Lenovo

Intel Xeon SP (第 1 世代、第 2 世代) を搭載した XClarity Controller

ユーザーズ・ガイド

注：この情報を使用する前に、207 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 15 版 (2021 年 5 月)

目次

第 1 章　概要

Lenovo XClarity Controller (XCC) は、ベースボード管理コントローラー (BMC) を置き換える、Lenovo ThinkSystem サーバー向けの次世代の管理コントローラーです。

Integrated Management Module II (IMM2) サービス・プロセッサーの後継であり、サービス・プロセッサー機能、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・システム・ボード上の単一のチップに統合しています。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 1.0.2 およびスキーマ 2016.2 をサポートします

注：

- 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。
- Flex サーバーの場合、Chassis Management Module (CMM) が、システム管理機能のための 1 次管理モジュールです。XClarity Controller へは、CMM ネットワーク・ポートを経由してアクセスできます。

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 の標準、拡張、およびエンタープライズ・レベル機能

XClarity Controller では、標準、拡張、およびエンタープライズ・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

注：一部の機能は、Flex System サーバーには適用されない場合があります。

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

XClarity Controller の標準レベル機能

以下は、XClarity Controller の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
- CIM-XML
- DCMI 1.5
- SNMPv3
- SNMPv1 (トラップのみ) では、サーバーのタイプに応じて、バージョン 2.10 または 2.12 以降の XCC ファームウェア更新が必要です。詳細については、XCC ファームウェア更新の変更ファイルを参照してください。

その他の管理インターフェース

- Web
- レガシー 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

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、その他)
- 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 ローダー・ウォッチドッグ
- ブルー・スクリーン・キャプチャー (OS 障害)
- 組み込み診断ツール

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
- SNMPv1 (トラップのみ)
- SSL
- SSH
- SMTP
- LDAP クライアント
- NTP
- SLP
- SSDP

アラート

- PET Traps
- CIM 通知
- SNMP トラップ
- メール
- Redfish イベント

シリアル・リダイレクト

- IPMI SOL
- シリアル・ポート構成

セキュリティー

- XClarity Controller Core Root of Trust for Measurement (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
- シャーシ侵入検出 (一部のサーバー・モデルでのみ使用可能)
- UEFI TPM 物理プレゼンスの XCC リモート検出
- 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

リモート・プレゼンス

- カード上のリモート・ディスク (RDOC): CIFS、NFS、HTTP、HTTPS、FTP、SFTP、および LOCAL 経由でのリモート ISO/IMG ファイルの仮想メディア・マウント

電源管理

- リアルタイム電源メーター

ライセンス管理

- アクティベーション・キー検証およびリポジトリー

デプロイメントと構成

- リモート構成
- 組み込み XClarity Provisioning Manager を使用した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

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 の拡張レベル機能

以下は、XClarity Controller の拡張レベル機能のリストです。

XClarity Controller の標準レベルのすべての機能に加えて以下を利用できます:

アラート

- Syslog

リモート・プレゼンス

- リモート KVM

シリアル・リダイレクト

- SSH 経由のシリアル・リダイレクト

セキュリティー

- Security Key Lifecycle Manager (SKLM)
- IP アドレスのブロッキング

電源管理

- リアルタイム電源グラフィックス
- 電源カウンター履歴
- 温度グラフィックス

デプロイメントと構成

- 組み込み XClarity Provisioning Manager と XClarity Controller Remote KVM 機能を使用した リモート OS デプロイメント

XClarity Controller エンタープライズ・レベル機能

以下は、XClarity Controller のエンタープライズ・レベル機能のリストです。

XClarity Controller の標準および拡張レベルのすべての機能に加えて以下を利用できます:

RAS

- ブート・キャプチャー

リモート・プレゼンス

- 品質/帯域幅制御
- 仮想コンソール共有 (6 ユーザー)
- 仮想コンソール・チャット
- 仮想メディア
  - リモート・コンソールからのリモート ISO/IMG ファイルのマウント
  - ネットワークからのファイルのマウント: - ISO または IMG イメージ・ファイルをファイル・サーバー (HTTPS、CIFS、NFS) からホストに DVD または USB ドライブとしてマウントする

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

デプロイメントと構成

- Lenovo XClarity Administrator を使用したリモート・デプロイメント。オペレーティング・システム・デプロイメントに Lenovo XClarity Administrator を使用する場合は、「http://sysmgt.lenovofiles.com/help/index.jsp?topic=%2Fcom.lenovo.lxca.doc%2Fsupported_operating_system_images.html」を参照して、サポートされているオペレーティング・システムの詳細を確認してください。

XClarity Controller のアップグレード

ご使用のサーバーに基本レベルまたは拡張レベルの XClarity Controller ファームウェア機能が付属している場合は、ご使用のサーバーの XClarity Controller 機能をアップグレードできることもあります。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詳しくは、89 ページの 第 8 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 48.0 以上 (リモート・コンソールには 55.0 以上)
- Firefox ESR 38.6.0 以上
- Microsoft Edge
- Safari 9.0.2 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。

セキュリティーを強化するため、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。

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

ご使用のインターネット・ブラウザーのキャッシュには、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、ご使用のブラウザーが情報を 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、ブラウザー・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、ブラウザーによって判別される言語で表示されます。ブラウザー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・プロセッサー機能、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。XClarity Controller Web インターフェースを使用してリモートから XClarity Controller にアクセスするには、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:efff: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・コネクターを使用します。

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。

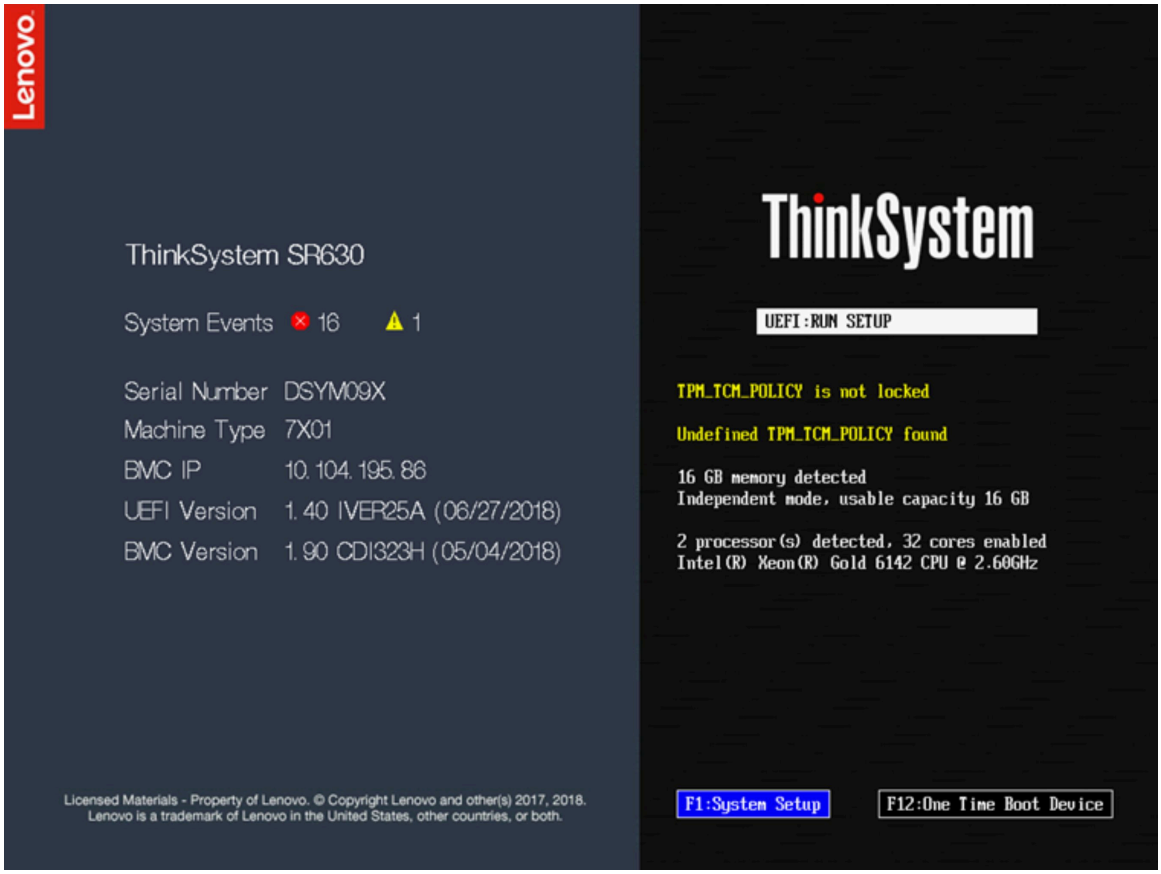
XClarity Provisioning Manager による XClarity Controller のネットワーク接続のセットアップ

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。



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。

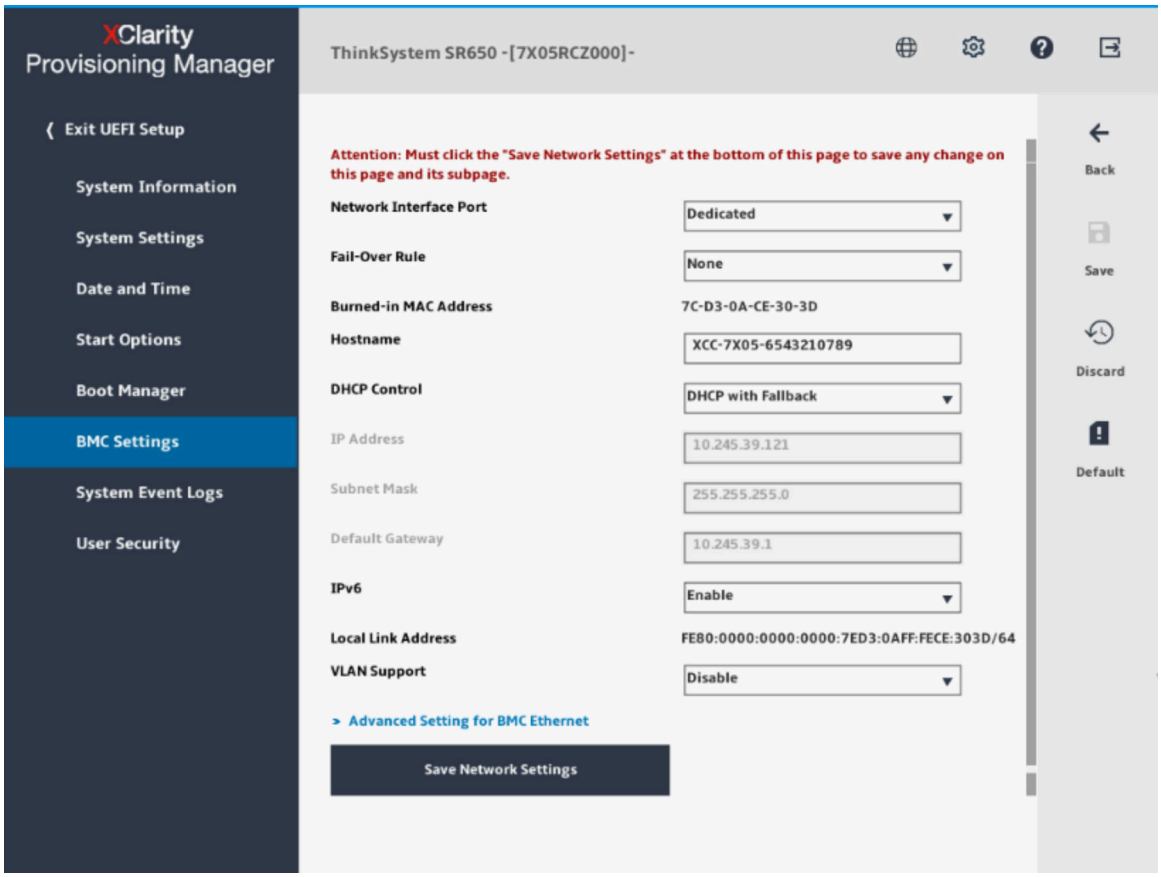
ステップ 3. XClarity Provisioning Manager のメインメニューから「**UEFI Setup**」を選択します。

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



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・コネクター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。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。

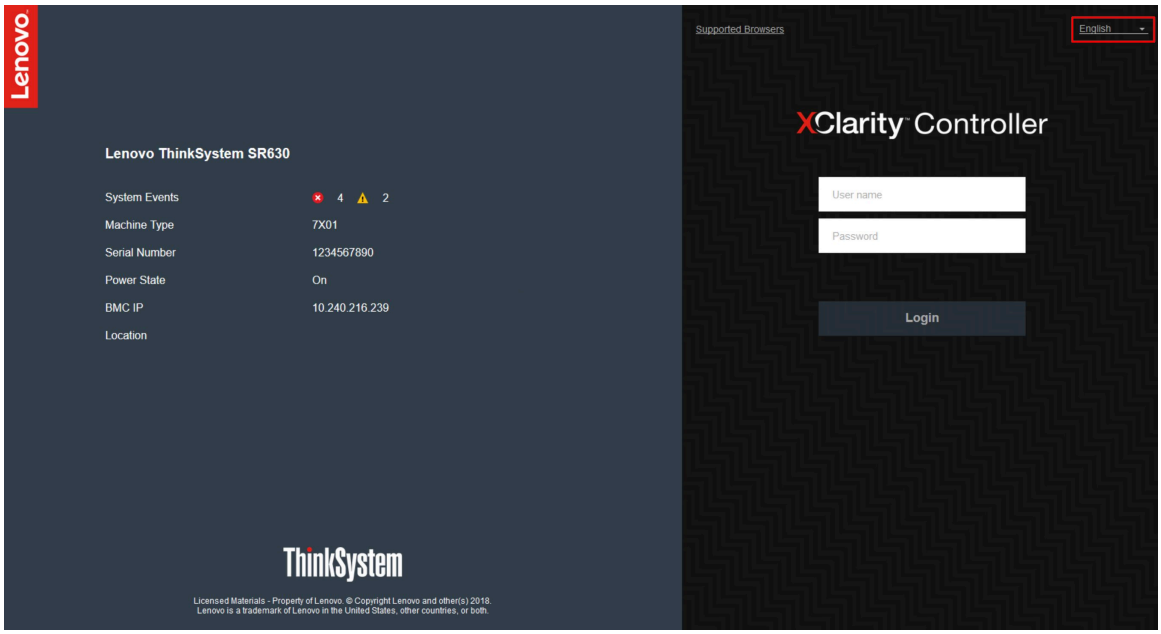
注：Flex System では、XClarity Controller のユーザー・アカウントは、Flex System Chassis Management Module (CMM) によって管理でき、上記の USERID/PASSW0RD の組み合わせとは異なる場合があります。

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、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。

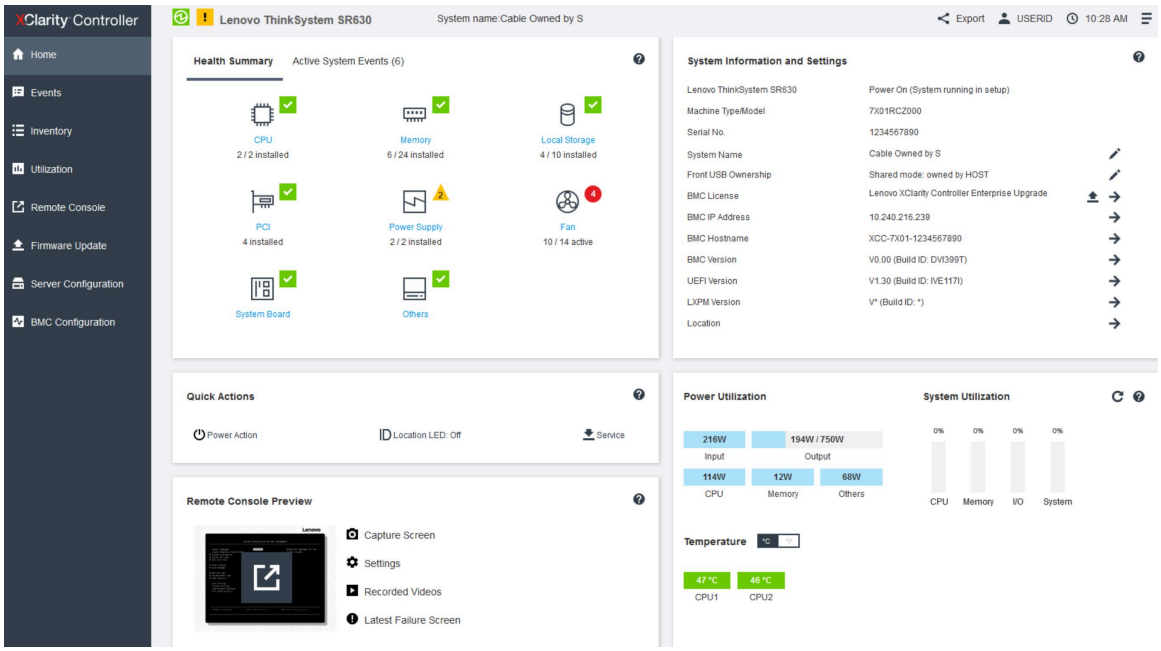
次の図にログイン・ウィンドウを示します。



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 1 を示すアイコンとともに表示されます。



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

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。

表 1. XClarity Controller の機能

XClarity Controller Web インターフェースから実行できる操作を説明する 3 列の表。

表 1. XClarity Controller の機能 (続き)

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/システム使用率/温度	現行の電力使用量、システム使用率、サーバー全体の温度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。右のツールバーには、以下のクイック操作が含まれています。 • キャプチャー画面 • 設定 • 録画済みビデオ • 最新の障害画面
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	Lenovo 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、IT システムの認証および管理を追跡および文書化できます。
	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	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。
インベントリー		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の詳細については、SMM2 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、システム・サブシステム使用率、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。
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。

表 1. XClarity Controller の機能 (続き)

タブ	選択	説明
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た USB ディスク・ドライブのように表示されます。
ファームウェア更新		• ファームウェア・レベルを表示します。 • 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。
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	• 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。 • ブート・モードおよびブート順序の設定を変更します。
	電源ポリシー	• 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。 • 電源キャッピング・ポリシーを構成します。 • 電源復元ポリシーを構成します。 **注：**ソリューションの電源ステータスの詳細については、SMM2 Web インターフェースを参照してください。
	サーバーのプロパティ	• 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。 • サーバー・ハングを検出してリカバリーするために、サーバーの起動タイムアウトを管理します。 • 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。
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。
	セキュリティー	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	• 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。 • 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。 • 「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。

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**」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

新規ユーザー・アカウントを作成するには、「**作成**」をクリックします。

以下のフィールドに入力します。「**ユーザー名**」、「**パスワード**」、「**パスワードの確認**」、「**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。

ユーザー権限レベル

以下のユーザー権限レベルが選択可能です。

スーパーバイザー
スーパーバイザー ユーザー権限レベルには、一切の制限がありません。

読み取り専用
読取り専用 ユーザー権限レベルには読み取り専用アクセス権限がありますが、ファイルの転送や電源と再起動の操作、またはリモート・プレゼンス機能などの操作を行うことはできません。

カスタム
カスタム ユーザー権限レベルでは、ユーザーが実行できる操作の設定で、よりカスタム化されたユーザー権限のプロファイルを使用できます。

以下の カスタム ユーザー権限レベルのうち 1 つ以上を選択してください。

アダプター構成 - ネットワーキングおよびセキュリティー
ユーザーは、「セキュリティー」、「ネットワーク」、「シリアル・ポート」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。

アダプター構成 - 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。

アダプター構成 - 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。

ユーザーが XClarity Controller ログイン ID の権限レベルを設定すると、対応する IPMI ユーザー ID の IPMI 特権レベルが以下の優先順位に従って設定されます。

- ユーザーが XClarity Controller ログイン ID の権限レベルを「**スーパーバイザー**」に設定すると、IPMI 特権レベルは「管理者」に設定されます。
- ユーザーが XClarity Controller ログイン ID の権限レベルを「**読み取り専用**」に設定すると、IPMI 特権レベルは「ユーザー」に設定されます。
- ユーザーが XClarity Controller ログイン ID の権限レベルを以下のいずれかのタイプのアクセス権限に設定すると、IPMI 特権レベルは「管理者」に設定されます。
  - ユーザー・アカウント管理アクセス
  - リモート・コンソール・アクセス
  - 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
  - アダプター構成 - ネットワーキングおよびセキュリティー
  - アダプター構成 - 拡張
- ユーザーが XClarity Controller ログイン ID の権限レベルを「**リモート・サーバーの電源/再起動アクセス**」または「**イベント・ログをクリアする権限**」に設定すると、IPMI 特権レベルは「オペレーター」に設定されます。
- ユーザーが XClarity Controller ログイン ID の権限レベルを「**アダプター構成 - 基本**」に設定すると、IPMI 特権レベルは「ユーザー」に設定されます。

SNMPv3 設定

ユーザーの SNMPv3 アクセスを有効にするには、「**SNMPv3 設定**」の横のチェック・ボックスを選択します。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。

トラップのアドレス
ユーザーのトラップ宛先を指定します。これは、IP アドレスまたはホスト名を指定することができます。トラップを使用して、SNMP エージェントは管理ステーションにイベントを通知します (たとえば、プロセッサー温度が制限を超過した場合)。

認証プロトコル
「HMAC-SHA」のみが認証プロトコルとしてサポートされます。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。

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。サポートされる方式は、「CBC-DES」および「AES」です。

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「*111111111*」(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。

詳細については、インターネット標準 RFC 3414 文書 (https://tools.ietf.org/html/rfc3414) の 72 ページ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、「**SSH 鍵**」の横のチェック・ボックスを選択します。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：

- 一部の Lenovo 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。この一時アカウントは表示できず、12 個のローカル・ユーザー・アカウントの位置のいずれも使用しません。アカウントは、ランダムなユーザー名 (たとえば「20luN4SB」) とパスワードを使用して作成されます。このアカウントは、Ethernet over USB 内部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され、CIM-XML および SFTP インターフェース専用です。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。
- SNMPv3 エンジン ID では、XClarity Controller は 16 進数の文字列により ID が表されます。この 16 進数の文字列は、デフォルトの XClarity Controller のホスト名から変換されます。次の例を参照してください。

  ホスト名「XCC-7X06-S4AHJ300」は、最初に次の ASCII 形式に変換されます: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  この 16 進数の文字列は、ASCII 形式により作成されます (間のスペースは無視してください): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

ユーザー・アカウントの削除

ローカル・ユーザー・アカウントを削除するには、このトピックの情報を使用します。

ローカル・ユーザー・アカウントを削除するには、削除するアカウントの行にあるゴミ箱アイコンをクリックします。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ます。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。

認証用にハッシュド・パスワードを使用

このトピックでは、認証にハッシュド・パスワードを使用する方法について説明します。

パスワードと LDAP/AD ユーザー・アカウントの使用に加えて、XClarity Controller では認証用にサード・パーティーのハッシュド・パスワードもサポートされます。この特別なパスワードでは、1 方向のハッシュ (SHA256) 形式を使用し、XClarity Controller Web、OneCLI、および CLI インターフェースでサポートされます。ただし、XCC SNMP、IPMI、および CIM インターフェースの認証では、サード・パーティーのハッシュド・パスワードはサポートされないことに注意してください。OneCLI ツールおよび XCC CLI インターフェースでのみ、ハッシュド・パスワードによる新しいアカウントの作成やハッシュの更新が可能です。XClarity Controller ではまた、OneCLI ツールおよび XClarity Controller CLI インターフェースにより、ハッシュド・パスワードの読み取り機能が有効である場合に、ハッシュド・パスワードを取得することもできます。

XClarity Controller Web を介したハッシュド・パスワードの設定

「**BMC 構成**」の「**セキュリティー**」をクリックし、「**Security Password Manager**」セクションまでスクロールして、サード・パーティー・パスワード機能を有効または無効にします。有効にした場合、ログイン認証にサード・パーティーのハッシュド・パスワードが使用されます。また、XClarity Controller からのサード・パーティーハッシュドの検索も無効または有効にできます。

注：デフォルトで、*サード・パーティーのパスワード*および*サード・パーティーのパスワードの取得*機能は無効です。

ユーザー・パスワードが*ネイティブ*または*サード・パーティーのパスワード*のいずれであるかをチェックするには、「**BMC 構成**」で「**ユーザー/LDAP**」をクリックし、詳細を確認します。この情報は、**Advanced Attribute (詳細な属性)**」列に表示されます。

注：

- サード・パーティーのパスワードである場合、ユーザーはパスワードを変更できず、「**パスワード**」および「**パスワードの確認**」フィールドはぼかし表示になります。
- 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 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  $ 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 Passw0rd123abc
  ```

```
$ 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るまで、元の標準パスワード *Passw0rd123abc* 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るまで、元の標準パスワード *Passw0rd123abc* 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使用します。

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使用します。

「**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はクローズされません。

アカウント・セキュリティー・ポリシーの設定

サーバーのアカウント・セキュリティー・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。

注：Flex System では、アカウントのセキュリティー・ポリシーの設定は Flex System Chassis Management Module (CMM) が管理するため、XCC では変更できません。アカウント・セキュリティー・ポリシーの構成に CMM を使用する場合、以下のことに注意してください。

- XCC とは異なり、CMM には*「パスワード失効の警告期間 (日数)」*設定はありません。*パスワードの有効期限までの期間*の CMM での構成が 5 日間より長い場合、XCC ではパスワード失効の警告期間が 5 日間に設定されます。逆に、5 日間より短い設定の場合、パスワード失効の警告期間は、*パスワードの有効期限までの期間*に入力された値と同じになります。
- *最大ログイン失敗数 (回数)* の CMM の設定範囲は 0 ～ 100 回です。ただし、XCC で定義される範囲は 0 ～ 10 回です。したがって、CMM でユーザーが 10 回を超える値を選択すると 、XCC では最大ログイン失敗数が依然として 10 回に設定されます。
- *パスワード変更の最小間隔 (時間)*の CMM の設定範囲は、0 ～ 1440 時間です。ただし、XCC で定義される範囲は 0 ～ 240 時間です。したがって、ユーザーが CMM で 240 時間を超える値を選択すると、XCC ではパスワード変更の最小間隔が 240 時間に設定されます。

セキュリティー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。

次回ログイン時にアカウント・パスワードの変更を指定
最初にログインに成功した後にデフォルトの USERID プロファイルをリセットするために、製造オプションが提供されます。このチェック・ボックスを有効にした場合、アカウントを使用するには、事前にデフォルトのパスワードを変更する必要があります。新規パスワードには、アクティブなすべてのパスワード実施規則が適用されます。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る。
  - 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 32 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 ～ 32 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。0 ～ 30 日までの値がサポートされます。このフィールドのデフォルト値は 14 日です。

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。この値が 0 に設定されている場合、警告は送信されません。0 ～ 30 日までの値がサポートされます。このフィールドのデフォルト値は 14 日です。

最小パスワード長
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。このフィールドでは、8 から 32 文字までがサポートされます。このフィールドのデフォルト値は 10 です。

最短パスワード再利用サイクル
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。最大 10 回前までのパスワードを比較することができます。0 を選択すると、以前に使用したすべてのパスワードを再使用できます。0 から 10 までの値がサポートされます。このフィールドのデフォルト値は 5 です。

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。0 から 240 時間までの値がサポートされます。このフィールドのデフォルト値は 1 時間です。

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。0 から 10 までの値がサポートされます。このフィールドのデフォルト値はログイン失敗 5 回です。

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。0 から 2,880 分までの値がサポートされます。このフィールドのデフォルト値は 60 分です。

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 アプリケーション・モード (Windows 2003 Server)
- Microsoft Lightweight Directory Service (Windows 2008、Windows 2012)
- Novell eDirectory Server、バージョン 8.7、8.8、および 9.4
- OpenLDAP サーバー 2.1、2.2、2.3、および 2.4

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、IBMRBSPermissions ストリングを使用して、各ユーザー・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。グループ名と特権は「Active Directory 設定」セクションで構成できます。
   - **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 4 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。このフィールドをブランクのまま残した場合、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、このフィールドはブランク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ー (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、38 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**」以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。

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。

- **資格情報不要**

  識別名 (DN) やパスワードを使用せずにバインドするには、この方式を使用します。ほとんどのサーバーは特定のユーザー・レコードに対する検索要求を許可しないように構成されているため、この方式を使用しないことを強く推奨します。

- **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。

初回のバインドが成功すると、LDAP サーバーでログインするユーザーに属するエントリーの検索が実行されます。必要であれば、2 回目のバインドが試行されます。今回は、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、「**資格情報不要**」か「**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。

ルート識別名 (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。

UID 検索属性

バインディング方式が「**資格情報不要**」または「**構成済み資格情報を使用**」に設定されている場合、LDAP サーバーへの初回バインドの直後に、ユーザーの DN、ログイン許可、およびグループ・メンバーシップなど、ユーザーに関する固有の情報を取得する検索要求が行われます。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「**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。このフィールドをブランクのまま残した場合、デフォルトは「**uid**」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 つにユーザーが属している必要があります。「**グ**

ループ・フィルター」フィールドがブランク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・メンバーシップのネストは、Active Directory 環境でのみサポートされます。たとえば、ユーザーが GroupA および GroupB のメンバーで、GroupA が GroupC のメンバーである場合、ユーザーは GroupC のメンバーでもあると見なされます。ネストされた検索は、128 個のグループを検索すると停止します。1 つのレベル内のグループが、その下位レベルのグループの前に検索されます。ループは検出されません。

グループ検索属性

Active Directory 環境または Novell eDirectory 環境では、「**グループ検索属性**」フィールドは、ユーザーの所属先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 環境では、この属性名は「**memberOf**」です。eDirectory 環境では、この属性名は「**groupMembership**」です。OpenLDAP サーバー環境では、通常、ユーザーは「objectClass」が PosixGroup である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。このフィールドがブランクのまま残されると、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。このフィールドをブランクのまま残した場合、ユーザーにはデフォルトの読み取り専用許可が割り当てられ、ユーザーはユーザー認証とグループ認証に合格するものと想定されます。
LDAP サーバーから返される属性値は、キーワード・ストリング IBMRBSPermissions= を使用して検索されます。このキーワード・ストリングの直後には、12 個の連続した 0 または 1 として入力されたビット・ストリングが続いている必要があります。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、右端のビットはビット位置 11 です。ビット位置が 1 の場合、そのビット位置に関連付けられた機能が有効にされています。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。
ストリング IBMRBSPermissions=010000000000 は有効な例です。「IBMRBSPermissions=」キーワードを使用すると、このフィールドの任意の位置に配置することが可能になります。これにより、LDAP 管理者は既存の属性を再使用することが可能になるため、LDAP スキーマの拡張を防ぎます。また、これによって属性を元の目的で使用することができるようになります。このフィールドの任意の場所にキーワード・ストリングを追加することができます。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 2. 許可ビット

ビット位置の説明を含む 3 列の表。

表 2. 許可ビット (続き)

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	ネットワーキングおよびセキュリティー	ユーザーは、「セキュリティー」、「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	Basic Adapter Configuration	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	Advanced Adapter Configuration	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、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アダプター構成の変更と復元、および XClarity Controller の再起動とリセットなどの拡張機能を実行できます。
11	予約済み	このビット位置は、将来の使用のために予約済みです。セットされたビットがない場合、ユーザーは読み取り専用権限を持ちます。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ります。 ログイン許可属性がユーザーのレコードに入っていない場合は、そのユーザーが属するグループから許可を取り出そうと試みられます。これは、グループ認証フェーズの一部として行われます。このユーザーには、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。

表 2. 許可ビット (続き)

ビット位置	機能	説明
		読み取り専用アクセス権限ビット (位置 2) は、他のすべてのビットがゼロに設定された場合にのみ設定されます。「常に拒否」ビット (位置 0) がいずれかのグループに設定されている場合、そのユーザーはアクセスを拒否されます。「常に拒否」ビット (位置 0) は、常に他のすべてのビットに優先します。

いずれのビットも設定されていない場合、デフォルトではユーザーに「**読み取り専用**」が設定されます。

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。

注：ユーザーに基本、ネットワーキング、および/またはセキュリティー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。

3. 「**Active Directory 設定**」で「**Active Directory ユーザーを使用可能にするための拡張役割ベース・セキュリティーを有効にする**」かどうかを選択 (「**認証と承認に LDAP サーバーを使用する**」モードが使用されている場合) するか、「**ローカル承認用グループ**」を構成 (「**認証のみに LDAP サーバーを使用する**」 (「**ローカル承認**」) モードが使用されている場合) します。

   - **Active Directory ユーザーを使用可能にするための拡張役割ベース・セキュリティーを有効にする**:

     拡張役割ベース・セキュリティー設定が有効になっている場合、自由な形式のサーバー名がその特定の XClarity Controller のターゲット名として機能するように構成する必要があります。ターゲット名は、役割ベース・セキュリティー (RBS) のスナップインを使用して Active Directory サーバー上の 1 つ以上の役割に関連付けることができます。これは、管理対象ターゲットを作成し、それらに固有の名前をつけて適切な役割に関連付けることで実現されます。このフィールドに名前が構成されている場合、ユーザーおよび同じ役割のメンバーである XClarity Controller (ターゲット) に特定の役割を定義することができます。ユーザーが XClarity Controller にログインし、Active Directory 経由で認証されると、このユーザーがメンバーである役割がディレクトリーから取得されます。ユーザーに割り当てられる権限は、メンバーとしてここで構成されたサーバー名と一致するターゲットがあるか、任意の XClarity Controller に一致しているターゲットがある役割から抽出されます。複数の XClarity Controller で同じターゲット名を共有できます。これは、たとえば、複数の XClarity Controller を 1 つのグループにして、単一の管理対象ターゲットを使用してそれを同じ役割に割り当てるために使用できます。逆に、各 XClarity Controller には固有の名前を指定できます。

   - **ローカル承認用グループ**

     グループ名は、ユーザーのグループに対するローカル承認の指定を提供するために構成されます。各グループ名は、上記の表で説明されているものと同じ権限 (役割) を割り当てることができます。LDAP サーバーは、ユーザーをグループ名と関連付けます。ユーザーがログインする際には、ユーザーが属するグループに関連付けられたアクセス権限が割り当てられます。追加グループは、「+」アイコンをクリックして構成できます。また、「x」アイコンをクリックして削除できます。

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。

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、USBLAN インターフェースや、サーバーの前面にある 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いてはなりません。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いてはなりません。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いてはなりません。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。

注：Flex System では、VLAN 設定は Flex System CMM が管理するため、XClarity Controller では変更できません。

仮想 LAN (VLAN) タグ付けを有効にするには、「**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 選択**」リストから、以下のいずれかの選択項目を選択します。

- 出荷時書き込み 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 `FFFFFFFFFFFF` 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。

「**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。最大伝送単位の範囲は 60 から 1500 までです。このフィールドのデフォルト値は 1500 です。

IPv6 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。

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。

注：Flex System では、DNS 設定を XClarity Controller で変更することはできません。DNS 設定は CMM が管理します。

「**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。

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、Linux または Windows フラッシュ・ユーティリティーを使用する 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。

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 に IPv4 リンク・ローカル・アドレスを使用する**: 169.254.0.0/16 の範囲にある IP アドレスが XClarity Controller およびネットワークのサーバー側に割り当てられます。
- **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：

1. 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。
2. 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。

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. **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。
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. 「**コミュニティー名**」フィールドに、コミュニティー名を入力します。名前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。

IPMI ネットワーク・アクセスの有効化または無効化

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。

「**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。IPMI 設定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。

IPMI over LAN アクセス
スイッチをクリックして、XClarity Controller への IPMI ネットワーク・アクセスを有効または無効にします。

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、セキュリティー向上のために、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が、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。

Web
ポート番号は 80 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。

Web over HTTPS
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。

REST over HTTPS

ポート番号は、Web over HTTPS フィールドに指定した番号に自動的に変更されます。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。

CIM over HTTP
このフィールドで、CIM over HTTP のポート番号を指定します。デフォルト値は 5989 です。

注：CIM は、デフォルトでは使用不可に設定されています。

Remote Presence
このフィールドで、リモート・プレゼンスのポート番号を指定します。デフォルト値は 3900 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：IPMI は、デフォルトでは使用不可に設定されています。

SFTP
このフィールドで、SSH ファイル転送プロトコル (SFTP) に使用するポート番号を指定します。ポート番号は 115 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：OneCLI インバンド更新には IMM.SFTPPortControl=open が必要です。

SLP
このフィールドで、SLP に使用するポート番号を指定します。ポート番号は 427 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：XClarity Controller が報告するサービス・タイプは 2 つあります。

- サービス: 管理ハードウェア。Lenovo: Lenovo-XClarity Controller
- サービス: wbem

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。

SNMP Traps
このフィールドで、SNMP トラップに使用するポート番号を指定します。デフォルト値は 162 です。有効なポート番号の値は、1 から 65535 までです。

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、コンマ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に 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。

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。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。

「**BMC 構成**」の下にある「**ネットワーク**」をクリックして XClarity Controller の前面パネル USB ポートから管理への設定を表示または変更します。

4 タイプの設定から選択できます。

ホスト専用モード
前面パネル USB ポートは常にサーバーにのみ接続されます。

BMC 専用モード
前面パネル USB ポートは常に XClarity Controller にのみ接続されます。

共用モード: BMC 所有
前面パネル USB ポートはサーバーと XClarity Controller の両方で共有されますが、ポートは XClarity Controller に切り替えられます。

共用モード: ホスト所有
前面パネル USB ポートはサーバーと XClarity Controller の両方で共有されますが、ポートはホストに切り替えられます。

モバイル・アプリについて詳しくは、以下のサイトを参照してください。

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

注：

- 前面パネル USB ポートが共用モードに構成されている場合、ポートは電源がない場合は XClarity Controller に、電源がある場合はサーバーに接続されます。電源がある場合は、前面パネル USB ポートの制御はサーバーと XClarity Controller 間でどちらにも切り替えることができます。共用モードでも、前面パネル識別ボタン (計算ノードでは USB 管理ボタンの場合があります) を 3 秒以上押し続けることで、ポートをホストと XClarity Controller 間で切り替えることができます。
- 共用モードに構成されていて、USB ポートが現在サーバーに接続されている場合、XClarity Controller で、前面パネル USB ポートを切り替えて XClarity Controller に戻す要求をサポートできます。この要求が実行されると、前面パネル USB ポートは、非アクティブ・タイムアウトで指定された期間 XClarity Controller に対する USB アクティビティーがない状態になるまで、XClarity Controller に接続されたままになります。

セキュリティー設定の構成

セキュリティー・プロトコルを構成するには、このトピックの情報を使用します。

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、ブラウザーや管理アプリケーションで必要であれば、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、152 ページの「tls コマンド」を参照してください。

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

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ついて説明します。

SSL は、自己署名証明書と一緒に使用するか、第三者証明機関によって署名された証明書と一緒に使用することができます。SSL の使用には、自己署名証明書の使用が最も単純な方法ですが、この方法では小さなセキュリティー・リスクが発生します。そのリスクは、SSL クライアントと SSL サーバーの間で試みられる最初の接続で、SSL クライアントに SSL サーバーの ID を検証する手段がないために発生します。たとえば、第三者が XClarity Controller Web サーバーの偽名を使用し、実際の XClarity Controller Web サーバーとユーザーの Web ブラウザーの間で送受信されるデータを傍受することが可能です。ブラウザーと XClarity Controller の間の初回接続時に、自己署名証明書がブラウザー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ーではセキュアです。

より完全なセキュリティーを実現するには、証明機関 (CA) が署名する証明書を使用できます。署名付き証明書を取得するには、「**証明書署名要求 (CSR) の生成**」を選択する必要があります。「**証明書署名要求 (CSR) のダウンロード**」を選択して、証明書署名要求 (CSR) を CA に送信し、署名済み証明書を入手します。署名済み証明書を受領したら、「**署名済み証明書のインポート**」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 XClarity Controller のデジタル署名が含まれます。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、ブラウザーは証明書を検証することができ、確実に XClarity Controller の Web サーバーを識別できます。

XClarity Controller には、HTTPS サーバー、CIM over HTTPS、およびセキュア LDAP クライアントに使用する証明書が必要です。さらに、セキュア LDAP クライアントには、1 つ以上のトラステッド証明書もインポートする必要があります。トラステッド証明書は、セキュア LDAP クライアントが LDAP サーバーを確実に識別するために使用されます。トラステッド証明書は、LDAP サーバーの証明書に署名した CA の証明書です。LDAP サーバーが自己署名証明書を使用する場合、トラステッド証明書を LDAP サーバー自体の証明書とすることもできます。構成の中で複数の LDAP サーバーを使用する場合は、追加のトラステッド証明書をインポートする必要があります。

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「**セキュリティー**」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 (www.openssl.org) などのサード・パーティー製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、「**鍵の再生成**」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。

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、セキュリティー向上のために、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・ファームウェアの下位レベルを防止します。

この機能を有効または無効にするには、「**BMC 構成**」の下にある「**ネットワーク**」をクリックします。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。

物理プレゼンスの検出

物理的にサーバーを操作する作業を行わず XClarity Controller Web ページから物理プレゼンスの検出および検出の解消を行うには、このトピックの情報を使用します。

この機能は、「**物理プレゼンス・ポリシー**」が UEFI により有効になっている場合にのみ使用できます。有効にすると、「**BMC 構成**」の下の「**セキュリティー**」をクリックして、物理プレゼンス機能にアクセスできます。

セキュリティー鍵管理 (SKM) の構成

セキュリティー・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。

XClarity Controller はネットワークを使用して鍵管理サーバーから鍵を取得するため、鍵管理サーバーは、XClarity Controller からアクセス可能である必要があります。XClarity Controller は、鍵管理サーバーと要求される ThinkSystem サーバー間の通信チャネルを提供します。XClarity Controller ファームウェアは、各構成済み鍵管理サーバーと接続を試み、正常な接続が確立されると停止します。

XClarity Controller は、以下の条件が満たされる場合に鍵管理サーバーとの通信を確立します。

- 1 つ以上の鍵管理サーバーのホスト名/IP アドレスが XClarity Controller で構成されている。
- 鍵管理サーバーとの通信に必要な 2 つの証明書 (クライアントおよびサーバー) が XClarity Controller にインストールされている。

注：デバイスに対して少なくとも 2 つ (1 次および 2 次) の鍵管理サーバーを同じプロトコルで構成します。1 次鍵管理サーバーが XClarity Controller からの接続試行に応答しない場合、正常な接続が確立されるまで他の鍵管理サーバーに対して接続試行が実行されます。

トランスポート層セキュリティー (TLS) の接続が XClarity Controller と鍵管理サーバー間で確立されている必要があります。XClarity Controller は、鍵管理サーバーから送信されたサーバー証明書と、事前に XClarity Controller の信頼ストアにインポートされた鍵管理サーバー証明書を比較することで、鍵管理サーバーを認証します。鍵管理サーバーでは、通信する各 XClarity Controller を認証し、XClarity Controller が鍵管理サーバーにアクセスする権限があるかどうかを確認するために検査します。この認証

は、XClarity Controller が送信するクライアント証明書と、鍵管理サーバーに保管されたトラステッド証明書のリストを比較することで行われます。

少なくとも 1 つの鍵管理サーバーに接続され、デバイス・グループはオプションと見なされます。鍵管理サーバー証明書はインポートする必要があり、クライアント証明書は指定する必要があります。デフォルトでは、HTTPS 証明書が使用されます。これを置き換える場合は、新規で生成できます。

注：KMIP サーバー (KeySecure および CipherTrust) を接続するには、証明書署名要求 (CSR) を生成する必要があります。その共通名は、KMIP サーバーで定義されているユーザー名と一致する必要があります。その後、CSR のために、KMIP サーバーによって信頼されている証明機関 (CA) によって署名された証明書をインポートします。

鍵管理サーバーの構成

鍵管理サーバーのホスト名または IP アドレス、および関連するポート情報を作成するには、このトピックの情報を使用します。

鍵管理サーバーの構成セクションは、次のフィールドで構成されます。

ホスト名または IP アドレス
このフィールドに、鍵管理サーバーのホスト名 (DNS が有効であり構成されている場合) または IP アドレスを入力します。サーバーを 4 つまで追加できます。

ポート
このフィールドに、鍵管理サーバーのポート番号を入力します。このフィールドをブランクのまま残した場合、デフォルト値 5696 が使用されます。有効なポート番号の値は、1 から 65535 までです。

デバイス・グループの構成

SKLM サーバーで使用されるデバイス・グループを構成するには、このトピックの情報を使用します。

SKLM サーバーでは、デバイス・グループを使用して、複数のサーバーの自己暗号化ドライブ (SED) の鍵をグループとして管理できます。同じ名前のデバイス・グループを、SKLM サーバーでも作成する必要があります。

デバイス・グループ・セクションには、以下のフィールドがあります。

デバイス・グループ
デバイス・グループを使用して、複数のサーバーの SED の鍵をグループとして管理できます。同じ名前のデバイス・グループを、SKLM サーバーでも作成する必要があります。このフィールドのデフォルト値は IBM_SYSTEM_X_SED です。

証明書管理の設定

このトピックでは、クライアントおよびサーバー証明書管理について説明します。

クライアント証明書およびサーバー証明書は、SKLM サーバーと ThinkSystem サーバーにある XClarity Controller 間の通信を認証するために使用されます。クライアントおよびサーバー証明書の管理が、このセクションで説明されています。

クライアント証明書管理

このトピックでは、クライアント証明書管理について説明します。

クライアント証明書は以下のいずれかに分類されます。

- XClarity Controller 自己署名証明書。
- XClarity Controller の証明書署名要求 (CSR) で生成され、サード・パーティー CA によって (外部) 署名された証明書。

クライアント証明書は SKLM サーバーとの通信に必要です。クライアント証明書には、CA および XClarity Controller のデジタル署名が含まれます。

注：

- 証明書は、ファームウェア更新をまたいで保持されます。
- クライアント証明書が SKLM サーバーとの通信で作成されていない場合、XClarity Controller では HTTPS サーバー証明書が使用されます。
- CA の機能は、XClarity Controller の ID を検査することです。

クライアント証明書を作成するには、プラス・アイコン ( ) をクリックして以下の項目の 1 つを選択します。

- 新しい鍵と自己署名証明書の生成
- 新しい鍵と証明書署名要求 (CSR) の生成

「**新しい鍵と自己署名証明書の生成**」操作項目は、新しい暗号鍵および自己署名証明書を生成します。「新しい鍵と自己署名証明書の生成」ウィンドウで、必須フィールドおよび構成に適用されるオプション・フィールドに情報を入力するか選択します (次の表を参照)。「**OK**」をクリックして暗号鍵と証明書を生成します。自己署名証明書の生成中は進行状況ウィンドウが表示されます。証明書が正常にインストールされると、確認ウィンドウが表示されます。

注：既存の鍵および証明書は、新しい暗号鍵および証明書に置き換えられます。

表 3. 新しい鍵と自己署名証明書の生成

「新しい鍵と自己署名証明書の生成」操作の必須フィールドおよびオプション・フィールドを示す見出し付きの 2 列の表。最下部の行は両方の列にまたがっています。

フィールド	説明
国[1]	リスト項目から、BMC が物理的に存在する国を選択します。
都道府県[1]	BMC が物理的に存在している都道府県を入力します。
市区町村または地域[1]	BMC が物理的に存在している市区町村または地域を入力します。
企業名[1]	BMC を所有する企業名または組織名を入力します。
BMC ホスト名[1]	Web アドレス・バーに表示される BMC ホスト名を入力します。
担当責任者名	BMC の担当責任者名を入力します。
メール・アドレス	BMC の担当責任者のメール・アドレスを入力します。
組織単位	BMC を所有する企業内の組織単位を入力します。
姓	BMC の責任担当者の姓を入力します。このフィールドには、最大 60 文字を入力できます。
名	BMC の責任担当者の名を入力します。このフィールドには、最大 60 文字を入力できます。
イニシャル	BMC の責任担当者のイニシャルを入力します。このフィールドには、最大 20 文字を入力できます。
DN 修飾子	BMC の識別名修飾子を入力します。このフィールドには、最大 60 文字を入力できます。
1. これは必須フィールドです。	

クライアント証明書が生成されたら、「**証明書のダウンロード**」操作項目を選択して、XClarity Controller のストレージに証明書をダウンロードできます。

「**新しい鍵と証明書署名要求 (CSR) の生成**」操作項目は、新しい暗号鍵および CSR を生成します。「新しい鍵と証明書署名要求の生成」ウィンドウで、必須フィールドおよび構成に適用されるオプション・フィールドに情報を入力するか選択します (次の表を参照)。「**OK**」をクリックして新しい暗号鍵と CSR を生成します。

CSR の生成中は進行状況ウィンドウが表示され、正常に完了すると確認ウィンドウが表示されます。CSR の生成後、CSR を CA に送信してデジタル署名を取得する必要があります。「**証明書署名要求 (CSR) のダウンロード**」操作項目を選択して「**OK**」をクリックし、CSR をサーバーに保存します。その後、署名のために CSR を CA に送信できます。

表 4. 新しい鍵および証明書署名要求の生成

「新しい鍵および証明書署名要求の生成」操作の必須フィールドおよびオプション・フィールドを示す見出し付きの 2 列の表。最下部の行は両方の列にまたがっています。

フィールド	説明
国[1]	リスト項目から、BMC が物理的に存在する国を選択します。
都道府県[1]	BMC が物理的に存在している都道府県を入力します。
市区町村または地域[1]	BMC が物理的に存在している市区町村または地域を入力します。
企業名[1]	BMC を所有する企業名または組織名を入力します。
BMC ホスト名[1]	Web アドレス・バーに表示される BMC ホスト名を入力します。
担当責任者名	BMC の担当責任者名を入力します。
メール・アドレス	BMC の担当責任者のメール・アドレスを入力します。
組織単位	BMC を所有する企業内の組織単位を入力します。
姓	BMC の責任担当者の姓を入力します。このフィールドには、最大 60 文字を入力できます。
名	BMC の責任担当者の名を入力します。このフィールドには、最大 60 文字を入力できます。
イニシャル	BMC の責任担当者のイニシャルを入力します。このフィールドには、最大 20 文字を入力できます。
DN 修飾子	BMC の識別名修飾子を入力します。このフィールドには、最大 60 文字を入力できます。
チャレンジ・パスワード	CSR へのパスワードを入力します。このフィールドには、最大 30 文字を入力できます。
非構造化名	BMC に割り当てられた非構造化された名前などの追加情報を入力します。このフィールドには、最大 60 文字を入力できます。
1. これは必須フィールドです。	

CSR は、*OpenSSL* や *Certutil* コマンド・ライン・ツールなど、ユーザーの証明書処理ツールを使用して CA によってデジタル署名されます。ユーザーの証明書処理ツールを使用して署名されたすべてのクライアント証明書には、同一の *ベース*証明書があります。この *ベース*証明書も SKLM サーバーにインポートし、ユーザーによってデジタル署名されたすべてのサーバーが SKLM サーバーで受け入れられるようにする必要があります。

証明書が CA によって署名された後、BMC にそれをインポートする必要があります。「**署名済み証明書のインポート**」操作項目を選択し、クライアント証明書としてアップロードするファイルを選択してから、「OK」ボタンをクリックします。CA 署名証明書のアップロード中は進行状況ウィンドウが表示されます。アップロード・プロセスが成功すると、証明書のアップロード・ウィンドウが表示されます。アップロード・プロセスが成功しなかった場合は、証明書のアップロード・エラー・ウィンドウが表示されます。

注：

- セキュリティーを強化する場合は、CA によってデジタル署名された証明書を使用します。
- XClarity Controller にインポートされた証明書は、以前に生成された CSR に対応している必要があります。

CA 署名証明書が BMC にインポートされた後、「**証明書のダウンロード**」操作項目を選択します。この操作項目を選択すると、CA 署名証明書が XClarity Controller からシステムにダウンロードされシステムに保存されます。

サーバー証明書管理

このトピックでは、サーバー証明書管理について説明します。

サーバー証明書は SKLM サーバーで生成され、セキュア・ドライブ・アクセス機能が動作する前に XClarity Controller にインポートされる必要があります。SKLM サーバーを BMC で認証する証明書をインポートするには、ドライブ・アクセス・ページの「サーバー証明書の状況」セクションから「**証明書のインポート**」をクリックします。ファイルが XClarity Controller のストレージに転送される間、進行状況インジケーターが表示されます。

サーバー証明書が XClarity Controller に正常に転送されると、「サーバー証明書状況」領域に以下の内容が表示されます。`A server certificate is installed`

トラステッド証明書を除去する場合は、対応する「**削除**」ボタンをクリックします。

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「**セキュリティー**」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。

暗号化設定

さまざまな暗号化設定を理解するには、このトピックの情報を使用します。

高セキュリティー・モード

- 最新および強力な暗号のみをサポートします。
- NIST 準拠
- PFS 準拠 (完全転送秘密)。

互換性モード

- 互換性を最大化するために、広範な暗号スイートをサポートしています。
- 非 PFS および非 NIST 準拠。

NIST 準拠モード

- 互換性を最大化するために、広範な暗号スイートをサポートしています。
- NIST 準拠。
- PFS 準拠。

TLS バージョン・サポート

- TLS 1.0 以上
- TLS 1.1 以上
- TLS 1.2 以上
- TLS 1.3

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 暗号スイートがサポートされるさまざまな設定については、次の表を参照してください

セキュリティー・モード	TLS バージョン	TLS 暗号スイート
高セキュリティー・モード	TLS 1.3 以下	• TLS_AES_256_GCM_SHA384
高セキュリティー・モード	TLS 1.2 以下	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
NIST 準拠モード	TLS 1.3 以下	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256
NIST 準拠モード	TLS 1.2 以下	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • 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 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

セキュリティー・モード	TLS バージョン	TLS 暗号スイート
互換性モード	TLS 1.3 以下	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256
互換性モード	TLS 1.2 以下	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • 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 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
互換性モード	TLS 1.1 以下	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

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、プロンプトが出されたらパスワードを入力します。
2. 「**コンテンツの表示**」をクリックして詳細を表示し、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、以前の構成の変更はすべて失われます。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。
   - 処理が完了した後、XClarity Controller は再起動されます。これがローカル・サーバーである場合は、TCP/IP 接続が失われるので、接続を復元するためにネットワーク・インターフェースを再構成する必要がある場合があります。
   - BMC の出荷時のデフォルト値へのリセットは、UEFI 設定には影響しません。

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。

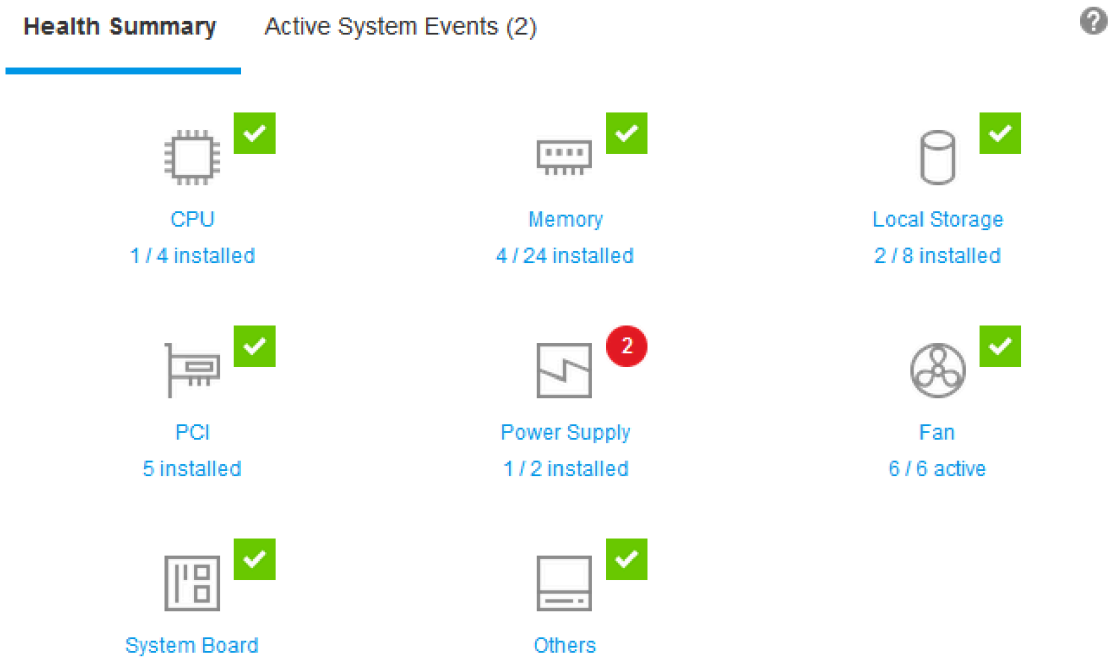
ヘルス・サマリー/アクティブ・システム・イベントの表示

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。

- プロセッサー (CPU)
- 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

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。



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。

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。テキストをクリックすると、「**システム一覧**」ページに移動します。

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・ページの左にある「System Information and Settings」ペインには、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 USB オーナーシップ
- BMC ライセンス
- BMC IP アドレス
- BMC ホスト名
- UEFI バージョン
- BMC バージョン
- LXPM 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 5. 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。

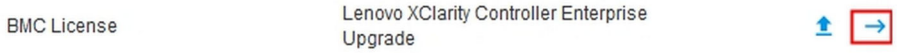
状態	説明
System power off/State unknown	サーバーの電源はオフです。
System on/starting UEFI	サーバーの電源はオンですが、UEFI は稼働していません。
System running in UEFI	サーバーの電源はオンで、UEFI が稼働しています。
システムが UEFI で停止	サーバーの電源はオンで、UEFI は問題を検出して実行を停止しています。
オペレーティング・システムのブートまたはサポートされていないオペレーティング・システム	サーバーは、以下のいずれかの理由でこの状態になる場合があります。 • オペレーティング・システム・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 • BMC Ethernet over USB インターフェースが無効になっている。 • 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。
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。
Suspend to RAM	サーバーは、スタンバイ状態またはスリープ状態に置かれています。
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。
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 LXPM メニューに入りました。
システムは LXPM 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 LXPM 保守モードに入りました。このモードではユーザーは LXPM 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。

前面 USB の所有権を変更する場合は、鉛筆アイコンをクリックし、ドロップダウン・メニューから目的の「**前面 USB オーナーシップ**」モードを選択します。次に、緑色のチェック・マークをクリックします。

サーバーに XClarity Controller Enterprise ライセンス以外のライセンスがある場合、拡張機能を有効にするライセンス・アップグレードを購入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。

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 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。

システム使用率の表示

左側のペインの「**Utilization**」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、プロセッサー、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、すべて ME (ノード・マネージャー) 側から送信され、以下の情報が含まれます。

- **CPU 使用率**
  - 集約された C 状態の存在
  - 1 秒あたりの、使用済みおよび最大の C0 存在のパーセンテージとして測定されます。
- **メモリー使用率**
  - すべてのメモリー・チャネルの集約された読み取り/書き込みボリューム。
  - これは、1 秒あたりの、使用された帯域幅と使用可能な最大メモリー帯域幅のパーセンテージとして計算されます。

- **I/O 使用率**
  - PCIe * バスのルート・ポートの集約された読み取り/書き込みボリューム。
  - 1 秒あたりの、使用された帯域幅と使用可能な最大 I/O 帯域幅のパーセンテージとして計算されます。

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・エントリーを表示します

  
  ログ内の警告エントリーを表示します

  
  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。アイコンを囲む青色の四角は、そのイベントのタイプが表示されることを示しています。
- **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 CIM-XML 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。

以下は、「**アラート受信者**」タブで実行できる操作の説明です。

以下は、「**メール/Syslog**」受信者セクションで実行できる操作項目です。

- **作成**: 追加の新規メール受信者または Syslog 受信者を作成するにはこの操作項目を選択します。最大 12 件のメールおよび Syslog 受信者を構成できます。
  - **メール受信者を作成**: メール受信者を作成するにはこの操作項目を選択します。
    - 受信者の名前およびメール・アドレスを入力します。
    - 選択してイベント通知を有効または無効にします。無効が選択される場合、アカウントの構成は残りますが、メールは送信されません。
    - 受信者に通知されるイベントのタイプを選択します。「クリティカル」、「注意」、「システム」のカテゴリー・ラベルの横にあるドロップダウンをクリックすると、カテゴリー内の特定のコンポーネントの通知を選択または選択解除できます。
    - メール・アラートにイベント・ログの内容を含めるかどうかを選択できます。
    - インデックスは、12 個の受信者スロットのどれを割り当てるかを指定します。
    - イベントが転送されるメール・サーバーの構成は、ここまたはセクション上部の SMTP サーバー操作をクリックして行うことができます。構成の詳細については、以下の「SMTP サーバー」を参照してください。

  - **Syslog 受信者を作成**: syslog 受信者を作成するにはこの操作項目を選択します。
    - Syslog サーバーの名前と IP アドレスまたはホスト名を入力します。
    - 選択してイベント通知を有効または無効にします。無効が選択される場合、アカウントの構成は残りますが、メールは送信されません。
    - インデックスは、12 個の受信者スロットのどれを割り当てるかを指定します。
    - Syslog サーバーに送信されるイベントのタイプを選択します。「クリティカル」、「注意」、「システム」のカテゴリー・ラベルの横にあるドロップダウン・メニューをクリックすると、カテゴリー内の特定のコンポーネントの通知を選択または選択解除できます。
- **SMTP サーバー**: SMTP メール・サーバー関連の設定を構成するには、この操作項目を選択します。メール・サーバーは 1 つのみ設定できます。構成済みメール受信者全員にアラートが送信される際は、同じメール構成が使用されます。定型的にポート 587 を経由して STARTTLS コマンドを使用したメール転送では、BMC がセキュア接続から暗号化接続に自動的に切り替わります (ターゲット・メール・サーバーでサポートされている場合)。
  - メール・サーバーのホスト名または IP アドレスと、ネットワーク・ポート番号を入力します。
  - メール・サーバーで認証が必要な場合は、「**認証が必要**」チェックボックスを選択し、ユーザー名とパスワードを入力します。メール・サーバーで必要な認証タイプを、チャレンジ応答方式 (CRAM-MD5) またはシンプルな資格情報 (**ログイン**) のいずれかから選択します。
  - 一部のネットワークでは、リバース・パス値が意図したものではない場合、送信されるメールがブロックされることがあります。デフォルトでは、XClarity Controller は alertmgr@domain を使用します。ここで domain は XClarity Controller ネットワーク Web ページの DDNS セクションで指定されたドメイン名です。デフォルトの代わりに独自の送信者情報を指定できます。
  - メールの設定が正しく構成されていることを確認するために、メール・サーバーへの接続をテストできます。XClarity Controller に、接続が成功したかどうかを示すメッセージが表示されます。
- **再試行および遅延**: 再試行および遅延オプション関連の設定を構成するには、この操作項目を選択します。
  - 再試行制限は、最初のアラートの送信が失敗したときに、XClarity Controller が試行を試みる回数を指定します。
  - エントリー間の遅延は、XClarity Controller が 1 人の受信者にアラートを送信してから、次の受信者にアラートを送信するまでの待機時間を指定します。
  - 試行間の遅延は、XClarity Controller がアラートの送信試行を失敗してから再試行するまでの待機時間を指定します。
- **プロトコル**: 接続プロトコル関連の設定を構成するには、この操作項目を選択します。
  - **TCP プロトコル**または **UDP プロトコル**のいずれかを選択できます。この設定は、すべての syslog 受信者に適用されることに注意してください。
- メールまたは Syslog の受信者が作成されると、このセクションにリストされます。
  - メールまたは Syslog 受信者の設定を編集するには、構成する受信者の次の行の操作ヘッダーの下にある鉛筆のアイコンをクリックします。
  - メールまたは Syslog 受信者を削除するには、ゴミ箱アイコンをクリックします。
  - メールまたは Syslog 受信者にテスト・アラートを送信するには、紙飛行機のアイコンをクリックします。

以下は、「SNMPv3」ユーザー・セグメントで実行できる操作です。

- **作成**: SNMPv3 トラップ受信者を作成するにはこの操作項目を選択します。
  - SNMPv3 トラップに関連付けられるユーザー・アカウントを選択します。このユーザー・アカウントは、12 個のローカル・ユーザー・アカウントの 1 つである必要があります。
  - SNMPv3 トラップを受信する SNMPv3 マネージャーのホスト名または IP アドレスを指定します。

- XClarity Controller は、HMAC-SHA ハッシュ・アルゴリズムを使用して SNMPv3 マネージャーで認証を行います。これはサポートされる唯一のアルゴリズムです。
- プライバシー・パスワードは、SNMP データを暗号化するためにプライバシー・プロトコルとともに使用されます。
- 「**SNMPv3 共通設定**」はすべての SNMPv3 トラップ受信者に適用されます。これらの設定は、SNMPv3 トラップ受信者の作成中、または「**SNMPv3**」ユーザー・セグメント上部の SNMPv3 設定の操作をクリックして構成できます。
  - SNMPv3 トラップを有効にするか無効にするかを選択します。無効の場合、設定の構成は残りますが、SNMPv3 トラップは送信されません。
  - BMC の連絡先およびロケーション情報は必須であり、サーバーのプロパティ Web ページで構成されます。詳しくは、79 ページの「ロケーションと連絡先の設定」を参照してください。
  - SNMPv3 マネージャーに送信される原因トラップであるイベントのタイプを選択します。「クリティカル」、「注意」、「システム」のカテゴリー・ラベルの横にあるドロップダウン・メニューをクリックすると、カテゴリー内の特定のコンポーネントの通知を選択または選択解除できます。

  注：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。**プライバシー・プロトコル**においてサポートされる方式は、CBC-DES および AES です。
- SNMPv3 トラップ受信者が作成されると、このセクションにリストされます。
  - SNMPv3 受信者の設定を編集するには、構成する受信者の次の行の操作ヘッダーの下にある鉛筆のアイコンをクリックします。
  - SNMPv3 受信者を削除するには、ゴミ箱アイコンをクリックします。

最新の OS 障害画面データのキャプチャー

オペレーティング・システム障害画面をキャプチャーして表示するには、このトピックの情報を使用します。

OS ウォッチドッグ・タイムアウトが発生すると、オペレーティング・システム画面が自動的にキャプチャーされます。OS の稼働停止を引き起こすイベントが発生すると、OS ウォッチドッグ機能が起動され、画面の内容がキャプチャーされます。XClarity Controller では、保存されるスクリーン・キャプチャーは 1 個のみです。OS ウォッチドッグ・タイムアウトが発生すると、新しいスクリーン・キャプチャーが前のスクリーン・キャプチャーを上書きします。OS 障害画面をキャプチャーするには、OS ウォッチドッグ機能を有効にする必要があります。OS ウォッチドッグ・タイムを設定するには、79 ページの「サーバー・タイムアウトの設定」で詳細を参照してください。OS 障害スクリーン・キャプチャー機能は、XClarity Controller の拡張レベルまたはエンタープライズ・レベルの機能でのみ使用可能です。ご使用のサーバーにインストールされている 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。

XClarity Controller ホーム・ページの「**リモート・コンソール**」セクションの「**直近の障害画面**」操作をクリックして、OS ウォッチドッグ・タイムアウトが発生したときにキャプチャーされたオペレーティングシステム画面のイメージを表示します。キャプチャーは、ホーム・ページの「**クイック操作**」セクションで「**サービス**」、「**直近の障害画面**」の順にクリックして表示することもできます。システムで OS ウォッチドッグ・タイムアウトが発生せず、OS 画面をキャプチャーしていない場合は、障害画面が作成されていないことを示すメッセージが表示されます。

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、この章の情報を使用します。

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

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使用します。

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ー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使用します。

「**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・モードと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・モードでは、次の 2 つのオプションを使用できます。

UEFI ブート
Unified Extensible Firmware Interface (UEFI) をサポートするサーバーを構成するには、このオプションを選択します。UEFI 対応のオペレーティング・システムをブートする場合、このオプションでは、レガシー・オプション ROM を無効にすることによって、ブート時間を短縮できます。

レガシー・ブート
レガシー (BIOS) ファームウェアを必要とするオペレーティング・システムをブートするサーバーを構成する場合は、このオプションを選択します。UEFI 非対応オペレーティング ・ システムをブートする場合にのみ、このオプションを選択します。

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、次回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。

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。

ブートのタイプを 1 回限りのブート・デバイスを使用して実行するように変更する場合、レガシー・ブートまたは UEFI ブートするようにブートを指定することもできます。ブートをレガシー BIOS ブートにするには、「**レガシー・ブート優先**」チェック・ボックスをクリックします。UEFI ブートにするにはボックスのチェック・マークを外します。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：ブレードまたは高密度サーバー・ノードを含むシャーシでは、シャーシの冷却と電源は XClarity Controller ではなくシャーシ管理コントローラーによって制御されます。

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。

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)**: このモードでは、1 つのパワー・サプライが失われた場合、サーバーは継続して稼働します。
  - **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 (N+1)**: このモードでは、4 つのパワー・サプライが取り付けられている場合に、1 つのパワー・サプライが失われると、サーバーは継続して稼働します。
- **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。

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。

電源キャッピングは AC 電力消費量の計測または DC 電力消費量の計測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。AC と DC の間で切り替えると、スライダーの数字がそれに応じて変化します。

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**: スライダー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。スライダー・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。

注：「**電源ポリシー**」オプションは、XClarity Controller がブレード・サーバーまたは高密度サーバーのノードを含むシャーシにある場合は使用できません。電源ポリシーは XClarity Controller ではなくシャーシ管理コントローラーによって制御されます。

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。

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。

注：「**電源復元ポリシー**」オプションは、ブレード・サーバーまたは高密度サーバーのノードを含むシャーシでは使用できません。電源復元ポリシーは XClarity Controller ではなくシャーシ管理コントローラーによって制御されます。

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 6. 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。
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。

表 6. 電源操作と説明 (続き)

電源アクション	説明
マスク不能割り込み (NMI) をトリガー	「ハング」したシステムでマスク不能割込み (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：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。	

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タに返されます。
- 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タに返されます。

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。

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 拡張機能および XClarity Controller エンタープライズ機能で、Web インターフェースを使用してのみ使用できます。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 標準から XClarity Controller 拡張または XClarity Controller エンタープライズへのアップグレードについて詳しくは、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、72 Hz または 75 Hz で最大 1280 x 1024 のグラフィックス解像度のビデオをリモート側で表示します。
- 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 50 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・コンソール機能をマルチユーザー・モード (XClarity Controller エンタープライズ機能セットを備えた XClarity Controller は 6 つまでの同時セッションをサポートします) で開始した場合、リモート・ディスク機能は同時に 1 つのセッションのみで実行できます。
- 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、34 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「**セキュリティー**」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 *.crt 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。

前述のように、XClarity Controller リモート・コンソール機能は、XClarity Controller 拡張機能および XClarity Controller エンタープライズ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拡張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、89 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、以下の手順を実行してください。

1. XClarity Controller ホーム・ページまたはリモート・コンソール Web ページのリモート・コンソールセクションにある、白い斜めの矢印が示すイメージをクリックします。
2. 以下のモードから 1 つを選択します。
   - シングルユーザー・モードでリモート・コンソールを起動する
   - マルチユーザー・モードでリモート・コンソールを起動する

   注：XClarity Controller エンタープライズ機能セットを備えた XClarity Controller では、マルチユーザー・モードで最大 6 つの同時ビデオ・セッションをサポートします。
3. リモート・コンソール機能がすでにシングルユーザー・モードで使用されているときにまたはマルチユーザー・モードで最大人数のユーザーがリモート・コンソール機能を使用しているときに、他のユーザーがリモート・コンソール機能を使用したい場合、他のユーザーがリモート・コンソール・ユーザーに切断要求を要求できるかどうかを選択します。「**応答なし時間間隔**」は、切断要求に対する応答がない場合に XClarity Controller が自動的にユーザーを切断するまでに待機する時間を指定します。
4. 直近 3 件のサーバー・ブート・ビデオの記録を許可するかどうかを選択します。
5. 直近 3 件のサーバー・クラッシュ・ビデオの記録を許可するかどうかを選択します。
6. HW エラーで OS 障害のスクリーン・キャプチャーを許可するかどうかを選択します。
7. 「**リモート・コンソールの起動**」をクリックすると、リモート・コンソール・ページを別のタブで開きます。可能なすべてのリモート・コンソール・セッションが使用中の場合は、ダイアログ・ボックスが表示されます。このダイアログ・ボックスで、「**他のユーザーからのリモート・セッション切断要求を許可**」の設定を有効にしているユーザーは、リモート・コンソールのユーザーに切断要求を送信できます。ユーザーは切断要求を受諾または拒否できます。ユーザーが「**応答なし時間間隔**」設定で指定された時間内に応答しない場合、ユーザー・セッションは XClarity Controller によって自動的に終了します。

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使用します。

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、PNG 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ー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。サーバーによって定義される他のマクロは、Lenovo XClarity Essentials を使用して定義でき、XClarity Controller からダウンロードできます。これらのマクロはリモート・コンソール機能のすべてのユーザーに定義されます。

- 「**構成**」をクリックしてユーザー定義マクロを追加または削除します。ユーザー定義マクロは、現在のリモート・コンソール・ユーザーのみに定義されます。他のリモート・コンソール・ユーザーは相互にユーザー定義マクロを見ることはできません。
  - マクロ追加アイコンをクリックして必要なキー・シーケンスを押し、「**追加**」をクリックして新しいマクロを追加します。
  - ユーザー定義マクロを削除するには、マクロをリストから選択し、ゴミ箱アイコンをクリックします。
  - サーバーにユーザー定義マクロを送信するには、「**ユーザー定義マクロ**」オプションを選択し、送信するマクロをクリックします。

リモート・コンソールのマウス・サポート

以下の情報を使用して、リモート・マウス制御のオプションを理解します。

リモート・コンソール・ウィンドウは、絶対マウス制御、相対マウス制御 (加速なし)、マウス制御 (RHEL、古い Linux) を含む、マウス制御に関するいくつかのオプションを提供します。

絶対マウス制御と相対マウス制御

マウス制御の絶対および相対オプションにアクセスするには、この情報を使用します。

マウス制御の絶対および相対オプションにアクセスするには、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、「**マウス**」をクリックします。

ステップ 2. ドロップダウン・メニューから「**マウス設定**」をクリックします。

ステップ 3. 以下のいずれかの「**マウス加速**」モードを選択します。

絶対位置 (Windows、最近のバージョンの Linux および Mac OS X)
クライアントは、表示エリアの原点 (左上のエリア) からの相対位置であるマウス・ロケーション・メッセージをサーバーに送信します。

相対位置、加速なし
クライアントは、マウスの位置を以前の位置からの相対位置として送信します。

相対位置 (古いバージョンの Linux)
個のモードは、加速係数を適用して一部の Linux ターゲット上でマウスをより正確に位置合わせします。加速設定は、古い Linux ディストリビューションとの互換性を最大化するように選択されています。

画面モニターの録画/再生

リモート・プレゼンス画面モニターを録画または再生するには、このトピックに記載されている情報を使用します。

XClarity Controller の Web インターフェースは、リモート・プレゼンス画面モニターの録画および再生をサポートする DVR のような機能を提供します。この機能は、ネットワーク・フォルダーへのビデオの書き込みのみサポートしています。現在、NFS および CIFS プロトコルがサポートされています。録画および再生機能を使用する手順を次に示します。

1. リモート・コンソールの Web ページで、「**画面の録画**」をクリックして、「設定」ウィンドウを開きます。
2. 「設定」ウィンドウで、以下の情報を指定する必要がある場合があります。

- 「CIFS」マウント・タイプが選択されている場合は、**リモート・フォルダー**、**ユーザー名**、**パスワード**のパラメーターを指定します。CIFS リモート・フォルダーの形式は、「//<**リモート IP アドレス**>/<**フォルダー名**>」です。例: //xxx.xxx.xxx.xxx/folder
- 「NFS」マウント・タイプが選択されている場合は、**リモート・フォルダー** のパラメーターを指定します。NFS リモート・フォルダーの形式は、「<**リモート IP アドレス**>:/<**フォルダー名**>」です。例: xxx.xxx.xxx.xxx:/folder。
- 必要に応じて、ビデオ・ファイル名を指定します。ファイル名が既に指定されている場合は、エラー・メッセージのボックスが表示されます。既存のファイル名を上書きするには、「ファイル名の上書き」を選択します。「自動」ボックスがオンになっている場合、ビデオ・ファイル名は自動的に生成されます。
- 「最大ファイル・サイズ」は、ビデオ録画が自動的に停止するまでのビデオ・ファイルの最大サイズを示します。
- 「最長ファイル時間」は、録画が自動的に停止するまでのビデオ録画の最長時間を示します。

3. 「**録画開始**」をクリックしてビデオ録画を開始します。
4. 「**録画停止**」をクリックしてビデオ録画を停止します。「ビデオ録画が完了しました」というポップアップ・ウィンドウが開いて、関連するビデオ録画情報が表示されます。
5. 録画されたビデオを NFS または CIFS からローカル・フォルダーにダウンロードします。XClarity Controller のホーム・ページの「リモート・コンソールのプレビュー」セクションで、「**録画されたビデオ**」をクリックし、再生するビデオ・ファイルを選択します。

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。

画面の拡張
拡張を有効にすると、イメージ全体がコンソール・ウィンドウに収まるようにビデオ・イメージが拡大縮小されます。

元の画面
ビデオ・イメージはサーバー側と同じ大きさです。必要に応じてスクロール・バーが表示され、ビデオ・イメージのウィンドウ内に収まらない部分を表示できます。

カラー・モード
リモート・コンソール・ウィンドウのカラー階調を調整します。2 つのカラー・モード選択項目があります。

- カラー: 7、9、12、15、および 23 ビット
- グレースケール: 16、32、64、および 128 階調

注：カラー・モードの調整は通常、リモート・サーバーへの接続の帯域幅が制限されており、帯域幅の要求を削減する必要がある場合に行われます。

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 Enterprise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・メディアのマウント**」セクションで「**アクティブにする**」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。

  注：

  – Google Chromeブラウザーを使用している場合は、「**Mount files/folders**」という追加のマウントオプションを使用して、ファイル/フォルダーをドラッグアンドドロップできます。
  – 複数の並列リモート・コンソール・セッションがXClarity Controllerで進行中の場合、この機能はセッションうちの1つでのみアクティブにできます。
- 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、セキュリティー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。

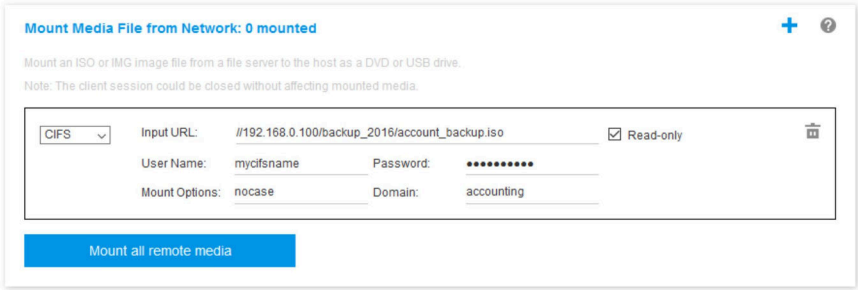
  注：Microsoft IIS で生成されたセキュリティー証明書のマウント処理中にエラーが発生することがあります。この状態が発生した場合は、77 ページの「メディアのマウント・エラーに関する問題」を参照してください。

「**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。

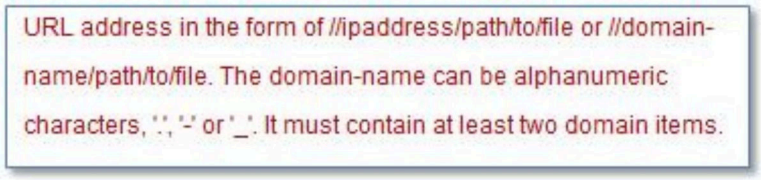
- 2 つまでのファイルを XClarity Controller メモリーにアップロードして、XClarity Controller RDOC 機能を使用して仮想メディアとしてマウントできます。両方のファイルの合計サイズが 50 MB を超えてはなりません。これらのファイルは、リモート・コンソール・セッションが終了しても、削除されるまで XClarity Controller メモリーに残ります。RDOC 機能はファイルをアップロードするときに以下のメカニズムをサポートします。
  - **CIFS - 共通インターネット・ファイル・システム**: 詳細は上記の説明を参照。

    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。ファイル名の大文字と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。



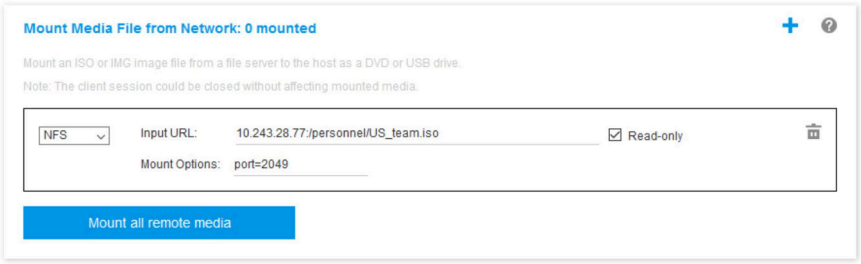
    BMC では、URL を指定する際のガイダンスを提供しています。入力された URL が有効ではない場合、マウント・ボタンがグレー表示になり、URL フィールドの下に URL の適切な形式を示す赤字のテキストが表示されます。



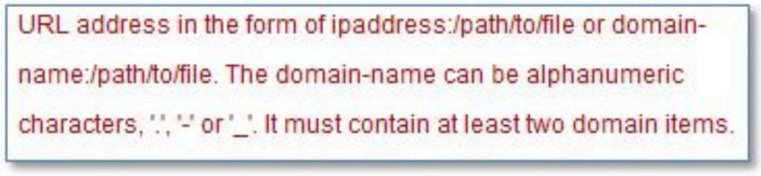
– NFS - **ネットワーク・ファイル・システム**: 詳細は上記の説明を参照。

  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。



  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。



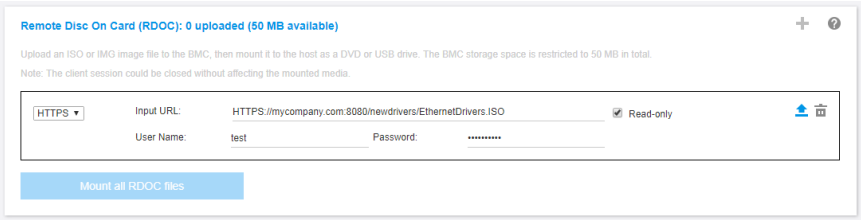
– HTTPS – Hypertext Transfer Protocol Secure:
  – リモート・システム上のファイルがある URL を入力します。
  – ファイルを読み取り専用仮想メディアとしてサーバーに表示する場合は、チェック・ボックスにチェックを入れます。
  – XClarity Controller がリモート・システム上のファイルにアクセスするために必要な資格情報を入力します。

  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、77 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
```

Java クライアントを使用したリモート・ディスク

このセクションでは、Java クライアントを使用してローカル・メディアをマウントする方法について説明します。

Java クライアントを使用してご使用のコンピューター上の CD または DVD ドライブ、ディスケット・ドライブ、USB フラッシュ・ドライブをサーバーに割り当てることができます。また、ご使用のコンピューター上のディスク・イメージをサーバーで使用するように指定することもできます。そのドライブを使用して、サーバーの再始動 (ブート)、コードの更新、サーバーへの新規ソフトウェアのインストール、サーバー上のオペレーティング・システムのインストールまたは更新などの機能を実行できます。リモート・ディスクにアクセスできます。ドライブおよびディスク・イメージは、サーバー上では USB ドライブとして表示されます。

注：リモート・コンソール Java は以下のいずれかの Java 環境をサポートし、HTML5 クライアントが実行されていない場合にのみ開くことができます。

1. Oracle Java Runtime Environment 1.8/Java SE 8 以降のバージョン
2. OpenJDK 8。HotSpot JVM による AdoptOpenJDK の配布がサポートされています。

AdoptOpenJDK を使用する場合、OSX、Windows、および Linux で https://openwebstart.com/ を使用する必要があります。

イメージ・ファイルの作成

指定されたソース・フォルダーから新しいイメージ・ファイルを作成するには、以下のステップを実行します。

1. 「仮想メディア Java クライアント」ウィンドウで、「**仮想メディア**」タブの下にある「**イメージの作成**」オプションをクリックします。「フォルダーからのイメージの作成」ウィンドウが表示されます。
2. 「**ソース・フォルダー**」フィールドに関連付けられた「**参照**」ボタンをクリックして、特定のソース・フォルダーを選択します。
3. 「**新しいイメージ・ファイル**」フィールドに関連付けられた「**参照**」ボタンをクリックして、使用するイメージ・ファイルを選択します。
4. 「**イメージの作成**」ボタンをクリックします。

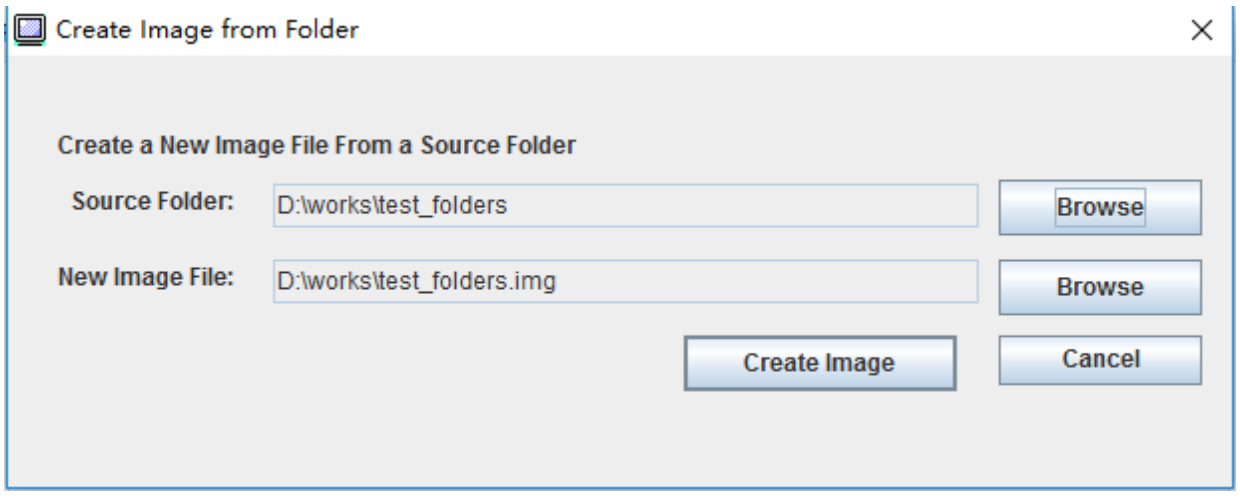


図 1. イメージ・ファイルの作成

マウントするデバイスの選択

ローカル・イメージ、フォルダー、および CD/DVD/USB ドライブをマウントするには、次のステップを実行してください。

「仮想メディア Java クライアント」ウィンドウで、「**仮想メディア**」タブの下にある「**マウントするデバイスの選択**」オプションをクリックします。「マウントするデバイスの選択」ウィンドウが表示されます。

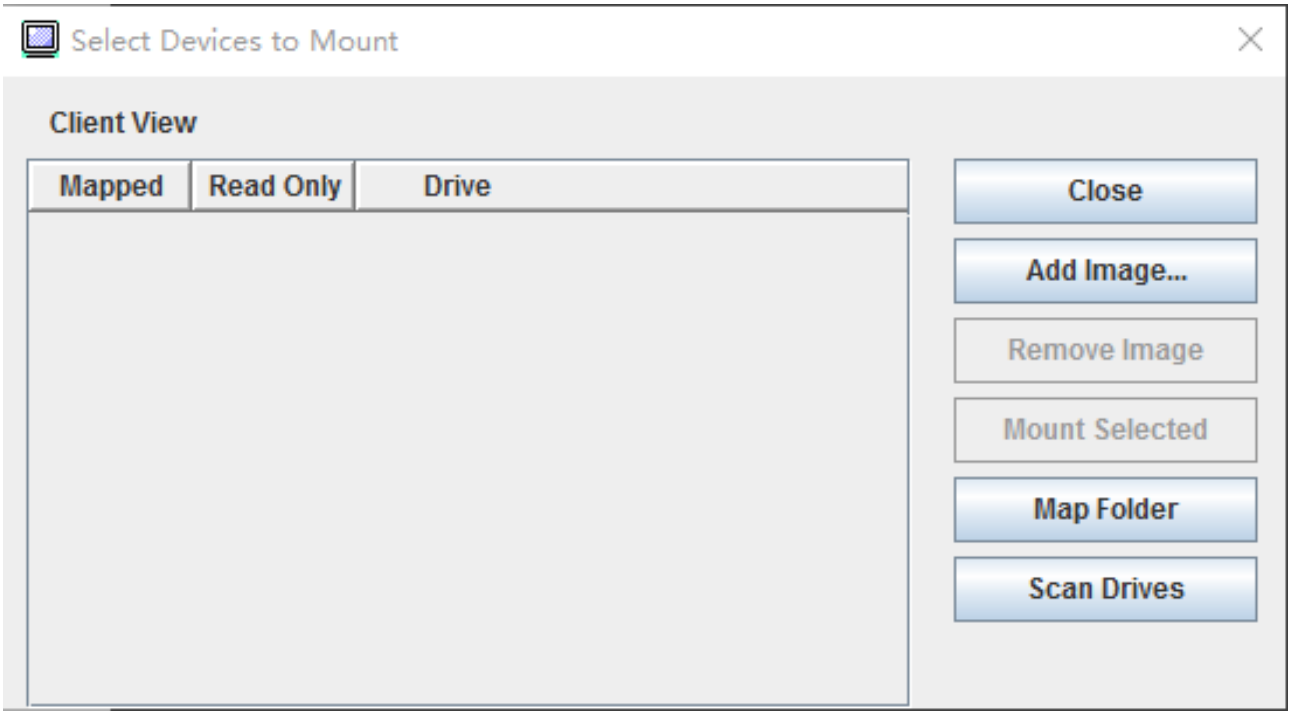


図 2. 「マウントするデバイスの選択」ウィンドウ

次のステップを実行することで、ローカル・イメージ、フォルダー、および CD/DVD/USB ドライブをマウントできます。

- **ローカル・イメージをマウントする**:
  1. 「**イメージの追加**」ボタンをクリックして、マウントするイメージを選択します。
  2. **マッピングされた** オプションを確認します。
  3. 必要に応じて、**読み取り専用** オプションをオンにして機能を有効にします。
  4. 「**選択した項目をマウント**」ボタンをクリックすると、ローカル・イメージを正常にマウントすることができます。

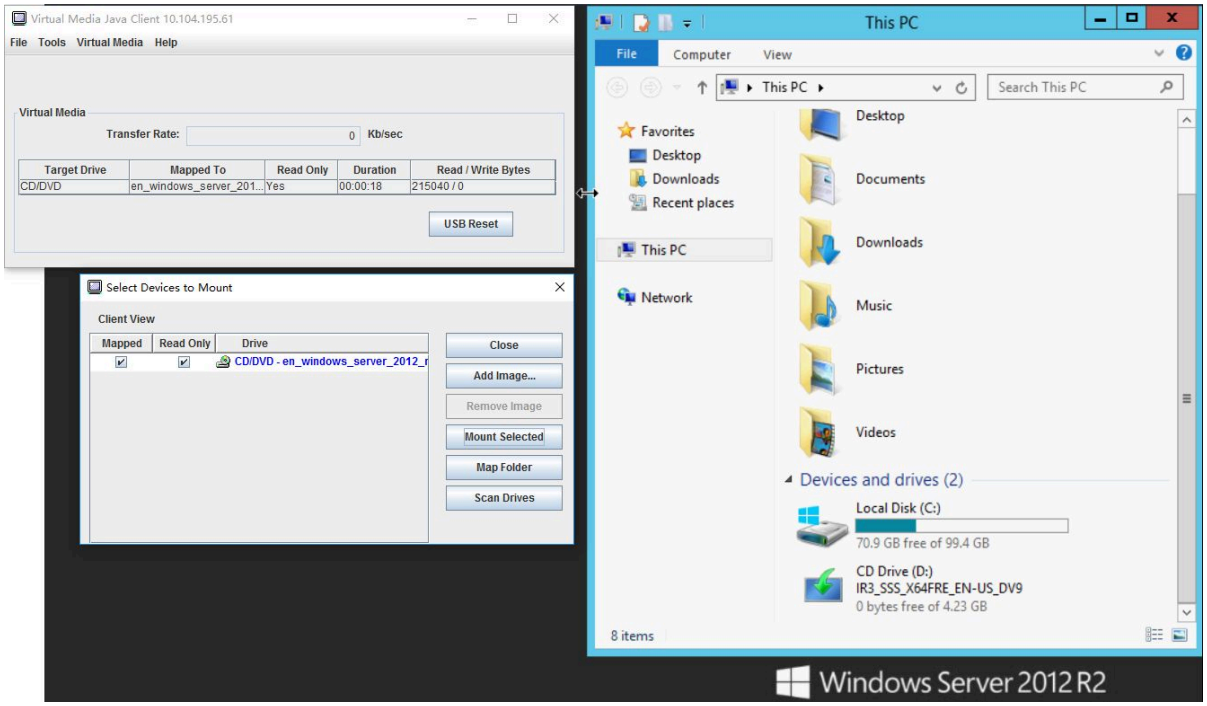


図3. ローカル・イメージをマウントする

- **ローカル・フォルダーをマウントする**:
  1. 「**フォルダーをマッピング**」ボタンをクリックして、マウントするローカル・フォルダーを選択します。
  2. 「**選択した項目をマウント**」ボタンをクリックすると、ローカル・フォルダーを正常にマウントすることができます。

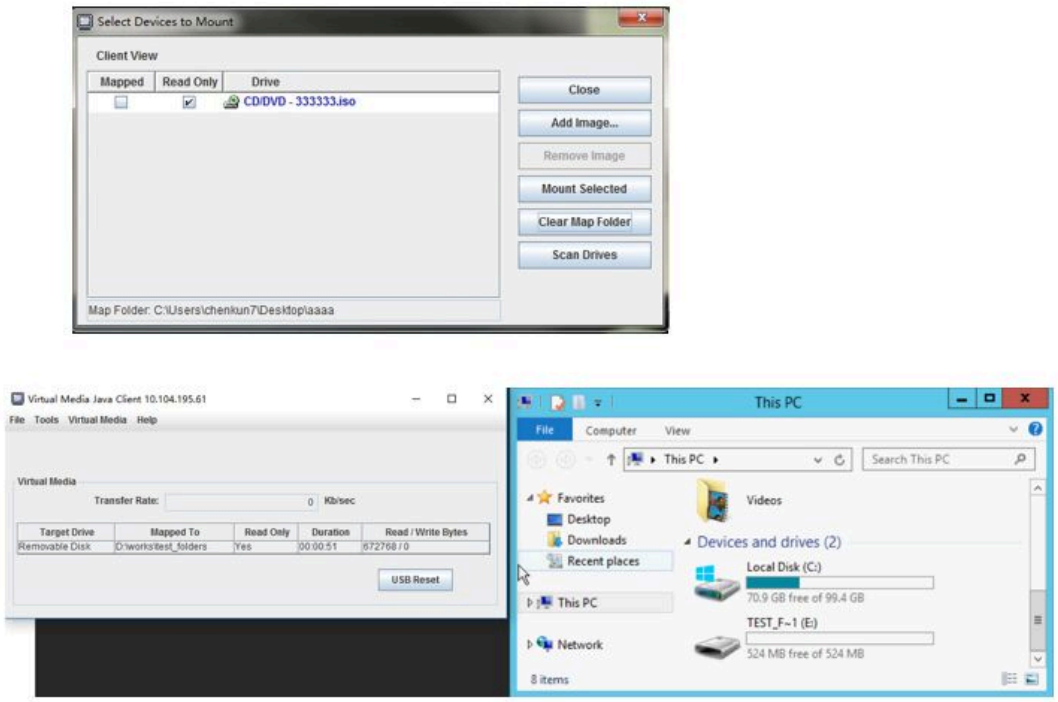


図4. ローカル・フォルダーをマウントする

- CD/DVD または USB ドライブをマウントする:
  1. 「**ドライブのスキャン**」ボタンをクリックして、接続されている CD/DVD または USB ドライブを検出します。
  2. **マッピングされた** オプションを確認します。
  3. 必要に応じて、**読み取り専用** オプションをオンにして機能を有効にします。
  4. 「**選択した項目をマウント**」ボタンをクリックすると、ローカル・イメージを正常にマウントすることができます。

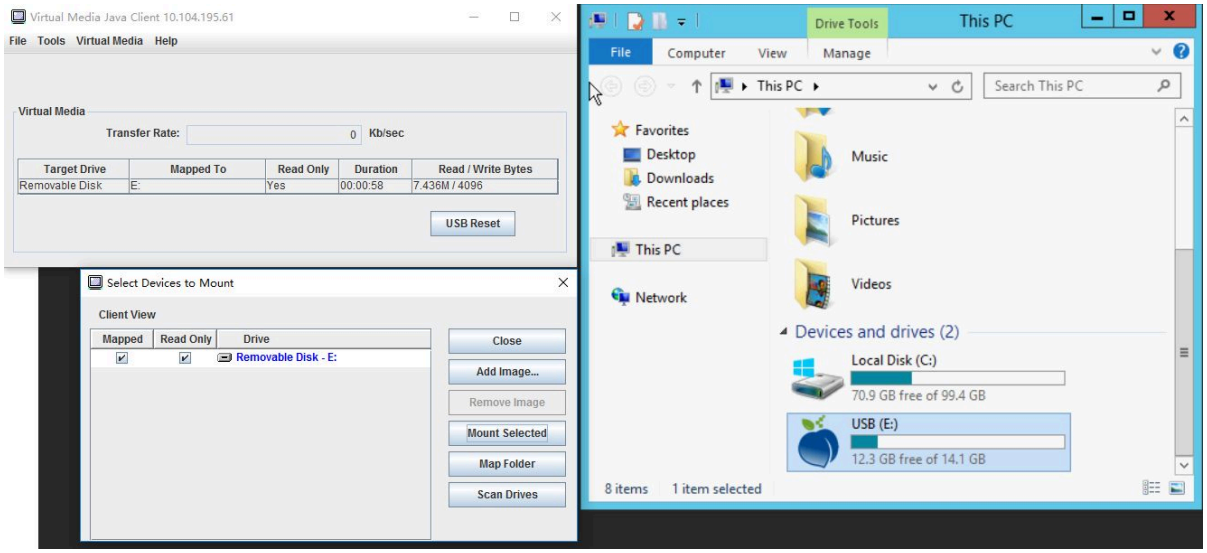


図 5. CD/DVD または USB ドライブをマウントする

「マウントするデバイスの選択」ウィンドウには、マウント可能な現在のローカル・デバイスのリストが表示されます。このウィンドウには、以下のフィールドおよびボタンが含まれています。

- **マッピング**されたフィールドには、マウントまたはマッピングするデバイスを選択するためのチェック・ボックスがあります。
- 「**読み取り専用**」フィールドには、ホスト・サーバーで *読み取り専用* となる、マッピングされたデバイスまたはマウント済みデバイスを選択するためのチェック・ボックスがあります。
- **ドライブ**・フィールドには、ローカル・マシンのデバイス・パスが含まれています。
- 「**閉じる**」ボタンをクリックして、「マウントするデバイスの選択」ウィンドウを閉じます。
- 「**イメージの追加**」ボタンをクリックして、デバイスのリストに追加するローカル・ファイル・システム内のディスケット・イメージと ISO イメージ・ファイルを参照します。
- 「**イメージの削除**」ボタンをクリックして、デバイスのリストに追加されたイメージを削除します。
- 「**選択した項目をマウント**」ボタンをクリックして、マウントまたはマッピングすることを確認されたすべてのデバイスを、**マッピングされた** フィールドにマウントまたはマッピングします。

  注：フォルダーは、読み取り専用としてマウントされます。
- 「**ドライブのスキャン**」ボタンをクリックして、ローカル・デバイスのリストを更新します。

アンマウントするデバイスの選択

ホスト・サーバーのデバイスをアンマウントするには、以下の手順を実行します。

1. 「仮想メディア Java クライアント」ウィンドウで、「**仮想メディア**」タブの下にある「**すべてをアンマウント**」オプションをクリックします。
2. 「**すべてをアンマウント**」オプションを選択すると、「すべてをアンマウント」の確認ウィンドウが表示されます。同意すると、サーバー 上の すべての ホスト・サーバー・デバイスがアンマウントされます。

   注：ドライブを個別にアンマウントすることはできません。

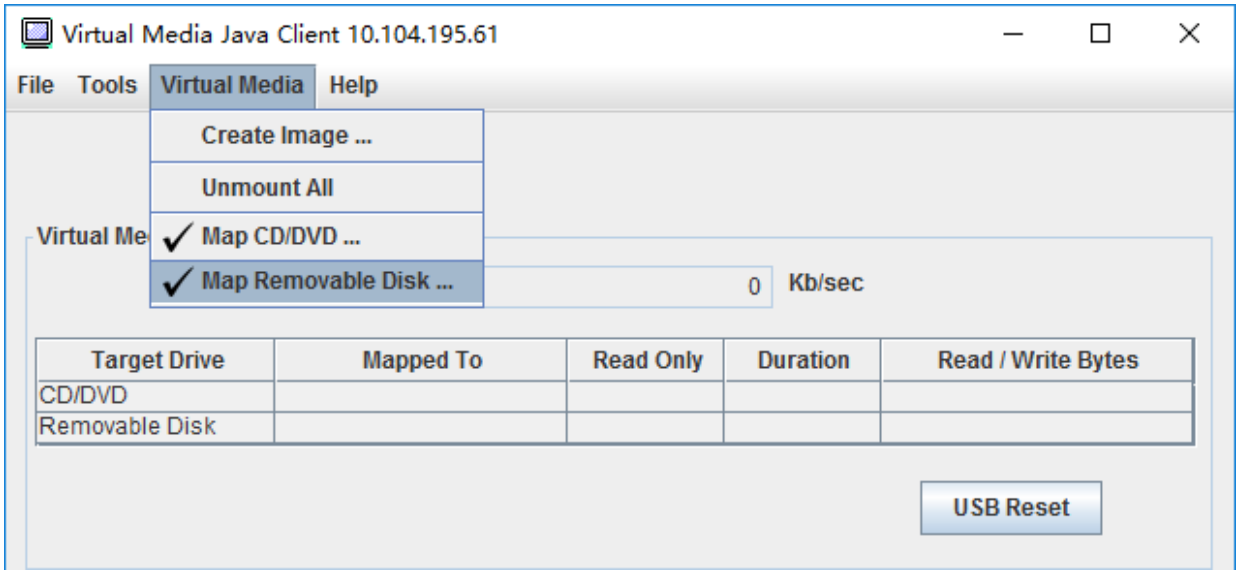


図 6. すべてをアンマウント

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。

サービス・データのダウンロード

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**」オプションをクリックし、「**サービス・データのダウンロード**」を選択します。「OK」をクリックしてサービス・データ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、サービス・データを生成するために数分かかります。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>_xcc_<date>-<time>.tgz

例: 7X2106Z01A_2345678_xcc_170511-175656.tgz.

tgz 形式に加えて、サービス・データは tzz 形式を使用してダウンロードすることもできます。Tzz では、異なる圧縮アルゴリズムを使用し、「lzop」などのユーティリティーにより展開できます。

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できます。

注：このフィールドはオプションであり、Flex ノードでは構成しません。

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できます。

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できます。

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できます。

注：このフィールドはオプションであり、Flex ノードでは構成しません。

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。

OS ウォッチドッグ
OS ウォッチドッグは、オペレーティング・システムを監視してハングしていないことを確認するために使用されます。この機能を使用するには、Ethernet over USB インターフェースを有効にする必要があります。詳しくは、32 ページの 「Ethernet over USB の構成」を参照してください。XClarity Controller は「**OS ウォッチドッグ・タイム**」で構成された間隔でオペレーティング・システムと連絡します。次のチェックまでにオペレーティング・システムが応答しない場合、XClarity Controller はオペレーティング・システムがハングしているとみなします。XClarity Controller はサーバーの表示内容

をキャプチャーし、サーバーをリブートして復元操作を試みます。XClarity Controller は一度だけサーバーをリブートします。リブート後もオペレーティング・システムがハングし続ける場合は、連続してサーバーをリブートするのではなく、問題を調査して修正できるようにサーバーをハング状態のままにします。OS ウォッチドッグを再装着するには、サーバーの電源をオフにしてからオンにします。OS ウォッチドッグを有効にするには、「OS ウォッチドッグ・タイム」のドロップダウンから間隔を選択して、「**適用**」をクリックします。OS ウォッチドッグを無効にするには、「OS ウォッチドッグ・タイム」のドロップダウン・メニューで「**なし**」を選択します。

ローダー・ウォッチドッグ
ローダー・ウォッチドッグは POST 完了からオペレーティング・システムが実行を開始するまでの間隔を監視します。この機能を使用するには、Ethernet over USB インターフェースを有効にする必要があります。詳しくは、32 ページの 「Ethernet over USB の構成」を参照してください。POST が完了すると、XClarity Controller はタイマーを起動し、オペレーティング・システムと連絡を始めます。ローダー・ウォッチドッグの選択で構成された時間内にオペレーティング・システムが応答しない場合、XClarity Controller はオペレーティング・システムがハングしているとみなします。XClarity Controller はサーバーをリブートして復元操作を試みます。XClarity Controller は一度だけサーバーをリブートします。リブート後もオペレーティング・システムのブートがハングし続ける場合は、連続してサーバーをリブートするのではなく、問題を調査して修正できるようにサーバーをハング状態のままにします。ローダー・ウォッチドッグは、サーバーの電源がオフになった後再度オンになるか、サーバーが正常にブートしてオペレーティング・システムが起動したときに再装着されます。ローダー・ウォッチドッグを有効にするには、「ローダー・ウォッチドッグ」のドロップダウンから間隔を選択して、「**適用**」をクリックします。ローダー・ウォッチドッグを無効にするには、「ローダー・ウォッチドッグ」のドロップダウン・メニューで「**なし**」を選択します。

電源オフ遅延を有効にする
電源オフ遅延フィールドを使用して、XClarity Controller サブシステムが電源を強制的に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つ時間 (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。

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・システムもあれば、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。
- 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、飛ばされた時間の間に 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。
- XClarity Controller の日付と時刻の設定は、Flex System では変更できません。

第 6 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、この章の情報を使用します。

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。

- 詳細
- RAID セットアップ

RAID の詳細

RAID の詳細機能を使用するには、このトピックの情報を使用します。

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。

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使用します。

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使用します。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使用します。

「**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ー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、コントローラー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。

「コントローラー操作」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ーのすべての構成およびデータをクリアします。

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。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。

      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。

      1) このような場合、Web インターフェースにデフォルトで「**スパン 1**」と表示されます。
      2) ドライブを選択し、「**メンバーを追加**」をクリックして「**スパン 1**」にドライブを追加します。「**スパン 1**」に十分なドライブがない場合は、「**スパンを追加**」リンクは無効です。
      3) 「**スパンを追加**」をクリックして「**スパン 2**」を追加します。ドライブを選択し、「**メンバーを追加**」をクリックして「**スパン 2**」に追加します。
      4) 「**メンバーを追加**」をクリックして、最後のスパンにドライブを追加します。もう一度「**スパン 1**」にドライブを追加する場合は、スパン 1 をクリックしてからドライブを選択して「**スパン 1**」に追加する必要があります。
      5) スパン数が最大容量に達したら、「**スパンを追加**」リンクが無効になります。

   b. 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、すべてのストレージ容量を使用する仮想ディスクを作成します。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. 複数の仮想ディスクがある場合、「**削除**」アイコンが有効になります。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. 「**仮想ディスクの作成を開始**」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使用します。

「**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**: 基本プロパティ (ドライブ名、RAID 状態、タイプ、シリアル番号、部品番号、FRU 番号および操作) 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。
  - **ディスク・ドライブを再使用可能にする**: ドライブを再使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。
  - **JBOD に対してドライブを正常として設定する**: JBOD 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 ドライブ**」テーブルに表示されます。「**JBOD 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 7 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使用します。

概要

サーバー・ファームウェアの更新に関する一般情報。

ナビゲーション・パネルの「**ファームウェア更新**」オプションには、次の4つの機能があります。

- **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とバージョンの概要。システム・ファームウェアの更新を実行します。
- **ックアップする自動プロモート・プライマリー XCC**: 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**: インストール済みのアダプター・ファームウェア、そのステータス、およびバージョンの概要。アダプター・ファームウェアの更新を実行します。

BMC、UEFI、LXPM、LXPM ドライバーのファームウェア、およびアダプターの現在の状況とバージョンが表示されます (BMC の基本バージョンとバックアップ・バージョンを含む)。ファームウェア状況には、次の 4 つのカテゴリーがあります。

- **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。
- **保留**: ファームウェアはアクティブ化を待機しています。
- **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、不適切または正しくない動作を引き出す可能性があります。
- 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・ドライバー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・ドライバー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。
- 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。

第 8 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ければなりません。

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、89 ページの「アクティベーション・キーのインストール」、90 ページの「アクティベーション・キーの削除」、または 90 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、127 ページの「keycfg コマンド」を参照してください。

XClarity Controller のライセンス管理 ID を登録するには、以下のリンクをクリックします。
http://thinksystem.lenovofiles.com/help/index.jsp

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

注意：標準 XClarity Controller からエンタープライズ・レベル機能に直接アップグレードすることはできません。エンタープライズ・レベル機能をアクティブにする前に、拡張レベルにアップグレードする必要があります。

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使用します。

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するか、「**キャンセル**」をクリックしてインストールを

停止します。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「OK」をクリックするか、「**キャンセル**」をクリックしてインストールを停止します。

「成功」ウィンドウは、アクティベーション・キーがインストールされたことを示します。

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。

ステップ 4. 「OK」をクリックして「成功」ウィンドウを閉じます。

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・キーの削除を確認するか、「**キャンセル**」をクリックしてそのキー・ファイルを保持します。
選択されたアクティベーション・キーは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を確認するか、「**キャンセル**」をクリックしてキーのエクスポート要求を取り消します。

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 9 章　Lenovo XClarity Controller の Redfish REST API

Lenovo XClarity Controller には、Lenovo XClarity Controller フレームワークの外で実行されているアプリケーションから Lenovo XClarity Controller のデータとサービスにアクセスするために使用できる、Redfish に準拠した、使いやすい一連の REST API が用意されています。

これにより、ソフトウェアが Lenovo XClarity Controller サーバーと同じシステムで実行されているのか、同じネットワーク内のリモート・システムで実行されているのかに関係なく、Lenovo XClarity Controller の機能を他のソフトウェアに簡単に統合できます。これらの API は業界標準の Redfish REST API であり、HTTPS プロトコルを通じてアクセスできます。

XClarity Controller の Redfish REST API ユーザーズ・ガイドは、https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.restapi.doc/xcc_restapi_book.pdf にあります。

Lenovo は、Lenovo Redfish REST API と通信するソフトウェアを開発するための参照用に使用できる、オープン・ソースのサンプル Redfish スクリプトを提供します。これらのサンプル・スクリプトは、次の場所にあります。

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

Redfish API に関連する DMTF 仕様は、https://redfish.dmtf.org/ から入手できます。この Web サイトは、Redfish REST API の全般的な仕様およびその他の参照資料を提供します。

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、93 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。

コマンド・ラインへログインされます。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` と入力するまで継続します。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、出力バッファーの限度は 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、データはバッファーに格納されます)。
- 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> ?
```
- Flex System では、一部の設定は CMM が管理するため、XClarity Controller では変更できません。

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。

- 111 ページの 「accseccfg コマンド」
- 174 ページの 「adapter コマンド」
- 113 ページの 「alertcfg コマンド」
- 159 ページの 「alertentries コマンド」
- 113 ページの 「asu コマンド」
- 116 ページの 「backup コマンド」
- 162 ページの 「batch コマンド」
- 163 ページの 「clearcfg コマンド」
- 98 ページの 「clearlog コマンド」
- 163 ページの 「clock 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。

次の表は、オプションの引数を示しています。

表 7. clearlog コマンド

次の表は、オプションとその説明で構成される 1 行 2 列の表です。

オプション	説明
-t <all | platform | audit>	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。

イベント・タイプの説明

- 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。
- platform: プラットフォーム・イベント・タイプ。
- audit: 監査イベント・タイプ。

例:

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

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

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>
```

ffdc 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。

First Failure Data Capture (**ffdc**) コマンドは、サービス・データを生成し、サポートに転送するために使用します。

ffdc 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。

- **generate**: 新規のサービス・データ・ファイルを作成する
- **status**: サービス・データ・ファイルの状況をチェックする
- **copy**: 既存のサービス・データをコピーする
- **delete**: 既存のサービス・データを削除する

次の表は、オプションの引数を示しています。

表 8. ffdc コマンド

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。

オプション	説明	値
-t	タイプ番号	1 (プロセッサー・ダンプ) および 4 (サービス・データ)。プロセッサー・ダンプには使用可能なすべてのログおよびファイルが含まれています。サービス・データにはログおよびファイルのサブセットのみが含まれます。デフォルト値は 1 です。
-f [1]	リモート・ファイル名または sftp ターゲット・ディレクトリー。	sftp の場合は、ディレクトリー名 (~/ 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 [1]	tftp/sftp サーバーのアドレス	
-pn [1]	tftp/sftp サーバーのポート番号	デフォルト値は 69/22 です。
-u [1]	sftp サーバーのユーザー名	
-pw [1]	sftp サーバーのパスワード	
1. **generate** コマンドおよび **copy** コマンドの追加引数		

構文:
```
ffdc [options]
option:
 -t 1 or 4
 -f
 -ip ip_address
 -pn port_number
 -u username
  -pw password
```

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


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

hreport コマンド

組み込みヘルス・レポートを示すには、このコマンドを使用します。

下の表は、hreport コマンドを示しています。

表 9. hreport コマンド

次の表は、さまざまな hreport コマンドの説明で構成される複数行 2 列の表です。

オプション	説明
generate	新しいヘルス・レポートを作成します
status	ステータスを確認します
copy	既存のヘルス・レポートをコピーします
削除	既存のヘルス・レポートを削除します

次の表は、generate および copy オプションの引数を示しています。

表 10. generate および copy コマンド

次の表は、generate および copy コマンドのオプションとオプションの説明で構成される複数行 2 列の表です。

オプション	説明
-f	リモート・ファイル名または sftp ターゲット・ディレクトリー (デフォルトはシステムが生成した名前 (sftp の場合は、ディレクトリー名 (~/ または /tmp/) に絶対パスまたは後書きの / を使用します)
-ip	tftp/sftp サーバーのアドレス
-pn	tftp/sftp サーバーのポート番号 (デフォルトは 69/22)
-u	sftp サーバーのユーザー名
-pw	sftp サーバーのパスワード

mhlog コマンド

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

次の表は、オプションの引数を示しています。

表 11. mhlog コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

オプション	説明
-c <count>	「count」項目数を表示します (1-250)
-i <index>	インデックスで始まる項目を表示します (1-250)
-f	ログ・ファイルのリモート・ファイル名
-ip	tftp/sftp サーバーのアドレス
-pn	tftp/sftp サーバーのポート番号 (デフォルトは 69/22)
-u	sftp サーバーのユーザー名
-pw	sftp サーバーのパスワード

例

表示は次のようになります。

```
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: D1DG94C0075) is added.                            05/08/2020,06:43:28
```

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。

表 12. led コマンド

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。

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	
-chklog	チェック・ログ LED をオフにする	オフ
-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)

構文:
```
led [options]
option:
 -l
 -chklog off
 -identify state
  -d time
```

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。

readlog は、初回の実行時には、イベント・ログ内の最初の 5 つの項目を最も新しいものから順に表示し、その後、後続の呼び出しごとに次の 5 つを表示します。

readlog -a は、イベント・ログ内のすべての項目を、最も新しいものから順に表示します。

readlog -f は、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。

readlog -date *date* は、指定された日付 (mm/dd/yy の形式で指定) のイベント・ログ項目を表示します。日付は、パイプ (|) で区切ってリストにすることができます。

readlog -sev *severity* は、指定された重大度レベル (E、W、I) のイベント・ログ項目を表示します。重大度レベルは、パイプ (|) で区切ってリストにすることができます。

readlog -i *ip_address* は、イベント・ログが保存される TFTP または SFTP サーバーの IPv4 あるいは IPv6 IP アドレスを設定します。**-i** および **-l** 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。

readlog -l *filename* は、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 **-l** 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。

readlog -pn *port_number* は、TFTP または SFTP サーバーのポート番号 (デフォルト 69/22) を表示または設定します。

readlog -u *username* は、SFTP サーバーのユーザー名を指定します。

readlog -pw *password* は、SFTP サーバーのパスワードを指定します。

構文:
```
readlog [options]
option:
 -a
 -f
 -date date
 -sev severity
 -i ip_address
 -l filename
 -pn port_number
 -u username
  -pw password
```

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>
```

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、プロセッサー、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 [argument]
argument:
 summary    -display the system health summary
 activeevents -display active events
 cooling - display cooling devices health status
 power - display power modules health status
 storage - display local storage health status
 processors - display processors health status
  memory - display memory health status
```

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。

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR       W       T      SS      HS
-----------------------------------------------
CPU1     N/A     N/A    80/27    N/A     N/A
CPU2     N/A     N/A    80/27    N/A     N/A
DASD1  66/19   73/23   82/28   88/31   92/33
Amb    59/15   70/21   83/28   90/32   95/35
system>
```

注：

1. 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)
2. 温度値は、すべて華氏/摂氏となっています。
3. 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。

```
Example:
system> volts

     i HSL    SSL    WL     WRL    V      WRH    WH    SSH     HSH
-------------------------------------------------------------------
5v     5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75   6.00
3.3v   3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70   3.85
12v    12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40  12.65
-5v    -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40  -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80  -2.70
VRM1                          3.45
VRM2                          5.45
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 sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw  - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

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。

次の表には、**power** コマンドと一緒に使用できるコマンドのサブセットが記載されています。

表 13. power コマンド

次の表は、電源コマンド、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
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。	on、off
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。 **注：**-s 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します。	on、off
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。 **注：**-s 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します。	
power enterS3	オペレーティング・システムを S3 (スリープ) モードに移行させるには、このコマンドを使用します。 **注：**このコマンドは、オペレーティング・システムが稼働している場合にのみ使用します。S3 モードは、一部のサーバーではサポートされていません。	
power rp	このオプションは、ホストの電源復元ポリシーを指定するのに使用します。	alwayson|alwaysoff|restore
power S3resume	オペレーティング・システムを S3 (スリープ) モードからウェイクアップさせるには、このコマンドを使用します。 **注：**このコマンドは、オペレーティング・システムが稼働している場合にのみ使用します。S3 モードは、一部のサーバーではサポートされていません。	
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。	on、off

次の表には、**power on**、**power off**、および **power cycle** の各コマンドのオプションが記載されています。

表 14. power コマンド

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 14. power コマンド (続き)

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。	**注：**このオプションの値は、スペース上の制限が原因で、複数の行に分かれて表示されます。 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。	

構文:
```
power on
power off [-s]
power state
power cycle [-s]
```

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 13:00
```

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。

次の表は、オプションの引数を示しています。

表 15. reset コマンド

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。

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。	

構文:
```
reset [option]
option:
-s
-d
-nmi
```

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。次の表は、オプションの引数を示しています。

表 16. fuelg コマンド

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。

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。	input、output

表 16. fuelg コマンド (続き)

オプション	説明	値
-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)	時間単位の数値
-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。	• **bt-** スロットルあり基本 • **rt-** スロットルあり冗長 (デフォルト) • **ort-** N_1 スロットルあり冗長
-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	システム、マイクロプロセッサーおよび I/O を含む現行のコンピュート使用率を表示します。	パーセンテージ
-pc	現在の電力消費量を表示します	• **output-** 現在の DC 電力消費量を表示します。ラックおよびタワー・サーバーの場合は、システム、CPU、メモリー、およびその他のコンポーネントの電力消費量が含まれ、ITE ブレード・サーバーの場合は、システムの電力消費量のみが含まれます。 • **input** - 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。

構文:
```
fuelg [options]
option:
 -pme on/off
 -pcapmode input/output
 -pcap
 -history
 -period
 -pm bt/r/rt
 -zm on/off
 -perf
  -pc input/output
```

例:
```
system> fuelg
-pme: on
system>
```

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。

オプションを指定せずに **pxeboot** を実行すると、Preboot eXecution Environment の現行設定が返されます。次の表は、オプションの引数を示しています。

表 17. pxeboot コマンド

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 1 行 3 列の表です。

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

構文:
```
pxeboot [options]
option:
 -en state
```

例:
```
system> pxeboot
-en disabled
system>
```

serial redirect コマンド

このトピックには、serial redirect コマンドが含まれています。

シリアル・リダイレクト・コマンドは 111 ページの 「console コマンド」 の 1 つのみです。

console コマンド

このコマンドは、シリアル・リダイレクト・コンソール・セッションを開始するために使用します。

console コマンドを使用すると、指定された IMMのシリアル・ポートに対するシリアル・リダイレクト・コンソール・セッションが開始されます。

構文:
```
console 1
```

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・セキュリティー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。

オプションを指定せずに **accseccfg** コマンドを実行すると、すべてのアカウント・セキュリティー情報が表示されます。次の表は、オプションの引数を示しています。

表 18. accseccfg コマンド

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 18. accseccfg コマンド (続き)

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。
-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
-chgdft	初回ログイン後のデフォルト・パスワードの変更。	on、off
-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

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication method
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgdft state
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

例:

```
system> accseccfg
-legacy
```

```
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

alertcfg コマンド

IMM グローバル・リモート・アラート・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。

オプションを指定せずに **alertcfg** コマンドを実行すると、すべてのグローバル・リモート・アラート・パラメーターが表示されます。次の表は、オプションの引数を示しています。

表 19. alertcfg コマンド

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。

オプション	説明	値
-dr	IMM がアラートを再送するまでの再試行と再試行の間の待ち時間を設定します。	0 から 4.0 分 (0.5 分の増分で設定)
-da	IMM が、リストにある次の受信者にアラートを送信するまでの待ち時間を設定します。	0 から 4.0 分 (0.5 分の増分で設定)
-rl	前回の試行が失敗した場合に、IMM がアラートの送信を試行する追加の回数を設定します。	0 から 8

構文:

```
alertcfg [options]
 options:
  -rl retry_limit
  -dr retry_delay
   -da agent_delay
```

例:

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
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。

次の表には、**asu** コマンドと一緒に使用できるコマンドのサブセットが記載されています。

表 20. asu コマンド

次の表は、**asu** コマンドと一緒に使用できるコマンドのサブセットで構成される、複数行 3 列の表です。コマンドの説明情報および関連する値が示されます。

コマンド	説明	値
削除	設定のインスタンスまたはレコードを削除するには、このコマンドを使用します。設定は、削除できるインスタンスであることが必要です (たとえば、iSCSI.AttemptName.1)。	*setting_instance*
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*
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：** • 設定/値のペアを 1 つ以上設定します。 • 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。 • 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。 • 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"	*setting value*
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、取り付けたデバイスによって異なる場合があります。	*setting*
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*
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：** • 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。 • 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。 • デフォルト値があれば、それも表示されます。 • デフォルト値は、開く不等号括弧と閉じる不等号括弧 (< と >) で囲まれます。 • 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。	*setting*

注：

- コマンド構文の中で、*setting* は表示または変更する設定の名前を示し、*value* は設定に指定する値を示しています。
- *setting* は複数の名前にすることができます (**set** コマンドを使用する場合は除く)。
- *setting* には、たとえばアスタリスク (*) 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。
- *setting* は、グループ、設定名、または **all** とすることができます。

asu コマンドの構文の例を、次のリストに示します。

- 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。
- すべてのコマンドの詳細なヘルプを表示するには、`asu -v –help` と入力します。
- あるコマンドの詳細なヘルプを表示するには、`asu -v set –help` と入力します。
- 値を変更するには、`asu set` *`setting value`* と入力します。
- 現行値を表示するには、`asu show` *`setting`* と入力します。
- 長いバッチ形式で設定を表示するには、`asu show -l -b all` と入力します。
- 設定で指定できるすべての値を表示するには、`asu showvalues` *`setting`* と入力します。**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>
```

次の表は、オプションの引数を示しています。

表 21. 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。

オプション	説明	値
-b	バッチ形式で表示します。	
–help[1]	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 **asu --help show** のように、コマンドの前に置きます。	
–help[1]	コマンドのヘルプを表示します。–help オプションは、たとえば **asu show --help** のように、コマンドの後に置きます。	
-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[2]	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、**asu** 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 22. 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
tropen *id*	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。	*Id* は識別ストリングで、1 文字から 3 文字の英数字です。
trset *id*	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。	*Id* は識別ストリングで、1 文字から 3 文字の英数字です。
trlist *id*	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。	*Id* は識別ストリングで、1 文字から 3 文字の英数字です。
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。

次の表は、オプションの引数を示しています。

表 23. backup コマンド

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 23. backup コマンド (続き)

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
-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

構文:

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

例:

```
system> backup f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

dhcpinfo 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。

dhcpinfo 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:

```
dhcpinfo eth0
```

```
Example:
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

次の表は、上記の例からの出力を説明したものです。

表 24. dhcpinfo コマンド

次の表は、前述の例で使用されたオプションを説明する複数行 2 列の表です。

オプション	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
-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。

注：Flex System では、DNS 設定を IMMで変更することはできません。DNS 設定は CMM が管理します。

オプションを指定せずに **dns** コマンドを実行すると、DNS のすべての構成情報が表示されます。次の表は、オプションの引数を示しています。

表 25. dns コマンド

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 25. dns コマンド (続き)

オプション	説明	値
-state	DNS の状態	on、off
-ddns	DDNS の状態	enabled、disabled
-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)
-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)
-p	IPv4/IPv6 の優先順位	ipv4、ipv6

構文:
```
dns [options]
option:
 -state state
 -ddns state
 -i1 first_ipv4_ip_address
 -i2 second_ipv4_ip_address
 -i3 third_ipv4_ip_address
 -i61 first_ipv6_ip_address
 -i62 second_ipv6_ip_address
 -i63 third_ipv6_ip_address
  -p priority
```

注: 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。

例:
```
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>
```
次の表は、上記の例で使用するオプションについて説明しています。

表 26. dns コマンド出力

次の表は、前述の例で使用されたオプションを説明する複数行 2 列の表です。

表 26. dns コマンド出力 (続き)

オプション	説明
-state	DNS の状態 (on または off)
-i1	1 次 IPv4 DNS サーバーの IP アドレス
-i2	2 次 IPv4 DNS の IP アドレス
-i3	3 次 IPv4 DNS サーバーの IP アドレス
-i61	1 次 IPv6 DNS サーバーの IP アドレス
-i62	2 次 IPv6 DNS の IP アドレス
-i63	3 次 IPv6 DNS サーバーの IP アドレス
-ddns	DDNS の状態 (enabled または disabled)
-dnsrc	優先 DDNS ドメイン名 (dhcp または manual)
-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 または ipv6)

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。

次の表は、オプションの引数を示しています。

表 27. encaps コマンド

次の表は、オプションとその説明で構成される 1 行 2 列の表です。

オプション	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。

オプションを指定せずに **ethtousb** コマンドを実行すると、Ethernet-over-USB の情報が表示されます。次の表は、オプションの引数を示しています。

表 28. ethtousb コマンド

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 28. ethtousb コマンド (続き)

オプション	説明	値
-en	Ethernet-over-USB の状態	enabled、disabled
-m*x*	インデックス *x* のポート・マッピングを構成	コロン (:) で区切ったポートのペア (*port1*:*port2* の形式)。 ここで、それぞれ以下の意味があります。 • ポートのインデックス番号 *x* 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。 • ポート・ペアの *port1* は、外部イーサネットのポート番号です。 • ポート・ペアの *port2* は、Ethernet-over-USB のポート番号です。
-rm	指定されたインデックスのポート・マッピングを削除	1 ～ 10。 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 **ethtousb** コマンドを使用すると表示されます。

構文:
```
ethtousb [options]
option:
 -en state
 -mxport_pair
  -rm map_index
```

例:
```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
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。

次の表は、オプションの引数を示しています。

表 29. firewall コマンド

次の表は、オプションとオプションの説明で構成される複数行 3 列の表です。

オプション	説明	値
-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)	有効な IP アドレス **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。
-bmacs	1 ～ 3 個の MAC アドレスをブロックする (コンマ区切り)	有効な MAC アドレス **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。
-bbd	ブロックの開始日	<YYYY-MM-DD> 形式の日付
-bed	ブロックの終了日	<YYYY-MM-DD> 形式の日付

表 29. firewall コマンド (続き)

オプション	説明	値
-bbt	ブロックの開始時刻	<HH:MM> 形式の時刻
-bet	ブロックの終了時刻	<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) たとえば、*firewall - bti 01:00–02:00,05:05–10:30* 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。	<HH:MM-HH:MM> 形式の時間範囲
-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。 **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。	0 から 32 の間の数値。0 = ロックしない
-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。	del、clrall、show • -**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。 • -**clrall** : ブロック中のすべての IP をクリアします。 • -**show**: ブロック中のすべての IP を表示します。

例:
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”: Delete all blocking IP addresses.
· “firewall –ipbl –show”: Show all blocking IP addresses.

gprofile コマンド

IMM のグループ・プロファイルを表示および構成するには、このコマンドを使用します。

次の表は、オプションの引数を示しています。

表 30. gprofile コマンド

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 30. gprofile コマンド (続き)

オプション	説明	値
-clear	グループを削除します	enabled、disabled
-n	グループの名前	*group_name* の最大 63 文字のストリング *group_name* は、固有でなければなりません。
-a	役割ベースの権限レベル	supervisor、 operator、 rbs <role list>: nsc|am|rca|rcvma|pr|bc|cel|ac 役割リストの値は、値のパイプ区切りリストを使用して指定します。
-h	コマンドの使用法とオプションを表示します。	

構文:
```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n group_name
-a authority level:
  -nsc network and security
  -am user account management
  -rca remote console access
  -rcvma remote console and remote disk access
  -pr remote server power/restart access
  -bc basic adapter configuration
  -cel ability to clear event logs
  -ac advanced adapter configuration
-h help
```

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。

次の表は、オプションの引数を示しています。

表 31. hashpw コマンド

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。

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 ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f -a super
```

```
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c0665991881f383d4473e94f
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。

現行イーサネット・インターフェース構成を表示するには、**ifconfig eth0** と入力します。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・ネットワーキング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。

注：Flex System では、VLAN 設定は Flex System CMM が管理するため、IMM では変更できません。

次の表は、オプションの引数を示しています。

表 32. ifconfig コマンド

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。

オプション	説明	値
-b	組み込み MAC アドレス (読み取り専用で構成不可能)	
-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 **try dhcp server, if it fails use static config** オプションに対応します。)
-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、アンダースコアー、およびハイフンを含めることができます。
-r	Data rate	10、100、auto
-d	二重モード	full、half、auto
-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ことが必要です)。
-dn	ドメイン・ネーム	有効な形式のドメイン名。
-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

表 32. ifconfig コマンド (続き)

オプション	説明	値
-ghn	DHCP からホスト名を取得する	disabled、enabled
-nic	スイッチ NIC モード[1]	shared、dedicated、shared:nixX[2]
-failover[2]	フェイルオーバー・モード	none、shared、shared:nicX
-nssync[3]	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の長さの表 **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。	この値は読み取り専用であり、構成できません。
-ipv6	IPv6 の状態	disabled、enabled
-lla	リンク・ローカル・アドレス **注：**リンク・ローカル・アドレスが表示されるのは、IPv6 が有効な場合のみです。	リンク・ローカル・アドレスは、IMM によって決定されます。この値は読み取り専用であり、構成できません。
-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	DHCPv6 の状態	enabled、disabled
-sa6	IPv6 ステートレス自動構成の状態	enabled、disabled
-vlan	VLAN タグ付けを有効または無効にする	enabled、disabled
-vlanid	IMM のネットワーク・パケット識別タグ	1 から 4094 までの数値。

注：

1. -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。
2. shared:nicX 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す。IMM は、このメザニン・ネットワーク・カードを使用できます。
3. 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。
4. 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・ポートで使用される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。

構文:
```
ifconfig eth0 [options]
options:
```

-state *interface_state*
-c *config_method*
-i *static_ipv4_ip_address*
-g *ipv4_gateway_address*
-s *subnet_mask*
-n *hostname*
-r *data_rate*
-d *duplex_mode*
-m *max_transmission_unit*
-l *locally_administered_MAC*
-b *burned_in_MAC_address*
-dn *domain_name*
-auto *state*
-nic *state*
-failover mode
-nssync *state*
-address_table
-lla ipv6_link_local_addr
-dhcp6 *state*
-ipv6 *state*
-ipv6static *state*
-sa6 *state*
-i6 *static_ipv6_ip_address*
-g6 *ipv6_gateway_address*
-p6 *length*
-vlan *state*
-vlanid *VLAN ID*

例:

```
system> ifconfig eth0
-state  :  enabled
-c     :  dthens
-ghn    :  disabled
-i     :  192.168.70.125
-g     :  0.0.0.0
-s     :  255.255.255.0
-n     :  IMM00096B9E003A
-auto   :  true
-r     :  auto
-d     :  auto
-vlan   :  disabled
-vlanid :  1
-m     :  1500
-b     :  00:09:6B:9E:00:3A
-l     :  00:00:00:00:00:00
-dn    :
-ipv6   :  enabled
-ipv6static :  disabled
-i6    :  ::
-p6    :  64
-g6    :  ::
-dhcp6  :  enabled
-sa6    :  enabled
-lla    :  fe80::6eae:8bff:fe23:91ae
-nic :  shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot #5 [active]
-address_table  :

system> ifconfig eth0 -c static -i 192.168.70.133
```

```
These configuration changes will become active after the next reset of the IMM.
```

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：

- 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。
- 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。

次の表は、オプションの引数を示しています。

表 33. keycfg コマンド

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。

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、および -f コマンド・オプションの値
-ip	追加するアクティベーション・キーがある TFTP サーバーの IP アドレス	TFTP サーバーの有効な IP アドレス
-pn	追加するアクティベーション・キーがある 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	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	SFTP サーバーの有効なユーザー名
-pw	追加するアクティベーション・キーがある 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
-f	追加するアクティベーション・キーのファイル名	アクティベーション・キー・ファイルの有効なファイル名
-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

構文:

```
keycfg [options]
option:
```

```
-add
  -ip tftp/sftp server ip address
  -pn pn port number of tftp/sftp server (default 69/22)
  -u  username for sftp server
  -pw password for sftp server
  -f  filename
  -del  n ( where n is a valid ID number from listing)
  -deltype x ( where x is a Type value)
```

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。

次の表は、オプションの引数を示しています。

表 34. ldap コマンド

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。

オプション	説明	値
-a	ユーザー認証方式	ローカルのみ、LDAP のみ、最初がローカルで次に LDAP、最初が LDAP で次にローカル
-aom	認証専用モード	enabled、disabled
-b	バインディング方式	匿名、ClientDN とパスワードを使用したバインド、ログイン資格情報を使用したバインド
-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
-f	グループ・フィルター	*group_filter* の最大 127 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。
-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。
-ep	暗号化されたパスワード	パスワードのバックアップ/復元 (内部でのみ使用)
-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

表 34. ldap コマンド (続き)

オプション	説明	値
-rbs	Active Directory ユーザーの拡張役割ベース・セキュリティー	enabled、disabled
-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
-t	サーバーのターゲット名	rbs オプションが有効に設定されている場合、このフィールドは、ロール・ベース・セキュリティー (RBS) スナップイン・ツールを使用して Active Directory サーバー上の 1 つ以上の役割に関連付けることができるターゲット名を指定します。
-u	UID 検索属性	*search_attrib* 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	

構文:

```
ldap [options]
options:
  -a loc|ldap|locld|ldloc
  -aom enable/disabled
  -b anon|client|login
  -c client_dn
  -d search_domain
  -f group_filter
  -fn forest_name
  -g group_search_attr
  -l string
  -p client_pw
  -pc confirm_pw
  -ep encrypted_pw
  -r root_dn
  -rbs enable|disabled
  -s1ip host name/ip_addr
  -s2ip host name/ip_addr
  -s3ip host name/ip_addr
  -s4ip host name/ip_addr
  -s1pn port_number
  -s2pn port_number
```

-s3pn *port_number*
-s4pn *port_number*
-t *name*
-u *search_attrib*
-v *offlon*
-h

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。

次の表は、オプションの引数を示しています。

表 35. ntp コマンド

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。

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[1]	Network Time Protocol サーバーの名前または IP アドレス。これは、Network Time Protocol サーバーのインデックス番号です。	クロック同期には NTP サーバーの名前を使用します。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。
-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。

1. -i は i1 と同じです。

構文:
```
ntp [options]
options:
-en state
-i hostname/ip_addr
-f frequency
-synch
```

例:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

portcfg コマンド

シリアル・リダイレクト機能のために IMM を構成するには、このコマンドを使用します。

IMM の構成は、サーバーの内部シリアル・ポートの設定と一致させる必要があります。シリアル・ポート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。シリアル・ポート構成を変更するには、少なくとも「アダプター・ネットワーキングおよびセキュリティー構成」権限を持っている必要があります。

注：サーバーの外部シリアル・ポートは、IPMI 機能のために IMM のみが使用できます。CLI は、シリアル・ポートではサポートされていません。Remote Supervisor Adapter II の CLI に存在していた **serred** オプションと **cliauth** オプションは、サポートされていません。

オプションを指定せずに **portcfg** コマンドを実行すると、シリアル・ポート構成が表示されます。
次の表は、オプションの引数を示しています。

注：データ・ビット (8) の番号はハードウェアに設定されているため、変更できません。

表 36. portcfg コマンド

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。

オプション	説明	値
-b	ボー・レート	9600, 19200, 38400, 57600, 115200
-p	パリティー	none、odd、even
-s	ストップ・ビット	1, 2
-climode	CLI モード	0, 1, 2 ここで、それぞれ以下の意味があります。 • 0 = none: CLI は無効になります。 • 1 = cliems: CLI は EMS 互換キー・ストローク・シーケンスで有効になります。 • 2 = cliuser: CLI は、ユーザー定義キー・ストローク・シーケンスで有効になります。

構文:
```
portcfg [options]
 options:
  -b baud_rate
  -p parity
  -s stopbits
   -climode mode
```

例:
```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

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。

このコマンドは現在、IPMI プロトコルのポートのコントロールのみをサポートしています。IPMI ポートの状態を表示するには、**portcontrol** と入力します。IPMI ネットワーク・ポートを有効または無効にするには、**-ipmi** オプションを入力し、その後に **on** または **off** の値を入力します。

表 37. portcontrol コマンド

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。

オプション	説明	値
-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
-cim	CIM ディスカバリーを有効または無効にする	on、off
-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 アクセスを有効または無効にする	on、off
-rest	REST ディスカバリーを有効または無効にする	on、off
-slp	SLP 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

構文:
```
portcontrol [options]
 options:
  -ipmi on/off
```

例:
```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

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。

オプションを指定せずに **ports** コマンドを実行すると、すべての IMM ポートの情報が表示されます。次の表は、オプションの引数を示しています。

表 38. ports コマンド

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。

オプション	説明	値
-open	オープン・ポートの表示	
-reset	ポートをデフォルトの設定値にリセット	
-httpp	HTTP ポート番号	デフォルトのポート番号: 80
-httpsp	HTTPS ポート番号	デフォルトのポート番号: 443
-sshp	SSH のレガシー CLI ポート番号	デフォルトのポート番号: 22
-snmpap	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
-snmptp	SNMP トラップのポート番号	デフォルトのポート番号: 162
-rpp	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
-cimhp	CIM over HTTP ポート番号	デフォルトのポート番号: 5988
-cimhsp	CIM over HTTPS ポート番号	デフォルトのポート番号: 5989

構文:
```
ports [options]
option:
 -open
 -reset
 -httpp port_number
 -httpsp port_number
 -sshp port_number
 -snmpap port_number
 -snmptp port_number
 -rpp port_number
 -cimhp port_number
  -cimhsp port_number
```

例:
```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
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用をマウントするには、このコマンドを使用します。

次の表は、オプションの引数を示しています。

表 39. rdmount コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

表 39. rdmount コマンド (続き)

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。

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) -o オプション (Samba および NFS マウント用の追加オプション・ストリング) -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>	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。

次の表は、オプションの引数を示しています。

表 40. restore コマンド

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 40. restore コマンド (続き)

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

構文:
```
restore [options]
option:
 -f filename
 -pp password
 -ip ip_address
 -pn port_number
 -u username
  -pw password
```

例:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

restoredefaults コマンド

IMM 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。

- **restoredefaults** コマンドにオプションはありません。
- コマンドを処理する前に、コマンドの確認を求められます。

構文:
```
restoredefaults
```

例:
```
system> restoredefaults

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
```

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。

次の表は、オプションの引数を示しています。

表 41. roles コマンド

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。

オプション	説明	値
-n	構成する役割	32 文字に制限される
-p	特権の設定	カスタム: am | rca | rcvma | pr | cel | bc | nsc | ac | us • **am**: ユーザー・アカウント管理アクセス • **rca**: リモート・コンソール・アクセス • **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 • **pr**: リモート・サーバー電源/再起動アクセス • **cel**: イベント・ログを消去する機能 • **bc**: アダプター構成 (基本) • **nsc**: アダプター構成 (ネットワークおよびセキュリティー) • **ac**: アダプター構成 (拡張) • **us**: UEFI セキュリティー **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	

構文

```
 roles [-options] - display/configure roles
  - role_account -role number[3-31]
options:
  -n     - role name (limited to 32 characters)
  -p     - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
    am   - User account management access
    rca  - Remote console access
    rcvma - Remote console and remote disk (virtual media) access
    pr   - Remote server power/restart access
    cel  - Ability to clear event logs
    bc   - Adapter Configuration (basic)
    nsc  - Adapter Configuration (network and security)
    ac   - Adapter Configuration (advanced)
    us   - UEFI Security
    Note: the above custom permission flags can be used in any combination
  -d     - delete a row
```

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
```

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。

次の表は、オプションの引数を示しています。

表 42. seccfg コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

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	yes、no
-rppen	リモート物理プレゼンスが有効です (読み取り専用)	/
-rppto	リモート物理プレゼンスがタイムアウトです (読み取り専用)	/
-rpp	物理プレゼンス (BIOS で有効の場合)	yes、no
-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の有効化または無効化	enabled、disabled

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 43. 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
```

smtp コマンド

SMTP インターフェースの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。

オプションを指定せずに **smtp** コマンドを実行すると、SMTP インターフェースのすべての情報が表示されます。次の表は、オプションの引数を示しています。

表 44. smtp コマンド

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。

オプション	説明	値
-auth	SMTP 認証のサポート	enabled、disabled
-authepw	SMTP 認証の暗号化パスワード	有効なパスワード・ストリング
-authmd	SMTP 認証方式	CRAM-MD5、LOGIN
-authn	SMTP 認証のユーザー名	ストリング (256 文字の制限)
-authpw	SMTP 認証のパスワード	ストリング (256 文字の制限)
-pn	SMTP ポート番号	有効なポート番号
-s	SMTP サーバーの IP アドレスまたはホスト名	有効な IP アドレスまたはホスト名 (63 文字の制限)。

構文:
```
smtp [options]
option:
 -auth enabled|disabled
 -authepw password
 -authmd CRAM-MD5|LOGIN
 -authn username
 -authpw password
 -s ip_address_or_hostname
  -pn port_number
```

例:
```
system> smtp
-s test.com
-pn 25
system>
```

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。

オプションを指定せずに **snmp** コマンドを実行すると、SNMP インターフェースのすべての情報が表示されます。次の表は、オプションの引数を示しています。

表 45. snmp コマンド

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 45. snmp コマンド (続き)

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。 • 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。 • 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。
-t1	SNMPv1 トラップ	on、off
-t2	SNMPv2 トラップ	on、off
-t	SNMPv3 トラップ	on、off
-l	IMM の位置	ストリング (47 文字の制限)。 **注：** • 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。 • 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。
-cn	IMM の連絡先名	ストリング (47 文字の制限)。 **注：** • 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。 • 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。
-c	SNMP コミュニティー名	ストリング (15 文字の制限)。 **注：** • 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。 • 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 コミュニティー名がクリアされます。
-ct	SNMPv2 トラップのコミュニティー名	ストリング (15 文字の制限)。 **注：** • 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。 • 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。
-ci	SNMP コミュニティーの IP アドレス/ホスト名	有効な IP アドレスまたはホスト名 (63 文字の制限)。 **注：** • 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。 • 引数を指定しないと、SNMP コミュニティーの IP アドレスまたはホスト名がクリアされます。

表 45. snmp コマンド (続き)

オプション	説明	値
-cti	SNMPv2 トラップのコミュニティー IP アドレス/ホスト名	有効な IP アドレスまたはホスト名 (63 文字の制限)。 **注：** • 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。 • 引数を指定しないと、SNMP コミュニティーの IP アドレスまたはホスト名がクリアされます。
-eid	SNMP エンジン ID	ストリング (1 から 27 文字の制限)

構文:
```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
  -t2 state
  -ct community name
  -cti community IP address/hostname
   -eid engine id
```

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。

オプションを指定せずに **snmpalerts** を実行すると、すべての SNMP アラート設定が表示されます。次の表は、オプションの引数を示しています。

表 46. snmpalerts コマンド

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 46. snmpalerts コマンド (続き)

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 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、**snmpalerts -crt custom:te|vo** 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。 • te: クリティカルな温度しきい値超過 • vo: クリティカルな電圧しきい値超過 • po: クリティカルな電源障害 • di: ハードディスク・ドライブ障害 • fa: ファン障害 • cp: マイクロプロセッサー障害 • me: メモリー障害 • in: ハードウェアの互換性なし • re: 電源の冗長性の障害 • ot: その他すべてのクリティカル・イベント
-crten	クリティカル・イベント・アラートを送信	enabled、disabled
-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 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、**snmpalerts -wrn custom:rp|te** 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。 • rp: 電源の冗長性の警告 • te: 警告の温度しきい値超過 • vo: 警告の電圧しきい値超過 • po: 警告の電力しきい値超過 • fa: クリティカルではないファン・イベント • cp: マイクロプロセッサーが機能低下状態 • me: メモリーの警告 • ot: その他すべての警告イベント
-wrnen	警告イベント・アラートを送信	enabled、disabled
-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 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、**snmpalerts -sys custom:lo|tio** 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。 • lo: 正常なリモート・ログイン • tio: オペレーティング・システムのタイムアウト • 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 • po: システムの電源オン/オフ • bf: オペレーティング・システムのブート障害 • 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 • pf: 予知された障害 (PFA)

表 46. snmpalerts コマンド (続き)

オプション	説明	値
		• el: イベント・ログ 75% フル • ne: ネットワーク変更
-sysen	ルーチン・イベント・アラートを送信	enabled、disabled

構文:
```
snmpalerts [options]
 options:
  -status status
  -crt event_type
  -crten state
  -wrn event_type
  -wrnen state
  -sys event_type
   -sysen state
```

srcfg コマンド

シリアル・リダイレクト・モードから CLI に入るキー・シーケンスを示すには、このコマンドを使用します。

シリアル・リダイレクト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。シリアル・リダイレクト構成を変更するには、少なくとも「アダプター・ネットワーキングおよびセキュリティー構成」権限を持っている必要があります。

注：IMM ハードウェアは、シリアル・ポートからシリアル・ポートのパススルー機能を備えていません。したがって、Remote Supervisor Adapter II の CLI に存在する `-passthru` オプションと `entercliseq` オプションはサポートされていません。

オプションを指定せずに **srcfg** コマンドを実行すると、現行のシリアル・リダイレクトのキー・ストローク・シーケンスが表示されます。次の表は、`srcfg -entercliseq` コマンド・オプションの引数を示しています。

表 47. srcfg コマンド

次の表は、オプション、オプションの説明、そのオプションの値の情報で構成される 1 行 3 列の表です。

オプション	説明	値
-entercliseq	CLI キー・ストローク・シーケンスに入ります。	CLI に入るためのユーザー定義キー・ストローク・シーケンス。 **注：**このシーケンスには、1 から 15 個の文字が必要です。このシーケンスでは、脱字記号 (^) には特別な意味があります。これは、Ctrl シーケンスにマップするキー・ストロークの Ctrl を意味しています (たとえば、^[は Esc キー、^M は復帰)。^ が出現すると、それらはすべて Ctrl シーケンスの一部と解釈されます。すべての Ctrl シーケンスのリストについては、ASCII/キー変換テーブルを参照してください。このフィールドのデフォルト値は ^[(であり、これは Esc の後に (が付いたものです。

構文:
```
srcfg [options]
options:
```

-entercliseq *entercli_keyseq*

例:
```
system> srcfg
-entercliseq ^[Q
system>
```

sshcfg 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。

オプションを指定せずに **sshcfg** コマンドを実行すると、すべての SSH パラメーターが表示されます。次の表は、オプションの引数を示しています。

表 48. sshcfg コマンド

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。

オプション	説明	値
-cstatus	SSH CLI の状態	enabled、disabled
-hk gen	SSH サーバーの秘密鍵を生成	
-hk rsa	サーバーの RSA 公開鍵を表示	

構文:
```
sshcfg [options]
option:
 -cstatus state
 -hk gen
 -hk rsa
```

例:
```
system> sshcfg
-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>
```

ssl コマンド

SSL 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。

SSL クライアントを有効にするには、クライアント証明書がインストールされている必要があります。オプションを指定せずに **ssl** コマンドを実行すると、SSL パラメーターが表示されます。次の表は、オプションの引数を示しています。

表 49. ssl コマンド

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 49. ssl コマンド (続き)

オプション	説明	値
-ce	SSL クライアントの有効化または無効化	on、off
-se	SSL サーバーの有効化または無効化	on、off
-cime	SSL サーバー上での CIM over HTTPS の有効化または無効化	on、off

構文:
```
portcfg [options]
 options:
  -ce state
  -se state
   -cime state
```

パラメーター: 以下のパラメーターは、**ssl** コマンドのオプション状況表示でのみ提示され、CLI でのみ出力されます。

Server secure transport enable
この状況表示は読み取り専用で、直接設定することはできません。

Server Web/CMD key status
この状況表示は読み取り専用で、直接設定することはできません。コマンド・ライン出力値には、以下の値があります。

プライベート・キーおよび証明書/CSR は使用できません

プライベート・キーおよび CA 署名済み証明書インストール済み

プライベート・キーおよび自動生成自己署名済み証明書インストール済み

プライベート・キーおよび自己署名済み証明書インストール済み

プライベート・キー保存済み、CSR ダウンロード可能

SSL server CSR key status
この状況表示は読み取り専用で、直接設定することはできません。コマンド・ライン出力値には、以下の値があります。

プライベート・キーおよび証明書/CSR は使用できません

プライベート・キーおよび CA 署名済み証明書インストール済み

プライベート・キーおよび自動生成自己署名済み証明書インストール済み

プライベート・キーおよび自己署名済み証明書インストール済み

プライベート・キー保存済み、CSR ダウンロード可能

SSL client LDAP key status
この状況表示は読み取り専用で、直接設定することはできません。コマンド・ライン出力値には、以下の値があります。

プライベート・キーおよび証明書/CSR は使用できません

プライベート・キーおよび CA 署名済み証明書インストール済み

プライベート・キーおよび自動生成自己署名済み証明書インストール済み

プライベート・キーおよび自己署名済み証明書インストール済み

プライベート・キー保存済み、CSR ダウンロード可能

SSL client CSR key status

この状況表示は読み取り専用で、直接設定することはできません。コマンド・ライン出力値には、以下の値があります。

プライベート・キーおよび証明書/CSR は使用できません

プライベート・キーおよび CA 署名済み証明書インストール済み

プライベート・キーおよび自動生成自己署名済み証明書インストール済み

プライベート・キーおよび自己署名済み証明書インストール済み

プライベート・キー保存済み、CSR ダウンロード可能

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。

オプションを指定せずに **sslcfg** コマンドを実行すると、SSL のすべての構成情報が表示されます。**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。次の表は、オプションの引数を示しています。

表 50. sslcfg コマンド

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。

オプション	説明	値
-server	SSL サーバー状況	enabled、disabled **注：**SSL サーバーは、有効な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。
-client	SSL クライアントの状況	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。
-cim	CIM over HTTPS の状況	enabled、disabled **注：**CIM over HTTPS 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：** • 自己署名証明書を生成する際には、**-c**、**-sp**、**-cl**、**-on**、および **-hn** コマンド・オプションの値は必須です。 • 自己署名証明書を生成する際には、**-cp**、**-ea**、**-ou**、**-s**、**-gn**、**-in**、および **-dq** コマンド・オプションの値はオプションです。
-csr	CSR の生成	server、client、sysdir、storekey **注：** • CSR を生成する際には、**-c**、**-sp**、**-cl**、**-on**、および **-hn** コマンド・オプションの値は必須です。 • CSR を生成する際には、**-cp**、**-ea**、**-ou**、**-s**、**-gn**、**-in**、**-dq**、**-cpwd**、および **-un** コマンド・オプションの値はオプションです。
-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

表 50. sslcfg コマンド (続き)

オプション	説明	値
-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	証明書ファイルのダウンロード	このオプションには引数を使用しませんが、**-cert** または **-csr** コマンド・オプション (ダウンロードする証明書のタイプによって異なる) にも値を指定する必要があります。このオプションには引数を使用しませんが、**-i** コマンド・オプション、および **-l** (オプション) コマンド・オプションにも値を指定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、**-cert**、**-i**、および **-l** コマンド・オプションは指定する必要があります。
-tc*x*	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 3 の整数として指定されます。
-c	国	国別コード (2 文字) **注：**自己署名証明書または CSR を生成する際には必須です。
-sp	都道府県/州	引用符で区切ったストリング (最大 60 文字) **注：**自己署名証明書または CSR を生成する際には必須です。
-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) **注：**自己署名証明書または CSR を生成する際には必須です。
-on	組織名	引用符で区切ったストリング (最大 60 文字) **注：**自己署名証明書または CSR を生成する際には必須です。
-hn	IMM ホスト名	ストリング (最大 60 文字) **注：**自己署名証明書または CSR を生成する際には必須です。
-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) **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。
-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) **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。
-ou	組織単位	引用符で区切ったストリング (最大 60 文字) **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。
-s	姓	引用符で区切ったストリング (最大 60 文字) **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。
-gn	名	引用符で区切ったストリング (最大 60 文字) **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。
-in	イニシャル	引用符で区切ったストリング (最大 20 文字) **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。
-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) **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。
-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) **注：**CSR を生成する際にはオプションです。
-un	非構造化名	引用符で区切ったストリング (最大 60 文字) **注：**CSR を生成する際にはオプションです。

構文:
```
sslcfg [options]
option:
 -server state
 -client state
 -cim state
 -cert certificate_type
 -csr certificate_type
 -i ip_address
 -pn port_number
 -u username
 -pw password
 -l filename
 -dnld
 -upld
 -tc xaction
 -c country_code
 -sp state_or_province
 -cl city_or_locality
 -on organization_name
 -hn bmc_hostname
 -cp contact_person
 -ea email_address
 -ou organizational_unit
 -s surname
 -gn given_name
 -in initials
 -dq dn_qualifier
 -cpwd challenge_password
  -un unstructured_name
```

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 CIM 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 Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

上記の例は、スペース上の制約のため、複数の行に表示されます。

- 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 tklm.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 Lenovo -hn XCC-5cf3fc6e0c9d
-cp Contact -ea "" -ou "
ok
```
上記の例は、スペース上の制約のため、複数の行に表示されます。

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 tklm-server.der
ok
```

storekeycfg コマンド

SKLM サーバーのホスト名または IP アドレス、およびネットワーク・ポートを構成するには、このコマンドを使用します。

最大 4 個の SKLM サーバーのターゲットを構成できます。**storekeycfg** コマンドは、IMM で SKLM サーバーへの認証に使用される証明書のインストールおよび削除にも使用されます。

次の表は、オプションの引数を示しています。

表 51. storekeycfg コマンド

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。

オプション	説明	値
-add	アクティベーション・キーの追加	値は -ip、-pn、-u、-pw、および -f コマンド・オプションです。
-ip	TFTP/SFTP サーバーのホスト名または IP アドレス	TFTP/SFTP サーバーの有効なホスト名または IP アドレス
-pn	TFTP または 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 (デフォルト値は 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
-f	アクティベーション・キーのファイル名	アクティベーション・キー・ファイル名の有効なファイル名。
-del	アクティベーション・キーをインデックス番号で削除するには、このコマンドを使用します	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
-dgrp	デバイス・グループの追加	デバイス・グループ名

表 51. storekeycfg コマンド (続き)

オプション	説明	値
-sxip	SKLM サーバーのホスト名または IP アドレスの追加	SKLM サーバーの有効なホスト名または IP アドレス。1、2、3、または 4 の数値。
-sxpn	SKLM サーバーのポート番号の追加	SKLM サーバーの有効なポート番号1、2、3、または 4 の数値。
-testx	構成および SKLM サーバーへの接続のテスト	1、2、3、または 4 の数値
-h	コマンドの使用法とオプションを表示します。	

構文:
```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

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 tklm-server.der
system> ok
```

SKLM サーバー・アドレスとポート番号を構成するには、次のコマンドを入力します。
```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

デバイス・グループ名を設定するには、次のコマンドを入力します。
```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

syncrep コマンド

リモート・リポジトリーからファームウェア同期を開始するには、このコマンドを使用します。

次の表は、オプションの引数を示しています。

表 52. syncrep コマンド

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。

オプション	説明	値
-t	リポジトリーを接続するためのプロトコル	samba、nfs
-l	リモート・リポジトリーの場所	URL 形式
-u	ユーザー	
-p	パスワード	
-o	オプション	Samba および NFS マウント用の追加オプション・ストリング
-d	ドメイン	Samba マウント用ドメイン
-q	現在の更新ステータスの照会	
-c	同期プロセスをキャンセルする	

構文

```
syncrep [options]  Launch firmware sync from remote repository
 options:
   -t <samba|nfs> protocol to connect repository
   -l location of remote repository (URL format)
   -u User
   -p Password
   -o option (extra option string for samba and nfs mounts)
   -d domain (domain for samba mount)
   -q query current update status
   -c cancel the sync process
```

例

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

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。

表 53. thermal コマンド

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 53. thermal コマンド (続き)

オプション	説明	値
-mode	サーマル・モードの選択	normal、performance、minimal、efficiency、custom
-table	ベンダー、デバイス識別 (ID) および代替サーマル・テーブル	

構文:
```
thermal [options]
option:
 -mode thermal_mode
 -table vendorID_devicetable_number
```

例:
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

timeouts コマンド

タイムアウト値を表示または変更するには、このコマンドを使用します。

- タイムアウトを表示するには、timeouts と入力します。
- タイムアウト値を変更するには、オプションと、それに続けて値を入力します。
- タイムアウト値を変更するには、少なくとも「アダプター構成」権限を持っている必要があります。

次の表は、タイムアウト値の引数を示しています。これらの値は、Web インターフェースでサーバー・タイムアウトを選択する、選択値が列記されたプルダウン・オプションに一致します。

表 54. timeouts コマンド

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 4 列の表です。

オプション	タイムアウト	単位	値
-f	電源オフ遅延	分	disabled、0.5、1、2、3、4、5、7.5、10、15、20、30、60、120
-l	ローダー・タイムアウト	分	disabled、0.5、1、1.5、2、2.5、3、3.5、4、4.5、5、7.5、10、15、20、30、60、120
-o	オペレーティング・システムのタイムアウト	分	disabled、2.5、3、3.5、4
-s	HW エラーで OS 障害のスクリーン・キャプチャー	/	disabled、enabled

構文:
```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
```

-l *loader_watchdog_option*
-s *OS failure screen capture with HW error*

例:
```
system> timeouts
-o disabled
-l 3.5
-f disabled
-s disabled
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
-f disabled
-s disabled
```

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。

次の表は、オプションの引数を示しています。

表 55. tls コマンド

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。

オプション	説明	値
-min	TLS の最小レベルを選択します。	1.0, 1.1, 1.2[1], 1.3
-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。

使用例:
```
tls [-options] - configures the minimum TLS level
  -min <1.0 | 1.1 | 1.2 | 1.3> - Selects the minimum TLS level
  -h - Lists usage and options
```

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。

次の表は、オプションの引数を示しています。

表 56. uefipw コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

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

構文:

```
usage:
  trespass display the trespass message
  -s <trespass message> configure trespass message
  -h - Lists usage and options
```

例:

注 : 侵入警告メッセージにはスペースが含まれていません。

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

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。

次の表は、オプションの引数を示しています。

表 57. uefipw コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

表 57. uefipw コマンド (続き)

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)
-cep	暗号化された現在のパスワード
-ep	暗号化された新しいパスワード

構文:
```
usage:
  uefipw [-options] - Configure the UEFI admin password
options:
  -cp    - current password (limited to 20 characters)
  -p     - new password (limited to 20 characters)
  -cep   - current password encrypted
  -ep    - new password encrypted
```

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。

構文:
```
usbeth [options]
options:
-en <enabled|disabled>
```

例:
```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

usbfp コマンド

前面パネル USB ポートの BMC の使用を制御するには、このコマンドを使用します。

次の表は、オプションの引数を示しています。

表 58. usbfp コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

オプション	説明
-mode <bmc | server | shared>	使用モードを BMC、サーバー、または共用に設定します
-it <minutes>	非アクティブ・セッションのタイムアウト (分) (共用モード
-btn <on | off>	ID ボタンを使用したオーナーの切り替えを有効にします (共用モード)
-own <bmc | server >	オーナーを BMC またはサーバーに設定します (共用モード)

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。次の表は、オプションの引数を示しています。

表 59. users コマンド

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。

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	1 から 12、またはすべてのユーザーの場合は all。
-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ーのみを含む固有のストリング。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ストリング。最小で 6 文字、最大で 20 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。
-a	権限レベル	権限レベルは、以下のいずれかのレベルにすることができます。 • super (スーパーバイザー) • ro (読み取り専用) • 以下の値を | で区切って任意に組み合わせたもの – am (ユーザー・アカウント管理アクセス) – rca (リモート・コンソール・アクセス) – rcvma (リモート・コンソールおよび仮想メディア・アクセス) – pr (リモート・サーバーの電源/再起動アクセス) – cel (イベント・ログをクリアする権限) – bc (アダプター構成 - [基本]) – nsc (アダプター構成 - [ネットワークおよびセキュリティー]) – ac (アダプター構成 - [拡張])
-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
-clear	指定されたユーザー・アカウントの削除 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ます。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。	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。 users -clear -*user_index*

表 59. users コマンド (続き)

オプション	説明	値
-curr	現在ログイン中のユーザーの表示	
-sauth	SNMPv3 認証プロトコル	HMAC-SHA、なし
-spriv	SNMPv3 プライバシー・プロトコル	CBC-DES、AES、none
-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、set
-strap	SNMPv3 トラップ・ホスト名	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：** • 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。 • 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` の形式で使用する必要があります。 • すべての鍵は、OpenSSH フォーマットです。 • Flex ノードの場合、ユーザー・コマンドはローカルの IPMI および SNMP アカウントにのみ制限されます。オプション `-pk` は Flex Systems ではサポートされていません。
-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。 • Flex ノードの場合、ユーザー・コマンドはローカルの IPMI および SNMP アカウントにのみ制限されます。オプション `-remove` は Flex Systems ではサポートされていません。

表 59. users コマンド (続き)

オプション	説明	値
-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：** • -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。 • 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 "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ==" • Flex ノードの場合、ユーザー・コマンドはローカルの IPMI および SNMP アカウントにのみ制限されます。オプション -add は Flex Systems ではサポートされていません。
-upld	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：** • -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)。 • 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。 • 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。 • Flex ノードの場合、ユーザー・コマンドはローカルの IPMI および SNMP アカウントにのみ制限されます。オプション -upld は Flex Systems ではサポートされていません。
-dnld	指定された SSH 公開鍵のダウンロード *(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 -*key_index* オプションが必要で、TFTP サーバーを稼働している別のコンピューター上のダウンロード・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：** • -dnld 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、-l、および -*key_index* を除く)。 • 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 -dnld -1 -i tftp://9.72.216.40/ -l file.key の形式で使用する必要があります。
-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 サーバーの IP アドレス *(SSH 公開鍵オプション)*	有効な IP アドレス **注：** -i オプションは、users -pk -upld および users -pk -dnld コマンド・オプションで必要です。

表 59. users コマンド (続き)

オプション	説明	値
-pn	TFTP/SFTP サーバーのポート番号 *(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：**users -pk -upld および users -pk -dnld コマンド・オプションのオプション・パラメーター。
-u	SFTP サーバーのユーザー名 *(SSH 公開鍵オプション)*	有効なユーザー名 **注：**users -pk -upld および users -pk -dnld コマンド・オプションのオプション・パラメーター。
-pw	SFTP サーバーのパスワード *(SSH 公開鍵オプション)*	有効なパスワード **注：**users -pk -upld および users -pk -dnld 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：**-l オプションは、users -pk -upld および users -pk -dnld 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、-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 -cm "This is my comment." の形式で使用する必要があります。

構文:

```
users [-options] - display/configure user accounts
options:
  -[1-12] - user account number
  -l    - display password expiration days
  -n    - username (limited to 16 characters)
  -p    - password (limited to 32 characters)
  -shp   - set hashpassword (total 64 characters)
  -ssalt  - set salt (limited to 64 characters)
  -ghp   - get hashpassword
  -gsalt  - get salt
  -ep    - encrypted password (used with backup/restore )

  -a    - authority level (super, ro, custom:am|rca|rcvma|pr|cel|bc|nsc|ac)
    -am   - User account management access
    -rca  - Remote console access
    -rcvma - Remote console and remote disk (virtual media) access
    -pr   - Remote server power/restart access
    -cel  - Ability to clear event logs
    -bc   - Adapter Configuration (basic)
    -nsc  - Adapter Configuration (network and security)
    -ac   - Adapter Configuration (advanced)

  -clear  - clear user account
  -curr   - display current users
  -sauth  (none|HMAC-SHA)       - snmpv3 authentication protocol
  -spriv  (none|CBC-DES|AES)    - snmpv3 privacy protocol
  -spw   password           - snmpv3 privacy password
  -sepw   encryptedpassword     - snmpv3 privacy password (encrypted)
  -sacc   (Get)          - snmpv3 Access type
```

```
  -strap  hostname           - snmpv3 trap hostname

  -pk    - SSH public keys options:
    -e     - Displays the entire key in OpenSSH format
    -remove  - Removes the specified key for the specified user
    -add    - Adds a public key for the specified user
    -upld   - Used to upload a public key in OpenSSH/RFC4716 format
    -dnld   - Used to download the specified public key to a TFTP/SFTP server
    -i     - IP address of the TFTP/SFTP
    -pn     - port number of tftp/sftp server (default 69/22)
    -u     - username for sftp server
    -pw     - password for sftp server
    -l     - Filename of the key file when uploading or downloading via TFTP/SFTP
    -af     - accept connections from host, in the format: from="<list>", where
          <list> is a comma-separated list of hostnames and IP addresses
          (limited to 511 characters)
    -cm     - comment (limited to 255 characters, must be quote-delimited)
```

注：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

例:

```
system> users
 Account    Login ID    Advanced Attribute        Role       Password Expires
 -------    --------    ------------------       ------      ----------------
   1       USERID           Native          Administrator           89 day(s)
system> users -2 -n sptest -p Passw0rd12 -a super
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account    Login ID    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 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -a super
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system> users -2 -n sptest -p Passw0rd12 -a custom:am|rca
The user is required to change the password when the user logs in to the management server for the first time
ok
```

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。

alertentries コマンド

アラート受信者を管理するには、このコマンドを使用します。

- オプションを指定しない **alertentries** では、すべてのアラート項目の設定が表示されます。
- **alertentries -number -test** では、指定された受信者のインデックス番号にテスト・アラートが生成されます。

- **alertentries -number** (ここで number は 0 ～ 12) では、指定された受信者のインデックス番号に対するアラート項目の設定が表示されるか、その受信者のアラート設定の変更が可能になります。

次の表は、オプションの引数を示しています。

表 60. alertentries コマンド

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。

オプション	説明	値
-number	表示、追加、変更、または削除するアラート受信者のインデックス番号	1 ～ 12
-status	アラート受信者状況	on、off
-type	アラート・タイプ	email、syslog
-log	アラートメールにイベント・ログを含める	on、off
-n	アラート受信者名	ストリング
-e	アラート受信者のメール・アドレス	有効なメール・アドレス
-ip	Syslog の IP アドレスまたはホスト名	有効な IP アドレスまたはホスト名
-pn	Syslog ポート番号	有効なポート番号
-del	指定された受信者のインデックス番号を削除	
-test	指定された受信者のインデックス番号に対するテスト・アラートを生成	
-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 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、**alertentries -crt custom:te|vo** 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。 • te: クリティカルな温度しきい値超過 • vo: クリティカルな電圧しきい値超過 • po: クリティカルな電源障害 • di: ハードディスク・ドライブ障害 • fa: ファン障害 • cp: マイクロプロセッサー障害 • me: メモリー障害 • in: ハードウェアの互換性なし • re: 電源の冗長性の障害 • ot: その他すべてのクリティカル・イベント
-crten	クリティカル・イベント・アラートを送信	enabled、disabled

表 60. alertentries コマンド (続き)

オプション	説明	値
-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 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、**alertentries -wrn custom:rp|te** 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。 • rp: 電源の冗長性の警告 • te: 警告の温度しきい値超過 • vo: 警告の電圧しきい値超過 • po: 警告の電力しきい値超過 • fa: クリティカルではないファン・イベント • cp: マイクロプロセッサーが機能低下状態 • me: メモリーの警告 • ot: その他すべての警告イベント
-wrnen	警告イベント・アラートを送信	enabled、disabled
-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 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、**alertentries -sys custom:lo|tio** 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。 • lo: 正常なリモート・ログイン • tio: オペレーティング・システムのタイムアウト • 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 • po: システムの電源オン/オフ • bf: オペレーティング・システムのブート障害 • 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 • pf: 予知された障害 (PFA) • el: イベント・ログ 75% フル • ne: ネットワーク変更
-sysen	ルーチン・イベント・アラートを送信	enabled、disabled

構文:

```
alertentries [options]
  options:
  -number recipient_number
    -status status
    -type alert_type
    -log include_log_state
    -n recipient_name
    -e email_address
    -ip ip_addr_or_hostname
    -pn port_number
    -del
    -test
    -crt event_type
    -crten state
    -wrn event_type
```

```
   -wrnen state
   -sys event_type
    -sysen state
```

例:
```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

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。

- 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。

次の表は、オプションの引数を示しています。

表 61. batch コマンド

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。

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

構文:
```
batch [options]
option:
```

```
 -f filename
 -ip ip_address
 -pn port_number
 -u username
  -pw password
```

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>
```

clearcfg コマンド

IMM の構成を出荷時のデフォルト値に設定するには、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。IMM の構成がクリアされた後、IMM は再起動されます。

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。

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。

+2、-7、-6、-5、-4、および -3 の UTC 時差では、以下のように特殊な夏時間の設定が必要です。

- +2 の場合、夏時間オプションには、off、ee (東欧)、tky (トルコ)、bei (ベイルート)、amm (アンマン)、jem (エルサレム) があります。
- -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。
- -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。
- -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。
- -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。
- -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。

構文:
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

例:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

identify コマンド

シャーシ識別 LED を点灯、または消灯、あるいは点滅させるには、このコマンドを使用します。

-d オプションを **-s on** オプションと一緒に使用すると、**-d** オプションで指定した秒数だけ LED を点灯させることができます。その秒数を経過すると、LED は消灯します。

構文:
```
identify [options]
options:
-s on/off/blink
-d seconds
```

例:
```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

info コマンド

IMM 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。

オプションを指定せずに **info** コマンドを実行すると、IMM のロケーションおよびお問い合わせ先情報すべてが表示されます。次の表は、オプションの引数を示しています。

表 62. info コマンド

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。

オプション	説明	値
-name	IMM の名前	ストリング
-contact	IMM の連絡先担当者の名前	ストリング
-location	IMM の位置	ストリング
-room[1]	IMM のルーム ID	ストリング
-rack[1]	IMM のラック ID	ストリング
-rup[1]	ラック内での IMM の位置	ストリング
-ruh	ラック・ユニットの高さ	読み取り専用
-bbay	ブレード・ベイのロケーション	読み取り専用
1. IMM が Flex System 環境にある場合、値は読み取り専用であり、リセットすることができません。		

構文:
```
info [options]
option:
 -name xcc_name
 -contact contact_name
 -location xcc_location
 -room room_id
 -rack rack_id
 -rup rack_unit_position
 -ruh rack_unit_height
```

-bbay *blade_bay*

spreset 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。

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。

次の表は、オプションの引数を示しています。

表 63. storage コマンド

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。

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。	*controllers|pools|volumes|drives* ここで、*ターゲット*は以下のとおりです。 • *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。[1] • *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。[1] • *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。[1] • *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。[1]
-list -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。	*pools|volumes|drives ctrl[x]|pool[x]* ここで、*target* および *target_id* は、以下のとおりです。 • *pools 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。[1] • *volumes 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。[1] • *drives 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。[1]
-list flashdimms	IMM によって管理されているフラッシュ DIMM をリストします。	

表 63. storage コマンド (続き)

オプション	説明	値
-list devices	IMM によって管理されているすべてのディスクおよびフラッシュ DIMM の状況を表示します。	
-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* は以下のとおりです。 *ctrl[x]/vol[x]/disk[x]/pool[x]* */flashdimm[x]* [3]
-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* は以下のとおりです。 *ctrl[x]/vol[x]/disk[x]/pool[x]* */flashdimm[x]* [3]
-show *target_id firmware*[3]	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* は以下のとおりです。 *ctrl[x]/disk[x]/flashdimm[x]*[2]
-showlog *target_id<m:n|all>*[3]	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イベント・ログを表示します。	ここで、*target_id* は *ctrl[x]*[4] です。 *m:n|all* ここで、*m:n* はイベント・ログの 1 から最大数です。 ここで、*all* はすべてのイベント・ログです。
-config ctrl -scanforgn -target *target_id*[5]	外部 RAID 構成を検出します。	ここで、*target_id* は *ctrl[x]*[5] です。
-config ctrl -imptforgn -target *target_id*[5]	外部 RAID 構成をインポートします。	ここで、*target_id* は *ctrl[x]*[5] です。
-config ctrl -clrforgn -target *target_id*[5]	外部 RAID 構成をクリアします。	ここで、*target_id* は *ctrl[x]*[5] です。
-config ctrl -clrcfg -target *target_id*[5]	RAID 構成をクリアします。	ここで、*target_id* は *ctrl[x]*[5] です。
-config drv -mkoffline -target *target_id*[5]	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]*[5] です。
-config drv -mkonline -target *target_id*[5]	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]*[5] です。
-config drv -mkmissing -target *target_id*[5]	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]*[5] です。
-config drv -prprm -target *target_id*[5]	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]*[5] です。
-config drv -undoprprm -target *target_id*[5]	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]*[5] です。
-config drv -mkbad -target *target_id*[5]	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]*[5] です。

表 63. storage コマンド (続き)

オプション	説明	値
-config drv -mkgood -target *target_id*[5]	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 (JBOD) 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]*[5] です。
-config drv -addhsp -*[dedicated pools]* -target *target_id*[5]	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]*[5] です。
-config drv -rmhsp -target *target_id*[5]	ホット・スペアを削除します。	ここで、*target_id* は *disk[x]*[5] です。
-config vol -remove -target *target_id*[5]	1 つのボリュームを削除します。	ここで、*target_id* は *vol[x]*[5] です。
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target *target_id*[5]	1 つのボリュームのプロパティを変更します。	• [-N *volume_name*] はボリュームの名前です • [-w *<0|1|2>*] はキャッシュの書き込みポリシーです。 – ライト・スルー・ポリシーの場合は *0* を入力します – ライト・バック・ポリシーの場合は *1* を入力します – バッテリー・バックアップ・ユニット (BBU) 使用書き込みポリシーの場合は *2* を入力します • [-r *<0|1|2>*] はキャッシュの読み取りポリシーです。 – 先読みなしポリシーの場合は *0* を入力します – 先読みポリシーの場合は *1* を入力します – 適応先読みポリシーの場合は *2* を入力します • [-i *<0|1>*] はキャッシュの I/O ポリシーです。 – ダイレクト I/O ポリシーの場合は *0* を入力します – キャッシュ I/O ポリシーの場合は *1* を入力します • [-a *<0|2|3>*] はアクセス・ポリシーです。 – 読み取り/書き込みポリシーの場合は *0* を入力します – 読み取り専用ポリシーの場合は *2* を入力します – ブロック・ポリシーの場合は *3* を入力します • [-d *<0|1|2>*] はディスクのキャッシュ・ポリシーです。 – ポリシーを変更しない場合は *0* を入力します – ポリシーを有効にするには *1* を入力します[6] – ポリシーを無効にするには *2* を入力します

表 63. storage コマンド (続き)

オプション	説明	値
		• [-b *<0|1>*] はバックグラウンドの初期化です。 – 初期化を有効にするには *0* を入力します – 初期化を無効にするには *1* を入力します • *-target_id* は *vol[x]*[5] です
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3],[7]	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。 または 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。	• [-R *<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>*] 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。 • [-D disk *[id11]:disk[id12]:..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 • [-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 • [-1 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 • [-N *volume_name*] はボリュームの名前です • [-w *<0|1|2>*] はキャッシュの書き込みポリシーです。 – ライト・スルー・ポリシーの場合は *0* を入力します – ライト・バック・ポリシーの場合は *1* を入力します – バッテリー・バックアップ・ユニット (BBU) 使用書き込みポリシーの場合は *2* を入力します • [-r *<0|1|2>*] はキャッシュの読み取りポリシーです。 – 先読みなしポリシーの場合は *0* を入力します – 先読みポリシーの場合は *1* を入力します – 適応先読みポリシーの場合は *2* を入力します
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target *target_id*[8]	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。 または 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。	• [-i *<0|1>*] はキャッシュの I/O ポリシーです。 – ダイレクト I/O ポリシーの場合は *0* を入力します – キャッシュ I/O ポリシーの場合は *1* を入力します • [-a *<0|2|3>*] はアクセス・ポリシーです。 – 読み取り/書き込みポリシーの場合は *0* を入力します – 読み取り専用ポリシーの場合は *2* を入力します – ブロック・ポリシーの場合は *3* を入力します • [-d *<0|1|2>*] はディスクのキャッシュ・ポリシーです。

表 63. storage コマンド (続き)

オプション	説明	値
		– ポリシーを変更しない場合は *0* を入力します – ポリシーを有効にするには *1* を入力します[6] – ポリシーを無効にするには *2* を入力します • [-f *<0/1/2>*] は初期化のタイプです。 – 初期化なしの場合は *0* を入力します – クイック初期化の場合は *1* を入力します – 完全初期化の場合は *2* を入力します • [-S *volume_size*] は新規ボリュームのサイズ (MB) です • [-P *strip_size*] はボリュームのストリップ・サイズ (例: 128K または 1M) です • -target *target_id* は: – *ctrl[x]* (新規ストレージ・プール)[5] – *pool[x]* (既存のストレージ・プール)[5]
-config vol -getfreecap[-R] [-D disk] [-H disk] -target *target_id*[5]	ドライブ・グループの空き容量を取得します。	• [-R *<0/1/5/1E/6/10/50/60/00/1ERLQ0/1E0RLQ0>*] 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。 • [-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 • [-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 • -target *target_id* は: – *ctrl[x]*[5]
-help	コマンドの使用法とオプションを表示します。	

注:
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。
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。
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。
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。
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。
6. *Enable* 値は RAID レベル 1 構成をサポートしません。
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。

構文:
```
storage [options]
option:
 -config ctrl|drv|vol -option [-options] -target target_id
 -list controllers|pools|volumes|drives
 -list pools -target ctrl[x]
 -list volumes -target ctrl[x]|pool[x]
 -list drives -target ctrl[x]|pool[x]
```

-list devices
-list flashdimms
-show *target_id*
-show {*ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]*} *info*
-show {*ctrl[x]|disk[x]|flashdimm[x]*}*firmware*
-showlog *ctrl[x]m:n|all*
-h *help*

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 flashdimms
flashdimm[1]   Flash DIMM 1
flashdimm[4]   Flash DIMM 4
flashdimm[9]   Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]   Storage Pool 0
pool[0-1]   Storage Pool 1
system>
system> storage
-list volumes
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
Manfacture: 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.: 1234567890
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
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
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ー情報を表示するために使用します。

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.`
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。

次の表は、オプションの引数を示しています。

表 64. adapter コマンド

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。

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。	*target_id [info|firmware|ports|chips]* ここで、それぞれ以下の意味があります。 • *info*: アダプターのハードウェア情報を表示する • *firmware*: アダプターのすべてのファームウェア情報を表示する

表 64. adapter コマンド (続き)

オプション	説明	値
		• *ports*: 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 • *chips*: アダプターのすべての GPU チップ情報を表示する
-h	コマンドの使用法とオプションを表示します。	

構文:
```
adapter [options]
option:
 -list
 -show target_id [info|firmware|ports|chips]
  -h help
```

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> 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: dici
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: dici
```

m2raid コマンド

M.2 に関連するインベントリー情報を取得し、仮想ボリュームを管理するには、このコマンドを使用します。

次の表は、オプションの引数を示しています。

表 65. m2raid コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

オプション	説明
-h/?	このコマンドのヘルプ情報を印刷する
-version	コントローラーのファームウェア情報を表示する
-disks	メディア・ディスク情報を表示する
-volumes	仮想ボリューム情報を表示する
-create	仮想ボリュームを作成する。VD_Name、RaidLevel および StripeSize の指定が可能
-delete	仮想ボリュームを削除する
-import	外部の仮想ボリュームをインポートする仮想ボリュームをインポートした後、システムをリブートすると、仮想ボリュームが自動的に再構築されます。

使用例

```
m2raid [-options] - raid configuration for M.2 adapter with Mirroring Enablem
options:
  -version            - displays controller firmware version.
  -disks             - displays information of media disks.
  -volumes            - displays information of virtual volumes
  -create -VD_Name <nameStr> -RaidLevel <0|1> -StripeSize <32|64>  - create virt
  -delete -VD_ID <0|1>     - delete the virtual volume
  -import -VD_ID <0|1>     - import a foreign virtual volume
```

例

```
system> m2raid -version
  ThinkSystem M.2 with Mirroring Enablement Kit
 Firmware Version = 2.3.10.1193

system> m2raid -disks
  M.2 Bay0      32GB M.2 SATA SSD    LEN    100%
M.2 Bay1      32GB M.2 SATA SSD    LEN    100%

system> m2raid -volumes
  VD_ID   VD_Name   RaidLevel   StripSize   VD Capacity   Status
   0     M2RAID     1         64k       29 GB       Optimal

system> m2raid -delete -VD_ID 0
VD_ID 0 is deleted

system> m2raid -create -VD_Name M2RAID -RaidLevel 1 -StripeSize 64
New volume is created

system> m2raid -import -VD_ID 0
VD_ID 0 is imported
```

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 177 ページの 「dbgshimm コマンド」 の 1 つのみです。

dbgshimm 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。

表 66. dbgshimm コマンド

次の表は、オプションとオプションの説明で構成される複数行 2 列の表です。

オプション	説明
状況	ステータスを表示します
有効にする	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)
無効	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 PASSW0RD (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/PASSW0RD 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、179 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、179 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	データ 1 [7:4] – 予約済み [3:0] – アドレスのソース 0h = 未指定 1h = 静的アドレス (手動構成) 2h = XCC 実行中の DHCP によるアドレスの取得 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 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。 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。

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
OEM パラメーター 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。 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。 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。 バイト 1 = 完了コード バイト 2 = リビジョン バイト 3 = eth0 の場合は 00h、eth1 の場合は 01h など。 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)	C0h	データ 1 00h = eth0 01h = eth1 02h = eth2 etc… FFh = すべての外部ネットワーク・ポートを無効にする) 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 データ 2 00h = チャネル 0 01h = チャネル 1 etc… 要求で データ 2 が指定されていない場合、チャネル 0 が想定されます

データ 1 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。

データ 2 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 データ 2 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 データ 2 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
OEM パラメーター (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。) 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 (無効)、または 01h (有効)	C1h	データ 1 0x00 = 無効 0x01 = 有効

データ 1 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。

データ 2 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 データ 2 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 データ 2 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

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
OEM パラメーター (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。) 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	C2h	

パラメーター	#	パラメーター・データ
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 = パラメーターのリビジョン (IPMI 仕様と同じ) バイト 3 = 後続のデータ・バイトの長さ (現在は 16 バイト) バイト 4-n DUID_LLT		

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
OEM パラメーター (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。) 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 (無効)、または 01h (有効)	C3h	データ 1 0x00 = 無効 0x01 = 有効 注: Flex および Stark システムでは、CMM と SMM 経由のネットワーク通信パスを破壊する可能性があるため、自動ネゴシエーション設定を変更することはできません。
OEM パラメーター (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。) 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 (10Mb)、または 01h (100Mb)	C4h	データ 1 0x00 = 10Mbit 0x01 = 100Mbit

パラメーター	#	パラメーター・データ
OEM パラメーター (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。) 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 (半二重)、または 01h (全二重)	C5h	データ 1 0x00 = 半二重 0x01 = 全二重
OEM パラメーター (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。) 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 3-4 = MTU のサイズ	C6h	データ 1 MTU のサイズ
OEM パラメーター (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)。 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 – 8 = MAC アドレス	C7h	データ 1 - 6 MAC アドレス

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
OEM パラメーター 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。 応答データは以下を返します。 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 = IPV6 アドレスのプレフィックスの長さ バイナリ形式のバイト4-19 のローカル・リンク・アドレス	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
OEM パラメーター 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。 応答データは以下を返します。 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 = 00h (無効)、または 01h (有効)	C9h	データ 1 0x00 = 無効 0x01 = 有効

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
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。 「取得」応答データは以下を返します。 バイト 1 = 完了コード	CAh	LAN 構成パラメーターの設定: データ 1 予約済み (= 00h) データ 2:3 Ethernet-over-USB ポート番号、LSByte から データ 4:5 外部イーサネット ポート番号、LSByte から

パラメーター	#	パラメーター・データ
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) 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)。 • バイト 8 = 事前定義済みのモード: 00h = パススルーが無効になりました 01h = CMM の IP アドレスが使用されています 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) 完了コード: 00h – 成功 80h – パラメーターがサポートされていません C1h – コマンドがサポートされていません C7h – リクエスト・データの長さが無効です		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)。 データ 6 00h = パススルーを無効にする 01h = CMM の IP アドレスを使用する データ 6:9 IPv4 外部ネットワーク IP アドレス (バイナリ形式) データ 6:21 IPv6 外部ネットワーク IP アドレス (バイナリ形式)
OEM パラメーター 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。 応答データは以下を返します。 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 3:10 = 最初に IP アドレスおよびネットマスク値 (MS バイト)	CBh	データ 1:4 XCC 側の LAN over USB インターフェースの IP アドレス。 データ 5:8 XCC 側の LAN over USB インターフェースのネットマスク
OEM パラメーター 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。 応答データは以下を返します。	CCh	データ 1:4 ホスト側の LAN over USB インターフェースの IP アドレス。

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。 パッケージ・インベントリー操作の照会 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・インベントリーの照会 --> 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
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。 そのコマンドは、2 つの操作のみをサポートします。 • パッケージの優先順位の読み取り • パッケージの優先順位の設定 パッケージの優先操作の読み取り 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。 パッケージの優先順位の読み取り --> 0x0C 0x02 0x01 0xD4 0x00 0x00 応答 --> 0x00 0x00 0x00 0x12 0x23 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 パッケージの優先操作の設定 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。 パッケージの優先順位の設定	D4	LAN 構成パラメーターの取得/設定: ビット [7-4] = 論理パッケージの優先順位 (1 = 最高、15 = 最低) ビット [3:0] = 論理パッケージ番号

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 モードと共用 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、共用 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
OEM パラメーター 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。 応答データは 4 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 = 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ネル ID	D6h	LAN 構成パラメーターの設定: データ 1 設定すべきネットモード LAN 構成パラメーターの取得: データ 1 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。

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	**要求**: 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 **応答**: 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	**要求**: リクエストされているデータはありません **応答**: 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	**要求**: 該当なし **応答**: 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	**要求**: 該当なし **応答**: バイト 1 – 完了コード バイト2:10 – ASCIIZ Build 名 バイト 11:23 – ASCIIZ 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	**要求**: 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**
		応答: 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	**要求**: データはありません。 **応答**: 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	**要求**: なし **応答**: バイト 1 – 完了コード バイト2 – ビン番号 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: ビ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。

<table>
<tr><th colspan="4">ネット関数 = 0x2E</th></tr>
<tr><th>コード</th><th>コマンド</th><th>要求、応答データ</th><th>説明</th></tr>
<tr><td>0x1E</td><td>シャーシの電源復元遅延オプション</td><td>要求:
<table><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>応答:

バイト 1 – 完了コード

バイト 2 – 遅延オプション (照会要求のみ)</td><td>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。

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。</td></tr>
<tr><td>0x38</td><td>NMI およびリセット</td><td>要求:

バイト1 – 秒数
0 = NMI のみ

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

応答:

バイト 1 – 完了コード</td><td>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。

「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。

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。</td></tr>
</table>

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。

<table>
<tr><th colspan="4">ネット関数 = 0x3A</th></tr>
<tr><th>コード</th><th>コマンド</th><th>要求、応答データ</th><th>説明</th></tr>
<tr><td>0x55</td><td>ホスト名の取得/設定</td><td>要求の長さ = 0:

リクエスト・データがありません

応答:

<table><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>
要求の長さ 1-64:

<table><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></td><td>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。

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。</td></tr>
<tr><td>0x98</td><td>FP USB ポートの制御</td><td>要求:

バイト 1

<table><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>
応答:

バイト 1 – 完了コード

バイト 2

<table><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>
要求:

バイト 1

<table><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>
応答:</td><td>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。

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。

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。

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。

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ることができます。</td></tr>
</table>

<table>
<tr><th colspan="4">ネット関数 = 0x3A</th></tr>
<tr><th>コード</th><th>コマンド</th><th>要求、応答データ</th><th>説明</th></tr>
<tr><td></td><td></td><td>バイト 1 – 完了コード

バイト 2
<table><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><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)

要求:

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><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><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)

応答:

バイト 1 – 完了コードバイト 2</td><td>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。

SD530 サーバー

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。
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。
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。
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。
非 SD530 サーバー

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。

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。</td></tr>
</table>

<table>
<tr><th colspan="4">ネット関数 = 0x3A</th></tr>
<tr><th>コード</th><th>コマンド</th><th>要求、応答データ</th><th>説明</th></tr>
<tr><td></td><td></td><td>
<table>
<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>
応答:
バイト 1 – 完了コード
バイト 1
<table>
<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>
バイト 2
<table>
<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>
応答:
バイト 1 – 完了コード
要求:
バイト 1
<table>
<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>
応答:
バイト 1 – 完了コード
バイト 2</td><td></td></tr>
<tr><td>0xC7</td><td>ネイティブ NM IPMI スイッチ</td><td>要求の長さ = 0:
リクエスト・データがありません
応答:
<table>
<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>
要求の長さ= 1:</td><td>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。</td></tr>
</table>

<table>
<tr><th colspan="4">ネット関数 = 0x3A</th></tr>
<tr><th>コード</th><th>コマンド</th><th>要求、応答データ</th><th>説明</th></tr>
<tr><td></td><td></td><td>
<table>
<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>
</table>
応答:
<table>
<tr><td>バイト 1</td><td>完了コード</td></tr>
</table>
</td><td></td></tr>
</table>

第 12 章 Edge サーバー

このトピックでは、Edge サーバー固有の機能について説明します。

注：

1. 初回のログイン時に、XCC パスワードを変更するよう求められます。
2. IPMI over LAN は、デフォルトで無効になっています。
3. IPMI over KCS は、デフォルトで無効になっています。

システム・ロックダウン・モード

システム・ロックダウン・モードがアクティブ状態である場合、システムがロックダウン・モードになっていることを意味します。システムをアクティブにすればロックを解除できますが、そうしない場合、ホスト・システムをブートすることはできません。

注：システム・ロックダウン・モードはセキュリティー・バック付きの SE350 でのみ使用可能で、標準の SE350 では使用できません。「**システム情報と設定**」の「**ホーム**」タブでバージョンを確認できます。

「**BMC 構成**」の下の「**セキュリティー**」をクリックし、「**システムのロックダウン・モード**」までスクロールします。

システム・ロックダウン・モード

システムをアクティブにし、**システム・ロックダウン・モード**を終了するには、次のステップを実行してください。

1. 「**非アクティブ**」ボタンをクリックすると、**チャレンジ・テキスト**を示す **Key Vault アクティベーション** のウィンドウがポップアップ表示されます。
2. IT 管理者に連絡し、**チャレンジ・テキスト**を提供します。
3. IT 管理者から **チャレンジ・レスポンス** を取得し、それを「**Key Vault アクティベーション**」ウィンドウに入力します。.
4. 「**適用**」 をクリックし、「**OK**」 ボタンをクリックします。
5. すべての設定が正常に機能している場合は、**システム・ロックダウン・モード** が **非アクティブ** に変更されます。

注：システム・ロックダウン・モードがアクティブ状態のときは、システム・シークレットへのアクセスが **拒否されます。** SED 鍵など。

システムを強制的にロックダウン・モードにするには、次のステップを実行してください。

1. 「**アクティブ**」ボタンをクリックします。
2. 「**適用**」 をクリックし、「**OK**」 ボタンをクリックします。

動作の検出

サーバーの物理的な移動を検出することによって、この機能を有効にしてサーバーを保護することができます。
動作の検出が有効になっている場合は、設定および構成に応じて以下の項目を設定することができます。

- **感度レベル**: 設定に従って、「**低**」、「**中**」、「**高**」から感度レベルを選択します。
- **方向**: **スタンド・デスクトップ**、**壁面の取り付け (水平)**、**壁面の取り付け (垂直)**、**本棚**、および**天井の取り付け**から構成を選択します。

注：システムがロックダウン・モードに入ると、動作検出は自動的に無効になります。

シャーシ侵入検出
トップ・カバーの物理的な移動を検出することによって、この機能を有効にしてサーバーを保護することができます。

追加の構成
ワイヤレス対応の LOM パッケージがインストールされている場合、検出された不正のイベントに対して選択できる設定は 3 つあります。
一部の異常な状況では、**チャレンジ・テキスト** が ThinkShield Key Vault Portal で検証されないことがあります。IT 管理者の要請によりデバイスをアクティブにする前にデバイスの内部カウンターをリセットする必要がある場合があります。

SED 認証キー (AK) マネージャー

この機能は、SED (自己暗号化ドライブ) とともに取り付けられているシステムに対して、 SED 鍵をデプロイする BMC を制御します。SED 鍵を使用してブート・ドライブとデータ・ドライブを暗号化し、手動操作なしでシステムをブートできます。

注：システムがアクティブ化されていない (システム・ロックダウン・モードが検出されている) 場合、または現在のユーザーに SED 鍵を管理する権限がない場合、この操作は許可されません。

注：システム・ロックダウン・モードはセキュリティー・バック付きの SE350 でのみ使用可能で、標準の SE350 では使用できません。「**システム情報と設定**」の「**ホーム**」タブでバージョンを確認できます。

注：ThinkSystem M.2 イネーブルメント・キットまたは ThinkSystem M.2 ミラーリング・イネーブルメント・キットが正常である間は、SE350 が自動バックアップ機能もサポートします。ハードウェアが損傷しているが、SED と M.2 キットの両方が正常な場合は、それらを別の SE350 に取り付けて SED AK を復元することができます。ただし、ハードウェアが完全にクラッシュした場合に備えて、Lenovo は SED AK バックアップを作成することをお勧めします。

「**BMC 構成**」の下の「**セキュリティー**」をクリックし、「**SED 認証鍵 (AK) マネージャー**」までスクロールします。

SED AK の変更
パスフレーズから SED AK を生成する: パスワードを設定し、確認のためにもう一度入力します。「**再生成**」をクリックして、新しい SED AK を取得します。
ランダム SED AK を生成する:「**再生成**」をクリックして、ランダム SED AK を取得します。
SED AK をバックアップする: パスワードを設定し、確認のためにもう一度入力します。「**Start Backup (バックアップの開始)**」をクリックして SED AK をバックします。次に、SED AK ファイルをダウンロードして、今後の使用に備えて安全に保管します。

注：バックアップ SED AK ファイルを使用して構成を復元する場合、システムはここで設定したパスワードを要求します。

SED AKのリカバリー: このタスクは、SED が正常に機能していないときにのみ実行できます。SED AK をリカバリーする方法は 2 つあります。

- **パスフレーズを使用して SED AK をリカバリーする**: **SED AK をパスフレーズから生成する** モードで設定されたパスワードを使用して、SED AK をリカバリーします。
- **バックアップ・ファイルから SED AK をリカバリーする**: **SED AK のバックアップ** モードで生成されたバックアップ・ファイルをアップロードし、対応するバックアップ・ファイルのパスワードを入力して、SED AK をリカバリーします。

Edge ネットワーキング

この機能ページは、ワイヤレス対応の LOM パッケージがインストールされている場合のみサポートされます。

ネットワーク・トポロジーのプリセット・テーブルの詳細については https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html を参照してください。

Wi-Fi 接続
「**有効**」をクリックすると、Wi-Fi の構成に応じて設定を構成できます。

LTE 接続
これにより、Edgenetwork ボードの LTE 接続を制御することができます。

Edge ネットワーク・ボードのアドレス

IPv4 または IPv6 の状況	DHCP サーバー の状況	方式
無効	**無効**	**DHCP から IP を取得**
使用可能	**使用可能**	**静的 IP アドレスを使用**
使用可能	**無効**	使用方法に応じて、**DHCP から IP を取得**するか、または**静的 IP アドレスを使用**します。

BMC ネットワーク・ブリッジ
BMC には、「**ダウン リンク・ポート**」、「**Wi-Fi ポート**」、「**アップ リンク・ポート**」または「**なし**」からアクセスできます。

注：「**なし**」を選択すると、この機能は無効になります。

Edge ネットワーク・ボードのトラブルシューティング
直ちに再起動: このボタンを使用してネットワーク・ボードを再起動できます。
出荷時のデフォルト値へのリセット: このボタンを使用して、ネットワーク・ボードをデフォルト設定にリセットできます。

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す。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。

http://thinksystem.lenovofiles.com/help/index.jsp

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 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けると、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・インベントリー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、http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/NN1ia_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、http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/nn1ia_r_ffdccommand.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 http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/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、http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/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て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/supportphonelist 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、お客様に対してなん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が、その測定値が、一般に利用可能なシステムのもの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

プロセッサーの速度とは、マイクロプロセッサー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、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応答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、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されることで、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る場合があります。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 67. 微粒子およびガスの制限

汚染物質	制限
微粒子	• 室内の空気は、ASHRAE Standard 52.2[1] 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)。 • 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。 • 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 [2]。 • 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。
ガス	• 銅: ANSI/ISA 71.04-1985 準拠の Class G1[3] • 銀: 腐食率は 30 日間で 300 Å 未満

[1] 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.

[2] 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。

[3] 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。

http://thinksystem.lenovofiles.com/help/index.jsp

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^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

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.

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.

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.

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

i

k

l

m

n

o

p

r

s

t

u

v

w

x

あ

い

え

お

か

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

ね

の

は

ひ

ふ

へ

ほ

ま

め

も

や

ゆ

よ

ら

り

る

ろ

Lenovo

部品番号: SP47A30085

Printed in China

(1P) P/N: SP47A30085