
  - ユーザー・アカウント・セキュリティー・レベル
    - 構成 103
  - ユーティリティー・コマンド 91

## よ

- 要件
  - Web ブラウザー 6
  - オペレーティング・システム 6

## ら

- ライセンス管理 85

## り

- リモート電源制御 70
- リモート・アクセス 2
- リモート・コンソール
  - 仮想メディア・セッション 69
  - キーボード・サポート 71
  - スクリーン・キャプチャー 70
  - 電源および再起動コマンド 70
  - ビデオ・ビューアー 69
- リモート・コンソール機能 69
  - 有効化 70
- リモート・コンソールのキーボード・サポート 71
- リモート・コンソールの画面モード 71

リモート・コンソール・セッションの終了 76  
リモート・コンソール・ポート  
設定 118  
粒子汚染 179

## る

ルート識別名

LDAP サーバー 115

## ろ

ログイン許可属性  
LDAP 115  
ログイン試行の認証 17  
ロケーションと連絡先の設定 64





**Lenovo**