

# HP ProLiant Lights Out-100

## ユーザー ガイド

### HP ProLiant G6 および G7 サーバー用

#### 概要

このユーザー ガイドでは、ProLiant ML110 G6、ML150 G6、DL120 G6、DL160 G6、DL160se G6、DL170h G6、DL170e G6、DL180 G6、SL160z G6、SL160s G6、SL170z G6、SL2x170z G6、SL170s G6、DL165 G7、SL165z G7、および SL165s G7 サーバーでの HP ProLiant Lights Out-100 の設定と使用について説明します。



## ご注意

本書の内容は、将来予告なしに変更されることがあります。HP 製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、脱落に対して、責任を負いかねますのでご了承ください。

本書で取り扱っているコンピューター ソフトウェアは秘密情報であり、その保有、使用、または複製には、HP から使用許諾を得る必要があります。FAR 12.211 および 12.212 に従って、商業用コンピューター ソフトウェア、コンピューター ソフトウェア ドキュメンテーション、および商業用製品の技術データ (Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items) は、ベンダー標準の商業用使用許諾のもとで、米国政府に使用許諾が付与されます。

Microsoft、Windows および Windows Server は、Microsoft Corporation の米国における登録商標です。Intel、インテル、Pentium、および Itanium は、インテル コーポレーションまたはその子会社のアメリカ合衆国およびその他の国における商標または登録商標です。UNIX は、The Open Group の米国ならびに他の国における登録商標です。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に掲載されている製品情報には、日本国内で販売されていないものも含まれている場合があります。

製品番号 616302-194

## 対象読者

このガイドは、サーバーおよびストレージシステムのインストール、管理、トラブルシューティングの担当者を対象とし、コンピューター機器の保守の資格があり、高電圧製品の危険性について理解していることを前提としています。

# 目次

<b>1 動作の概要</b> .....	<b>5</b>
概要.....	5
新機能.....	5
サーバー管理.....	5
サーバーの管理機能.....	5
LO100 の標準機能.....	6
LO100 のオプション（ライセンス済み）機能.....	6
<b>2 設定</b> .....	<b>7</b>
LO100CFG ユーティリティによる LO100 の設定.....	7
ネットワーク アクセスの設定.....	7
ユーザー アカウントの設定.....	8
BIOS セットアップ ユーティリティへのアクセスとファンクション キーの使用.....	8
シリアル ポートの使用 .....	8
シリアル アクセスの有効化.....	9
シリアル ポートの設定.....	9
TCP/IP over Ethernet マネジメント ポートの使用.....	10
共有 Ethernet マネジメント ポートの選択.....	10
BIOS セットアップ ユーティリティからの DHCP IP アドレスの取得.....	11
DNS 命名機能の使用.....	12
BIOS セットアップ ユーティリティからの静的 IP アドレスの設定.....	12
BIOS セットアップ ユーティリティからの Telnet および HTTP サービスの有効化または無効化.....	13
LO100 で使用する TCP および UDP ポート番号.....	14
ファームウェアの更新.....	14
ファームウェアのリモート更新.....	15
Web ブラウザーを介したファームウェアのインストール.....	17
オンライン フラッシュ ユーティリティを使用したファームウェアの更新.....	17
<b>3 LO100 の使用</b> .....	<b>19</b>
SSL の使用.....	19
SSH の使用.....	19
SSH ユーティリティの使用.....	19
PuTTY ユーティリティの使用.....	20
OpenSSH ユーティリティの使用.....	20
CLP の使用.....	20
CLP 構文.....	20
基本コマンド.....	21
各コマンドについて.....	25
DCMI 1.0 サポート.....	25
IPMI 2.0 のサポート.....	25
LO100 へのログイン.....	26
Web ブラウザー経由でのログイン.....	26
CLP を使用したログイン.....	26
ブラウザーのメイン メニュー オプション.....	26
サーバー電源のリモート制御.....	27
ブラウザー経由でのサーバー電源の制御.....	27
CLP を使用したサーバー電源の制御.....	29
センサーの監視.....	29

Web ブラウザーからのセンサー データ表示.....	29
BIOS セットアップ ユーティリティからのセンサー データの表示.....	30
Platform Event Filtering 設定.....	31
Platform Event Trap の設定.....	32
システム イベント ログの使用.....	33
Web ブラウザーからのシステム イベント ログへのアクセス.....	33
CLP を使用したシステム イベント ログへのアクセス.....	33
BIOS セットアップ ユーティリティを使用したシステム イベント ログへのアクセス.....	34
仮想 KVM の使用.....	34
リモート グラフィック コンソールの使用.....	35
リモート グラフィック コンソールの設定.....	36
マウスの同期化.....	37
システム ボタン.....	38
仮想メディアの使用.....	38
仮想メディア デバイスの追加.....	39
仮想メディア デバイスの共有.....	40
Telnet 経由でのリモート コンソール アクセス.....	40
Telnet 経由での BIOS コンソール テキストのリダイレクト.....	41
Linux のコンソールのリダイレクト.....	42
Microsoft Windows EMS による管理.....	43
[Hardware Inventory] ページ.....	45
[User Administration].....	45
Web ブラウザーを介したユーザー設定の変更.....	46
CLP を使用したユーザー設定の変更.....	47
ネットワーク設定.....	47
Web ブラウザーを介したネットワーク設定の変更.....	47
BIOS セットアップ ユーティリティを使用したネットワーク設定の指定.....	49
CLP を使用したネットワーク設定の指定.....	50
ライセンス キーの適用.....	51
証明書のインポート.....	51
証明書の作成.....	51
Web ブラウザー経由での証明書またはプライベート キーのインストール.....	52
CLP を使用した証明書またはプライベート キーのインストール.....	53
HP Systems Insight Manager のサポート.....	54
文字とライン フィードに関する問題の解決.....	54
VLAN タギングの使用.....	56
サーバー サポート.....	56
IPMI コマンドを使用した VLAN タギングの設定.....	56
Web ブラウザーを介した VLAN タギングの変更.....	56

<b>4 テクニカル サポート.....</b>	<b>57</b>
ソフトウェア テクニカル サポートとアップデート サービス.....	57

<b>頭字語と略語.....</b>	<b>58</b>
--------------------	-----------

<b>索引.....</b>	<b>59</b>
----------------	-----------

# 1 動作の概要

## 概要

このガイドでは、次の HP ProLiant サーバー モデルで使用可能な HP Onboard Administrator Powered by Lights-Out 100 (LO100) 標準およびオプションの動作機能について説明します。

- ML110 G6 サーバー
- ML150 G6 サーバー
- DL120 G6 サーバー
- DL160 G6 サーバー
- DL160se G6 サーバー
- DL170h G6 サーバー
- DL180 G6 サーバー
- SL160z G6 サーバー
- SL170z G6 サーバー
- SL2x170z G6 サーバー
- HP ProLiant DL165 G7 サーバー
- HP ProLiant SL165z G7 サーバー
- HP ProLiant SL170s G6 サーバー
- HP ProLiant DL170e G6 サーバー

## 新機能

LO100 の今回のリリースでは、次が新たにサポートされています。

- HP ProLiant SL160s G6
- HP ProLiant SL165s G7

## サーバー管理

LO100 は、重要なサーバー リソースの基本的なリモート制御を可能にする、IPMI 2.0、DCMI 1.0 対応の製品です。この LO100 により、管理者は、オペレーティングシステムがインストールされる前も含めサーバーにいつでもアクセスできるようになります。

LO100 を使用すると、リモートからリダイレクションされるテキスト モードのコンソール (DMTF SMASH 準拠コマンドラインインターフェイス) を使用できます。またブラウザからも、このコンソールのシステム管理機能の多くにアクセスできます。LO100 には、専用の Ethernet ポートまたはサーバーのシリアル ポートを介してアクセスできます。

## サーバーの管理機能

LO100 を使用すると、次の作業を行うことができます。

- リモート グラフィック コンソールへのアクセス (仮想 KVM)
- 標準ベースのクライアント ユーティリティを使用して、ネットワーク経由で、ホスト オペレーティング システムのシリアル コンソールにアクセス
- シリアル コンソール リダイレクションと LO100 コマンド ライン インターフェイス間での切り替え
- SSL および SSH による安全な通信

- サーバーの電源ボタンをリモートから制御（サーバーの電源投入/切断）。また、サーバーのウォーム/コールド リブートを実行
- サーバーのファン速度およびシステム電源状態（S0 または S5）をリモートから監視
- システム イベント ログへのアクセス
- 仮想メディアへのアクセス
- LO100 NIC 用の TCP/IP 設定
- ユーザー アクセスの制御
- HP Systems Insight Manager からの LO100 の検出、識別、および起動
- 標準的なブラウザや新しい業界規格の SMASH CLP コマンド ライン インターフェイスを使用した、LO100 へのアクセスとサーバーの制御
- コマンド ライン ヘルプへのアクセス
- IPMI 2.0 および DCMI 1.0 準拠アプリケーションを使用したサーバーの管理
- Telnet によるアクセス

このガイドで示す機能や説明する機能は、すべてのシステムに共通ではありません。ご使用のシステムでサポートされる機能を確認するには、「[LO100 の標準機能](#)」および「[LO100 のオプション（ライセンス済み）機能](#)」を参照してください。

## LO100 の標準機能

HP ProLiant ML110 G6、ML150 G6、DL120 G6、DL160 G6、DL160se G6、DL170h G6、DL180 G6、SL160s G6、SL160z G6、SL165s G7、SL170z G6、SL2x170z G6、SL170s、および DL170e G6 サーバー、ならびに HP ProLiant DL165 および SL165z G7 サーバーでの LO100 の標準機能は、次のとおりです。

- オペレーティング システム（サポートされている場合）を介して使用できる IPMI 2.0 および DCMI 1.0 エレメント
- IPMI-over-LAN のサポート
- 電源制御、システム イベント ログ、ハードウェア ステータス、およびオプション機能のライセンス キー アクティベーションへの Web ブラウザー アクセス（HTTP）
- リモート電源制御、システム イベント ログ、ハードウェア ステータス、およびオペレーティング システムのシリアル コンソールへの SMASH CLP インターフェイス アクセス
- 工場出荷時のデフォルトの自己署名証明書とキーによる、SSL、SSH、および IPMI 2.0 セキュリティのサポート

## LO100 のオプション（ライセンス済み）機能

LO100 オプション機能をアクティブにするには、Lights-Out 100i Advanced Pack パッケージを購入します。Lights-Out 100i Advanced Pack は、次の品目を含みます。

- 仮想メディア アクセス
- 仮想 KVM

## 2 設定

### LO100CFG ユーティリティによる LO100 の設定

SmartStart Scripting Toolkit は、大量の ProLiant サーバーの自動インストールを可能にするサーバー デプロイメント製品です。ツールキットには、Win32 エディションと Linux エディションがあり、Windows および Linux 環境で、ProLiant DL および ML モデルの 300、500、700 シリーズ サーバーならびに ProLiant BL サーバーをサポートします。今回、この Toolkit のサポート対象に一部の ProLiant 100 シリーズ サーバーが含まれるようになりました。このツールキットには、モジュール式のユーティリティ セットと、この新しいユーティリティ セットを使用して自動サーバー デプロイメント プロセスを作成する方法を記載した非常に役立つマニュアルが含まれています。

さらに、LO100CFG ユーティリティという名前の、大量の LO100 の設定とデプロイメントを目的にする重要なツールが含まれます。SmartStart Scripting Toolkit の LO100CFG ユーティリティ ツールを始めとする多くの構成ツールを使用すると、LO100 を始めとする 100 シリーズサーバーの構成を、スクリプトを使用して迅速にインストールできます。Windows および Linux 用の SmartStart Scripting Toolkit ユーザー ガイド、ダウンロード リンク、および LO100CFG ユーティリティに関するこれ以外の情報については、次の Web サイトを参照してください。

<http://h18000.www1.hp.com/products/servers/management/toolkit/index.html>

### ネットワーク アクセスの設定

リモート マネジメント CLP へのアクセス、リモートからの POST（電源投入時セルフテスト）の確認、Web ブラウザーを通じたサーバーへのアクセス、BIOS セットアップ ユーティリティへのリモート アクセスには、お使いのサーバー ネットワーク接続を使用します。

ネットワーク アクセスを設定するには、以下の手順に従ってください。

1. 標準の Ethernet ケーブルを LO100 NIC からネットワーク ジャックに接続します。
2. **F10** キーを押して BIOS にアクセスします。
3. DHCP IP アドレスを取得します。
  - ML110 G6 または DL120 G6 を使用している場合は、以下の手順に従ってください。
    - a. 右矢印（→）キーを押して [Advanced] タブまで移動し、次に [IPMI] に移動します。Enter キーを押します。
    - b. **[LAN Settings]** に移動して Enter キーを押し、次に **[IP Address Assignment]** で **[DHCP]** を設定します。
  - ML150 G6 を使用している場合は、右矢印（→）キーを押して [Advanced] タブまで移動し、次に [IPMI] に移動します。
  - DL160 G6、DL160se G6、SL165s G7、DL170h G6、DL180 G6、SL160z G6、SL170z G6、SL160s G6、SL2x170z G6、SL170s、DL170e G6 サーバー、あるいは DL165 または SL165 G7 サーバーを使用している場合は、右矢印（→）キーを押して [Advanced] タブに移動し、次に以下のいずれかの方法を使用します。
    - a. 下矢印（↓）キーを押して、[IPMI Configuration] に移動します。Enter キーを押します。
    - b. **[Set LAN Configuration]** で Enter キーを押します。

BIOS セットアップ ユーティリティの [Advanced]、[IPMI Configuration]、[LAN Configuration] の下から IP アドレスを取得します。詳しくは、「[BIOS セットアップ ユーティリティからの DHCP IP アドレスの取得](#)」を参照してください。

また、次のいずれかの方法を実行することもできます。

- DHCP クライアント テーブルを確認します。

- DNS クライアント レコードから LO100< サーバーのシリアル番号 > のエントリーを探します（各 LO100 のデフォルトの DNS ホスト名は一意です）。

LO100 では、デフォルトで DHCP が有効になっており、IP アドレスがオートネゴシエーションされます。

4. DHCP IP アドレスを使用して、Telnet でリモート マネジメント CLP にログインするか、Web ブラウザーで HTML インターフェイスにアクセスします。

静的 IP アドレスをセットアップするには、「[BIOS セットアップ ユーティリティからの静的 IP アドレスの設定](#)」を参照してください。

## ユーザー アカウントの設定

LO100 は、機能を表示および制御するためのさまざまな権限レベルを備えた 4 つのアカウントタイプをサポートします。ユーザー アカウントについては、「[\[User Administration\]](#)」(45 ページ)を参照してください。デフォルトでは、2 つのアカウント（管理者タイプのアカウントが 1 つと、オペレーター タイプのアカウントが 1 つ）が用意されています。

管理者タイプのアカウントを持つユーザーは、CLP コマンドをすべて使用でき、マネジメントプロセッサの設定を変更できます。デフォルトの管理者アカウントのユーザー名は **admin** で、デフォルトのパスワードも **admin** です。

オペレーター タイプのアカウントを持つユーザーは、一般的なコマンドや機能は使用できますが、ユーザー アカウント情報の追加および変更、マネジメントプロセッサの設定変更など、特定の機能へのアクセスは制限されています。一般的な機能を実行する場合は、オペレータータイプのアカウントでログインすることをおすすめします。デフォルトのユーザー名は Operator で、デフォルトのパスワードも Operator です。

LO100 へのログイン方法については、「[LO100 へのログイン](#)」(26 ページ)を参照してください。

## BIOS セットアップ ユーティリティへのアクセスとファンクションキーの使用

このガイドの全体を通じて、BIOS セットアップ ユーティリティへのアクセス、変更の保存、およびユーティリティの終了には、F10 キーが標準の方法として使用されます。ファンクションキー（F キー）を使用すると、Telnet クライアントのリモート システムへのパススルーが正しく機能しない場合があります。この場合は、以下のように、同じ機能の ESC キーを使用してください。

- F8 - ESC+8
- F10 - ESC+0
- F12 - ESC+@

## シリアル ポートの使用

サーバーのシリアル ポートは、シリアル ポートの基本機能を提供しますが、LO100 へのインターフェイスとしても利用できます。システムのシリアル ポートを LO100 専用にすることもできます。

**△ 注意:** LO100 で使用できるようにシリアル ポートを設定すると、従来のシリアル デバイスをシリアル ポートに接続しても機能しないことがあります。

LO100 のシリアル ポート ハードウェア パラメーターを各シリアル ポート通信ソフトウェアで使用できるように設定する必要があります。LO100 のシリアル ポート設定は、BIOS セットアップ ユーティリティで制御します。

## シリアル アクセスの有効化

1. サーバーの電源を入れます。
2. POST メッセージ「ROM-Based Setup」が表示されたら、**F10** キーを押します。管理者パスワードが設定されている場合は、パスワードの入力を求められます。パスワードが設定されていない場合は、BIOS セットアップユーティリティのメイン画面が表示されます。
3. 右矢印 (→) キーを押して、[Advanced] メニューに移動します。
4. 次のいずれかのオプションを選択します。

**注記:** [Serial Port Assignment] を変更すると、BMC の IP アドレスがリセットされます。再起動すると、BMC の IP アドレスが変更されている場合があります。

- ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[Console Redirection] に移動します。
    - b. [BIOS Serial Console Port] を **[Enabled]** に設定します。
  - ML150 G6 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
    - b. [Serial Port Assignment] を **[BMC]** に設定します。
    - c. [Serial Port Switching] を **[Enabled]**
    - d. [Serial Port Connection Mode] を **[Direct]** に設定します。
  - DL160 G6、DL160se G6、SL165s G7、DL170h、DL180 G6、SL160z G6、SL160s G6、SL170z G6、SL170s G6、SL2x170z、DL170e G6 サーバー、ならびに DL165 および SL165z G7 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[IPMI Configuration] に移動します。 **Enter** キーを押します。
    - b. [Serial Port Configuration] に移動します。
    - c. [Serial Port Assignment] を **[BMC]** に設定します。
    - d. [Serial Port Connection Mode] を **[Direct]** に設定します。
5. **F10** キーを押して変更を保存し、終了します。

## シリアル ポートの設定

1. フロント パネルの Power On/Off ボタンを押して、サーバーの電源を入れます。
2. POST メッセージ「ROM-Based Setup」が表示されたら、**F10** キーを押します。管理者パスワードが設定されている場合は、パスワードの入力を求められます。パスワードが設定されていない場合は、BIOS セットアップユーティリティのメイン画面が表示されます。
3. 右矢印 (→) キーを押して、[Advanced] メニューに移動します。
4. 下矢印 (↓) キーを押して [IO Device Configuration] に移動します。SL160z G6 または SL160s G6 サーバー、あるいは DL165 または SL165z G7 サーバーを使用している場合は、[Super IO Configurations] に移動します。 **Enter** キーを押します。
5. [Embedded Serial Port] を **[3F8/IRQ4]** に設定します。
6. [Remote Access Configuration] から、以下のように [BIOS Serial Console] を設定します。
  - BIOS Serial Console - Enabled
  - EMS Support - Disabled (ML150 G6 の場合)
  - Base Address/IRQ - 3F8h, 4
  - Serial Port Mode - 9600 8, n, 1
  - Flow Control - None
  - Redirection after BIOS/POST - Enabled
  - Terminal Type - VT100

- DL165 G7、SL165s G7 および SL165 G7 サーバーでは、[Remote Access Configuration] から、以下のように [BIOS Serial Console] を設定します。

- BIOS Serial Console Port - Enabled

---

**注記:** SL165s G7 サーバーでは、[BIOS Serial Console Port] は、[COM1] にのみ設定できます。

---

- BIOS Serial Console Port Baud Rate - [115200 8, n, 1]
  - Redirection after BIOS POST - Always
  - Terminal Type - ANSI
  - VT-UTF8 Combo Key Support - Enabled
- シリアル ポートの設定を参照して、設定が、LO100 への接続に使用するシリアル ポート通信ソフトウェアの設定と一致しているかどうか確認します。
  - Esc** キーを押して前の画面に戻るか、**F10** キーを押して変更を保存し、セットアップを終了します。

## TCP/IP over Ethernet マネジメント ポートの使用

LO100 の LAN ポート アクセスは、2 つの異なる Ethernet ポート（専用の 10/100 LO100 マネジメント ポートまたはサーバー内蔵 NIC を使用したサイドバンド接続）を使用して設定することができます。サイドバンド、共有、または UMP オプションは、サーバー ネットワークトラフィックおよび LO100 ネットワークトラフィックの両方に対して 1 つの Ethernet ポートを使用するので、サーバーに接続しなければならないネットワークケーブルの本数が少なくなります。

---

**注記:** サイドバンドと専用 NIC のどちらかを選ぶためのオプションは、一部のサーバーにはありません。どちらかのオプションしかないモデルもあります。

**注記:** なお、RBSU の IPMI LAN 設定で **[dedicated]** を選択する場合は、Lights-Out 管理を動作させるために、IPMI 管理専用のオプションの LO100i 10/100Mbps LAN ポート (RJ-45) をサーバーに取り付ける必要があります。

---

## 共有 Ethernet マネジメント ポートの選択

- フロント パネルの Power On/Off ボタンを押して、サーバーの電源を入れます。
- POST メッセージ「ROM-Based Setup」が表示されたら、**F10** キーを押します。管理者パスワードが設定されている場合は、パスワードの入力を求められます。パスワードが設定されていない場合は、BIOS セットアップユーティリティのメイン画面が表示されます。
- 右矢印 (→) キーを押して、[Advanced] メニューに移動します。

---

**注記:** ML150 G6、ML110 G6、および DL120 G6 システムでは、共有 NIC 機能で使用する仮想 KVM および仮想メディア機能は利用できません。ML150 G6 で LO100 Advanced Pack 機能が必要な場合は、専用 NIC モードを使用してください。

---

- 下矢印 (↓) キーを押して、[IPMI Configuration] に移動します。**Enter** キーを押します。
- 下矢印 (↓) キーを押して、[LAN Configuration] メニューに移動します。**Enter** キーを押します。
- 次のいずれかのオプションを選択します。
  - ML110 G6 または DL120 G6 では、下矢印 (↓) キーを押して、[IPMI] に移動します。**Enter** キーを押して、[BMC NIC Allocation] を **[Shared]** に設定します。
  - ML150 G6 では、[BMC NIC Allocation] を **[Shared]** に設定します。

- DL160 G6、DL160se G6、DL170h G6、DL180 G6、SL160s G6、および SL160z G6、SL170z G6、SL2x170z G6、SL165s G7、DL165 G7、DL170e G6 サーバーでは、[BMC NIC Allocation] を **[Enabled]** に設定します。
  - DL165 G7 では、下矢印（↓）キーを押して、[BMC NIC Allocation] に移動し、[Dedicated/Shared] を選択します。 **Enter** キーを押します。
7. **Esc** キーを押して前の画面に戻るか、**F10** キーを押して変更を保存し、セットアップを終了します。

TCP/IP over Ethernet マネジメント ポートは、専用の場合も共有の場合も、標準的な Ethernet ケーブルを使用してネットワークに接続される標準的な Ethernet 10/100Mb インターフェイスです。専用マネジメントポートを使用する前の手順として、DHCP IP アドレスの確認または静的 IP アドレスの設定のうちいずれかを決定して実行する必要があります。

## BIOS セットアップ ユーティリティからの DHCP IP アドレスの取得

LO100 では、デフォルトで DHCP が有効になっており、IP アドレスがオートネゴシエーションされます。DHCP IP アドレスを確認するには、BIOS セットアップ ユーティリティを実行するか、シリアルポート接続を介して CLP を使用し、DHCP IP アドレスを取得します。BIOS セットアップ ユーティリティを使用して DHCP IP アドレスを確認するには、以下の手順に従ってください。

1. フロント パネルの Power On/Off ボタンを押して、サーバーの電源を入れます。
2. POST メッセージ「ROM-Based Setup」が表示されたら、**F10** キーを押します。管理者パスワードが設定されている場合は、パスワードの入力を求められます。パスワードが設定されていない場合は、BIOS セットアップ ユーティリティのメイン画面が表示されます。
3. 右矢印（→）キーを押して、[Advanced] メニューに移動します。
4. DHCP IP アドレスを取得するには、サーバーモデルに応じて次のいずれかのオプションを選択します。
  - ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
    - b. 下矢印（↓）キーを押して、[LAN Settings] に移動します。 **Enter** キーを押します。
    - c. [IP Address Assignment] を **[DHCP]** に設定します。
  - ML150 G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[IPMI] に移動します。
    - b. [BMC LAN Configuration] に移動します。 **Enter** キーを押します。
  - DL160 G6、DL160se G6、SL160s G6、SL165s G7、DL180 G6、および SL160z G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[IPMI Configuration] に移動します。
    - b. [Set LAN Configuration] に移動し、次に、[BMC LAN Configuration] に移動します。 **Enter** キーを押します。
  - DL170h G6、SL170z G6、SL170s G6、DL170e G6、および SL2x170z G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[IPMI Configuration] に移動します。
    - b. [LAN Configuration] に移動し、次に、[DHCP IP Source] に移動します。
    - c. 以下のいずれかを選択します。
      - [BMC NIC] を [DHCP] に設定するには、[DHCP IP Source] に移動し、次に、有効にするために **Enter** キーを押します。
      - すべての変更を保存して終了するには、**F10** キーを押します。
5. **Esc** キーを押して前の画面に戻るか、**F10** キーを押して変更を保存し、セットアップを終了します。

ネットワーク設定の指定や変更については、「[ネットワーク設定](#)」を参照してください。

## DNS 命名機能の使用

DNS 命名機能を使用すると、サーバーの IP アドレスが分からなくても、または特定のサーバーの IP アドレスを取得しなくても、サーバーに割り当てられているサーバー名を参照することができます。このサーバー名参照は、LO100 によって割り当てられる LO100 - {サーバーのシリアル番号} 形式のデフォルト命名シーケンス (LO100 - CNQ123456 など) によってサーバーがサーバー名を DNS に登録することによって可能になります。

**注記:** この操作には DHCP が必要であり、静的 IP アドレスでは機能しません。

シリアル番号は、通常サーバーのフロントパネルにある引き出し式のラベルに記載されています。

サーバー名は、LO100 Web インターフェイスの [Network Settings] ページから変更できます。

サーバー名は、Telnet インターフェイスを使用して変更することもできます。

サーバー名を変更するには、Telnet インターフェイスで次の各コマンドを入力します。

```
cd map1/nic1
set oemhp_hostname=<new_name>
```

ここで

```
<new_name>
```

は、サーバーに割り当てる新しい DNS ホスト名です。

DNS 命名機能を使用してサーバーの IP アドレスを取得するには、同じネットワークに接続されているシステムを使用し、DOS コマンド プロンプトを開いて、nslookup {サーバー名} コマンド (nslookup {CBQ123456} など) を入力します。

DNS サーバーの設定によっては、DNS がサーバー名を登録するために最大 45 分かかる場合があります。LO100 での DNS オプションについて詳しくは、「[Web ブラウザーを介したネットワーク設定の変更](#)」を参照してください。

## BIOS セットアップ ユーティリティからの静的 IP アドレスの設定

LO100 では、デフォルトで DHCP が有効になっており、IP アドレスがオートネゴシエーションされます。DHCP を無効にして、静的 IP アドレスを有効にするには以下の手順に従ってください。

1. POST の実行時に **F10** キーを押して BIOS セットアップ ユーティリティを起動します。
2. 右矢印 (→) キーを押して、[Advanced] メニューに移動します。
3. ネットワーク BIOS 設定を設定するには、次のいずれかのオプションを選択します。
  - ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
    - b. 下矢印 (↓) キーを押して、[LAN Settings] メニューに移動します。 **Enter** キーを押します。
    - c. [IP Address Assignment] で、**[Static]** を選択します。
  - ML150 G6 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
    - b. 下矢印 (↓) キーを押して、メニューの一番下まで移動し、**[BMC LAN Configuration]** を選択します。
    - c. [BMC LAN Configuration] で、**[Static]** を選択します。
    - d. 下矢印 (↓) キーを押して下方向に移動し、有効な IP アドレス、サブネット マスク、およびゲートウェイ アドレスを入力します (アドレス フィールド間の移動には、**Tab** キーを使用)。

- DL160 G6、DL160se G6、DL165 G7、DL180 G6、SL160s G6、SL165s G7、SL165s G7、および SL160z G6 サーバーでは、次のように操作します。
  - a. 下矢印（↓）キーを押して、[IPMI] に移動します。Enter キーを押します。
  - b. 下矢印（↓）キーを押して、[LAN Configuration] メニューに移動します。Enter キーを押します。
  - c. [DHCP IP Source] で、**[Disabled]** を選択します。
  - d. 下矢印（↓）キーを押して下方向に移動し、有効な IP アドレス、サブネット マスク、およびゲートウェイ アドレスを入力します（アドレス フィールド間の移動には、**Tab** キーまたはピリオド（.）を使用）。
- DL170h G6、SL170z G6、SL170s G6、DL170e G6、および SL2x170z G6 サーバーでは、次のように操作します。
  - a. 下矢印（↓）キーを押して、[IPMI Configuration] に移動します。Enter キーを押します。
  - b. 下矢印（↓）キーを押して、[LAN Configuration] メニューに移動します。Enter キーを押します。
  - c. 下矢印（↓）キーを押して、メニューの一番下まで移動し、**[DHCP IP Source]** を選択します。
  - d. 以下のいずれかを選択します。
    - [BMC NIC] を [Disabled] に設定するには、Enter キーを押します。
- DL165 G7 および SL165 G7 サーバーでは、次のように操作します。
  - a. 下矢印（↓）キーを押して、[IPMI Configuration] に移動します。Enter キーを押します。
  - b. 下矢印（↓）キーを押して、[Set Lan Configuration] メニューに移動します。Enter キーを押します。
  - c. 下矢印（↓）キーを押して、[BMC LAN Configuration] メニューに移動します。Enter キーを押します。
  - d. [DHCP/static] を選択して、Enter キーを押します。
    - すべての変更を保存して終了するには、**F10** キーを押します。すべての変更を保存して終了するには、**F10** キーを押します。

#### 4. F10 キーを押して変更を保存し、終了します。

DHCP が割り当てたアドレスを再び使用するには、「[BIOS セットアップ ユーティリティを使用したネットワーク設定の指定](#)」を参照してください。

## BIOS セットアップ ユーティリティからの Telnet および HTTP サービスの有効化または無効化

ML110 G6 および DL120 G6 サーバーでは、次のように操作します。

1. 下矢印（↓）キーを押して、[IPMI] に移動します。Enter キーを押します。
2. 下矢印（↓）キーを押して、[LAN Settings] メニューに移動します。Enter キーを押します。
3. 下矢印（↓）キーを押して、[Telnet Services] または [HTTP Services] に移動します。必要に応じて、**[Enable]** または **[Disable]** を押します。

ML150 G6 サーバーでは、次のように操作します。

1. **[Advanced]**、**[IPMI]**
2. 次のように設定します。
  - [BMC HTTP Service] - 必要に応じて [Enabled] または [Disabled]
  - [BMC Telnet Service] - 必要に応じて [Enabled] または [Disabled]

DL160 G6、DL160se G6、DL180 G6、SL160z G6、DL165 G7、SL165s G7、および SL160z G7 サーバーでは、次のように操作します。

1. 以下のいずれかを選択します。
  - Telnet を有効または無効にする場合は、**[Advanced]**、**[IPMI Configuration]**、**[LAN Configuration]**、**[BMC Telnet Service]** を選択します。
  - HTTP を有効または無効にする場合は、**[Advanced]**、**[IPMI Configuration]**、**[LAN Configuration]**、**[BMC HTTP Service]** を選択します。
2. 有効または無効にするには、**Enter** を押します。
3. **F10** キーを押してすべての変更を保存し、終了します。

SL160s G6、DL170h G6、SL170z G6、SL170s G6、DL170e G6、および SL2x170z G6 サーバーでは、次のように操作します。

1. 右矢印 (→) キーを押して、**[Advanced]** タブに移動します。**Enter** キーを押します。
2. 下矢印 (↓) キーを押して、**[IPMI Configuration]** に移動します。**Enter** キーを押します。
3. 下矢印 (↓) キーを押して、**[Set LAN Configuration]** に移動します。**Enter** キーを押します。
4. **[LAN Protocol Control]** に移動します。**Enter** キーを押します。
5. 必要に応じて **[Enable]** または **[Disable]** を押して、Telnet または HTTP を有効にするか無効にします。

## LO100 で使用する TCP および UDP ポート番号

次の表に、LO100 のネットワークアクセス可能な各種機能によって使用される TCP および UDP ポート番号を示します。この情報は、ネットワークインフラストラクチャやセキュリティの設定に使用することができます。

ポート番号	プロトコル	サポート	デフォルトで内蔵
22	SSH	Secure Shell 接続	有効
23	Telnet	コマンドライン インターフェイス、リモートテキスト コンソール	有効
69	TFTP	ファームウェアのアップグレード	有効
80	HTTP	ファームウェアのアップグレード	有効
162	SNMP トラップ	Web ベース ユーザー インターフェイスおよび LO100 仮想 KVM	有効
443	HTTPS	Web ベースのユーザー インターフェイスへの安全なアクセス 仮想 KVM	有効
623	IPMI RMCP+	IPMI-over-LAN 接続	有効
664	セキュア IPMI RMCP+	IPMI-over-LAN 接続	有効
5901	ストレージ	ストレージ	有効

## ファームウェアの更新

LO100 のファームウェアを更新するには、ROMPaq ユーティリティを使用します。ROMPaq ユーティリティのダウンロードファイルは、HP の Web サイト <http://www.hp.com/jp/support>

で入手できます。ROMPaq ユーティリティの使用については、HP の Web サイト <http://www.hp.com/jp/servers/manage> を参照してください。

**注記:** LO100 は、仮想メディアからの ROMPAQ フラッシュをサポートしていません。

選択したデバイスの ROMPaq ユーティリティ フラッシュが完了したら、電源を手動でいったん切って再投入し、オペレーティング システムを再起動してください。

## ファームウェアのリモート更新

LO100 ファームウェアをリモートで更新するには、load コマンドを使用します。ファームウェア ファイルは、Lights-Out 100 Firmware Upgrade Diskette Utility に含まれる DOS ROMPAQ ユーティリティを使用して作成した解凍済みファームウェア イメージ ファイルでなければなりません。このユーティリティは、HP の Web サイト <http://www.hp.com/servers/lights-out> (英語) からダウンロードできます。

解凍済みイメージ ファイルを作成するには、DOS プロンプトで次のコマンドを入力します。

```
ROMPAQ /D <infile> <outfile>
```

ここで、<infile> は ROMPAQ ファームウェア イメージ ファイルで、<outfile> は解凍済みバイナリ イメージ ファイルのファイル名です。たとえば、次のように入力します。

```
ROMPAQ /D cpqq0801.D14 ldrImage.bin
ROMPAQ Firmware Upgrade Utility, Version 5.02 (R)
Copyright (c) Hewlett-Packard Corporation, 1994-2006
Input file: CPQQ0801.D14
Output file: LDRIMAGE.BIN
```

load コマンドは、特定の位置 (URL で指定) からバイナリ イメージを取得して特定のアドレスに配置する際に使用します。

load コマンドは、指定した位置から TFTP を使用して、ファームウェア イメージ ファイルをダウンロードしてフラッシュすることができます。

TFTP 設定を使用したファームウェアをフラッシュするには、以下の手順に従ってください。

- Windows オペレーティング システムの場合
  1. BMC ファームウェアをサーバー上のディレクトリにコピーします。
  2. 実行可能ファイル tftpd32.exe を実行して、TFTP を起動します。
  3. **[TFTP configuration]**、**[Settings]** の順に選択して、**[Timeout]** を 4 秒、**[Max Retransmit]** を 10 回に設定します。
  4. **[Base Directory]** と **[TFTP Server IP Address]** を入力します。**[Base Directory]** には、BMC ファームウェアの存在する位置のパスを指定します。**[TFTP Server IP Address]** には、TFTP サーバーの IP アドレス (例: 10.141.38.157) を指定します。
- Linux オペレーティング システムの場合
  1. **[アプリケーション]**、**[システム設定]**、**[サーバー設定]**、**[サービス]** の順に選択し、TFTP と xinetd が実行されていることを確認します。
  2. /etc/xinetd.d/tftp ファイルを開いて、server\_args パラメーターが「-T 4000000」を含むように変更します (たとえば、server\_args = -c -s /tftpboot -T 4000000)。  
このディレクトリで、サーバーパラメーターを変更するには、gedit と入力します。
  3. xinetd をリセットして、更新できるようにします。端末を開いて、service xinetd restart と入力します。RHEL 以外の Linux プラットフォームでは、**[Services]** メニューを開いて xinetd を手動でリセットします。
  4. ファイアウォールが有効な場合は、無効にするかファイアウォールが TFTP ポートへの接続を許可するように設定を変更します。ファイアウォール設定を変更するには、**[Applications]**、**[System Settings]**、**[セキュリティ レベル]** の順に選択して、**[他のポート]** のパラメーターに「69:udp」と入力します。

5. TFTP サーバー ルート ディレクトリにある /tftpboot フォルダの中に、イメージ ファイルを置きます。

ファームウェアを更新するには、CLP インターフェイスから管理者として LO100 にログインし、map1/firmware ディレクトリから load コマンドを実行してファームウェアをアップロードしインストールします。

1. CLP セッションを開始します。CLP にアクセスするには、次の手順を実行します。
  - a. **[スタート]**、**[すべてのプログラム]**、**[アクセサリ]**、**[コマンド プロンプト]** の順に移動します。
  - b. コマンド プロンプトで、telnet <IP アドレス > と入力します。

2. CLP プロンプトで、cd map1/firmware と入力します。

3. CLP プロンプトで、

```
load -source <URI> -oemhptype csr
```

と入力します。

ここで

- <URI> には、//<tftpserver IP>/<ダウンロードする filename> と入力します。
- また、<tftp server IP> は、ファームウェアが配置された TFTP サーバーの URL または IP アドレスです。
- <filename> は、イメージファイルのファイル名です（この例では、ldrImage.bin）。

たとえば、

```
load -source //10.141.38.157/LdrImage.bin - oemhptype csr
```

と入力します。

または、ブラウザを介してファームウェアをインストールすることもできます。詳しくは、「[Web ブラウザーを介したファームウェアのインストール](#)」を参照してください。

TFTP アプリケーションが、ファームウェア アップロード プロセスの早期段階のファームウェアイメージを確認する手順で、エラーを報告する場合があります。エラーの表示は必ずしもファームウェア アップロードの失敗を意味しません。また、このエラーの発生でファームウェアの正常なアップロードが妨げられることもありません。ファームウェアのアップロードには、通常、数分かかります。ファームウェアのアップグレードプロセスが完了したら、ファームウェアの新しいバージョンが有効になっているかどうかを確認してください。

5 分以上待っても、なおファームウェアのアップグレードが失敗している場合は、サーバーを再起動して、ファームウェアの以前のバージョンが有効かどうかを確認してください。ファームウェアのアップグレードをやり直す場合は、必ず、事前にサーバーを再起動してください。

ダウンロード中にシステムや BMC をリセットしないでください。サーバーが壊れることがあります。

ファームウェアのインストール後、サーバーの IP アドレスがデフォルト値にリセットされることがあります。その場合は、IP アドレスをローカルで再設定して使用したい値にする必要があります。

---

**注記:** load コマンドの使用後、LO100 はリセットして CLP インターフェイス セッションを終了します。終了後、CLP インターフェイスに、再接続する必要があります。

**注記:** TFTP32 とともに CLP の load コマンドを使用する場合は、タイムアウトを 4 秒、再試行を 10 回に設定することをおすすめします。

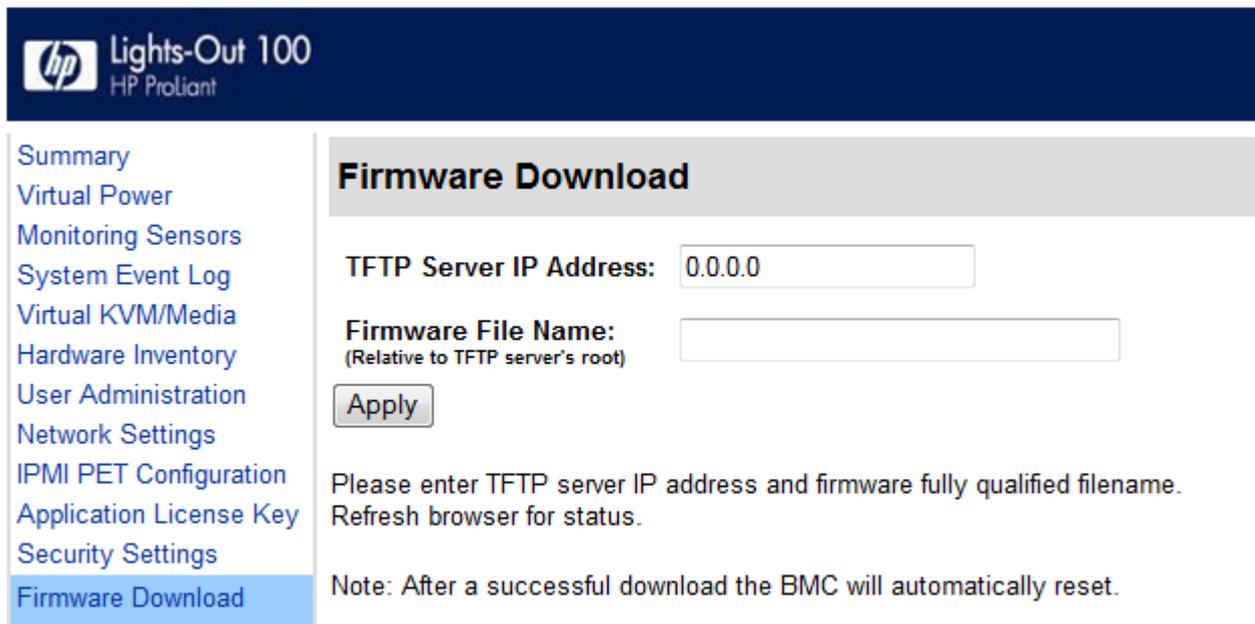
---

ダウンロードの完了後システムをリセットして SDRR と CFGs をロードします。これにより、LO100 は、「ProLiant Generic G6」ではなく、個々のサーバー プラットフォームを認識できます。

## Web ブラウザーを介したファームウェアのインストール

[Firmware Download] ページを使用すると、新しいファームウェア イメージをインストールすることができます。ブラウザ経由でファームウェアをインストールするには、以下の手順に従ってください。

1. 管理者として LO100 にログインします。
2. ブラウザー メイン リコグニション ボックスで **[Firmware Download]** をクリックします。
3. [TFTP server IP address] フィールドに、TFTP サーバーの IP アドレスを入力します。
4. [File Name] フィールドに、ファームウェア イメージのファイル名を入力します。ファイル名には、TFTP サーバーのルートからのファイルの相対パスを入力してください。
5. ファームウェアのインストールに Linux を使用している場合：
  - a. TFTP サーバー ルート ディレクトリにある /tftpboot フォルダの中に、イメージ ファイルを置きます。
  - b. [Firmware File name] フィールドに、ファームウェア イメージのファイル名を入力します。ファイル名には、TFTP サーバーのルートからのファイルのパスを入力します。
6. **[Apply]** をクリックすると、BMC がリセットされます。
7. Web ブラウザーに、再接続します。フラッシュには通常数分かかります。



hp Lights-Out 100  
HP ProLiant

Summary  
Virtual Power  
Monitoring Sensors  
System Event Log  
Virtual KVM/Media  
Hardware Inventory  
User Administration  
Network Settings  
IPMI PET Configuration  
Application License Key  
Security Settings  
Firmware Download

### Firmware Download

TFTP Server IP Address:

Firmware File Name:  
(Relative to TFTP server's root)

Please enter TFTP server IP address and firmware fully qualified filename.  
Refresh browser for status.

Note: After a successful download the BMC will automatically reset.

## オンラインフラッシュユーティリティを使用したファームウェアの更新

Lights-Out 100 のオンラインフラッシュユーティリティを使用すると、サーバーをリセットすることなく、サポートされるオペレーティングシステムを介して BMC ファームウェアを更新できます。オンラインフラッシュユーティリティは、HP の Web サイト <http://www.hp.com/jp> のプラットフォームごとのダウンロード セクションからダウンロードできます。

次のオペレーティングシステムがサポートされています。

- Red Hat Enterprise Linux 5.4 (i386、x86\_64)
- Red Hat Enterprise Linux 4.8 (i386、x86\_64)
- SuSE Linux Enterprise Server 10 (i386、x86\_64)
- SuSE Linux Enterprise Server 11 (i386、x86\_64)

- Windows Server 2008 (x86、x64) - すべてのエディション
- Windows Server 2008 R2 - すべてのエディション

---

**注記:** Windows Server 2003 は、サポートされません。

---

Windows オペレーティングシステム上でオンラインフラッシュコンポーネントを使用するには、以下の手順に従ってください。

1. LO-100 オンラインフラッシュユーティリティをサーバーのファイルシステム上のディレクトリにコピーします。
2. 実行可能ファイルをダブルクリックします。
3. **[Install]** をクリックします。
4. インストールプロセスが完了するまで待ちます。

---

**注記:** サーバーによっては、最大 45 分かかることがあります。サーバーのシャットダウンやフラッシュプロセスの中断は避けてください。

---

5. **[Finish]** をクリックします。完了後、再起動する必要はありません。

Linux オペレーティングシステム上でオンラインフラッシュコンポーネントを使用するには、以下の手順に従ってください。

1. LO100 オンラインフラッシュユーティリティをサーバーのファイルシステム上のディレクトリにコピーします。
2. オンラインフラッシュコンポーネントを配置しているディレクトリで、bash シェルを開きます。
3. 次の各コマンドを実行します。

```
chmod 777 CPxxxxxxx.scexe
./CPxxxxxxx.scexe
```

4. インストールプロセスが完了するまで待ちます。

---

**注記:** サーバーによっては、最大 15 分かかることがあります。サーバーのシャットダウンやフラッシュプロセスの中断は避けてください。

---

5. **[Finish]** をクリックします。完了後、再起動する必要はありません。

## 3 LO100 の使用

### SSL の使用

SSL は、インターネット経由で機密性の高い文書を送受信する際に使用されるプロトコルで、プライベート キーや証明書を使用して、SSL 接続経由で転送されるデータを暗号化します。Lights-Out 100 は、非セキュア ネットワーク上を転送されるデータに業界標準の暗号化プロトコルを使用することにより、分散 IT 環境でのリモート管理に強力なセキュリティ機能を付加します。SSL は、デフォルトで使用できます。

LO100 には、あらかじめ証明書がインストールされています。ユーザー固有の証明書をインストールするには、「証明書のインポート」で 1 回限りサポートされている、インポート手順を参照してください。

ログイン ページにアクセスできない場合は、ブラウザの SSL 暗号化レベルが 128 ビットに設定されているかどうかを確認する必要があります。マネジメント プロセッサの SSL 暗号化レベルは 128 ビットに設定されており、変更することはできません。また、ブラウザとマネジメント プロセッサの暗号化レベルは一致していなければなりません。

インストール済みの証明書を使用するには、SSL 暗号化通信を使用するブラウザのアドレスボックスに `https://<IP アドレス >` と入力してください。SSL で暗号化しないで通信を行う場合は、`http://<IP アドレス >` と入力してください。

### SSH の使用

SSH は、リモート マシンにログインしてコマンドを実行するための Telnet によく似たプロトコルです。ただし、SSH には、認証、暗号化、およびデータの整合性機能が含まれるため安全です。Lights-Out 100 リモート マネジメント プロセッサは、4 つの SSH クライアントからの同時アクセスをサポートします。SSH の接続および認証後、ユーザーは、コマンドライン インターフェイスを使用できます。LO100 は、同時に 2 つの SSH 接続をサポートします。SSH は、デフォルトで使用できます。

LO100 は、SSH バージョン 2 および以下のクライアント ユーティリティをサポートします。

- PuTTY 0.54 以降
- OpenSSH

LO100 には、あらかじめ証明書がインストールされています。ユーザー固有の証明書をインストールするには、「証明書のインポート」で 1 回限りサポートされている、インポート手順を参照してください。

### SSH ユーティリティの使用

SSH ユーティリティを使用してサーバーに初めて接続すると、ユーティリティは、サーバーパブリック キー（ホスト キーと呼ばれることもあります）を受け取るようにユーザーに指示します。このキーを受け取ることで、ユーティリティは自身のデータベースにパブリック キーのコピーを保存できます。以降の接続で、ユーティリティは、パブリック キーをデータベースに保存したものと比較することでサーバーを識別します。

**注記:** SSH セッションへのログインには、最大 90 秒かかります。使用するクライアントによっては、この間、画面が変化しないことがあります。

SSH を使用してリモート マネジメント プロセッサにアクセスするには、以下の手順に従ってください。

1. SSH ウィンドウを開きます。
2. プロンプトが表示されたら、IP アドレス、ログイン名、およびパスワードを入力します。

## PuTTY ユーティリティの使用

PuTTY 0.54 は、Telnet および SSH プロトコルのサポートを含む、端末エミュレーション製品です。PuTTY 0.54 は、インターネットからダウンロードできます。

- PuTTY セッションを開始するには、PuTTY をインストールしたディレクトリにある PuTTY アイコンをダブルクリックします。
- コマンド ラインから PuTTY セッションを開始するには、以下の手順に従ってください。
  - host という名前のサーバーへの接続を開始するには、次のように入力します。

```
putty.exe [-ssh | -telnet | -rlogin | -raw] [user@]host
```
  - Telnet セッションの場合は、次の構文を入力することもできます。

```
putty.exe telnet://host[:port]/
```
  - session name という名前の保存済みの既存セッションを開始するには、次のように入力します。

```
putty.exe -load "session name"
```

PuTTY のバージョン 0.54 より前のバージョンでは、**Enter** キーを押すと、1 行の改行操作で 2 行が改行される可能性があります。この問題を防止して最適な結果を得るために、バージョン 0.54 以降の PuTTY を使用することをおすすめします。

## OpenSSH ユーティリティの使用

OpenSSH は、インターネット上でダウンロードできる、SSH プロトコルの無償バージョンです。

Linux マシンで OpenSSH クライアントを起動するには、コマンド プロンプトで次のように入力します。

```
ssh -l <ログイン名> <IPアドレス>/<DNS名>
```

## CLP の使用

HP は、DMTF (Distributed Management Task Force, Inc) に所属する主要な業界パートナー企業と協力して業界標準コマンド セットを定義しました。SMASH スイートは、サーバー用の管理インターフェイスを標準化します。Lights-Out 100 リモート マネジメント プロセッサは、**Server Management Command Line Protocol Specification, 1.00 Draft** で定義されたコマンド セットを実装します。CLP は、以前にリリースされ現在はサポートされていない単純な CLI に代わるコマンド セットです。

SMASH CLP からアクセスできるマネジメント プロセッサ機能は、低帯域幅のインターフェイスであり、Web インターフェイスと同様の機能を提供します。CLP は、グラフィカル インターフェイス以外のインターフェイスを使いたいユーザー向けに設計されています。CLP には、次の方法でアクセスできます。

- Telnet
- SSH 接続
- 物理シリアル ポート

LO100 CLP は、同時に 4 つの SSH 接続、2 つの SSH 接続および 2 つの Telnet 接続、または 1 つの SSH 接続および 3 つの Telnet 接続をサポートします。同時に 4 つを超える SSH 接続および同時に最大 3 つの (Telnet および SSH) 接続を持つことはできません。

## CLP 構文

CLP コマンドの一般構文は、次のとおりです。

<動詞> <ターゲット> <オプション> <プロパティ>

- **動詞** - サポートされる動詞は、次のとおりです。
  - cd
  - help
  - load
  - reset
  - set
  - show
  - start
  - stop
  - exit
  - version
- **ターゲット** - デフォルトのターゲットは、/です。ターゲットは、cd コマンドによって、またはコマンドラインでターゲットを指定することによって変更できます。
- **オプション** - 次のオプションは有効です。
  - -help/-h
  - -all/-a
- **プロパティ**は、ターゲットの変更可能な属性です。
- **出力** - 出力の構文は、テキストです。

コマンドの有効な Boolean 値は、*true* および *false* です。

### 一般的な注意事項

CLP コマンドでコマンドが複数行にわたる場合、異なる行の間を移動することはできません。

### オペレーティングシステム固有の注意事項

- Microsoft Windows 2000 の Telnet クライアントは、ファンクションキー (F1~F12)、Insert キー、Home キー、および End キーをサポートしていません。これらのキーは、Lights-Out 100 コマンドラインセッションでは機能しません。
- Lights-Out 100 の CLP 実装では、Backspace キーは、0x8 という値にマッピングされています。一部のクライアントオペレーティングシステム (Novell Linux Desktop および Red Hat Enterprise Linux 4 Desktop) は、Backspace キーを 0x7f という値にマッピングします。この値は、Windows の Telnet クライアントでは Delete キーに使用されます。Backspace キーは、このキーが 0x7f の値を持つクライアントでは機能しません。Linux クライアントについては、Home または End キーを使用することにより、Backspace キーが 0x7f の値を使用するように Lights-Out 100 CLP サービスが再マッピングするので、キーが機能するようになります。

Windows の PuTTY クライアントでは、[端末] の [キーボード] の設定を [Control-H] に変更することによって、Backspace キーを 0x8 の値にマッピングすることができます。

## 基本コマンド

- help コマンドは、コンテキストヘルプを表示します。  
help と入力すると、サポートされているすべてのコマンドが表示されます。  
< コマンド名 > help

と入力すると、そのコマンドに関するヘルプメッセージが表示されます。

- 動詞に関する ヘルプ情報

動詞を指定してヘルプを呼び出すと、その動詞の発行に関わる情報（一般構文および使用法）が戻されます。カレントディレクトリに存在しない動詞を指定してヘルプを呼び出すと、Unsupported Command メッセージが戻されます。次に示す例は、どれも動詞についてのヘルプ情報を取得するための有効な方法です。

```
- ./-> help show
Usage:
show [<target>] [<options>] [<properties>]

- ./-> show -h
Usage:
show [<target>] [<options>] [<properties>]

- ./-> show -help
Usage:
show [<target>] [<options>] [<properties>]

- ./->
```

- ターゲットに関する ヘルプ情報

ターゲットを指定してヘルプを呼び出すと、ターゲットとその内容に関する情報が戻されます。カレントディレクトリに含まれていないターゲットでも、そのターゲットについてのヘルプを呼び出せます（たとえば、help map1 を、system1 から呼び出せます）。

```
- ./-> system1 -h
Invalid command

- ./-> system1 -help
Invalid command

- ./-> help system1
Host System Directory

- ./-> help map1
Management Service Processor Directory

- ./-> cd system1

- ./system1/-> help map1
Management Service Processor Directory
```

- プロパティに関する ヘルプ情報

ヘルプ情報のない、プロパティまたは他のオプションを指定してヘルプを呼び出すと、Unsupported Command または Invalid command メッセージが戻されます。たとえば、次のように入力します。

```
./system1/-> show
./system1
Targets
  oemhp_sensors
  oemhp_frus
  log1
  led1
  console 1
```

```

Properties
  name=Hewlett-Packard
  enabledstate=enabled
Verbs
  cd
  version
  exit
  show
  reset
  start
  stop
  help
./system1/-> help name
Unsupported Command
./system1/-> help enabledstate
Unsupported Command
./system1/-> help properties
Unsupported Command ./system1/-> name -h
Invalid command ./system1/->

```

- exit コマンドは、CLP セッションを停止します。
- cd コマンドは、現在のデフォルト ターゲットを設定します。コンテキストは、ディレクトリパスと同様に機能します。サーバーのルート コンテキストおよび CLP システムの起点は、/。（スラッシュ、ピリオド）です。コンテキストを変更することによって、コマンドを短縮することができます。

たとえば、次のように入力します。

- cd コマンドは、ディレクトリを変更します。
- cd .. コマンドは、ツリー内で、1 つ上のディレクトリに移動します。
- myfolder がカレント ディレクトリにある場合は、cd myfolder コマンドは、myfolder に移動します。
- show コマンドは、収集ターゲットのプロパティの値または内容を表示します。たとえば、次のように入力します。

```

././> show
/.
Targets
  system1
  map1
Properties
Verbs
  cd
  version
  exit
  show
  help

```

show コマンドによって返される情報の最初の行は、現在のコンテキストです。この例では、

```
/.
```

が現在のコンテキストです。コンテキストの後に、現在のコンテキストに対応するサブターゲット (Targets) とプロパティ (Properties) のリストが表示されます。動詞 (Verbs) セクションには、このコンテキストに使用できるコマンドが表示されます。

show コマンドには、明示的または非明示的コンテキストや特定のプロパティを指定することもできます。明示的コンテキストは /map1/firmware であり、現在のコンテキストに依存しません。非明示的コンテキストは、指定されるコンテキストが現在のコンテキストの子コンテキストであることを前提としています。現在のコンテキストが /map1 である場合、show firmware コマンドは、/map1/firmware のデータを表示します。プロパティが指定されていない場合は、すべてのプロパティが表示されます。

- load コマンドは、バイナリ イメージを URL から map に移動させます。load コマンドは、特定の位置（URL で指定）からバイナリ イメージを取り出して特定のアドレスに配置する際に使用します。リモート マネジメント プロセッサの実装では、ファームウェアは TFTP を使用して、指定した位置からフル イメージ ファイルをダウンロードし、プログラムはそのイメージでフラッシュします。

リモート マネジメント プロセッサの実装では、/map1/firmware は有効なターゲットです。

load コマンドで使用できるオプションは、次のオプションだけです。

- -source < 位置 > - このオプションは指定する必要があります。
- (h)elp - このオプションは、コマンド行に表示されます。このコマンドは -output (terse または verbose 出力を指定) 以外の、すべてのオプションとプロパティを無視します。-output オプションは、このコマンドでは、-help オプションが使用されている場合のみ有効です。

source < 値 > - このオプションは、バイナリ イメージの転送元になるターゲットを指定します。指定する値は、有効な URL でなければなりません。書式は、//tftpserverip/path/filename です。このオプションは、-help を使用する場合を除いて、load コマンドを実行するときに指定する必要があります。ファイルは、Lights-Out 100 Firmware Upgrade Diskette Utility に含まれる DOS ROMPAQ ユーティリティを使用して作成した解凍済みファームウェア イメージ ファイルでなければなりません。このユーティリティは、HP の Web サイト <http://www.hp.com/servers/lights-out> (英語) からダウンロードできます。

- 以下のいずれかを指定します。
  - -oemhpfiletype csr (ファームウェアのロード)
  - -oemhpfiletype key (キーのロード)
  - -oemhpfiletype cer (証明書のロード)

例：

```
./map1/firmware/-> load -s //16.110.181.187/404.bin -oemhpfiletype csr
Firmware download is in progress.
BMC will be automatically reset once image is programmed and validated.
Checking Image 197120
Erasing Memory 2227924
Dnlding/Prgming 4194304
Time elapsed: 53 seconds.
Download Complete.
```

- reset コマンドは、ターゲットを有効から無効にして、もう一度有効に戻します。
- set コマンドは、特定の値をプロパティまたはプロパティのグループに割り当てます。set コマンドの標準構文は、

```
set property = new value
```

です。

変更可能なプロパティを変更するには、set コマンドを使用します。カレント ディレクトリに変更したいプロパティがない場合、変更するプロパティを入力する前にプロパティのターゲットを指定する必要があります。

- start コマンドは、system1 ターゲットの電源を入れます。
- stop コマンドは、system1 ターゲットの電源を切ります。
- version コマンドは、CLP 実装のバージョンまたはその他の CLP 要素のクエリを実行します。たとえば、次のように入力します。

```

./map1/-> version Version 1.00
./map1/-> cd firmware
./map1/firmware/-> version
Version 1.00
./map1/firmware/-> show
./map1/firmware
  Targets
  Properties
    fwversion=0.59
  Verbs
    cd
    version
    exit
    show
    reset
    load
    help
./map1/firmware/-> show fwversion
fwversion=0.59
./map1/firmware/-> fwversion
Invalid command
./map1/firmware/->

```

## 各コマンドについて

各コマンドの CLP 構文については、各項で紹介します。これらの項では、CLP の構文とともに Web インターフェイス経由での機能についても説明します。

## DCMI 1.0 サポート

LO100 は、Data Center Manageability Interface (DCMI) をサポートします。DCMI を使用すると、堅牢性を強化しつつプラットフォーム管理実装を簡素化することができます。仕様は、サーバー管理およびシステムヘルス監視用にコンピューター産業で広く採用されている Intelligent Platform Management Interface (IPMI) 2.0 から派生したものです。詳しくは、Intel 社の Web サイト <http://developer.intel.com/technology/product/DCMI/index.htm> (英語) を参照してください。

## IPMI 2.0 のサポート

LO100 は、業界標準の IPMI 2.0 をサポートします。IPMI 2.0 仕様は、プラットフォームハードウェアに組み込まれた機能の監視および制御に使用できる、標準化されたインターフェイスを抽象レベルで定義しています。

LO100 では、IPMI 2.0 の必須コマンドに加え、次に示す追加 IPMI 2.0 機能をサポートします。

- 追加 IPMI 2.0 コマンド
  - Get Channel Cipher Suites
  - Set/Get Channel Security Keys
  - Suspend/Resume Payload Encryption
- ペイロードのタイプ
  - IPMI Message
  - RMCP+ Open Session Request/Response
  - RAKP Message 1 / 2
  - RAKP Message 3 / 4
- 認証アルゴリズム
  - RAKP-none

- RAKP-HMAC-SHA1
- 整合性アルゴリズム
  - None
  - HMAC-SHA1-96
- 機密保持アルゴリズム
  - None
  - AES-CBC-128

## LO100 へのログイン

リモート マネジメント プロセッサには、Web ブラウザー経由または CLP を使用してログインできます。使用している DHCP IP アドレスがわからない場合は、「[ネットワーク アクセスの設定](#)」(7 ページ) を参照してください。

### Web ブラウザー経由でのログイン

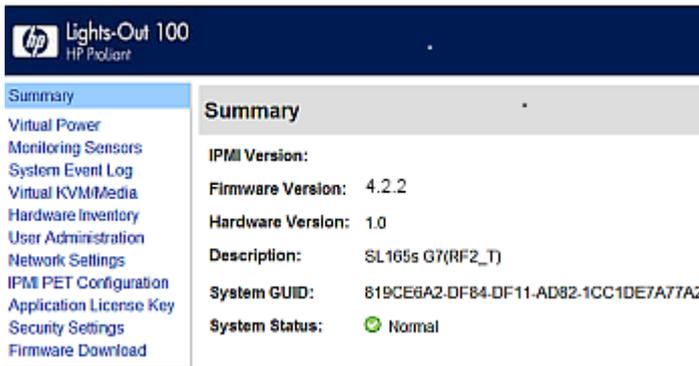
1. リモート マネジメント プロセッサの IP アドレスを指定して、ログイン画面にアクセスします。
2. ユーザー名とパスワードを入力します。管理者アカウントのデフォルトのユーザー名は `admin` で、デフォルトのパスワードも `admin` です。オペレーター アカウントのデフォルトのユーザー名は `Operator` で、デフォルトのパスワードも `Operator` です。

### CLP を使用したログイン

1. TelnetセッションまたはSSHセッションを開始して、リモート マネジメント プロセッサへの接続を確立します。
2. ログインプロンプトで、ユーザー名を入力します。管理者アカウントのデフォルトのユーザー名は `admin` です。Operator アカウントのデフォルトのユーザー名は `Operator` です。
3. パスワードプロンプトで、パスワードを入力します。管理者アカウントのデフォルトのパスワードは `admin` です。オペレーター アカウントのデフォルトのパスワードは `Operator` です。
4. CLP を終了して Console モードに入るには、コマンドプロンプトに  
`exit`  
コマンドを入力します。

## ブラウザーのメイン メニュー オプション

LO100 の基本的なリモート マネジメント機能には、すべて、Web ブラウザー経由でアクセスできます。このガイドで示す機能や説明する機能は、すべてのシステムに共通ではありません。ご使用のシステムでサポートされる機能を確認するには、「[LO100 のオプション \(ライセンス済み\) 機能](#)」を参照してください。



**Summary**

- IPMI Version: 4.2.2
- Firmware Version: 4.2.2
- Hardware Version: 1.0
- Description: SL165s G7(RF2\_T)
- System GUID: 819CE6A2-DF84-DF11-AD82-1CC1DE7A77A2
- System Status: ✔ Normal

オプション	説明
[Summary]	メインメニューのナビゲーションバーにアクセスするか、ユーザーをこのナビゲーションバーに戻します。
[Virtual Power]	システム電源および UID 制御オプションにアクセスします。
[Monitoring Sensors]	種類、名前、ステータス、測定値、PEF 設定など、センサーに関するすべての情報を示します。
[System Event Log]	システム イベント ログを表示します。
[Virtual KVM/Media]	仮想メディアまたはリモート グラフィック コンソールにアクセスします。
[Hardware Inventory]	システム ハードウェア情報を表示します。
[User Administration]	ユーザー設定画面にアクセスします。
[Network Settings]	ネットワーク パラメーター設定画面にアクセスします。
[IPMI PET Configuration]	PET ディスティネーションおよびアラート ポリシーテーブルにアクセスします。
[Application License Key]	ライセンス画面を表示します。
[Security Settings]	LO100 のセキュリティ、カスタム証明書およびキー インストール オプションにアクセスします。
[Firmware Download]	Web ブラウザーを介してファームウェアをフラッシュできます。

**注記:** 仮想 KVM/メディア オプションはライセンスアップグレードで使用できるアドバンスド機能であり、ライセンスを購入しない限り、すべての G6 システムで使用できるわけではありません。システムの構成によっては、このリンクが [Virtual Media] と表示されることや、全く表示されないことがあります。ご使用のシステムでサポートされる機能を確認するには、「[LO100 のオプション \(ライセンス済み\) 機能](#)」を参照してください。

## サーバー電源のリモート制御

LO100 を使用すると、Web ブラウザーまたは CLP を使用して、ホスト サーバーの電源ボタンをリモートで操作できます。LO100 仮想電源のサポートにより、ホスト サーバーの電源オン、オフ、および電源の再投入ができます。この仮想電源サポートは、オペレーティングシステムの状態とは関係なく機能します。

## ブラウザ経由でのサーバー電源の制御

[Virtual Power] 画面には、現在の電源ステータス、サーバーの電源投入継続時間、および最新のサーバー再起動の発生理由が表示されます。[Virtual Power] 画面を表示するには、メインメニューのナビゲーションバーで **[Virtual Power]** をクリックします。

Summary

Virtual Power

- Monitoring Sensors
- System Event Log
- Virtual KVM/Media
- Hardware Inventory
- User Administration
- Network Settings
- IPMI PET Configuration
- Application License Key
- Security Settings
- Firmware Download

## Virtual Power

### Chassis Information

Power Status: ON  
Power On Counter: 15 days 3 hrs 50 minutes  
Last Restart Cause: Unknown

### Chassis Actions

Power Control Options:    
UID:

### Power Restore Policy

- Always power up
- Restore to powered state prior to power loss
- Power pushbutton or command required to power on system

Please note that the Power Restore Policy will be active after successful BIOS post.

シャーシ アクションを変更するには、[Chassis Actions] セクションで電源制御オプションを選択して **[Apply]** をクリックします。

ラック内のサーバーの位置を確認するために UID（サーバーのフロント パネルの LED）を点灯するには、[UID] リストから UID の点灯時間を選択し、**[Identify]** をクリックします。

**注記:** UID は、すべての LO100 サーバーにあるわけではありません。詳しくは、サーバーのユーザー ガイドを参照してください。

リストアポリシーは、サーバーに電源が接続されたときのシステムの対応を制御します。リストア ポリシーを設定するには、以下の手順に従ってください。

1. [Power Restore Policy] で次のいずれかを選択します。
  - [Always power up] - 電源が復旧した後で、すぐにサーバーに電源が投入されます。
  - [Restore to powered state prior to power loss] - 停電前にシステムに電源が投入されていた場合にのみシステムに電源が投入されます。
  - [Power pushbutton or command required to power on system] - 外部からの操作が行われるまでサーバーに電源は投入されません。

2. **[Set]** をクリックします。  
電源のリストア ポリシーは、BIOS の POST が正常に終了した後に有効になります。

## CLP を使用したサーバー電源の制御

1. 「[LO100 へのログイン](#)」 (26 ページ) の説明に従って、LO100 CLP にログインします。
2. `cd system1` と入力して、`system1` ターゲットに移動します。
3. サーバーの電源を入れるには、`start /system1` と入力します。たとえば、次のように入力します。

```
./system1/> start /system1  
System1 started.
```

4. サーバーの電源を切るには、`stop /system1` と入力します。たとえば、次のように入力します。

```
./system1/> stop /system1  
System1 stopped.
```

`stop` コマンドで `-force` オプションを指定することもできます。このオプションは、ターゲットを強制的に停止します。たとえば、ポリシーによって通常は `stop` コマンドを実行できない場合でも、このオプションを指定すると `stop` コマンドが実行されます。リモート マネジメント プロセッサの実装では、このプロセスはハード電源切断と同じです。

5. サーバーをリセットするには、`reset /system1` と入力します。たとえば、次のように入力します。

```
./system1/> reset  
System1 reset.
```

## センサーの監視

LO100 を使用すると、システムの温度、ファン、電圧など、ターゲット サーバーの主要センサーの最新ステータスをオペレーティング システムに依存することなくリモート監視できます。この機能のデータは、Web ブラウザーを使用して [\[Monitoring Sensors\]](#) ページで確認するか、または BIOS セットアップ ユーティリティを使用して確認できます。

## Web ブラウザーからのセンサー データ表示

[\[Monitoring Sensors\]](#) 画面には、センサーの種類、名前、ステータス、現在の測定値など、温度、ファン、および電圧センサーデータのスナップショットが表示されます。Web ブラウザーからこのページにアクセスするには、メイン メニュー ナビゲーション バーで **[Monitoring Sensor]** をクリックします。

Lights-Out 100 H7 Platform						
Summary	Monitoring Sensors					
Virtual Power	Sensor Type	Sensor Name	Sensor Status	Current Reading	PEF Setup	
Monitoring Sensors	<input checked="" type="checkbox"/>	Processor	CPU2 Therm Trip	Limit Not Exceeded	0	<input type="button" value="PEF"/>
System Event Log	<input checked="" type="checkbox"/>	Processor	CPU1 PROC Hot	Limit Not Exceeded	0	<input type="button" value="PEF"/>
Virtual KVM/Media	<input checked="" type="checkbox"/>	Processor	CPU2 PROC Hot	Unavailable		<input type="button" value="PEF"/>
Hardware Inventory	<input checked="" type="checkbox"/>	Processor	CPU1 Therm Trip	Limit Not Exceeded	0	<input type="button" value="PEF"/>
User Administration	<input checked="" type="checkbox"/>	Module/Board	NMI Detect	State Deasserted	0	<input type="button" value="PEF"/>
Network Settings	<input checked="" type="checkbox"/>	Power Supply	PS1 Status	Presence Detected	Bit 0 Asserted	<input type="button" value="PEF"/>
IPMI/PET Configuration	<input checked="" type="checkbox"/>	Power Supply	PS2 Status	Presence Detected	Bit 0 Asserted	<input type="button" value="PEF"/>
Application License Key	<input checked="" type="checkbox"/>	Power Supply	PS3 Status	Presence Detected	Bit 0 Asserted	<input type="button" value="PEF"/>
Security Settings	<input checked="" type="checkbox"/>	Power Supply	PS4 Status	Presence not Detected	Bit 0 Deasserted	<input type="button" value="PEF"/>
Firmware Download	<input checked="" type="checkbox"/>	Power Unit	PS Redundancy	Full Redundancy	Bit 0 Asserted	<input type="button" value="PEF"/>
	<input checked="" type="checkbox"/>	Voltage	PVCORE1	Normal operating range	1.0094 Volts	<input type="button" value="PEF"/>
	<input checked="" type="checkbox"/>	Voltage	PVMB CPU1	Normal operating range	1.0584 Volts	<input type="button" value="PEF"/>
	<input checked="" type="checkbox"/>	Voltage	P1V5 DDR3 CPU1	Normal operating range	1.4896 Volts	<input type="button" value="PEF"/>
	<input checked="" type="checkbox"/>	Voltage	PVCORE2	Unavailable		<input type="button" value="PEF"/>

表示を更新するには、**[Refresh]** ボタンをクリックします。PEF アクションを表示または追加するには、**[PEF]** をクリックします。詳しくは、「Platform Event Filtering 設定」を参照してください。

## BIOS セットアップ ユーティリティからのセンサー データの表示

- POST の実行時に **F10** キーを押して BIOS セットアップ ユーティリティを起動します。
- 右矢印 (→) キーを押して、[Advanced] メニューに移動します。
- 下矢印 (↓) キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
- サーバー モデルに応じて次のいずれかのオプションを選択します。
  - ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - 下矢印 (↓) キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
    - 下矢印 (↓) キーを押して、[Realtime Sensor Data] に移動します。 **Enter** キーを押します。
  - ML150 G6 サーバーでは、下矢印 (↓) キーを押して、[Hardware Health Information] に移動します。 **Enter** キーを押します。
  - DL160 G6、DL160se G6、SL160s G6、DL180 G6、SL160z G6、DL165 G7、および SL165z G7 サーバーでは、下矢印 (↓) キーを押して、[Hardware Health Information] メニューに移動します。 **Enter** キーを押します。
  - DL170h G6、DL170e G6、SL170z G6、SL170s G6、SL165s G7、および SL2x170z G6 サーバーでは、下矢印 (↓) キーを押して、[Hardware Health Information] メニューに移動します。次に、[Ambient Sensor Health Information] メニューに移動します。 **Enter** キーを押します。

Loading data. Please wait メッセージが表示されます。このメッセージが消えたあと、温度および電圧センサー データが表示されます。このデータはリアルタイム データであり、定期的に更新されます。

## Platform Event Filtering 設定

[PEF Configuration] 画面を利用して、受信または内部生成されたイベント メッセージに対して LO100 が選択した動作を行うように LO100 を設定できます。この動作には、システム電源の切断、システムのリセット、およびアラート生成のトリガなどがあります。

PEF 機能を有効にするには、CLP で次のコマンドを実行する必要があります。

```
cd map1
oemhp i 20 10 D0 18 00 12 01 03 D2
oemhp i 20 10 D0 18 00 12 02 3F 95
```

特定のセンサーを対象に PEF を設定するには、[Monitoring Sensors] 画面でそのセンサー行の右端にある **[PEF]** ボタンをクリックします。各センサーの [PEF] ボタンをクリックすると、そのセンサーの [PEF Configuration] ページが開きます。

[PEF Configuration] 画面は、[Current PEF Entries] と [Add PEF Entry] という 2 つのセクションで構成されます。[Current PEF Entries] セクションには、センサー タイプ、センサー名、PEF アクション、および PEF 制御情報が含まれます。ユーザーは、[Add PEF Entry] セクションを使用して、アクションを設定できます。

この画面を最初に開いた時点では、PEF が定義されていないため、[Current PEF Entries] セクションにエントリはありません。PEF エントリが定義されると、[PEF Control] フィールドを使用できるようになり、各エントリを有効化、無効化、または削除に設定することができます。

Sensor Type	Sensor Name	PEF Action	PEF Control	Alert Policy Entry
Temperature	Rear Board	Power Off	Enabled	No Alert Policy

アクション（PEF エントリ）を設定するには、目的の [Event Offsets] を選択し、目的の [PEF Action] 設定を選択して、**[Add]** をクリックします。

- [Event Offsets] - アクションをトリガするセンサー イベントの種類を定義する、トリップポイント（スレッシュホルドを超える変化）です。[Events Offsets] セクションに表示される情報は、センサーのタイプにより異なり、すべてのセンサーですべてのオプションを利用できるわけではありません。ユーザーは、使用可能なオプションのいずれかを選択できます。
- [PEF Action] - すべてのセンサーについて同じ情報が表示されます。
  - [Sensor Type] - 選択されたセンサーのタイプが表示されます。
  - [Sensor Name] - センサーの名前が表示されます。
  - [PEF Action] - [Power Off]、[Power Cycle]、[Hard Reset]、および [Send Alert] からの選択が可能です（IPMI 1.5 以降をサポートするシステム マネジメント コンソールが必要です）。

- [PEF Control] - センサーの有効と無効を切り替えることができます。
- [Alert Policy] ([Add] ボタンの横にあるリスト) - アラート ポリシー (定義されている場合) を選択できます。アラート ポリシーは、[PET Configuration] 画面で定義します。詳しくは、「Platform Event Trap の設定」を参照してください。  
アラート ポリシーが定義されていない場合 (デフォルト)、[Alert Policy] リストには、「No Alert Policy」と表示されます。[Alert Policy] リストには、アラート ポリシーが定義および設定された後で、情報が埋め込まれます。アラート ポリシーを設定すると、このセンサーおよび PEF を対象にして定義済みのアラート ポリシーを選択できるようになります。
- [Add] ボタン - 新しいエントリーを、ページ上部の [PEF Current Entry] テーブルに追加するために使用します。

## Platform Event Trap の設定

[IPMI PET Configuration] 画面では、IPMI 2.0 でサポートされるシステム マネジメント コンソールにアラートを送信するための、アラームの設定やサーバー上で発生する特定の条件の設定を行います。[IPMI PET Configuration] 画面を表示するには、メイン メニューのナビゲーションバーで **[IPMI PET Configuration]** をクリックします。

The screenshot shows the 'IPMI PET Configuration' page for an HP ProLiant server. The left sidebar contains navigation links such as 'Summary', 'Virtual Power', 'Monitoring Sensors', and 'IPMI PET Configuration'. The main content area is titled 'IPMI PET Configuration' and includes a 'Global PEF Configuration' section. In this section, 'PEF Enable' is currently set to 'Disabled'. Under 'PEF Actions', there are six checkboxes, all of which are checked: Alert, PowerOff, Reset, PowerCycle, SoftPowerOff, and NMI. An 'Apply' button is located below these settings. The 'PET Destinations' section contains a table with columns for 'Destination', 'IP Address', and 'MAC Address'. Two entries are shown: 'Alert1' and 'Alert2', both with '0.0.0.0' in the IP Address field and '00:00:00:00:00:00' in the MAC Address field. Each entry has an 'Apply' button to its right.

Destination	IP Address	MAC Address
Alert1:	0.0.0.0	00:00:00:00:00:00
Alert2:	0.0.0.0	00:00:00:00:00:00

ユーザーは、[Global PEF Enable] セクションを使用して、グローバル PEF アクションを設定できます。グローバル PEF アクションを作成するには、[PEF Enable] ボックスで **[Enabled]** を選択し、[PEF action] を選択して **[Apply]** をクリックします。

[PET Destinations] セクションは、LO100 による PET の送信先を示します (設定されている場合)。このセクションには、IP アドレスと MAC アドレスを指定する最大 8 つのエントリーがあります。[PET Destinations] セクションで、IP アドレスまたは MAC アドレスを入力して、**[Apply]** をクリックしてください。MAC アドレスと IP アドレスをともに入力した場合、IP アドレスが使用されます。

ポリシーを設定するには、以下の手順に従ってください。

1. [Policy Enable] ステートを選択して、[Policy Number] および [Destination Selector] 情報を入力します。
  - [Policy Enable] - トラップの転送を選択的に有効または無効に設定できます。
  - [Policy Number] - PEF 設定で使用するポリシーを選択できます。

- [Destination Selector] - [PET Destinations] セクションで定義した送信先の中から PET トラップの送信先を選択できます。

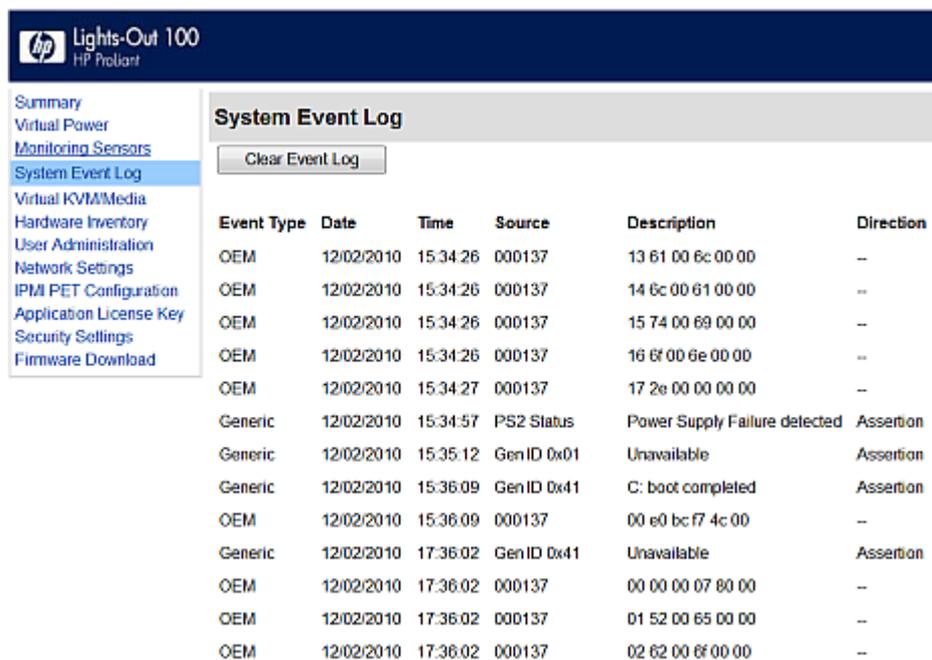
2. **[Apply]** をクリックします。

## システム イベント ログの使用

LO100 は、サーバーが動作していない場合でも、IPMI イベント ログを取得して保存します。このログには、ブラウザー、CLP、BIOS セットアップ ユーティリティ、および RBSU を使用してアクセスできます。システム イベント ログには、それぞれのシステム イベントの短い説明が表示されます。記録されるイベントには、異常温度、ファン イベント、システム リセット、およびシステム電源切断などがあります。

## Web ブラウザーからのシステム イベント ログへのアクセス

[System Event Log] 画面には、イベントのタイプ、発生日付、時刻、ソース、説明、および指示が表示されます。



Event Type	Date	Time	Source	Description	Direction
OEM	12/02/2010	15:34:26	000137	13 61 00 6c 00 00	-
OEM	12/02/2010	15:34:26	000137	14 6c 00 61 00 00	-
OEM	12/02/2010	15:34:26	000137	15 74 00 69 00 00	-
OEM	12/02/2010	15:34:26	000137	16 6f 00 6e 00 00	-
OEM	12/02/2010	15:34:27	000137	17 2e 00 00 00 00	-
Generic	12/02/2010	15:34:57	PS2 Status	Power Supply Failure detected	Assertion
Generic	12/02/2010	15:35:12	GenID 0x01	Unavailable	Assertion
Generic	12/02/2010	15:36:09	GenID 0x41	C: boot completed	Assertion
OEM	12/02/2010	15:36:09	000137	00 e0 bc f7 4c 00	-
Generic	12/02/2010	17:36:02	GenID 0x41	Unavailable	Assertion
OEM	12/02/2010	17:36:02	000137	00 00 00 07 80 00	-
OEM	12/02/2010	17:36:02	000137	01 52 00 65 00 00	-
OEM	12/02/2010	17:36:02	000137	02 62 00 6f 00 00	-

Web ブラウザーから [System Event Log] ページにアクセスするには、メインメニューナビゲーションバーで **[System Event Log]** をクリックします。システム イベント ログをクリアするには、**[Clear Event Log]** をクリックします。

## CLP を使用したシステム イベント ログへのアクセス

1. 「[LO100 へのログイン] (26 ページ) の説明に従って、CLP にログインします。
2. `cd ../system1/log1` と入力します。
3. `show` と入力して、システム イベント レコードの総数を表示します。
4. `show record<n>` と入力して、各レコードの詳細を表示します。たとえば、次のように入力します。

```
./map1/log1/-> show record1
record
Targets
Properties
number=1
date=05/07/2008
time=16:42:52
sensordescription=Identify
```

```
eventdescription=State Asserted
eventdirection=Assertion
Verbs
cd
version
exit
show
reset
oemhp
help
```

## BIOS セットアップユーティリティを使用したシステム イベント ログへのアクセス

1. POST の実行時に **F10** キーを押して BIOS セットアップ ユーティリティを起動します。
2. 右矢印 (→) キーを押して、[Advanced] メニューに移動します。
3. 下矢印 (↓) キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
4. サーバー モデルに応じて次のいずれかのオプションを選択します。
  - ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[IPMI] に移動します。 **Enter** キーを押します。
    - b. 下矢印 (↓) キーを押して、[System Event Log] に移動します。 **Enter** キーを押します。
  - DL160 G6、DL160se G6、DL170h G6、DL170e G6、DL180 G6、SL160z G6、SL160s G6、SL165s G7、SL170z G6、SL170s G6、SL2x170z G6、DL165 G7、および SL165z G7 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[System Event Log Configuration] メニューに移動します。 **Enter** キーを押します。
    - b. 下矢印 (↓) キーを押して、[Clear System Event Log] または [View System Event Log] のいずれか必要な方に移動します。
5. **Enter** キーを押して、強調表示されたセットアップ項目を表示します。
6. **Esc** キーを押して前の画面に戻るか、**F10** キーを押して変更を保存し、セットアップを終了します。

## 仮想 KVM の使用

LO100 の仮想 KVM を特徴付けているのが、リモート グラフィック コンソールです。このコンソールによって、サポートされるブラウザを仮想デスクトップとして使用し、ホストサーバーのディスプレイ、キーボード、およびマウスをフル制御できます。コンソールはオペレーティングシステムに依存することなくグラフィック モードをサポートし、シャットダウンおよびスタートアップ操作など、リモートのホストサーバーの動作を表示します。

仮想 KVM は、Lights-Out 100i Advanced Pack を購入することで使用できます。詳しくは、「[LO100 のオプション \(ライセンス済み\) 機能](#)」を参照してください。

仮想 KVM アプレットに初めて接続すると、アプレットはエラーを報告します。エラーをクリアして仮想 KVM アプレットに接続するには、ブラウザセッションを閉じてから、仮想 KVM アプレットに再接続します。

仮想 KVM アプレットは、標準 VNC クライアントとの互換性はなく、VNC プロトコルは標準実装されていません。サーバーに接続するには、提供されている Java アプレットを使用する必要があります。仮想 KVM アプレットは、F10 キーシーケンスをターゲット システムに渡すことができません。この問題を解決するために、リモートサーバーで仮想キーボードを使用し、F10 キーを転送してください。

リモート グラフィック コンソールを使用するには、クライアント システムに JVM バージョン 1.4.2 以降をインストールする必要があります。システム構成に適合する推奨 JVM をダウンロードするには、HP の Web サイトを参照してください。

Web ブラウザーを使用して IO100 のリモート グラフィック コンソールを起動するには、以下の手順に従ってください。

1. IO100 にログインします。
2. **[Virtual KVM / Media]** をクリックします。IO100 のリモート グラフィック コンソール ウィンドウが表示されます。

---

**注記:** 仮想 KVM/メディア オプションはライセンス アップグレードで使用できるアドバンスド機能であり、ライセンスを購入しない限り、すべての G6 システムで使用できるわけではありません。システムの構成によっては、このリンクが [Virtual Media] と表示されることや、全く表示されないことがあります。ご使用のシステムでサポートされる機能を確認するには、「[IO100 のオプション \(ライセンス済み\) 機能](#)」を参照してください。

---

3. **[OK]** をクリックしてシステムをフル制御するか、**[Cancel]** をクリックしてシステムに表示のみのモードでアクセスします。

IO100 リモート グラフィック コンソールでマウスを使用する前に、ローカル マウス ポインターとリモート マウス ポインターの同期を取ることをおすすめします。詳しくは、「[マウスの同期化](#)」(37 ページ) を参照してください。

## リモート グラフィック コンソールの使用

リモート KVM/メディア ビューアーは、仮想デスクトップを表示し、ホスト サーバーのディスプレイ、キーボード、およびマウスをフル制御できます。リモート グラフィック コンソールのメニュー バーには、[Control]、[Preferences]、および [Help] の 3 つのメニューがあります。

- [Control] - 仮想メディア デバイスおよび仮想キーボードへのアクセスや、画面の更新、クライアントの終了を行うことができます。
- [Preferences] - マウス、キーボード、およびログ オプションを設定できます。
- [Help] - [About] ボックスが表示され、IO100 リモート グラフィック コンソールのバージョンおよびビルド日時が示されます。

リモート グラフィック コンソールの [Control] メニュー オプションには、いくつかのオプションがあります。

- [Virtual Media] - [Virtual Media Devices] ページが表示されます。[Virtual Media Devices] ページには、ストレージ サーバーのアクセス可能なすべてのメディア ドライブが表示されます。サポートされているデバイスは、CD-ROM、DVD-ROM、ディスク、および大容量記憶装置です。詳しくは、「[仮想メディアの使用](#)」(38 ページ) を参照してください。
- [Virtual Keyboard] - 仮想キーボードが表示されます。このキーボード上で仮想キーボードの言語を変更できます。キーボード設定を変更するには、「[リモート グラフィック コンソールの設定](#)」(36 ページ) を参照してください。

仮想キーボード上の [Lock] ボタンは、各言語に追加されています。[Lock] ボタンをクリックすると、同時に押した Shift、Alt、Ctrl、コンテキスト、Windows などの特殊キーが押し続けたままの状態になります。押した状態の特殊キーを解除するには、**[Lock]** ボタンをクリックし、次にそのキーをクリックします。

---

**注記:** ESC キー シーケンスを入力すると、余分な文字がバッファされ、リモート側で不適切なファンクション キー入力が認識される場合があります。この問題を回避してファンクション キーと Alt キー シーケンスを実行するには、**ESC** キーを押し続けてから放し、その後他のキー シーケンスを押してください。

---

- [Turn local monitor on] - ローカル モニターの電源を入れます。

- [Turn local monitor off] - ローカル モニターの電源を切ります。  
[Turn local monitor off] 設定が有効な場合は、仮想 KVM が起動されたときにローカル モニター（接続されている場合）が黒色（ブランク/オフ）で表示されます。これは、セキュリティ機能です。仮想 KVM を終了すると、ローカル モニターは正常動作に戻ります。  
仮想 KVM アプレットは、標準 VNC クライアントとの互換性はなく、VNC プロトコルは標準実装されていません。サーバーに接続するには、提供されている Java アプレットを使用する必要があります。仮想 KVM アプレットは、F10 キー シーケンスをターゲット システムに渡すことができません。この問題を解決するために、リモート サーバーで仮想 キーボードを使用して F10 キーを転送してください。
- [Refresh Screen] - 画面上の情報が更新されます。
- [Take Full Control] - 現在、表示のみのモードで操作を行っているユーザーがリモート コンソールを制御できるようになります。リモート コンソールを複数のユーザーが同時に制御することはできません。
- [Disconnect Session] - 選択したユーザーのセッションが切断されます。
- [Relinquish Full Control] - セッションの制御機能が解除され表示のみの状態になります。
- [Exit] - リモート セッションが終了します。

---

**注記:** [Keyboard]、[Refresh Screen]、[Take Full Control]、[Disconnect Session]、および [Relinquish Full Control] メニュー オプションは、フル仮想 KVM アクセスのみで使用できる、アドバンスド機能です。

---

## リモート グラフィック コンソールの設定

マウス、キーボード、およびログ設定を変更するには、**[Preferences]** を選択します。

- [Mouse] タブでは、マウス モードを設定できます。次のオプションのある [Mouse Mode] リストを表示するには、**[Mouse]** を選択します。
  - [Hide mode (Relative)] を選択すると、LO100 リモート グラフィック コンソールが [Relative mode] に変わります。  
[Relative mouse mode] を選択すると、ローカル マウス カーソルが非表示になります。  
[Hide Mode Relative] は、DOS ベースのプログラムを実行していてマウスが正しくトラッキングしていないときに使用してください。  
[Hide Mode] を使用すると、ローカル マウスにアクセスできなくなります。ローカル マウス（normal モード）にアクセスするには、**Ctrl+Alt+O** キーを押します。
  - [Absolute Mode] を選択すると、LO100 リモート グラフィック コンソールは、**x** 座標および **y** 座標の値をそのままサーバーに送信します。
  - [Relative Mode] を選択すると、LO100 リモート グラフィック コンソールのマウス位置の相対座標（以前マウス ポインターの位置からの移動分 (+/-)）がサーバーに送信されます。Linux および Windows では、このモードがデフォルト モードです。
- [Keyboard] タブでは、仮想キーボードの言語および接続タイプを設定できます。デフォルトの言語は、英語です。仮想キーボードの言語は、12 の言語から選択することで変更できます。

仮想キーボードを正しく機能させるには、リモート側のサーバーとローカル側のサーバー（LO100 リモート グラフィック コンソール）の言語を一致させる必要があります。

LO100 は、次の接続タイプをサポートします。

- [VNC (port 5900)] は、仮想 KVM と LO100 仮想メディアをサポートします。ポート 5900 は、デフォルトの設定です。
- [unsecured keyboard]（ポート 5902）は、キーボードをサポートします。ポート 5902 は、ビデオ、マウス、および LO100 仮想メディアをサポートします。

- [secure keyboard] (ポート 5904) は、このポートを介して送信されるすべてのキーボード データを暗号化します。ポート 5904 は、ビデオ、マウス、および LO100 仮想メディアをサポートする非セキュア ポートです。
- [Logging] タブを選択すると、Java コンソールでログ メッセージを表示できます。[Logging] タブでは、KVM の使用時間を通知するタイムアウト変数を確認することもできます。  
[Global Logging] は、デフォルトでは無効になっていますが、このオプションを有効にすると Java コンソールでログ メッセージを表示できます。  
このコンソールを 2 時間以上実行しないでください。2 時間以上使用すると、コンソールがすべての空きメモリを消費して、LO100 リモート グラフィック コンソールやユーザーの Web ブラウザーがクラッシュする可能性があります。イベント ログは定期的にクリアして、接続の遅延やクラッシュを防止してください。  
すべてのログ メッセージをコンソールに記録するには、[Logging] リストで **[Console]** を選択します。Java コンソール ウィンドウでログ メッセージをチェックするには、Internet Explorer のメニューバーにある [ツール] メニューのリストで **[Sun Java Console]** を選択します。  
すべてのログ メッセージをファイルに記録するには、[Logging] リストで **[Log File]** を選択します。これにより、[Console Log File] テキストボックスが有効になります。**[Browse]** ボタンをクリックして、ログメッセージを保存するファイルを選択するか、選択したファイルの完全修飾ファイル名をテキストボックスに入力してください。ユーザーが選択したファイルにも Java コンソールにもログ メッセージを送信するには、**[Console]** および **[Log File]** を選択してください。

## マウスの同期化

ローカル マウスのポインターとサーバーのマウスのポインターの同期を取るには、ローカル マウスを左上隅に移動して、サーバーのマウス ポインターを左上隅に誘導してください。両方のポインターが重なれば、ポインターの同期が取れるようになります。

マウスの同期を正しく取れるようにするには、LO100 リモート グラフィック コンソールを使用してリモート マシン (サーバー側) のマウス ポインターの精度オプションとハードウェア アクセラレータ オプションを変更する必要があります。

Windows オペレーティング システムでは、以下の手順に従ってください。

マウス ポインターの精度オプションを変更するには、以下の手順に従ってください。

1. **[スタート]** メニューから、**[コントロール パネル]** を選択します。
2. **[マウス]** をダブルクリックします。[マウスのプロパティ] ウィンドウが表示されます。
3. **[ポインター オプション]** を選択します。
4. [ポインター オプション] ウィンドウで次の操作を実行します。
  - a. [速度] バーを中程度に設定します。
  - b. [ポインターの精度を高める] オプションが選択されていないことを確認します。

ハードウェア アクセラレータ オプションを変更するには、以下の手順に従ってください。

1. デスクトップ画面を右クリックします。
2. **[プロパティ]** を選択します。[画面のプロパティ] ウィンドウが表示されます。
3. **[設定]**、**[詳細設定]** の順にクリックします。ビデオ カードとモニターのプロパティ ウィンドウが表示されます。
4. **[トラブルシューティング]** をクリックします。
5. ハードウェア アクセラレータを **[なし]** に設定して、カーソルおよびビットマップのアクセラレータを無効にします (スケールまたはオプションが **[最大]** より 1 つだけ下の値になるようにする)。
6. **[Apply]** をクリックします。
7. **[OK]** をクリックして [画面のプロパティ] ウィンドウを終了します。

Linux オペレーティング システムでは、以下の手順に従ってください。

- SLES 9 の場合：
  1. `xsetpointer -1` コマンドを使用してすべてのマウス デバイスを表示し、リモート コンソールのマウスであるマウス デバイスを決定します。
  2. `xsetpointer` の出力と X configuration (`/etc/X11/XF86Config` または `/etc/X11/xorg.conf`) を相互参照し、変更するマウスを特定します。
  3. リモート コンソールのマウスを変更するマウスとして選択します。たとえば、次のように入力します。

```
xsetpointer Mouse[2]
```
  4. `acceleration` パラメーターを設定します。たとえば、次のように入力します。

```
xset m 1 1
```
- Red Hat Enterprise Linux では、次のコマンドを使用して `acceleration` パラメーターを設定してください。

```
xset m 1 1
```

## システム ボタン

仮想キーボード上には、8 つのシステム ボタン (L`Ctrl`、L`Win`、L`Alt`、R`Alt`、R`Win`、R`Ctrl`、Context、および [Lock]) が用意されています。これらのボタンは、仮想キーとして使用でき、ローカル マシンの物理キーボードのキーとよく似ています。

たとえば、物理キーボードで **Ctrl+Alt+Del** キーを押すと、サーバーのタスク マネージャーに加えてローカル マシンのタスク マネージャーが表示されます。または、ログイン用のサーバーのロックが解除されます。同様の仮想キーを押してリモート サーバーのタスク マネージャーを表示するには、LO100 リモート グラフィック コンソール ウィンドウで、L`Ctrl` および L`Alt` ボタンをクリックし、物理キーボードで Del キーを押します。このキーの組み合わせを使用すると、LO100 リモート グラフィック コンソールのタスク マネージャーが表示されます。物理および仮想の Alt、C`tl` および Del キーの任意の組み合わせを使用できます。

- [Lock] ボタンと特殊ボタンをクリックすると、ボタンを放すまで押したままの状態になります。押した状態の特殊ボタンを解除するには、**[Lock]** ボタンをクリックしシステムのボタンを押します。
- L`Ctrl` と R`Ctrl`、L`Alt` と R`Alt`、L`Win` と R`Win` の選択またはペアリングは、英語キーボード上と同じように機能します。ただし、他の言語のキーボードでは別の動作が発生します。
- **[Context]** をクリックすると、LO100 リモート グラフィック コンソール ウィンドウを右クリックするのと同じ機能を利用できます。

## 仮想メディアの使用

LO100 仮想メディアの画面では、メディア デバイスの追加、アクセス、削除、および共有や、表示されている仮想メディア デバイス リストの更新を実行できます。LO100 仮想メディアは、Lights-Out 100i Advanced Pack を購入することで使用できます。詳しくは、「[LO100 のオプション \(ライセンス済み\) 機能](#)」を参照してください。

LO100 仮想メディアにアクセスするには、以下の手順に従ってください。

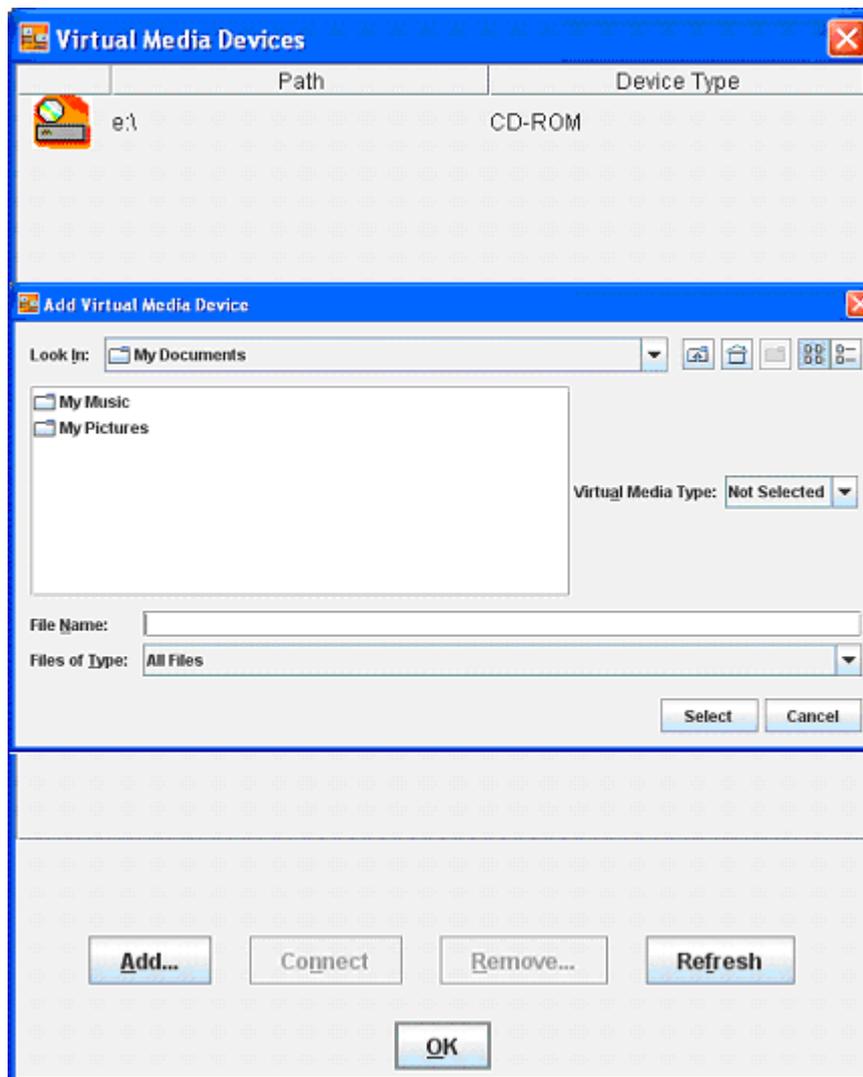
1. **[Virtual KVM / Media]** をクリックします。[Virtual KVM] 画面が表示されます。
2. [Virtual KVM] メニューで、[Control] メニューから **[Virtual Media]** を選択します。[Virtual Media] ウィンドウが表示されます。以下のオプションがあります。
  - **[Add]** をクリックすると、ストレージ デバイス リストに新しい仮想メディア デバイスを追加できます。詳しくは、「[仮想メディア デバイスの追加](#)」を参照してください。
  - **[Connect]** をクリックすると、選択されたデバイスを共有します。一度に共有できるデバイスは 1 つだけです。

- デバイスを選択して **[Remove]** をクリックすると、仮想メディア デバイス リストからデバイスが削除されます。
- **[Refresh]** をクリックすると、再スキャンが行われマシン上の現在のデバイスが表示されます。

仮想 KVM または仮想メディア アプレットを介してマウントした CD-ROM、DVD-ROM または ISO イメージは、ローカルにマウントしたメディア デバイスと同じように機能し、（ブート順に）表示されます。

## 仮想メディア デバイスの追加

LO100 の仮想メディア オプションにより、仮想メディア ドライブを使用できます。この機能を利用すると、ネットワーク上の任意の場所からリモートのホスト サーバーを起動して標準メディアを使用できます。仮想メディア デバイスは、ホストシステムの起動時に使用できます。



新しい仮想メディア デバイスを追加するには、[Virtual Media] ページで **[Add]** をクリックします。[Add Virtual Media Devices] ウィンドウが表示されます。このウィンドウには、次のオプションが用意されています。

- [参照] リストでは、表示するディレクトリやドライブを変更できます。
- [Virtual Media Type] リストでは、共有するファイルのタイプを指定できます。LO100 が共有するデバイスのタイプを認識するには、事前に仮想メディア タイプを示す必要があります。

- [ファイル名] テキストボックスには、イメージの共有名が表示されます。
- [ファイル タイプ] リストから値を選択し、共有するファイルのタイプを選択します。

## 仮想メディア デバイスの共有

仮想メディア デバイスの共有は、[Storage Devices] ウィンドウから設定できます。一度に共有できるデバイスは 1 つだけです。

仮想メディア デバイスを共有するには、以下の手順に従ってください。

1. [Virtual KVM] メニューで、[Control] メニューから **[Virtual Media]** を選択します。[Virtual Media] ウィンドウが表示されます。
2. 追加するデバイスがリストにない場合は、**[Refresh]** をクリックします。
3. デバイスを追加するには、「仮想メディア デバイスの追加」を参照してください。
4. デバイスを選択して、**[Connect]** をクリックします。メッセージ ボックスが表示され、デバイスが正しく接続されたと報告されるか、問題が発生したと報告されます。
5. **[OK]** をクリックして、[Virtual Media] ウィンドウを閉じます。

仮想メディアの共有デバイスを削除するには、以下の手順に従ってください。

1. 共有デバイスを削除する前に、デバイスを削除しても問題ないことを確認してください。必要に応じて、サーバー上でリムーバブル メディア デバイスを取り出しても問題がないことを確認する手順を実行します。
2. [Virtual KVM] メニューで、[Control] メニューから **[Virtual Media]** を選択します。[Virtual Media] ウィンドウが表示されます。
3. 削除したいデバイスを選択して、**[Remove]** をクリックします。ダイアログ ボックスが表示され、デバイスの接続が正しく切断されたことを示します。
4. **[OK]** をクリックして、[Virtual Media] ウィンドウを閉じます。

## Telnet 経由でのリモート コンソール アクセス

BIOS コンソールのテキスト リダイレクション機能または Windows Server 2003 のテキスト ベース コンソールを使用して、リモート コンソールにアクセスすることができます。一度に開くことのできるリモート コンソール ウィンドウは 1 つだけです。

リモート コンソール セッションを開始するには、**Esc+Q** キーを押します。リモート コンソール セッションを終了して CLP に戻るには、**Esc+** キーを押します。

**注記:** ESC キー シーケンスを入力すると、余分な文字がバッファーされ、リモート側で不適切なファンクション キー入力が認識される場合があります。この問題を回避してファンクション キーと Alt キー シーケンスを実行するには、**ESC** キーを押し続けてから放し、その後他のキー シーケンスを押してください。

Telnet およびリモート コンソールのタイムアウト設定を変更するには、Linux の raw IPMI コマンドまたは Telnet を介して

```
oemhp
```

コマンドを使用してください。次の例ではタイムアウトを無効にしています。

- Linux IPMI tool の Raw コマンドの例 :  

```
ipmitool raw 0x0c 0x01 0x02 0xf6 0x00 0x00
```
- Telnet を使用してセキュリティ タイムアウトを無効にする例 :  

```
oemhp i 20 30 b0 18 00 01 02 f6 00 00 ef
```

予想される応答 :

```
18 34 B4 20 00 01 00 DF .4.....
```

**注記:** これらのコマンドはファームウェア バージョン 3.05 以降でのみ動作します。

## Telnet 経由での BIOS コンソール テキストのリダイレクト

LO100 BIOS コンソールのテキスト リダイレクションを使用すると、ブート処理をリモートで確認したり、BIOS セットアップ ユーティリティをリモート コンピューターから変更したりすることができます。このユーティリティは、サーバーのトラブルシューティングや管理をリモートで行う際に役立ちます。

ターゲットシステムの BIOS セットアップ ユーティリティを設定するには、以下の手順に従ってください。

1. POST の実行時に **F10** キーを押して BIOS セットアップ ユーティリティを起動します。
2. 右矢印 (→) キーを押して、[Advanced] メニューに移動します。
3. サーバー モデルに応じて次のいずれかのオプションを選択します。
  - ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[Console Redirection] オプションに移動し、**Enter** キーを押します。
    - b. [BIOS Server console] を **[Enabled]** に設定します。
      - Baud Rate - 9600 (他に変更可能な設定はありません)
  - ML150 G6 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[Console Redirection] オプションに移動し、**Enter** キーを押します。
    - b. 次の設定を確認します。
      - Console Redirection-Enabled
      - Serial Port Mode-9600 8,n,1
      - Terminal Type-VT100+
      - Flow Control-None
      - Redirection after BIOS POST-On
  - DL160 G6、DL160se G6、DL170h G6、DL170e G6、DL180 G6、SL165s G7、SL160z G6、SL170z G6、SL170s G6、SL2x170z G6、DL165 G7、および SL165z G7 サーバーでは、次のように操作します。
    - a. 下矢印 (↓) キーを押して、[Remote Access Configuration] オプションに移動し、**Enter** キーを押します。
    - b. 次の設定を確認します。
      - Remote Access-Enabled
      - EMS support(SPCR)-Enabled
      - Base Address-IRQ4/3F8
      - Serial Port Mode-9600 8,n,1
      - Flow Control-None
      - Terminal Type-VT100
      - Redirection after BIOS/POST-Enabled
4. 前の画面に戻るには、**Esc** キーを押します。
5. [I/O Device Configuration] オプションに移動して、**Enter** キーを押します。
6. [Serial Port] が [Enabled] に設定されていることを確認します。

7. 有効な IP アドレスを設定または取得するには、「ネットワーク設定」(47 ページ)の指示に従います。

8. **F10** キーを押して変更を保存し、終了します。

コンソールリダイレクションプロセスが完了したら、LO100 の IP アドレスに対して確立した Telnet セッションを通じて、クライアント PC からリモートでブート プロセスを確認できます。Telnet セッションの確立方法については、ご使用のオペレーティングシステムのマニュアルを参照してください。

Telnet セッションにコンソールをリダイレクションしブート プロセスを参照するには、サーバーの起動時に Telnet セッションで **Esc+Q** キーを押します。Telnet 接続を使用してサーバーをリセットしたあと **Esc+Q** キーを押した場合、ブート プロセスがすぐには表示されないことがあります。サーバーのリセット後に、ブート プロセスが表示されます。コンソールリダイレクションを終了して CLP に戻るには、**Esc+**(キーを押してこのセッションを終了します。

**注記:** リモート コンソールにログインする際に問題が発生した場合は、一部の Telnet プログラムで send line feed at end of line (行末で改行を送信する) オプションを有効にする必要があります。リモート コンソールが Enter キーに応答しない場合は、ご使用の Telnet プログラムでこのオプションを設定してください。

**注記:** 「ネットワーク設定」(47 ページ)の指示に従って、ネットワークアクセスを正しく設定する必要があります。

## Linux のコンソールのリダイレクト

リモート コンソールと Linux オペレーティングシステムが搭載されているサーバーの組み合わせでは、BIOS セットアップユーティリティとブート ドキュメントに以下の変更を加えることで、ttyS0 へのリモート ログインを有効にすることができます。

**注記:** 実際の手順は、Linux のバージョンにより異なります。

1. BIOS セットアップユーティリティを使用し、サーバー モデルに応じて次のいずれかのオプションを選択してシステム設定を確認します。

- ML110 G6 および DL120 G6 サーバーでは、以下の設定を確認してください。

### Console Redirection

- BIOS Serial console-Enabled
- Baud Rate-9600

### I/O Device Configuration

- Embedded Serial Port Mode-BMC
- Embedded Serial Port-Enabled

- ML150 G6 サーバーでは、以下の設定を確認してください。

### Console Redirection

- BIOS Serial console-Enabled
- EMC Support (SPCR)-Enabled
- Serial Port Mode-9600 8,n,1
- Console Type-VT100
- Continue C.R. after POST-On

### I/O Device Configuration

- Serial Port A-Enabled
- Base I/O address-3F8

- Interrupt-IRQ 4
- DL160 G6、DL160se G6、DL170h G6、DL170e G6、DL180 G6、SL160s G6、SL160z G6、SL165s G7、SL170z G6、および SL2x170z G6 サーバー、ならびに SL165z G7 サーバーの場合、以下の設定を確認してください。

### Remote Access Configuration

**注記:** SL160s G6 サーバーの場合、設定は SuperIO Configuration でなければなりません。

- Serial Port Address-3F8
  - Serial Port IRQ-IRQ 4
  - Remote Access-Enabled
  - EMS support(SPCR)-Enabled
  - Terminal Type-VT100
  - Flow Control-None
  - Redirection after BIOS POST-Always
2. /boot/grub/menu.lst ファイルで、カーネル起動行に次の設定を追加します。  

```
console=ttyS0 115200
```

**グラフィック表示行**  
 をコメントアウトします。  

```
# splashimage=(hd0,0)/grub/splash.xpm.gz
```
  3. /etc/inittab に、エントリーを追加して、シリアル コンソール ログインを可能にします。たとえば、次のように入力します。  

```
S0:12345:respawn:/sbin/agetty -L 115200 ttyS0 vt102
```
  4. /etc/securetty に、ttyS0 を追加して root が ttyS0 にアクセスできるようにします。
  5. /etc/sysconfig/kudzu で、ブート時にシリアル ポートへのプローブを実行しないように kudzu を設定します。たとえば、次のように入力します。  

```
SAFE=yes
```
  6. ここまでのファイルを修正して保存したら、サーバーを再起動します。以上で、リモート コンソールからオペレーティング システムにログインできるようになります。

リモート コンソールで、POST 終了後、ログインが指示されます。有効なログイン名を入力し、通常のログインと同じ方法でサーバーを使用してください。Telnet を介してリモート コンソール セッションを開始するには ESC+Q キー、Telnet でリモート コンソールを終了するには、ESC+(キーを押します)。

## Microsoft Windows EMS による管理

Windows Server 2003 は、テキストベースのコンソール アクセスが可能です。ノート PC を LO100 に接続して、ターゲット システムの基本的な管理作業を行うことができます。Windows EMS コンソールを有効にすると、実行中のプロセスが表示され、ビデオ、デバイス ドライバー、またはその他のオペレーティング システム機能により通常の動作や通常の修正措置が妨げられる場合に管理者がプロセスを停止することもできます。

ターゲット システムで Windows EMS による管理を有効にするには、以下の手順に従ってください。

1. POST の実行時に **F10** キーを押して BIOS セットアップ ユーティリティを起動します。
2. **[Advanced]**、**[Console Redirection]** メニューに移動します。

3. サーバー モデルに応じて次のいずれかのオプションを選択します。
- ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[Console Redirection] オプションに移動し、**Enter** キーを押します。
    - b. 次の設定を確認します。
      - Baud Serial Console Port-Enabled
      - Baud Rate-9600
  - ML150 G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[Remote Access Configuration] オプションに移動し、**Enter** キーを押します。
    - b. 次の設定を確認します。
      - Remote Access-Enabled
      - EMS support(SPCR)-Enabled
      - Serial Port Mode-9600 8,n,1
      - Flow Control-None
      - Console Type-VT100
      - Continue C.R. after POST-Always
  - DL160 G6、DL160se G6、SL165s G7、DL170h G6、DL170e G6、DL180 G6、SL160z G6、SL170z G6、SL170s G6、SL2x170z G6、DL165 G7、SL165s G7、および SL165z G7 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[Remote Access Configuration] オプションに移動し、**Enter** キーを押します。
    - b. 次の設定を確認します。
      - Remote Access-Enabled
      - EMS support(SPCR)-Enabled
      - Serial Port Mode-9600 8,n,1
      - Terminal Type-VT100
      - Flow Control-None
      - Redirection after BIOS POST-Always
4. **Esc** キーを押して前の画面に戻るか、**F10** キーを押して変更を保存し、セットアップを終了します。

Windows EMS による管理を有効にしたら、Esc+Q キーを押すことにより、ターゲット サーバーの IP アドレスに対して確立した Telnet セッションを通じて、クライアント PC からリモートで Windows EMS 管理コンソールを表示できます。EMS セッションを終了するには、Esc+(キー)を押します。Telnet セッションの確立方法については、ご使用のオペレーティングシステムのマニュアルを参照してください。

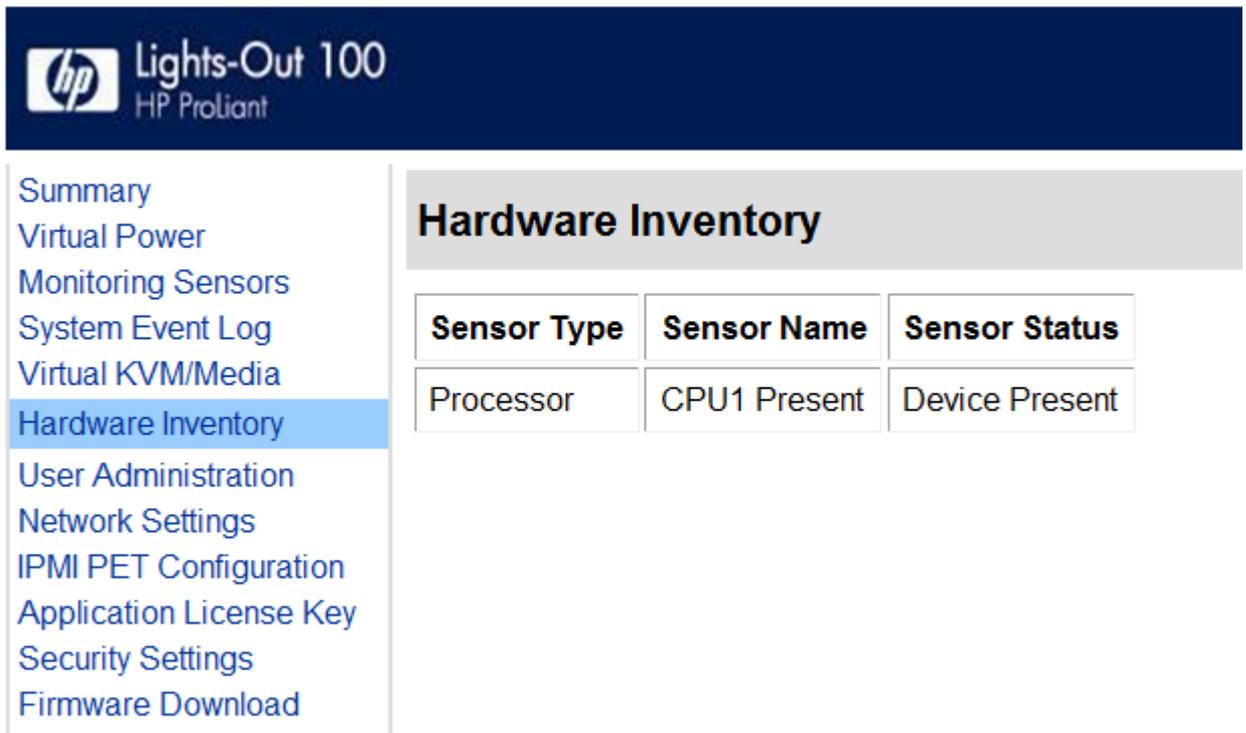
**注記:** リモート コンソールにログインする際に問題が発生した場合は、一部の Telnet プログラムで

send line feed at end of line (行末で改行を送信する)

オプションを有効にする必要があります。リモート コンソールが Enter キーに応答しない場合は、ご使用の Telnet プログラムでこのオプションを設定してください。

## [Hardware Inventory] ページ

[Hardware Inventory] ページにアクセスすると、ターゲット サーバーのプロセッサの存在をリモートから確認できます。Web ブラウザーからこのページにアクセスするには、メインメニュー ナビゲーション バーで **[Hardware Inventory]** をクリックします。



Summary  
Virtual Power  
Monitoring Sensors  
System Event Log  
Virtual KVM/Media  
**Hardware Inventory**  
User Administration  
Network Settings  
IPMI PET Configuration  
Application License Key  
Security Settings  
Firmware Download

### Hardware Inventory

Sensor Type	Sensor Name	Sensor Status
Processor	CPU1 Present	Device Present

## [User Administration]

メインメニュー ナビゲーション バーの [User Administration] オプションを（権限のあるユーザーが）選択すると、既存のユーザーのユーザー名やパスワードを編集できます。ただし、新しいユーザーを作成することはできません。ユーザーパスワードは不揮発性メモリに保存されており、Web ブラウザー（「Web ブラウザーを介したユーザー設定の変更」を参照）または CLP を介して変更できます。

CLP 経由のアクセスでは、ユーザーが適切な権限を持っていない場合、警告メッセージが表示されます。警告メッセージが表示される場合は、Telnet 接続を終了して接続を再確立する必要があります。OEM としてログインする場合も administrator としてログインする場合も、制限はありません。ユーザー アカウントおよびオペレーター アカウントには、次のアクセス権限があります。

オプション	ユーザー	オペレーター
[Hardware Inventory]	あり	あり
[Virtual Power]	なし	あり

オプション	ユーザー	オペレーター
[Monitoring Sensors]	表示のみ	あり
[System Event Log]	あり	あり
[Network Settings]	なし	なし
[PET Configuration]	なし	なし
[User Configuration]	なし	なし
[Virtual KVM]	なし	なし
[Application License Key]	なし	なし
[Security Settings]	なし	なし

## Web ブラウザーを介したユーザー設定の変更

[User Administration] 画面にはユーザー情報が表示されます。この画面では、ユーザー設定の変更やユーザーアカウントの無効化/有効化を行えます。最初のユーザーアカウントの値は、固定 NULL です。最初のユーザーのプロパティを変更したり、そのユーザーをログインに使ったりすることはできません。デフォルトでは、固定 null 値の次の2つのユーザーだけをログインに使用できます。ユーザーは、ブラウザー インターフェイスからのみ有効にできます。

**警告!** すべてのユーザー アカウントを無効にすることは避けてください。ユーザー アカウントがすべて削除されると、LO100にログインできなくなります。管理者権限を持つユーザーを少なくとも 1 つ残すようにすることをおすすめします。

User Name	Password Size	Password	Confirm Password	Enabled	User Privilege
Fixed Null Username	16 Byte			<input type="checkbox"/>	User
Operator	16 Byte	*****	*****	<input checked="" type="checkbox"/>	Operator
admin	16 Byte	*****	*****	<input checked="" type="checkbox"/>	Administrator
OEM	16 Byte	***	***	<input type="checkbox"/>	OEM
Operator	16 Byte	*****	*****	<input type="checkbox"/>	Operator
admin	16 Byte	*****	*****	<input type="checkbox"/>	Administrator
OEM	16 Byte	*****	*****	<input type="checkbox"/>	OEM
Operator	16 Byte	*****	*****	<input type="checkbox"/>	Operator
admin	16 Byte	*****	*****	<input type="checkbox"/>	Administrator
OEM	16 Byte	*****	*****	<input type="checkbox"/>	OEM
Operator	16 Byte	*****	*****	<input type="checkbox"/>	Operator

ユーザー設定を変更するには、以下の手順に従ってください。

1. メイン ナビゲーション バーで **[User Administration]** をクリックします。
2. [Password] および [Confirm Password] フィールドに、パスワードを入力します。
3. リストから適切な **[User Privilege]** レベルを選択します。ユーザー権限とアクセス権について詳しくは、「**[User Administration]**」(45 ページ)を参照してください。
4. (オプション) ユーザー名を変更します。
5. 変更を保存するには、**[Set]** をクリックします。

## CLP を使用したユーザー設定の変更

最初のユーザーの値は、固定 NULL です。設定を変更できるのは、user2 から user16 までのユーザーです。ユーザーのログインを有効にできるのは、ブラウザを介してアクセスしている場合ですが、ユーザーの設定値はどの接続からでも変更できます。

1. 「LO100 へのログイン」(26 ページ) の説明に従って、CLP にログインします。
2. コマンド プロンプトで、`cd map1/accounts` と入力します。
3. `cd user1` または `cd user#` と入力して、ユーザーを選択します。ここで、# は変更するユーザーの番号 (2 から 16 の整数) です。
4. ユーザー名を変更するには、`set username=< 新しいユーザー名 >` と入力します。たとえば、次のように入力します。

```
./map1/accounts/user2/> set username=testuser2
```

5. ユーザーのパスワードを変更するには、`set password=< 新しいパスワード >` と入力してプロンプトが表示されたら新しいパスワードを入力します。たとえば、次のように入力します。

```
./map1/accounts/user2/> set password=testpswd2
```

パスワードは最大 16 文字で、大文字と小文字を区別します。また、引用符とアンパサンド (&) を含めることができます。

6. グループ名を変更するには、`set group=< 新しいグループ名 >` と入力します。有効なグループ設定値は、administrator、user、oemhp、および operator です。たとえば、次のように入力します。

```
./map1/accounts/user2/> set group=user
```

## ネットワーク設定

LO100 のネットワーク設定は、Web ブラウザー、CLP、または BIOS セットアップ ユーティリティを使用して、表示および変更できます。IP アドレスを変更した場合は、サーバーへの接続は切断されます。その場合は、新しい IP アドレスでサーバーに再接続する必要があります。

## Web ブラウザーを介したネットワーク設定の変更

[Network Settings] 画面は、IP アドレス、サブネット マスク、およびその他の TCP/IP 関連の設定を表示します。[Network Settings] 画面から、DHCP を有効または無効にすることができ、また DHCP を使用しないサーバーについては、静的な IP アドレスを設定できます。OEM としてログインする場合も管理者 (admin) としてログインする場合も、ネットワーク設定を表示および変更できます。

ネットワーク設定を変更するには、ブラウザーのメインメニューナビゲーションバーから **[Network Settings]** をクリックして、新しい設定を入力し **[Apply]** をクリックします。

[Network Settings] ページに以下の情報が一覧表示されます。

- [MAC Address] - MAC アドレスが表示されます。
- [IP Address] -現在の BMC IP アドレスが表示され、このアドレスを静的 IP に設定することができます。
- [Subnet Mask] - LO100 の IP ネットワークサブネットマスクが表示されます。DHCP を使用している場合、サブネットマスクは自動的に提供されます。DHCP を使用していない場合は、ネットワークのサブネットマスクを入力してください。
- [Gateway] - ネットワークゲートウェイの IP アドレスが表示されます。DHCP を使用している場合、ネットワークゲートウェイ IP アドレスは自動的に提供されます。DHCP を使用していない場合は、ネットワークゲートウェイアドレスを入力してください。

静的 IP が機能するには、すべてのネットワーク設定が適切である必要があります。

- [DHCP] - [Enabled] ボックスを選択することにより BMC IP を DHCP に設定し、[Enabled] の選択を解除することにより BMC IP を静的 IP に設定することができます。変更を有効にするには、**[Apply]** をクリックします。

BMC IP を静的 IP に設定する場合、有効な静的 IP を設定するには、**[Apply]** をクリックする前に [IP Address] フィールドに静的 IP を入力する必要があります。

- [DNS Server IP Address] - DNS サーバーの IP アドレスが表示されます。
- [DNS Server Alternate IP Address] - セカンダリ DNS IP アドレスを表示します。
- [DNS Host Name] - ユーザーによって設定されるホスト名（デフォルト設定は lo100<シリアル番号>）が表示されます。この名前は、IP アドレスに関連付けられた DNS 名です。DHCP および DNS が適切に設定されている場合、IP アドレスの代わりにこの名前を使用して LO100 サブシステムに接続することができます。
- [DNS Current Domain Name] - LO100 サブシステムが存在するドメインの現在の名前が表示されます。この名前は、DHCP によって割り当てられます。この名前は、オプション 6 によって返されたものであり、デフォルトとしてローカルで設定されたものであり、現在登録されているものです。

- [DNS Configured Domain Name] - ユーザーによってデフォルト ドメイン名として設定されたドメイン名が表示されます。
- [Register this Connection's Addresses in DNS] - これらのサーバー アドレスをネットワーク上の DNS サーバーに登録することができます。DHCP サーバーを介して DNS サーバーに対する適切な DNS サフィックスのあるホスト名を登録するために、DHCP オプション 81 が使用されます。
- [Use this connection's DNS suffix in the DNS Registration] - DNS サフィックスを DNS サーバーに登録することができます。DHCP サーバーが DHCP オプション 6 を通じてドメイン名を提供しない場合は、デフォルト ドメイン名を設定して使用することができます。このオプションを無効にすると、プライマリ DNS サフィックス（通常、参加しているアクティブ ディレクトリ ドメインの DNS 名）を使用して接続される場合があります。
- [Telnet Inactivity Timeout] - Telnet 接続時に非アクティブになってから接続が終了するまでの時間制限（秒単位）を設定することができます。  
[Telnet Inactivity Timeout] を無効にするには、0 を設定します。  
Windows Vista または Windows Server 2008 を使用している場合は、コントロールパネルの [プログラムと機能] メニューの [Windows の機能の有効化または無効化] オプションで、[Telnet サーバー] と [Telnet クライアント] をアクティブにする必要があります。
- [Enabled] - VLAN 設定は有効です。
- [VLAN ID] - 通信先の ID です。
- [Priority] - 設定値：1～8。優先順位はデフォルト（1）のまま変更しないことをおすすめします。

LO100 では、この接続のアドレスを DNS に登録し、この接続の DNS 登録を使用することができます。この DNS 登録機能は、DHCP を有効にしている場合にのみ使用できます。

## BIOS セットアップ ユーティリティを使用したネットワーク設定の指定

静的 IP アドレスを有効にするには、以下の手順に従ってください。

1. POST の実行時に **F10** キーを押して BIOS セットアップ ユーティリティを起動します。
2. 右矢印（→）キーを押して、[Advanced] メニューに移動します。
3. 下矢印（↓）キーを押して、[IPMI] に移動します。**Enter** キーを押します。
4. ネットワーク BIOS 設定を設定するには、次のいずれかのオプションを選択します。
  - ML110 G6 および DL120 G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[IPMI] に移動します。**Enter** キーを押します。
    - b. 下矢印（↓）キーを押して、[LAN Settings] に移動します。**Enter** キーを押します。
    - c. [IP Address Assignment] を **[Static]** に設定します。
  - ML150 G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、メニューの一番下まで移動し、**[BMC LAN Configuration]** を選択します。
    - b. [BMC LAN Configuration] で、**[Static]** を選択します。
    - c. 下矢印（↓）キーを押して下方向に移動し、有効な IP アドレス、サブネット マスク、およびゲートウェイ アドレスを入力します（アドレス フィールド間の移動には、Tab キーを使用）。
  - DL160 G6、DL160se G6、SL165s G7、DL170h G6、DL170e G6、DL180 G6、SL160z G6、SL170z G6、SL170s G6、SL2x170z G6、DL165 G7、SL165s G7、および SL165z G7 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[LAN Configuration] メニューに移動します。**Enter** キーを押します。

- b. [DHCP IP Source] で、**[Disabled]** を選択します。
- c. 下矢印（↓）キーを押して下方向に移動し、有効な IP アドレス、サブネット マスク、およびゲートウェイ アドレスを入力します（アドレス フィールド間の移動には、**Tab** キーまたはピリオド（.）を使用）。

5. **F10** キーを押して変更を保存し、終了します。

DHCP が割り当てるアドレスを有効にするには、以下の手順に従ってください。

1. POST の実行時に **F10** キーを押して BIOS セットアップ ユーティリティを起動します。
2. 右矢印（→）キーを押して、[Advanced] メニューに移動します。
3. 下矢印（↓）キーを押して、[IPMI] に移動します。**Enter** キーを押します。
4. ML110 G6 および DL120 G6 サーバーでは、下矢印（↓）キーを押して、[LAN Settings] に移動し、**Enter** キーを押して、[IP Address Assignment] を **[DHCP]** に設定します。
5. DL170h G6、SL170z G6、および SL2x170z G6 サーバーの BIOS 設定はデフォルトで設定されます。その他の G6 サーバーに対してネットワーク BIOS 設定を設定するには、次のいずれかのオプションを選択します。
  - ML150 G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、メニューの一番下まで移動し、**[BMC LAN Configuration]** を選択します。
    - b. [DHCP IP Source] を **[Static]** に設定します。
  - DL160 G6、DL160se G6、DL180 G6、および SL160z G6 サーバーでは、次のように操作します。
    - a. 下矢印（↓）キーを押して、[LAN Configuration] メニューに移動します。**Enter** キーを押します。
    - b. [DHCP IP Source] を **[Enabled]** に設定します。
6. **F10** キーを押して変更を保存するか、サーバーによる BIOS セットアップ ユーティリティのリセットおよび再入力を許可して新しい IP アドレスを表示します。

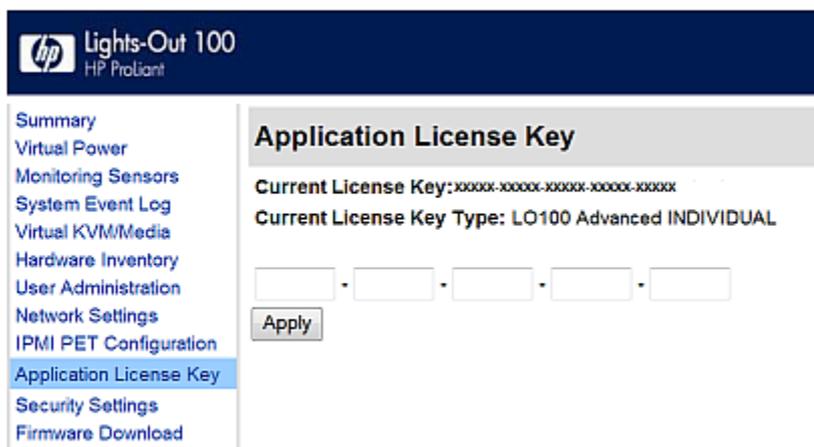
## CLP を使用したネットワーク設定の指定

1. 「[LO100 へのログイン](#)」(26 ページ) の説明に従って、LO100 CLP にログインします。
2. コマンド プロンプトで、`cd map1/nic1` と入力します。
3. `set < ネットワーク プロパティ >=< 新しい設定 >` と入力して、ネットワーク設定を指定します。設定可能で有効なネットワーク プロパティは、次のとおりです。
  - `networkaddress` は、NIC の IP アドレスを指定します。この設定は、動的です。
  - `oemhp_nonvol_networkaddress` は、不揮発性メモリに保存されている IP アドレスを指定します。
  - `oemhp_mask` は、NIC のサブネット マスクを指定します。この設定は、動的です。
  - `oemhp_nonvol_mask` は、不揮発性メモリに保存されているサブネット マスクを指定します。
  - `oemhp_gateway` は、NIC のゲートウェイ IP アドレスを指定します。この設定は、動的です。
  - `oemhp_nonvol_gateway` は、不揮発性メモリに保存されているゲートウェイ IP アドレスを指定します。
  - `oemhp_dhcp_enable` は、NIC に対して DHCP を有効にするかどうかを指定します。Boolean 値を使用できます。
  - `oemhp_nonvol_dhcp_enable` は、不揮発性メモリに保存されている NIC およびアドレスに対して、DHCP を有効にするかどうかを指定します。
  - `oemhp_hostname` は、LO100 のホスト名（デフォルト設定は `lo100<シリアル番号>`）を指定します。この名前は、IP アドレスに関連付けられた DNS 名です。DHCP お

よび DNS が適切に設定されている場合、IP アドレスの代わりにこの名前を使用して LO100 サブシステムに接続することができます。

## ライセンス キーの適用

1. サポートされているブラウザから LO100 にログインします。
2. ライセンス アクティベーション画面を表示するには、**[Application License Key]** をクリックします。[Application License Key] オプションが使用できない場合は、LO100 のファームウェアを更新する必要があります。詳しくは、「[ファームウェアの更新](#)」を参照してください。



3. 表示された領域にライセンス キーを入力します。フィールド間を移動するには、フィールド内をクリックするか、**Tab** キーを押します。[Activation License Key] フィールドは、データを入力するにつれて自動的に先に進みます。
4. **[Apply]** をクリックします。

## 証明書のインポート

インストール済みのパブリック キー（証明書）を使用したくない場合は、独自のプライベート キー（証明書）を作成およびインストールしてください。SSH および SSL の両方がキーまたは証明書のインポート手順をサポートするのは、1 回限りです。キーは、他社製の外部ソフトウェアを使用して生成し、TFTP サーバーに配置し、LO100 にアップロードします。Microsoft® Windows では、TFTP ソフトウェア パッケージがない場合、インターネット経由で入手できる TFTP32.EXE を使用してください。Linux では、通常、TFTP サーバーがオペレーティング システムと一緒にインストールされています。インストールされていない場合は、Linux のマニュアルを参照してください。

**注記:** TFTP32 とともに CLP の load コマンドを使用する場合は、タイムアウトを 4 秒、再試行を 10 回に設定することをおすすめします。

**注記:** CLP の load コマンドを Linux で使用する場合は、タイムアウトを 4000000 に設定してください。一部の Linux システムに組み込まれているファイアウォールが、TFTP サーバーによる情報の送受信を許可しないことがあります。上記の接続を許可するには、ファイアウォールを無効にする必要があります。ファイアウォールに問題がある場合は、ファイアウォール設定を変更してポート 69（TFTP サーバーのデフォルト ポート）での接続を許可してください。詳しくは、ファイアウォールのマニュアルを参照してください。

## 証明書の作成

LO100 では、TFTP サーバーに配置され、PEM（Base64 エンコード）フォーマットで保存された、1,024 ビット DSA キーが必要です。たとえば、以下のプロセスでは、Shining Light

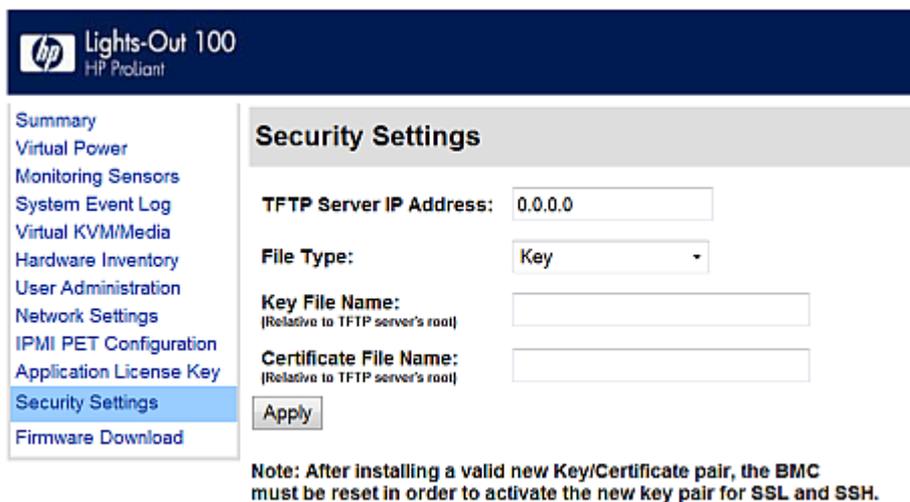
Productions の Web サイト <http://www.slproweb.com/products/Win32OpenSSL.html> からダウンロードした Win32 OpenSSL と DOS ウィンドウで発行したコマンドを使用して証明書を生成しています。Win32 OpenSSL を使用して証明書を生成するには、以下の手順に従ってください。

1. Win32 OpenSSL をダウンロードします。
2. OpenSSL をインストールしてセットアップします。
3. OpenSSL を使用して、DSA パラメーター ファイルを生成します。  
`openssl dsaparam -out server_dsaparam.pem 1024`
4. server\_privkey.pem という名前の DSA プライベート キー ファイルを作成します。  
`openssl gendsa -out server_privkey.pem server_dsaparam.pem`
5. server\_cacert.pem という名前の DSA 証明書（パブリック キー）ファイルを作成します。  
`openssl req -new -x509 -key server_privkey.pem -out server_cacert.pem -days 1095`
6. 識別名の入力を指示されたら、証明書を受け取る予定のサーバーのドメイン名を入力します。
7. 証明書を作成したら、LO100 と同じネットワーク上でアクセスできる TFTP サーバーにコピーします。

リモート KVMS セッションがある場合は、証明書またはキーをインポートする前に、すべて切断する必要があります。キーまたは証明書をインポートすると、使用中のセッションが切断され LO100 プロセッサがリセットされます。キーまたは証明書がインポートされ LO100 がアップロードの成功を確認してから、LO100 に再びログインする必要があります。

## Web ブラウザー経由での証明書またはプライベート キーのインストール

[Security Settings] ページを使用して、SSL および SSH 接続用の新しいキーや証明書をインストールできます。



Summary  
Virtual Power  
Monitoring Sensors  
System Event Log  
Virtual KVM/Media  
Hardware Inventory  
User Administration  
Network Settings  
IPMI PET Configuration  
Application License Key  
**Security Settings**  
Firmware Download

### Security Settings

TFTP Server IP Address:

File Type:

Key File Name:  
(Relative to TFTP server's root)

Certificate File Name:  
(Relative to TFTP server's root)

Note: After installing a valid new Key/Certificate pair, the BMC must be reset in order to activate the new key pair for SSL and SSH.

ブラウザー経由で証明書をインストールするには、以下の手順に従ってください。

1. 管理者として LO100 にログインします。
2. ブラウザー メイン ナビゲーション バーで **[Security Settings]** をクリックします。
3. [TFTP server IP address] フィールドに、TFTP サーバーの IP アドレスを入力します。
4. [File type] の下のメニューで、**[Certificate]** を選択します。
5. [File Name] フィールドに、作成した証明書のファイル名 (server\_cacert.pem) を入力します。ファイル名には、TFTP サーバーのルートからのファイルの相対パスを入力してください。

## 6. [Apply] をクリックします。

ブラウザ経由でプライベート キーをインストールするには、以下の手順に従ってください。

1. 管理者として LO100 にログインします。
2. ブラウザー メイン ナビゲーション バーで **[Security Settings]** をクリックします。
3. [TFTP server IP address] フィールドに、TFTP サーバーの IP アドレスを入力します。
4. [File type] の下のメニューで、**[Key]** を選択します。
5. [File Name] フィールドに、作成したキーのファイル名 (server\_privkey.pem) を入力します。ファイル名には、TFTP サーバーのルートからのファイルの相対パスを入力してください。

## 6. [Apply] をクリックします。

ブラウザ経由で証明書とプライベート キーの両方を同時にインストールするには、以下の手順に従ってください。

1. 管理者として LO100 にログインします。
2. ブラウザー メイン ナビゲーション バーで **[Security Settings]** をクリックします。
3. [TFTP server IP address] フィールドに、TFTP サーバーの IP アドレスを入力します。
4. [File type] の下のメニューで、**[Key and Certificate]** を選択します。
5. [File Name] フィールドに、証明書のファイル名 (server\_cacert.pem) および作成したキーのファイル名 (server\_privkey.pem) を入力します。ファイル名には、TFTP サーバーのルートからのファイルの相対パスを入力してください。
6. **[Apply]** をクリックします。

## CLP を使用した証明書またはプライベート キーのインストール

証明書をインストールするには、CLP インターフェイスから管理者として LO100 にログインし、load コマンドを実行して証明書をアップロードしインストールします。たとえば、次のように入力します。

```
load -source <URI> -oemhpfiletype cer
```

ここで

- <URI> は、//<tftpserver IP>/<Path>/<ダウンロードする filename> です。
- また、tftpserver は、証明書が配置されている TFTP サーバーの URL または IP アドレスです。
- Path は、TFTP サーバーのルートからのファイルの相対パスです。
- filename は、証明書ファイルのファイル名です (この例では、server\_cacert.pem)。

load コマンドを実行して証明書をアップロードおよびインストールしたら、次のコマンドを入力して BMC をリセットします。

```
reset map 1
```

BMC をリセットすると、LO100 はキーと証明書の組み合わせの有効性を確認します。

これらのコマンドは、/map1/firmware ディレクトリにもあります。

プライベート キーをインストールするには、CLP インターフェイスから管理者として LO100 にログインし、load コマンドを実行して証明書をアップロードしインストールします。たとえば、次のように入力します。

```
load -source <URI> -oemhpfiletype key
```

ここで

- <URI> は、//<tftpserver IP>/<Path>/<ダウンロードする filename> です。
- tftpserver は、プライベート キー ファイルが配置されている TFTP サーバーの URL または IP アドレスです。
- Path は、TFTP サーバーのルートからのファイルの相対パスです。

- `filename` は、プライベート キー ファイルのファイル名です（この例では、`server_privkey.pem`）。

`load` コマンドを実行して証明書をアップロードおよびインストールしたら、次のコマンドを入力して BMC をリセットします。

```
reset map 1
```

BMC をリセットすると、LO100 はキーと証明書の組み合わせの有効性を確認します。

これらのコマンドは、`/map1/firmware` ディレクトリにもあります。

CLI または GUI を通じてキーや証明書をロードした後に SSH/SSL 接続を正常に確立するには、**[Apply]** をクリックした後で、次のいずれかの方法で BMC をリセットする必要があります。

- CLI からコマンド (`./-> cd map1 a"reset map 1"`) を実行します。
- 物理的に AUX 電源を切断します。

## HP Systems Insight Manager のサポート

HP Systems Insight Manager は、LO100 を検出して、LO100 と、LO100 を取得またはデプロイするそのライセンス マネージャーを識別および起動します。LO100 と HP Systems Insight Manager の連携については、HP Systems Insight Manager のユーザー ガイドを参照してください。

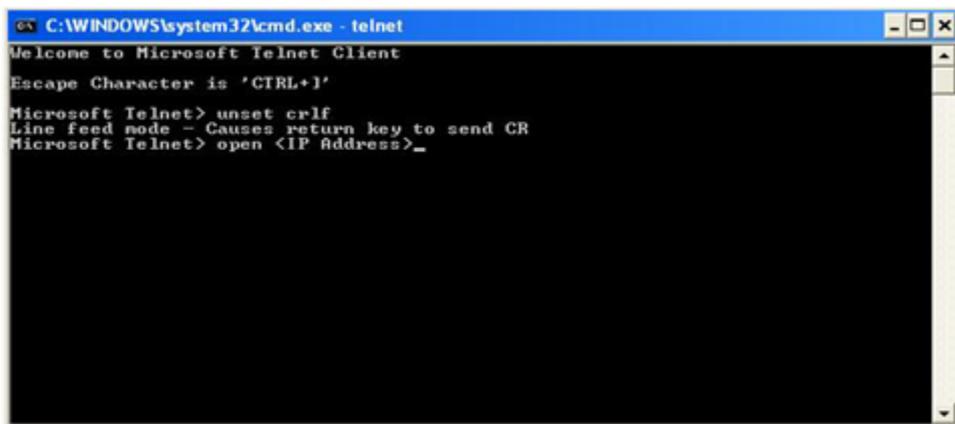
## 文字とライン フィードに関する問題の解決

CMS とアプリケーションまたはワークステーションとの間で通信を行うためには、同種のオペレーティング システムを使用することをおすすめします。たとえば、Linux の CMS が稼動している場合は、ワークステーションでも Linux を実行し、Linux の Telnet クライアントを使用します。同じように、Windows CMS が稼動している場合は、ワークステーションでも Windows を実行し、Windows の Telnet クライアントを使用します。

ご使用の環境で複数のオペレーティングシステムを実行すると、アプリケーションの制限の問題が発生する場合があります。たとえば、サーバーで Linux を実行して、Windows Telnet クライアントまたは PuTTY を使用すると、行末文字の問題が発生する場合があります。この問題が発生した場合は、以下のいずれかの手順に従ってください。

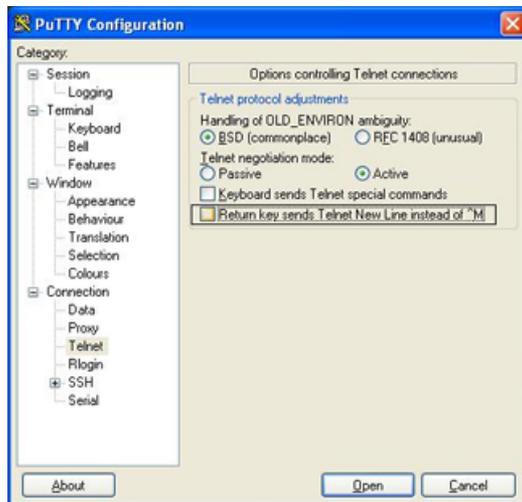
- Linux コンソールへのリダイレクトが設定された Windows Telnet クライアントでは、Windows Telnet が CR をライン フィードとして送信することを確認してください。CR を設定するには、Windows Telnet で以下のコマンドを実行します。

```
unset crlf
```



- PuTTY などのアプリケーションで Linux にリダイレクトする場合は、以下の手順に従ってください。
  1. **[Connection]**、**[Telnet]** の順にクリックします。

## 2. [Return key sends Telnet New Line instead of ^M] の選択を解除します。



LO100 のデフォルトのフィルター設定は 0x08（入力）および 0x03（出力）であり、これは変更しないでください。デフォルト設定を変更すると、機能に問題が発生し、デフォルト設定を復元する必要が生じます。デフォルト設定がリセットされると、シェルからログアウトして再度ログインし、通常の機能を復元する必要があります。デフォルト設定を復元するには、ご使用の環境およびオペレーティング システムで以下の IPMI コマンドを使用します。

- Telnet インバウンドを 0x08 に設定するには、次のように入力します。
  - CLP: oemhp I 20 c0 20 18 00 29 01 00 00 02 00 08 b4
  - DOS: ipmitool 20 c0 29 01 00 00 02 00 08
  - Linux: ipmitool raw 0x30 0x29 0x01 0x00 0x00 0x02 0x00 0x08
- Telnet アウトバウンドを 0x03 に設定するには、次のように入力します。
  - CLP: oemhp I 20 c0 20 18 00 29 01 00 00 02 01 03 b8
  - DOS: ipmitool 20 c0 29 01 00 00 02 01 03
  - Linux: ipmitool raw 0x30 0x29 0x01 0x00 0x00 0x02 0x01 0x03
- SSH インバウンドを 0x08 に設定するには、次のように入力します。
  - CLP: oemhp I 20 c0 20 18 00 29 01 00 01 02 00 08 b3
  - DOS: ipmitool 20 c0 29 01 00 01 02 00 08
  - Linux: ipmitool raw 0x30 0x29 0x01 0x00 0x01 0x02 0x00 0x08
- SSH アウトバウンドを 0x03 に設定するには、次のように入力します。
  - CLP: oemhp I 20 c0 20 18 00 29 01 00 01 02 01 03 b7
  - DOS: ipmitool 20 c0 29 01 00 01 02 01 03
  - Linux: ipmitool raw 0x30 0x29 0x01 0x00 0x01 0x02 0x01 0x03

たとえば、Windows で Telnet を使用してデフォルト設定を復元するには、以下の手順に従います。

1. Windows Telnet クライアントから、CLP インターフェイスにログインします。
2. 以下のコマンドを使用して、ディレクトリを map1 に変更します。  
cd map1
3. 以下のコマンドを使用して、入力デフォルトを 0x08 に設定します。  
oemhp I 20 c0 20 18 00 29 01 00 00 02 00 08 b4

4. 以下のコマンドを使用して、出力デフォルトを 0x03 に設定します。

```
oemhp I 20 c0 20 18 00 29 01 00 00 02 01 03 b8
```

5. ログアウトします。

## VLAN タギングの使用

VLAN タギングを使用すると、サーバーごとに複数の Ethernet ソケットを配線することなく（内部）管理トラフィックを実務トラフィックから隔離でき、シンプルな構成でセキュリティを確保できます。VLAN タギングでは、ネットワーク構成は幾分複雑にはなりますが、ネットワークのコストは（ポートやケーブルでの削減と同様に）大幅に削減できます。

## サーバー サポート

VLAN タギングは、専用の管理ポートと組み合わせて使用する場合、すべての ProLiant 100 シリーズ G5/G6/G7 サーバーでサポートされます。

---

**注記:** ML110 G6、DL120 G6、ML150 G6 の低速共有管理ポートで VLAN タギングをサポートするには、ファームウェアバージョン 4.22 以降が必要です。

---

## IPMI コマンドを使用した VLAN タギングの設定

VLAN タギングの設定には、次に示すホスト ベースの設定コマンドを使用します。

VLAN タギングを設定するには、IPMI コマンドを使用して次のように入力します。

```
linux: ipmitool raw 0x0c 0x01 0x02 0x14 XX YY
```

ここで、

XX は、VLAN ID の下位 8 ビットを示します。

YY の第 7 ビットが 1 の場合 VLAN は有効になり、0 の場合は無効です。

第 6～4 ビットの 0 は不使用を意味します。

第 3～0 ビットは、VLAN ID の上位 4 ビットを示します。

たとえば、VLAN ID の 809 を有効にするには、次のコマンドを入力します。

```
linux: ipmitool raw 0x0c 0x01 0x02 0x14 0x29 0x83
```

## Web ブラウザーを介した VLAN タギングの変更

詳しくは、「[Web ブラウザーを介したネットワーク設定の変更](#)」を参照してください。

---

## 4 テクニカル サポート

### ソフトウェア テクニカル サポートとアップデート サービス

HP LO100i Advanced Pack は、将来の任意のアップグレードを提供するテクニカル サポート およびアップデート ライセンスで利用できます。これらのオプションについては、HP の Web サイト <http://www.hp.com/servers/lights-out>（英語）を参照してください。

ライセンス アクティベーション キーに代えてライセンス権利付与証明書が配布されます。ライセンス権利付与証明書は、既存の製品番号では物理的に配布され（ライセンスの追跡を除く）、新しい電子ライセンス製品番号では電子メールによって配布されます。証明書には、ライセンス アクティベーション キーをオンラインまたはファックスでライセンス キーを取得するために必要な情報が記載されています。この新しい電子ライセンス取得プロセスによって、ライセンス管理が容易になり、サービスが向上し、追跡がサポートされます。詳しくは、HP の Web サイト <http://www.hp.com/jp/ice-license> を参照してください。

## 頭字語と略語

<b>BIOS</b>	Basic Input/Output System。基本入出力システム
<b>BMC</b>	baseboard management controller
<b>CLI</b>	Command Line Interface。コマンド ライン インターフェイス
<b>CLP</b>	command line protocol。コマンド ライン プロトコル
<b>CMS</b>	central management server。中央管理サーバー
<b>CR</b>	carriage return。キャリッジ リターン
<b>DCMI</b>	Data Center Manageability Interface
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DSA</b>	Digital Signature Algorithm。デジタル署名アルゴリズム
<b>EMS</b>	Emergency Management Services
<b>HTTP</b>	hypertext transfer protocol。ハイパーテキスト転送プロトコル
<b>IP</b>	Internet Protocol。インターネット プロトコル
<b>IPMI</b>	Intelligent Platform Management Interface
<b>JVM</b>	Java Virtual Machine。Java 仮想マシン
<b>KVM</b>	keyboard, video, and mouse。キーボード、ビデオ、およびマウス
<b>LO100</b>	HP Lights-Out 100
<b>MAC</b>	Media Access Control。メディア アクセス制御
<b>NIC</b>	network interface card。ネットワーク インターフェイス カード
<b>OS</b>	operating system。オペレーティング システム
<b>PEF</b>	Platform Event Filtering
<b>PEM</b>	Privacy Enhanced Mail
<b>PET</b>	Platform Event Trap
<b>POST</b>	Power-On Self-Test。電源投入時セルフテスト
<b>RBSU</b>	ROM-Based Setup Utility。ROM ベース セットアップ ユーティリティ
<b>SLES</b>	SUSE Linux Enterprise Server
<b>SMASH</b>	System Management Architecture for Server Hardware
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Sockets Layer
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TFTP</b>	Trivial File Transfer Protocol
<b>UID</b>	unit identification。ユニット識別子
<b>URL</b>	uniform resource locator
<b>VLAN</b>	virtual local area network。仮想ローカル エリア ネットワーク
<b>VNC</b>	virtual network computing。仮想ネットワーク コンピューティング

# 索引

## B

- base management controller (BMC) , 11
- BIOS、アップグレード, 14
- BIOS 設定, 11
- BIOS セットアップ ユーティリティ
  - BIOS セットアップ ユーティリティからの DHCP IP アドレスの取得, 11
  - センサーの監視, 29
  - ファームウェアの更新, 14
- BMC (base management controller) , 11

## C

- CLP (Command Line Protocol)
  - CLP を使用した証明書またはプライベート キーのインストール, 53
- CLP、一般構文, 20
- CLP 概要, 20
- CLP、コマンド
  - CLP を使用したサーバー電源の制御, 29
  - CLP を使用したシステム イベント ログへのアクセス, 33
  - CLP を使用したネットワーク設定の指定, 50
  - 各コマンドについて, 25
- CLP (コマンド ライン プロトコル)
  - CLP の使用, 20
  - CLP を使用したサーバー電源の制御, 29
  - CLP を使用したシステム イベント ログへのアクセス, 33
  - CLP を使用したネットワーク設定の指定, 50
  - CLP を使用したログイン, 26
  - 各コマンドについて, 25
  - 仮想 KVM の使用, 34
  - システム イベント ログの使用, 33
  - ネットワーク設定, 47
- CLP、接続オプション, 20
- Command Line Protocol (CLP)
  - CLP を使用した証明書またはプライベート キーのインストール, 53
- CR/LF 変換, 54

## D

- DHCP (Dynamic Host Configuration Protocol)
  - BIOS セットアップ ユーティリティからの DHCP IP アドレスの取得, 11
  - CLP を使用したネットワーク設定の指定, 50
  - Platform Event Trap の設定, 32
  - Web ブラウザーを介したネットワーク設定の変更, 47
- DHCP アドレス, 11
- DHCP、有効化, 11
- DSA (デジタル署名アルゴリズム) , 51
- Dynamic Host Configuration Protocol (DHCP)
  - BIOS セットアップ ユーティリティからの DHCP IP アドレスの取得, 11
  - CLP を使用したネットワーク設定の指定, 50

Web ブラウザーを介したネットワーク設定の変更, 47

## H

- [Hardware Inventory], 45
- HP SIM、サポート, 54
- HP 製品販売店
  - テクニカル サポート, 57

## I

- Intelligent Platform Management Interface (IPMI)
  - IPMI 2.0 のサポート, 25
  - Platform Event Trap の設定, 32
  - 仮想 KVM の使用, 34
  - サーバー管理, 5
  - サーバーの管理機能, 5
  - システム イベント ログの使用, 33
- IPMI (Intelligent Platform Management Interface)
  - IPMI 2.0 のサポート, 25
  - Platform Event Trap の設定, 32
  - 仮想 KVM の使用, 34
  - サーバー管理, 5
  - サーバーの管理機能, 5
  - システム イベント ログの使用, 33
- IPMI のサポート, 25
- IP (インターネット プロトコル)
  - BIOS セットアップ ユーティリティからの DHCP IP アドレスの取得, 11
  - ブラウザーのメイン メニュー オプション, 26

## K

- KVM、(キーボード、ビデオ、マウス)
  - [User Administration], 45
  - サーバーの管理機能, 5
  - リモート グラフィック コンソールの設定, 36

## L

- LO100、ブラウザー経由でのログイン, 26

## M

- MAC (メディア アクセス制御)
  - Platform Event Trap の設定, 32
  - システム ボタン, 38
  - マウスの同期化, 37

## N

- NIC (ネットワーク インターフェイス カード)
  - CLP を使用したネットワーク設定の指定, 50
  - TCP/IP over Ethernet マネジメント ポートの使用, 10
  - サーバーの管理機能, 5
  - シリアル ポートの使用, 8

## O

- OpenSSH ユーティリティ, 20

## P

### PEF (Platform Event Filtering)

- Platform Event Filtering 設定, 31
- Platform Event Trap の設定, 32
- Web ブラウザーからのセンサー データ表示, 29

### PEM (Privacy Enhanced Mail)

- CLP を使用した証明書またはプライベート キーのインストール, 53
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- 証明書の作成, 51

### PET (Platform Event Trap)

- CLP を使用した証明書またはプライベート キーのインストール, 53
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- 証明書の作成, 51

### Platform Event Filtering (PEF)

- Platform Event Filtering 設定, 31
- Platform Event Trap の設定, 32
- Web ブラウザーからのセンサー データ表示, 29

### Platform Event Trap (PET)

- CLP を使用した証明書またはプライベート キーのインストール, 53
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- 証明書の作成, 51

### Privacy Enhanced Mail (PEM)

- CLP を使用した証明書またはプライベート キーのインストール, 53
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- 証明書の作成, 51

### PuTTY ユーティリティ, 20

## R

### RBSU (ROM ベース セットアップ ユーティリティ)

- 仮想 KVM の使用, 34
- システム イベント ログの使用, 33

### ROMPaq ユーティリティ, 14

### ROM ベース セットアップ ユーティリティ (RBSU)

- 仮想 KVM の使用, 34
- システム イベント ログの使用, 33

## S

### Secure Shell (SSH)

- CLP の使用, 20
- CLP を使用したログイン, 26
- SSH の使用, 19
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- サーバーの管理機能, 5
- 証明書のインポート, 51

### Secure Sockets Layer (SSL)

- SSL の使用, 19
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- サーバーの管理機能, 5
- 証明書のインポート, 51

### 証明書の作成, 51

### SLES (SUSE Linux Enterprise Server), 37

### SMASH (System Management Architecture for Server Hardware)

- CLP の使用, 20
- サーバー管理, 5
- サーバーの管理機能, 5

### SSH (Secure Shell)

- CLP の使用, 20
- CLP を使用したログイン, 26
- SSH の使用, 19
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- サーバーの管理機能, 5
- 証明書のインポート, 51

### SSH キー、インポート

- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- 証明書のインポート, 51

### SSH ユーティリティ, 19

### SSL、(Secure Sockets Layer)

- SSL の使用, 19
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- サーバーの管理機能, 5
- 証明書のインポート, 51
- 証明書の作成, 51

### SSL、概要, 19

### SSL、キーおよび証明書のインポート, 51

### SSL、使用, 19

### SUSE Linux Enterprise Server (SLES), 37

### System Management Architecture for Server Hardware (SMASH)

- CLP の使用, 20
- サーバー管理, 5
- サーバーの管理機能, 5

## T

### Telnet

- Telnet 経由でのリモート コンソール アクセス, 40
- 文字とライン フィールドに関する問題の解決, 54

### TFTP (Trivial File Transfer Protocol)

- CLP を使用した証明書またはプライベート キーのインストール, 53
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- 証明書のインポート, 51
- 証明書の作成, 51

### Trivial File Transfer Protocol (TFTP)

- CLP を使用した証明書またはプライベート キーのインストール, 53
- Web ブラウザー経由での証明書またはプライベート キーのインストール, 52
- 証明書のインポート, 51
- 証明書の作成, 51

## U

### Uniform Resource Locator (URL), 53

### URL (Uniform Resource Locator), 53

## V

### VLAN

タギング, 56

VNC (仮想ネットワーク コンピューティング), 36

## あ

アップデート サービス, 57

アラート メッセージ, 32

### 暗号化

SSH の使用, 19

SSL の使用, 19

## い

### イベント ログ

CLP を使用したシステム イベント ログへのアクセス, 33

Web ブラウザーからのシステム イベント ログへのアクセス, 33

仮想 KVM の使用, 34

システム イベント ログの使用, 33

インポート、証明書, 51

## か

概要、CLP, 20

概要、SSH, 19

概要、SSL, 19

概要、サーバー管理, 5

概要、製品, 5

仮想デバイス, 38

仮想電源, 27

仮想ネットワーク コンピューティング (VNC), 36  
管理, 7

## き

キー、システム, 38

キー、プライベート

CLP を使用した証明書またはプライベート キーのインストール, 53

Web ブラウザー経由での証明書またはプライベート キーのインストール, 52

キーボード、ビデオ、マウス (KVM)

[User Administration], 45

サーバーの管理機能, 5

リモート グラフィック コンソールの設定, 36

キー、ライセンス, 51

機能、CLP, 20

機能、IPMI 2.0, 25

機能、LO100

サーバーの管理機能, 5

新機能, 5

機能、SSL, 19

共有ストレージ デバイス、削除, 40

共有ストレージ デバイス、追加, 40

## け

権限、ユーザー, 45

## こ

コマンドライン プロトコル (CLP)

CLP の使用, 20

CLP を使用したサーバー電源の制御, 29

CLP を使用したシステム イベント ログへのアクセス, 33

CLP を使用したネットワーク設定の指定, 50

CLP を使用したログイン, 26

各コマンドについて, 25

仮想 KVM の使用, 34

システム イベント ログの使用, 33

ネットワーク設定, 47

コンフィギュレーション設定, 45

## さ

サポート、IPMI, 25

サポート、HP SIM, 54

## し

### システム イベント ログ

CLP を使用したシステム イベント ログへのアクセス, 33

Web ブラウザーからのシステム イベント ログへのアクセス, 33

システム イベント ログ、CLP を使用したアクセス, 33

システム ボタン, 38

使用、LO100, 19

### 証明書

CLP を使用した証明書またはプライベート キーのインストール, 53

Web ブラウザー経由での証明書またはプライベート キーのインストール, 52

証明書のインポート, 51

証明書の作成, 51

シリアル ポート, 8

## す

ストレージ デバイス、共有, 40

ストレージ デバイス、使用, 38

ストレージ デバイス、追加, 39

## せ

設定, 7

設定、LOM プロセッサ, 7

設定、PEF, 31

設定、PET, 32

設定、電源オプション

CLP を使用したサーバー電源の制御, 29

ブラウザー経由でのサーバー電源の制御, 27

設定、ネットワーク, 47

設定、マウス, 37

センサー データ

Platform Event Filtering 設定, 31

Web ブラウザーからのセンサー データ表示, 29

センサーの監視, 29

専用マネジメント ポート, 10

## て

データ保護方法, 19

テクニカル サポート

ソフトウェア テクニカル サポートとアップデート  
サービス, 57  
テクニカル サポート, 57  
電源制御オプション  
CLP を使用したサーバー電源の制御, 29  
サーバー電源のリモート制御, 27  
ブラウザ経由でのサーバー電源の制御, 27  
電話番号  
テクニカル サポート, 57

と  
動作の概要, 5

ね  
ネットワーク インターフェイス カード (NIC)  
CLP を使用したネットワーク設定の指定, 50  
ネットワーク インターフェイス カード (NIC)  
TCP/IP over Ethernet マネジメント ポートの使用, 10  
サーバーの管理機能, 5  
シリアル ポートの使用, 8  
ネットワーク設定  
CLP を使用したネットワーク設定の指定, 50  
[Network Settings], 47  
Web ブラウザーを介したネットワーク設定の変更,  
47

は  
パスワード, 46

ふ  
ファームウェアの更新, 14  
プライベート キー  
CLP を使用した証明書またはプライベート キーのイ  
ンストール, 53  
Web ブラウザー経由での証明書またはプライベート  
キーのインストール, 52  
ブラウザベースのセットアップ, 47  
フラッシュ ROM, 14  
プロセッサ, 45

ほ  
ホット キーの定義, 38

ま  
マウス設定, 37

め  
メイン メニュー機能, 26  
メディア アクセス制御 (MAC)  
Platform Event Trap の設定, 32  
システム ボタン, 38  
マウスの同期化, 37

ゆ  
ユーザー アカウント、変更  
[User Administration], 45  
Web ブラウザーを介したユーザー設定の変更, 46  
ユーザー アクセス, 45  
ユーザー設定

[User Administration], 45  
Web ブラウザーを介したユーザー設定の変更, 46

よ  
要件、SSH, 19

ら  
ライセンス キー、インストール, 51  
ライセンス キー、適用, 51

り  
リモート グラフィック コンソール、アプレット, 35  
リモート コンソール, 40  
リモート コンソール、アプレット設定, 36  
リモート サーバーの電源、制御, 27  
リモート マネジメント、ブラウザ メイン メニュー,  
26  
リモート マネジメント プロセッサ、CLP を使用した  
ログイン, 26

ろ  
ログイン  
CLP を使用したログイン, 26  
LO100 へのログイン, 26  
Web ブラウザー経由でのログイン, 26