

HP内蔵Lights-Out ユーザ ガイド



2003年6月（第4版）
製品番号 238882-194

© 2003 Hewlett-Packard Development Company, L.P.

Microsoft®、Windows®、MS-DOS®、およびWindows NT®は、米国Microsoft Corporationの米国およびその他の国における登録商標です。

Java™は、米国Sun Microsystems, Inc.の商標です。

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、省略に対して、責任を負いかねますのでご了承ください。本書の内容は、そのままの状態を提供されるもので、いかなる保証も含みません。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製品に対する保証については、当該製品に付属の限定保証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。本書で取り扱っているコンピュータ 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ソフトウェア、コンピュータソフトウェア資料、および商業用製品の技術データは、ベンダ標準の商業用ライセンスのもとで米国政府に使用許諾が付与されます。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 사용되는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。

2003年6月（第4版）

製品番号 238882-194

対象読者

このガイドは、サーバのインストール、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

内蔵Lights-Outの設定	13
iLOの設定オプション	13
iLO RBSU	14
ブラウザ ベースのセットアップ	15
グラフィック リモート コンソールのパフォーマンスの最適化	16
推奨されるクライアントの設定	16
推奨されるサーバの設定	17
iLOの高度な機能の有効化	18
iLOデバイス ドライバのインストール	19
Microsoft Windows NT、Windows 2000、および	
Windows Server 2003ドライバのサポート	20
Novell NetWareサーバドライバのサポート	21
Red Hat LinuxおよびSuSE Linuxサーバドライバのサポート	22
内蔵Lights-Outの使い方	25
サポートされるサーバオペレーティングシステム ソフトウェア	25
サポートされるブラウザ	26
グラフィック リモート コンソールのシングル カーソル モードとデュアル カーソル モード	27
リモート コンソール (デュアル カーソル)	27
リモート コンソール (シングル カーソル)	27
共通利用モデル	28
接続の概要	29
企業ネットワークでの接続	29
内蔵Lights-Outネットワークでの接続	30
動作の概要	30
iLOに初めてアクセスする方法	35
失敗したブラウザ ログイン試行に対するプログレッシブ ディレイ	39
ヘルプ	40
システム ステータス	40
ステータスの概要	40
iLOステータス	40
サーバステータス	41
iLOのイベント ログ	42
インテグレートッド マネジメント ログ	43
サーバおよびiLOの診断	43
リモート コンソール	45
リモート コンソール情報オプション	46
リモート コンソール オプション	46

リモート コンソール (デュアル カーソル) モード	49
仮想デバイス	50
仮想電源ボタン	50
仮想メディア	52
iLO仮想メディア デバイスの使用	54
仮想シリアル ポート	60
仮想インジケータ	61
管理	62
ユーザ管理	62
ネットワーク設定	64
グローバル設定	67
SNMP/Insight マネージャの設定	71
iLOファームウェアのアップグレード	73
使用許諾	75
証明書管理	75
ディレクトリ設定	76
ProLiant BL p-Class	76
ラックの設定	76
ラック トポロジ	79
サーバ ブレード管理モジュール	80
電源管理モジュール	80
リダンダント電源管理モジュール	81
ProLiant BL p-ClassサーバのLEDのiLOによる制御	81
Telnetサポート	82
Insight マネージャ7との統合	85
機能の概要	85
識別と関連付け	85
ステータス	86
クエリ	86
リンク	86
アラート	87
ポートを一致させる	87
iLOの識別の設定	88
内蔵iLOとInsight マネージャ7との統合	89
Insight マネージャ7でSNMPアラートを受信	90
Insight マネージャ7でのiLO Advancedパック ライセンス情報の確認	91
ProLiant BL p-Classラックの視覚化	91
内蔵Lights-Outのセキュリティ	93
セキュリティに関する一般的なガイドライン	93
暗号化	93
iLOのセキュリティ オーバーライド スイッチによる管理	93
ユーザ アカウント	95

権限	95
グローバル セキュリティ 設定	95
ログイン セキュリティ	96
パスワード	96
電子証明書	97
ディレクトリ サービス	99
ディレクトリ サービスとは	99
スキーマに関する資料	99
ディレクトリ サービスのサポート	100
必要なソフトウェア	101
スキーマ インストーラ	101
[Schema Preview]	101
[Setup].....	102
[Results].....	104
マネジメント スナップイン インストーラ	104
Active Directoryのディレクトリ サービス	105
Active Directoryインストールの前提条件	105
Active Directoryでのディレクトリ サービスの準備	105
スナップインのインストールとActive Directory用の初期設定	107
Active Directory用のディレクトリ サービス オブジェクト	113
Active Directory Lights-Out Management.....	121
eDirectoryのディレクトリ サービス.....	122
eDirectoryインストールの前提条件	122
スナップインのインストールとeDirectory用の初期設定	123
eDirectory用のディレクトリ サービス オブジェクト	128
[Role Restrictions]	131
Lights-Out Management	134
ディレクトリの設定	135
ディレクトリ テスト	137
iLOへのユーザ ログイン	138
グループ管理と内蔵Lights-Outスクリプティング	141
Lights-Out設定ユーティリティの特長	141
Lights-Out設定ユーティリティおよび Insightマネージャ7を使用したグループ管理	142
Lights-Out設定ユーティリティ	142
Insightマネージャ7のクエリ定義	143
Insightマネージャ7を使用したアプリケーション起動	144
Lights-Out設定ユーティリティを使用したバッチ処理	145
Lights-Out設定ユーティリティのパラメータ	146
Lights-Out DOSユーティリティ	149
Lights-Out DOSユーティリティの概要	149

CPQLODOSの一般的なガイドライン	150
コマンド ライン 引数	150
CPQLODOS	152
CPQLODOSのパラメータ	152
CPQLODOSのランタイム エラー	152
MOD_NETWORK_SETTINGS	152
MOD_NETWORK_SETTINGSのパラメータ	153
MOD_DIR_CONFIG	155
MOD_DIR_CONFIGパラメータ	156
ADD_USER	157
ADD_USERのパラメータ	157

リモートInsightボード コマンド言語 159

リモートInsightボード コマンド言語の概要	160
RIBCLのサンプル スクリプト	160
RIBCLの一般的なガイドライン	160
XMLヘッダ	161
データ タイプ	161
ストリング	161
特殊ストリング	161
Booleanストリング	162
応答の定義	162
RIBCL	162
RIBCLのパラメータ	163
RIBCLのランタイム エラー	163
LOGIN	163
LOGINのパラメータ	164
LOGINのランタイム エラー	164
USER_INFO	164
USER_INFOのパラメータ	165
USER_INFOのランタイム エラー	165
ADD_USER	165
ADD_USERのパラメータ	166
ADD_USERのランタイム エラー	168
DELETE_USER	168
DELETE_USERのパラメータ	169
DELETE_USERのランタイム エラー	169
GET_USER	169
GET_USERのパラメータ	170
GET_USERのランタイム エラー	170
GET_USERが返すメッセージ	170
MOD_USER	171
MOD_USERのパラメータ	171
MOD_USERのランタイム エラー	173

GET_ALL_USERS	173
GET_ALL_USERSのランタイム エラー	174
GET_ALL_USERSが返すメッセージ	174
GET_ALL_USER_INFO	175
GET_ALL_USER_INFOのパラメータ	175
GET_ALL_USER_INFOのランタイム エラー	175
GET_ALL_USER_INFO	175
RIB_INFO	176
RIB_INFOのパラメータ	176
RIB_INFOのランタイム エラー	176
RESET_RIB	177
RESET_RIBのパラメータ	177
RESET_RIBのランタイム エラー	177
GET_NETWORK_SETTINGS	177
GET_NETWORK_SETTINGSのパラメータ	178
GET_NETWORK_SETTINGSのランタイム エラー	178
GET_NETWORK_SETTINGSが返すメッセージ	178
MOD_NETWORK_SETTINGS	179
MOD_NETWORK_SETTINGSのパラメータ	180
MOD_NETWORK_SETTINGSのランタイム エラー	182
MOD_DIAGPORT_SETTINGS	183
MOD_DIAGPORT_SETTINGSのパラメータ	183
MOD_DIAGPORT_SETTINGSのランタイム エラー	184
DIR_INFO	184
DIR_INFOのパラメータ	184
DIR_INFO のランタイム エラー	184
GET_DIR_CONFIG	185
GET_DIR_CONFIGのパラメータ	185
GET_DIR_CONFIGのランタイム エラー	185
GET_DIR_CONFIGが返すメッセージ	185
MOD_DIR_CONFIG	186
MOD_DIR_CONFIGのパラメータ	187
MOD_DIR_CONFIGのランタイム エラー	187
GET_GLOBAL_SETTINGS	188
GET_GLOBAL_SETTINGSのパラメータ	188
GET_GLOBAL_SETTINGSのランタイム エラー	188
GET_GLOBAL_SETTINGSが返すメッセージ	188
MOD_GLOBAL_SETTINGS	189
MOD_GLOBAL_SETTINGSのパラメータ	189
MOD_GLOBAL_SETTINGSのランタイム エラー	190
MOD_SNMP_IM_SETTINGS	190
MOD_SNMP_IM_SETTINGSのパラメータ	191
MOD_SNMP_IM_SETTINGSのランタイム エラー	192
CLEAR_EVENTLOG	192

CLEAR_EVENTLOGのパラメータ	192
CLEAR_EVENTLOGのランタイム エラー	193
UPDATE_RIB_FIRMWARE	193
UPDATE_RIB_FIRMWAREパラメータ	193
UPDATE_RIB_FIRMWAREのランタイム エラー	193
GET_FW_VERSION	194
GET_FW_VERSIONのパラメータ	194
GET_FW_VERSIONのランタイム エラー	194
GET_FW_VERSIONが返すメッセージ	195
HOTKEY_CONFIG	195
HOTKEY_CONFIGのパラメータ	196
HOTKEY_CONFIGのランタイム エラー	196
LICENSE	197
LICENSEのパラメータ	197
LICENSEのランタイム エラー	197
RACK_INFO	198
RACK_INFOのパラメータ	198
RACK_INFOのランタイム エラー	198
MOD_BLADE_RACK	199
MOD_BLADE_RACKのパラメータ	199
MOD_BLADE_RACKのランタイム エラー	200
GET_TOPOLOGY	200
GET_TOPOLOGYのパラメータ	201
GET_TOPOLOGYが返すメッセージ	201
SERVER_INFO	201
SERVER_INFOのパラメータ	202
SERVER_INFOのランタイム エラー	202
GET_HOST_POWER_STATUS	202
GET_HOST_POWER_STATUSのパラメータ	202
GET_HOST_POWER_STATUSのランタイム エラー	203
GET_HOST_POWER_STATUSが返すメッセージ	203
SET_HOST_POWER	203
SET_HOST_POWERのパラメータ	203
SET_HOST_POWERのランタイム エラー	204
RESET_SERVER	204
RESET_SERVERのパラメータ	204
RESET_SERVERのエラー	204
GET_UID_STATUS	205
GET_UID_STATUSのパラメータ	205
GET_UID_STATUSの応答	205
UID_CONTROL	205
UID_CONTROLのパラメータ	206
UID_CONTROLのエラー	206

内蔵Lights-Outのパラメータ	207
内蔵Lights-Outのパラメータに関する表	207
サーバの識別パラメータ	211
PCIリソース	211
サーバ名	211
シリアル番号	212
ファームウェアのバージョン	212
ファームウェアの日付	212
ユーザ管理のパラメータ	212
ユーザ名	212
ログイン名	212
パスワード	213
ユーザ アカウントの管理	213
リモート コンソールへのアクセス	213
仮想電源およびリセット	213
仮想メディア	213
iLOの設定	213
グローバル設定のパラメータ	214
アイドル時の接続タイムアウト（分単位）	214
Lights-Out機能の有効化	214
iLOのROMベース セットアップ ユーティリティを有効にする	214
iLO RBSUへのログインを要求	214
リモート コンソール ポートの設定	215
リモート コンソール データの暗号化	215
SSL暗号化強度	215
現在の暗号化アルゴリズム	215
Webサーバの非SSLポート	215
WebサーバのSSLポート	215
仮想メディア ポート	216
リモート コンソール ポート	216
パスワードの最小長	216
ネットワーク設定のパラメータ	216
NICの有効化	216
トランシーバ速度の自動選択	216
速度	217
デュプレックス	217
DNS/DHCP	217
WINSサーバの登録	217
DNSサーバの登録	218
起動時にゲートウェイにpingを送信	218
iLOのIPアドレス	218
iLOのサブネット マスク	218

iLOゲートウェイのIPアドレス	218
iLOサブシステムの名前	218
ドメイン名.....	219
DHCPサーバ.....	219
プライマリ、セカンダリおよびターシャリDNSサーバ.....	219
プライマリおよびセカンダリWINSサーバ.....	219
静的経路#1、#2、#3.....	219
ディレクトリ設定のパラメータ.....	219
ディレクトリ サービスによる認証	219
ディレクトリ サーバのアドレス	220
ディレクトリ サーバのLDAPポート.....	220
LOMオブジェクトの識別名	220
LOMオブジェクトのパスワード	220
ディレクトリ ユーザ コンテキスト1、ディレクトリ ユーザ コンテキスト2、 ディレクトリ ユーザ コンテキスト3	220
ディレクトリ設定のテスト.....	221
SNMP/Insightマネージャの設定のパラメータ.....	221
SNMPアラートの通知先.....	221
iLO SNMPアラートを有効にする.....	222
InsightマネージャのエージェントからのSNMPアラートを転送する	222
InsightマネージャのWebエージェントのURL.....	222
返すデータのレベル.....	222
ProLiant BL p-Classのパラメータ	223
ラック名	223
エンクロージャ名.....	223
ベイ名	223
ベイ	223
ラックのシリアル番号.....	224
エンクロージャのシリアル番号	224
ブレードのシリアル番号.....	224
電源	224
自動電源投入の有効化.....	225
iLO Advancedライセンス アクティベーション設定	225
iLO Advancedバック アクティベーション キー.....	225

内蔵Lights-Outのトラブルシューティング

227

最小要件	227
アラートおよびトラップの問題のトラブルシューティング	228
iLOからInsightマネージャ7のアラート（SNMPトラップ）を受信できない.....	228
iLOのセキュリティ オーバーライド スイッチ	228
iLOのPOST LEDインジケータ.....	229
ハードウェアおよびソフトウェア リンクに関連する問題	231
ハードウェア.....	231
ソフトウェア.....	232
ログイン時の問題.....	232

内蔵Lights-Outのリセット	234
ビデオおよびモニタの問題のトラブルシューティング	234
その他の問題のトラブルシューティング	236
イベント ログのエントリ	244

頭字語と略語	249
---------------	------------

索引	253
-----------	------------

内蔵Lights-Outの設定

この項の目次

iLOの設定オプション	13
グラフィック リモート コンソールのパフォーマンスの最適化	16
iLOの高度な機能の有効化	18
iLOデバイス ドライバのインストール	19

iLOの設定オプション

iLOでは、工場出荷時に、デフォルトのユーザ アカウントおよびパスワードなど、デフォルト設定が行われています。iLOがDNS/DHCPを実行するネットワークに接続されている場合、設定を変更せずにただちに使用できます。

iLOの機能のほとんどは、オペレーティング システムから独立して使用できます。一部の高度な機能を使用するには、オペレーティング システムのドライバをインストールする必要があります。また、以下の各項の情報を参照してiLOを設定し、セキュリティを向上させることもできます。

注：サーバのフロント パネルにあるiLOの診断ポートを介してProLiant BL p-Classサーバにアクセスすることもできます。

iLOでは、次の3つの設定オプションを使用できます。

- RBSU (F8キーを押すことにより起動)

iLOを新規にセットアップする場合は、RBSUの使用をおすすめします。RBSUは、サーバを起動するたびに使用でき、iLOのリモート コンソールを使用してリモートで実行できます。RBSUは、ネットワーク パラメータの設定、ディレクトリ設定、グローバル設定、およびユーザ アカウントの設定に使用できます。DHCPとDNS/WINSを使用しない環境では、iLOのネットワーク パラメータを新規に設定する場合、必ずRBSUを使用します。

RBSUは、[Global Settings]基本設定で無効にすることができます。この機能により、iLOのセキュリティ オーバーライド スイッチを設定している場合を除いて、ホストからの再設定ができなくなります。

- ブラウザ ベースのセットアップ

この方法を使って、DNS/DHCPを用いるiLOシステムを新規に設定して、IPアドレスを取得できます。また、設定済みのiLOの設定を変更する場合も、この方法を使用できます。

また、iLOの診断ポートを介してProLiant BL p-ClassのiLOシステムを新規に設定する場合にも使用できます。

- スクリプトを使用したセットアップ

この方法を使って、DNS/DHCPを用いるiLOシステムを新規に設定して、IPアドレスを取得できます。この方法では、*CPQLOCFG.EXE*ユーティリティを使用して、スクリプトファイルに書き込まれたiLOの設定がネットワーク経由で送信されます。

iLO RBSU

注：iLOを最初に設定する際に、英語以外のキーボードを設定する場合は、必ず、RBSUを使用してください。RBSU以外の方法では、国際キーボードは設定できません。

iLO RBSUを使用して、iLOの初期設定とセットアップを行うことをおすすめします。iLO RBSUは、ネットワーク上でのiLOのセットアップに役立つように設計されています。iLO RBSUは、継続的な管理を目的としたユーティリティではありません。

iLO RBSUを実行するには、以下の手順に従ってください。

1. サーバを再起動するかまたは電源を入れます。
2. POST実行中にプロンプトが表示されたら、**F8**キーを押します。iLO RBSUが起動します。
3. iLOがデフォルト値以外に設定されている場合は、該当するiLO権限（**ユーザ アカウントの管理権限**、**iLOの設定権限**）を備えた有効なiLOユーザIDとパスワードを入力します。デフォルトのアカウント情報は、iLOのデフォルト ネットワーク設定タグに記載されています。RBSUにログイン情報を提示するようにiLOを設定していない場合は、この手順は不要です。
4. iLOの設定に必要な変更を加えて、変更を保存します。
5. iLO RBSUを終了します。

インストールを簡単にするため、iLOでDNS/DHCPを使用することをおすすめします。DNS/DHCPを使用できない場合は、以下の手順に従ってDNS/DHCPを無効にし、IPアドレスとサブネット マスクを設定してください。

1. サーバを再起動するかまたは電源を入れます。

2. POST実行中にプロンプトが表示されたら、F8キーを押します。iLO RBSUが起動します。
3. 該当するiLO権限（**ユーザ アカウントの管理権限**、**iLOの設定権限**）を備えた有効なiLOユーザIDとパスワードを入力します。デフォルトのアカウント情報は、iLOのデフォルト ネットワーク設定タグに記載されています。
4. **[Network]**、**[DNS/DHCP]**の順に選択し、**Enter**キーを押します。次に**[DHCP Enable]**を選択します。スペースバーを押してDHCPをオフにします。**[DHCP Enable]**が**オフ**に設定されていることを確認してから変更を保存します。
5. **[Network]**、**[NIC]および[TCP/IP]**の順に選択し、**Enter**キーを押します。次に、**[IP Address]**フィールド、**[Subnet Mask]**フィールド、および**[Gateway IP Address]**フィールドに該当する情報を入力します。
6. 変更を保存します。iLO RBSUを終了すると、iLOシステムは新しい設定を使用するために自動的にリセットされます。

ブラウザ ベースのセットアップ

DHCP/DNSを用いるネットワークを使用する場合、この方法を使用してIPアドレスを取得してください。また、設定済みのiLOの設定を変更する場合も、この方法を使用できます。

1. 標準的なWebブラウザを使用して、リモートのネットワーク クライアントからiLOにアクセスし、サーバに取り付けられているネットワーク設定タグに記載されたデフォルトのDNS名、ユーザ名、およびパスワードを設定します。ネットワーク設定タグは、工場出荷時には通常、サーバの外側に取り付けられています。

iLOに正常にログインできれば、Webブラウザのインタフェースを介してネットワーク、ユーザ、およびSNMPアラート設定のデフォルト値を変更できます。

2. ブラウザ ベースのセットアップ画面にアクティベーション キーを入力して、iLO Advanced/バックの機能を有効にします。

iLO Advanced/バックの機能が使用許諾されると、仮想フロッピー ドライブを使用したオペレーティング システムのインストールや、グラフィック リモート コンソールを使用したりリモート ホスト サーバへのオペレーティングシステム ドライブおよびInsightマネージャのエージェントのインストールが可能になります。

注：ProLiant BL p-Classサーバの場合、内蔵Lights-Out Advanced/バックの機能は出荷時に有効になっており、無効にすることはできません。

グラフィック リモート コンソールのパフォーマンスの最適化

次に使用されるオペレーティング システムに応じた推奨されるクライアントおよびサーバ設定の一覧を示します。

推奨されるクライアントの設定

理想としては、リモート サーバのオペレーティング システムの表示解像度は、ブラウザを使用するコンピュータの解像度と同じかまたは低くなければなりません。サーバの解像度が高くなると転送される情報量も多くなるので、全体のパフォーマンスが低下します。

最大のパフォーマンスを発揮するために、次のクライアントおよびブラウザ設定を使用してください。

- **画面のプロパティ**
 - 256色以上のオプションを選択する
 - リモート サーバの画面解像度より高い解像度を選択する
 - LinuxのX Window Systemの画面のプロパティ - [X Preferences]画面で、フォント サイズを12に設定してください。
- **リモート コンソール**
 - リモート コンソールの速度については、128MB以上のメモリを搭載した処理速度700MHz以上のクライアントの使用をおすすめします。
 - リモート コンソールでJavaアプレットを実行する場合は、シングル プロセッサ クライアントの使用をおすすめします。
- **マウスのプロパティ**
 - [ポインタの速度]の速度を中程度に設定する
 - [ポインタの加速]を[低]または[いいえ]に設定する

推奨されるサーバの設定

次に使用されるオペレーティング システムに応じた推奨されるサーバ設定の一覧を示します。

注：クライアントのリモート コンソール アプレット上にホスト サーバの画面全体を表示するには、サーバの表示解像度をクライアントの解像度より低く設定してください。

Microsoft® Windows NT® 4.0およびWindows® 2000の設定

最高のパフォーマンスを発揮するには、次の設定を使用してください。

- サーバの画面のプロパティ
 - 背景なし（壁紙を使用しない）
 - 表示解像度は、800 × 600または1024 × 768ピクセル
 - 256色または24ビット カラー モード
- サーバのマウスのプロパティ
 - マウス ポインタの[デザイン]で[なし]を選択する
 - [ポインタの影を有効にする]の選択を解除する
 - [動作]または[ポインタ オプション]を選択して[ポインタの速度]のスライダを中程度に設定する
 - [ポインタの加速]を[なし]に設定する

Microsoft® Windows Server 2003の設定

最高のパフォーマンスを発揮するには、次の設定を使用してください。

- サーバの画面のプロパティ
 - 背景なし（壁紙を使用しない）
 - 表示解像度は、800 × 600または1024 × 768ピクセル
 - 256色または24ビット カラー モード
- サーバのマウスのプロパティ
 - マウス ポインタの[デザイン]で[なし]を選択する

- [ポインタの軌跡を表示する]の選択を解除する。
- [ポインタの影を有効にする]の選択を解除する。
- [動作]または[ポインタ オプション]を選択して[ポインタの速度]のスライダを中程度に設定する。
- [ポインタの精度を高める]の選択を解除する。

Red Hat LinuxおよびSuSE Linux Serverの設定

最高のパフォーマンスを発揮するには、次の設定を使用してください。

- サーバの画面のプロパティ
 - 1024 × 768ピクセル以下の画面解像度
 - 256色
- サーバのマウスのプロパティ
 - [Pointer Acceleration]を[1x]に設定する。KDEの場合、[Control Center]にアクセスして、[Peripherals/Mouse]、[Advanced]タブの順に選択します。
- X Window Systemの画面のプロパティ
 - [X Preferences]画面で、フォント サイズを12に設定する。

Novell NetWareの設定

最高のパフォーマンスを発揮するには、次の設定を使用してください。

サーバの画面のプロパティ

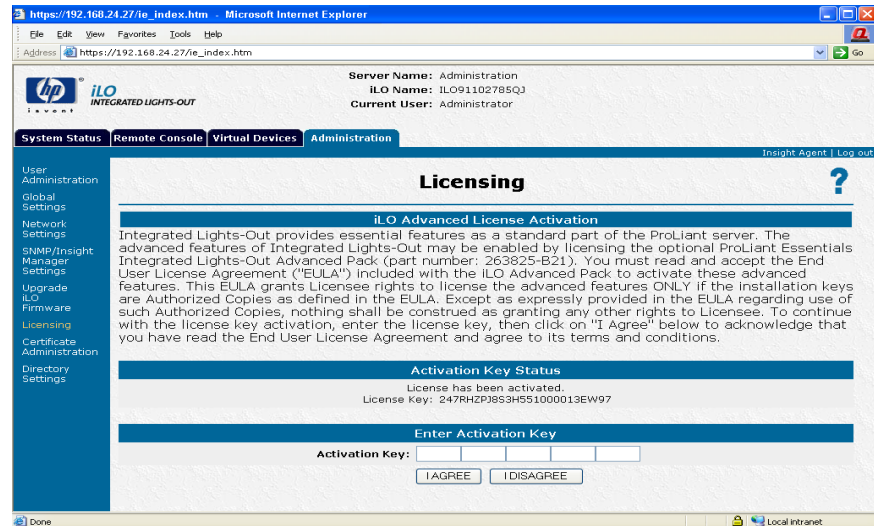
- 800 × 600ピクセル以下の画面解像度
- 256色

iLOの高度な機能の有効化

iLOの高度な機能は、オプションのiLO Advancedパックの使用許諾を受けることによって、有効にします。iLO Advancedパックには、高度な機能を有効にするためにiLOに入力する必要があるアクティベーション キーが含まれています。

iLOの高度な機能を有効にするには、以下の手順に従ってください。

1. サポートされているWebブラウザを介して、iLOにログインします。
2. [Administration]タブをクリックします。
3. [Licensing]をクリックして、[iLO Advanced License Activation]画面を表示します。



4. 入力フィールドにアクティベーション キーを入力します。
5. [I Agree]をクリックします。

以上でiLOの高度な機能は、有効になりました。

iLOデバイスドライバのインストール

iLOの機能のほとんどは、オペレーティング システム ベースのソフトウェアやドライバがなくても使用できますが、iLOマネジメント プロセッサには、2つのドライバインタフェースが提供されています。

- 最初のインタフェースは、iLO Advanced System Management Driver用です。このドライバは、ヘルス ドライバとも呼ばれ、サーバ コンポーネントの監視、イベント ログ機能、HPマネジメント エージェントのサポートなど、システム管理をサポートします。

- 2番目のインタフェースは、iLO Management Interface Driver用です。このドライバにより、システム ソフトウェアやSNMP Insightエージェントは、iLOと通信できます。

以下の各項では、次のオペレーティング システム用のiLOドライバのインストール手順について説明します。

- Microsoft®
- Novell
- Linux

このドライバの最新バージョンについては、HPのWebサイト<http://www.hp.com/jp/support/>を参照してください。

Microsoft Windows NT、Windows 2000、および Windows Server 2003ドライバのサポート

iLOをサポートするデバイス ドライバは、HPのWebサイト<http://www.hp.com/jp/support/>またはSmartStart CDで提供されるPSPに入っています。Windows®のドライバをインストールする前に、Windows®のマニュアルおよび最新のWindows® Service Packを入手してください。

Microsoft®関連ファイル

*CPQCIDRV.SYS*ファイルは、iLO Management Interface Driverのサポートを提供します。

CPQASM2.SYS ファイル、*SYSMGMT.SYS* ファイル、*SYSDOWN.SYS* ファイルは、iLO Advanced Server Management Controller Driverのサポートを提供します。

iLO Microsoft®ドライバのインストールまたは更新

Microsoft® Windows®製品用PSPには、システム要件を分析してすべてのドライバをインストールするインストーラが含まれています。

PSPは、HPのWebサイト<http://www.hp.com/jp/support/>またはSmartStart CDから入手できます。

注：iLOドライバを更新する場合、iLOが最新バージョンのiLOファームウェアで動作していることを確認してください。最新バージョンは、HPのWebサイト<http://www.hp.com/servers/lights-out/>（英語）からSmart Componentとして提供されます。

PSPに入っているドライバをインストールするには、HPのWebサイト<http://www.hp.com/jp/support/>からPSPをダウンロードし、ダウンロードしたファイルに含まれるSETUP.EXEファイルを実行して、インストール プログラムの指示に従います。PSPのインストールについて詳しくは、PSPのダウンロード ファイルに含まれるテキスト ファイルをお読みください。

Novell NetWareサーバ ドライバのサポート

iLOをサポートするために必要なデバイス ドライバは、SmartStart CDおよびHPのWebサイト<http://www.hp.com/jp/support/>で提供されるPSPに入っています。

NetWareの関連ファイル

CPQHLTH.NLMファイルは、NetWare用ヘルス ドライバを提供します。

CPQCL.NLMファイルは、iLO Management Interface Driverのサポートを提供します。

iLO NetWareドライバのインストールまたは更新

Novell NetWare用PSPには、システム要件を分析してすべてのドライバをインストールするインストーラが入っています。PSPは、HPのWebサイト<http://www.hp.com/jp/support/>およびSmartStart CDから入手できます。

注：iLOドライバを更新する場合、iLOが最新バージョンのiLOファームウェアで動作していることを確認してください。最新バージョンは、HPのWebサイト<http://www.hp.com/servers/lights-out/>（英語）からSmart Componentとして提供されます。

ドライバをインストールするには、PSPをHPのWebサイト<http://www.hp.com/jp/support/>からNetWareサーバにダウンロードします。PSPをダウンロードしたら、NetWareコンポーネントのインストール手順に従って、インストールを完了してください。PSPのインストールについて詳しくは、PSPのダウンロード ファイルに含まれるテキスト ファイルをお読みください。

注：NetWare 6.Xを使用する場合は、最適な結果を得られるように、必ず、オペレーティング システムが提供するRAGE-IICビデオ ドライバを使用してください。

Red Hat LinuxおよびSuSE Linuxサーバドライバのサポート

Red Hat LinuxおよびSuSE LinuxでiLOをサポートするために必要なデバイス ドライバは、SmartStart CD、マネジメントCD、またはHPのWebサイト<http://www.hp.com/jp/support/>で提供されます。

関連ファイル

iLOドライバ、基本エージェント、およびヘルス エージェントを含むPSPファイルは、HPのWebサイト<http://www.hp.com/jp/support/>からダウンロードできます。iLOドライバのインストールまたは更新方法については、Webサイトを参照してください。HPマネジメント エージェント for Linuxは、次で構成されます。

- ヘルス ドライバ、IMLビューア、基本エージェント、ヘルス エージェント、および標準装置エージェントを1つのパッケージにまとめたASM package 6.20.0以降 (hpasm)
- RIBドライバ、ラック デーモン、RIBエージェント、およびラック エージェントを1つのパッケージにまとめたRSM package 6.20.0以降 (hprsm)

これらのパッケージを使用して、以前のバージョンのエージェントやドライバをアップグレードすることはできません。新しいエージェントを適用する前に、以前のエージェントを削除してください。エージェントとドライバをアンインストールするには、次のコマンドを使用します。

- `rpm -e cpqrcki`
- `rpm -e cmanic`
- `rpm -e cmastor`
- `rpm -e cmasvr`
- `rpm -e cmafdtn`
- `rpm -e cpqhealth`

HP Linuxマネジメント エージェントをダウンロードしてインストールします。パッケージ名は、たとえば、`hpsm-6.20.0-11.Redhat7_3.i386.rpm`となります。

次のコマンドを使用して、パッケージをロードします。

```
rpm -ivh hpsm-d.vv.v-pp.Linux_version.i386.rpm
rpm -ivh hprsm-d.vv.v-pp.Linux_version.i386.rpm
```

ここで、*d*は、Linuxの製品名およびバージョンです。

*vv.v-pp*は、バージョン番号です。

詳しくは、HPのWebサイト<http://www.hp.com/jp/support/>の[ソフトウェアおよびドライバ]のページを参照してください。

必要に応じて、次のコマンドを使用してiLOをアンインストール、停止、または起動できます。

- アンインストール
`rpm -e cpqci`
- 停止
`/etc/rc.d/init.d/cpqci stop`
- 起動
`/etc/rc.d/init.d/cpqrci start`

詳しくは、HPのWebサイト<http://www.hp.com/jp/support/>の[ソフトウェアおよびドライバ]のページを参照してください。

内蔵Lights-Outの使い方

この項の目次

サポートされるサーバ オペレーティング システム ソフトウェア	25
サポートされるブラウザ	26
グラフィック リモート コンソールのシングル カーソル モードとデュアル カーソル モード.....	27
共通利用モデル	28
接続の概要	29
動作の概要	30
iLOに初めてアクセスする方法	35
システム ステータス	40
リモート コンソール	45
仮想デバイス	50
管理	62
ProLiant BL p-Class	76
Telnetサポート	82

サポートされるサーバ オペレーティング システム ソフトウェア

iLOは、内蔵のオペレーティング システムを実行する独立したマイクロプロセッサです。このアーキテクチャでは、ホストのオペレーティング システムとは関係なく、iLOのほとんどの機能を使用できます。

ホストのオペレーティング システムを適切にシャットダウンしたりInsightマネージャ7と統合したりするには、ヘルス ドライバおよびマネジメント エージェントが必要です。

iLOは、以下の2つのドライバ用のインタフェースを提供します。

- Advanced Server Management Controller Driver
- iLO Management Interface Driver

これらのドライバおよびエージェントは、以下のネットワーク オペレーティング システムで使用できます。

- Microsoft®

- Windows NT[®] 4.0 Server
 - Windows NT[®] 4.0, Enterprise Edition
 - Windows[®] 2000 Server
 - Windows[®] 2000 Advanced Server
 - Windows[®] Server 2003
- Linux
 - Red Hat 7.3
 - Red Hat 8.0
 - Red Hat 9
 - Red Hat Server 2.1
 - SuSE SLES 7.0
 - SuSE SLES 8.0
- Novell
 - NetWare 5.x
 - NetWare 6

サポートされるブラウザ

- Microsoft[®] Internet Explorer
 - 最小：Windows[®] 2000またはWindows[®] XP用Microsoft[®] Internet Explorer 5.5 Service Pack 2以降。リモート コンソールでシングル カーソル モードを使用する場合は、Java[™] 1.3.1_02 JVM以降が必要です。
 - 推奨：Windows[®] 2000またはWindows[®] XP用Microsoft[®] Internet Explorer 6.0以降およびJava[™] 1.4.X JVM。システム構成に合わせて推奨されるJVMをダウンロードするには、HPのWebサイト<http://www.hp.com/servers/manage/jvm/>（英語）を参照してください。
- Linux
 - Netscape 7.x

– Mozilla 1.2.1

Linux、Netscape、およびMozillaでは、Java™ 1.4.1 JVM以降が必要です。システム構成に合わせて推奨されるJVMをダウンロードするには、HPのWebサイト<http://www.hp.com/servers/manage/jvm/>（英語）を参照してください。

一部のブラウザとオペレーティング システムを組み合わせで使用した場合に正常に動作するかしないかは、そのオペレーティング システムに必要なブラウザ テクノロジーが実装されているかどうかによって決まります。

グラフィック リモート コンソールのシングル カーソル モードとデュアル カーソル モード

グラフィック リモート コンソールでは、シングルカーソル モードまたはデュアルカーソル モードを使用できます。

リモート コンソール（デュアルカーソル）

[Remote Console (dual cursor)] オプションは、リモート コンソール ウィンドウで2つのマウス カーソルを使用して、リモート サーバのマウス カーソルとローカル クライアントのマウス カーソルを示します。リモート コンソール ウィンドウでは、ローカル クライアントのカーソルは十字形で表示されます。デュアル カーソル オプションは、Java™ 1.1 VM以降でサポートされています。2つのカーソルが互いに離れる場合、同期させて元に戻すことができます。リモート カーソルとローカル カーソルを同期させるには、以下の手順に従ってください。

1. 十字形のローカル カーソルを右クリックし、ドラッグして移動して、リモートサーバのマウス カーソルの位置に合わせます。
2. **Ctrl**キーを押したまま、十字形のローカル カーソルを移動してリモート サーバのマウス カーソルの位置に合わせます。

カーソルが[Remote Console]アプレット ウィンドウを出る位置を確認できるため、デュアル カーソル オプションが好まれる場合があります。テキスト ベースのオペレーティング システムの場合は、リモート コンソールのデュアル カーソル モードを使用することをおすすめします。

リモート コンソール（シングルカーソル）

[Remote Console]オプションは、リモート コンソール セッションでの作業中シングルマウス カーソルを提供します。2つのカーソルの同期は必要なくなり、リモート コンソール ウィンドウでの操作が簡単になります。

シングルカーソルモードでの動作には、Microsoft® Internet Explorerの場合は、Java™ 1.3.1_02 JVM以降、NetscapeおよびMozillaの場合は、Java™ 1.4.1 JVMが必要です。システム構成に合わせて推奨されるJVMをダウンロードするには、HPのWebサイト <http://www.hp.com/servers/manage/jvm/>（英語）を参照してください。

注：このサイトにアクセスすると、メインサイトからjava.sun.comサイトに転送されます。JVMのバージョンについては、リモートコンソールのヘルプページで指定されているバージョンの使用をおすすめします。Internet Explorer用の指定されたバージョンは、java.sunサイトまたはマネジメントCDから入手できます。

共通利用モデル

iLOの共通利用モデルは、外部ネットワークを介して1つ以上のiLOデバイスに接続された、サポートされているブラウザを実行するクライアントPCです。iLOは、ホストサーバの電源に接続し、Ethernetケーブルをサーバの専用iLOマネジメントポートに接続することにより、DHCPおよびDNSを介して使用できるようになります。準備が完了すると、Webブラウザを使用してSSL接続経由でiLOに接続できます。ログインすると、クライアントデスクトップからサーバをリモート制御できます。

サポートされるWebブラウザを使用して、次のことが可能です。

- ホストサーバのコンソールへのリモートからのアクセス（テキストモードのみ）
- ホストサーバのコンソールに対するリモートからのアクセス（グラフィックモードでのキーボードおよびマウスのフル操作。iLO Advancedパックを使用して使用許諾されている場合）
- リモートからのホストサーバの電源投入、電源切断、または再起動
- ホストサーバをリモートで起動して仮想CDまたは仮想フロッピーイメージを使用することにより、ROMのアップグレードやオペレーティングシステムのインストールを実行（iLO Advancedパックを使用して使用許諾されている場合）
- ホストサーバの状態に関係なくiLOからアラートを送信
- iLOによって提供されるトラブルシューティング機能の使用
- Webブラウザの起動、SNMPアラート通知の使用、およびInsightマネージャ7を使用したiLOの診断

この項では、サポートされているWebブラウザを使用してiLOの機能にアクセスする方法を説明します。すべての機能について詳しく説明し、iLOのすべてのコンフィギュレーション設定を紹介します。

グラフィック リモート コンソールおよび仮想メディアは高度な機能で、iLO Advanced パック（オプション）の使用許諾を受けることによって有効にする必要があります。高度な機能についても説明し、注釈をつけています。

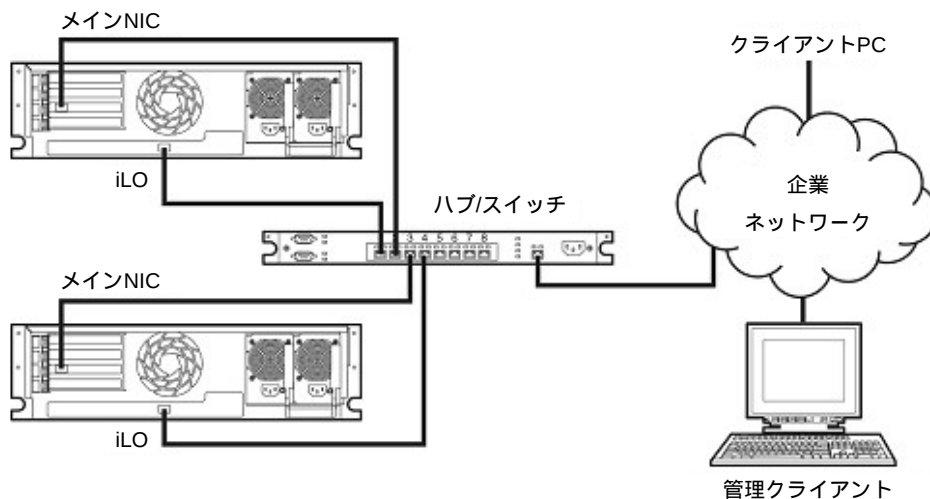
接続の概要

以下の各例では、サーバには、1つの10/100/1000Mbps NICおよび1つの10/100Mbps iLOポートの計2つのポートが搭載されています。ここで示す2つの一般的な接続の例では、企業ネットワーク上で両方のポートを接続するかまたはiLOポートを独立したiLOネットワークに接続しています。次に、それぞれの接続を使用する場合の長所と短所を説明します。

企業ネットワークでの接続

サーバには、企業ネットワークに接続できる2つのポートがあります。この接続では、ネットワーク上のどこからでもiLOにアクセスできます。ただし、企業ネットワーク上で、ネットワークトラフィックがiLOのパフォーマンスの妨げとなる可能性があります。

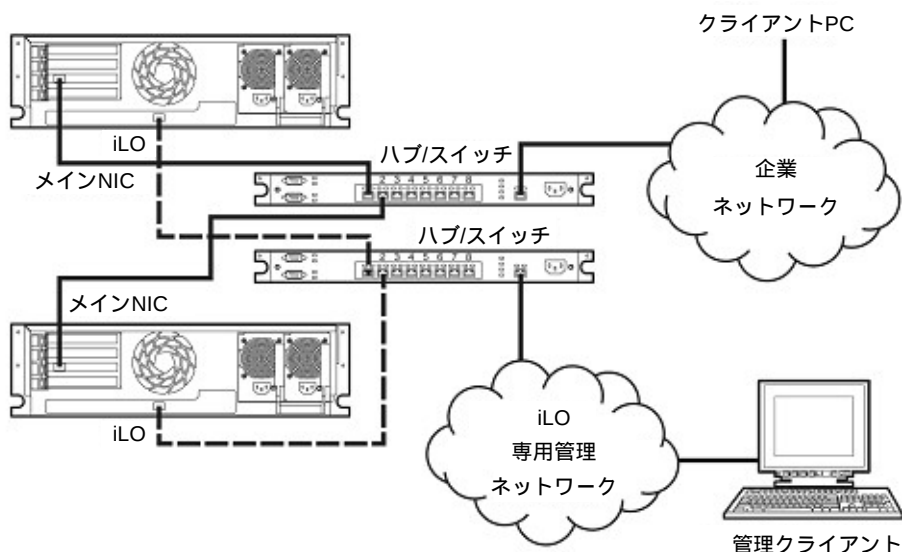
この構成は、iLOをサポートするために必要なネットワーク用ハードウェアおよびインフラストラクチャの総量を減らします。この方法で構成すると、iLOは、既存のDNS/DHCPサーバおよびルータを使用できます。



内蔵Lights-Outネットワークでの接続

内蔵Lights-Outは、独立した専用管理ネットワーク上に配置できます。独立したネットワークを使用すれば、パフォーマンスの向上は可能ですが、この構成では、企業ネットワークから直接iLOにアクセスできません。

専用管理ネットワークを使用して、iLOポートのセキュリティを向上させることもできます。独立したネットワークを使用することにより、管理ネットワークに接続できるワークステーションを物理的に制限できます。



動作の概要

- 仮想テキスト リモート コンソール

標準のiLOは、テキスト モードの画面で、内蔵ハードウェアによるリモート コンソール機能を提供します。オペレーティング システムに依存しないコンソールはテキスト モードをサポートし、シャットダウンやスタートアップ操作など、リモートのホスト サーバの動作を表示します。

- 仮想グラフィック リモート コンソール (iLO Advancedパックを使用して使用許諾されている場合)

iLOは、内蔵ハードウェアによるグラフィック リモート コンソール機能を実現します。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 サーバのディスプレイ、キーボード、およびマウスをフル操作できます。オペレーティングシステムに依存しないコンソールはグラフィック モードをサポートし、シャットダウンやスタートアップ操作など、リモートのホスト サーバの動作を表示します。

- 再起動（リセット）

リモートのサイトのホスト サーバが応答しない場合、管理者はこの機能を使ってコールド リブートまたはウォーム リブートを実行し、サーバをオンラインに復帰させることができます。

- 仮想メディア（iLO Advancedパックを使用して使用許諾されている場合）

仮想フロッピー ドライブ機能または仮想CDドライブ機能により、管理者はネットワーク上の任意の場所からリモートのホスト サーバを起動して標準メディアを使用できるようになります。これによって、時間を節約して作業効率を高めることができ、ディスクを挿入して使用するためだけにリモートのサーバまで行く必要がなくなります。これにより、管理者は以下の機能をリモートで実行できるようになります。

- リモートのサーバ上でROMPaqによるアップデートを実行する。
- 仮想CDドライブから、ネットワーク ドライブから、またはSmartStart Scripting Toolkitを使用してリモート サーバ上にオペレーティング システムをインストールする。

- 仮想電源ボタン

iLOを使用すると、サポートされるブラウザ インタフェースで、ホスト サーバの電源ボタンをリモート操作できます。

- 仮想シリアル ポート - サーバのシリアル ポートへの接続を可能にするJava™ アプレットを提供します。Java™アプレットにより、シリアル ポート用に設定されたアプリケーションへのアクセスを可能にするVT320端末エミュレーション機能を使用できるようになります。仮想シリアル ポートは、Windows® Server 2003のEMS用に使用できます。

- ディレクトリ サービスのサポート（iLO Advancedパックを使用して使用許諾されている場合） - Active DirectoryまたはeDirectoryのアカウントを使用してiLOにログインできます。MMCおよびConsoleOneへのスナップインが提供されるため、Lights-Outマネジメント デバイスに対する認証と権限付与を集中的に管理でき、管理の方法も簡単になります。

- ファームウェアのリモート アップデート

この機能を使えば、HPから入手可能な最新のファームウェアを用いてiLOを最新状態にしておくことができます。iLO上のROMコードのアップデートは、ブラウザ インタフェース上で行います。

- Insightマネージャ7との統合

Insightマネージャ7は、iLOと完全に統合されています。この統合により、以下のサポートが可能になります。

- Insightマネージャ7コンソールへのSNMPトラップの配信サポート
- SNMP管理のサポート

Insightマネージャ7は、iLOを介してInsightマネジメント エージェントの情報にアクセスできます。

- マネジメント プロセッサのサポート

Insightマネージャ7には、マネジメント プロセッサという新しいデバイス タイプのサポートが追加されています。ネットワーク上のサーバにインストールされたすべてのiLOデバイスは、Insightマネージャ7ではマネジメント プロセッサとして検出されます。マネジメント プロセッサは、そのマネジメント プロセッサを搭載しているサーバに関連付けられます。

- iLOマネジメント プロセッサのグループ化

すべてのiLOデバイスを、論理的なグループとしてまとめて1つのページに表示することができます。この機能により、Insightマネージャ7の単一箇所からiLOにアクセスできます。

- iLOのハイパーリンク

Insightマネージャ7は、サーバのデバイス ページでハイパーリンクを提供しており、ここからiLOを起動したりiLOに接続したりすることができます。

- HPマネジメント エージェント

iLOは、HPマネジメント エージェントと組み合わせられており、iLOのWebブラウザ インタフェースを介して、システム管理情報にリモート アクセスできます。

- ProLiant BL p-Classのサポート

- iLOは、ProLiant BL p-Classラックの情報を提供し、Insightマネージャ7がラックをグラフィカルに表示できるようにします。

- RILOE IIオプション ボードとの統合

iLOを装備するサーバでは、RILOE IIボードは、オプションとしてサポートされます。リモートInsightボード/PCIや第1世代のRILOEボードなど、以前の世代のリモートInsightボードは、iLOを搭載するサーバではサポートされません。

バージョン1.10以降の内蔵Lights-Outファームウェアは、RILOE IIの存在を検出して、iLOの機能を自動的に無効にします。また、第1世代のRILOEがインストールされている場合、iLOファームウェア バージョン1.10以降は、その存在を検出して無効な構成を示すメッセージを表示します。

RILOE IIを取り外した後、iLOの機能を再度有効にするには、セキュリティ オーバーライド スイッチおよびiLO用のROMベース セットアップ ユーティリティ (F8) を使用する必要があります。[Settings]を選択し、次に、[Lights-Out Functionality]の設定で[Enabled]を選択してください。

- 専用のLANネットワーク接続

iLO上の10/100Mbps Ethernetチップにより、管理者は、専用のネットワークでiLOに接続できます。iLOを使用すれば、サーバの問題をインバンドでリアルタイムにSNMP通知できるため電話接続やモデム共有デバイスを別に用意する必要はありません。NICは、10Mbpsと100Mbpsを自動選択して切り替えることができます。

- スクリプトを使用したiLOの設定

ユーザ設定、ネットワーク設定、グローバル設定、SNMP/Insight Manager設定など、iLOのすべての設定をスクリプト ファイルを介して行うことができます。スクリプト作成機能は、SmartStart Scripting Toolkit、ProLiant Essentials Rapid Deployment パック、またはInsightマネージャ7と統合されているWindows®クライアントから起動できます。

- ダイヤルアップ接続のサポート

iLOは、モデム ルータまたは外部からのRAS接続を使用してネットワークにログオンするダイヤルアップ接続を介して利用できます。

- VPNのサポート

iLOの機能は、VPNテクノロジーと組み合わせて使用すると、世界中で利用できます。

- iLOから管理コンソールへのSNMPアラート

管理コンソールを使用して、SNMPアラート、許可されていないアクセスに対するアラートなど、特定のサーバアラートにアクセスできます。

- ユーザ管理とセキュリティ

iLOは、カスタマイズ可能なアクセス権、ログイン名、および高度に暗号化されたパスワードを持つ最大12ユーザをサポートします。個々のユーザが使用できる機能は、権限により管理されます。各ユーザは、そのアクセス要件に合わせてカスタマイズされた権限を持つことができます。

iLO Advanced 1.40以降では、ディレクトリベースのユーザ アカウントとの統合が実現しているため、12を超えるユーザをサポートできます。これにより、ユーザ アカウント数の制限が実質的になくなります。

iLOにより、パスワードの安全な暗号化、すべてのログインのトラッキング、およびログインに失敗したときのすべての記録の管理が可能となります。また、ログインに失敗した場合にアラートを生成し、これをリモート管理コンソールに送信します。iLOにはまた、以下のようなセキュリティ機能があります。

- ユーザ定義のTCP/IPポート
- ユーザ操作をiLOイベント ログに記録
- 失敗したログインに対するプログレッシブ デイレイ
- Webページおよびリモート コンソール データの128ビット暗号化

iLOは、ネットワーク上で転送されるHTTPデータについて業界標準のSSL暗号化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提供します。SSL暗号化（最大128ビット）により、ネットワーク上で転送されるHTTP情報のセキュリティが確保されます。

SSLは、ネットワーク プロトコル層の1つで、アプリケーション層のすぐ下の階層になります。SSLは、クライアントとサーバ間の安全な（暗号化された）通信チャネルの管理に使用できます。

リモート コンソール データは、128ビットRC4双方向暗号化を使用して保護されます。

- DNS/DHCPを用いたIPアドレスの自動設定

iLOでは、ネットワーク設定を自動的に行うことができます。iLOは、出荷時にネットワークで使用するための名前およびDHCPが有効に設定されていて、ネットワーク上のDHCPサーバからIPアドレスを取得します。DNS/DHCPを使用しないシステムでは、iLOによって静的なIPアドレスを設定できます。

デフォルトのユーザ名、パスワードおよびDNS名は次のとおりです。

ユーザ名：Administrator

パスワード：無作為に選んだ英数字8文字による文字列

DNS名：ILOXXXXXXXXXXXXX（12個のXは、そのiLOプロセッサを搭載しているサーバのシリアル番号。iLOのDNS名はユーザが設定できます）

注：ユーザ名とパスワードでは、大文字と小文字が区別されます。

- IML

iLOは、サーバのIMLを管理するので、サーバが稼動していない場合でも、サポートされているブラウザを使用してこのログを参照できます。この機能は、リモートホストサーバの問題のトラブルシューティングに役立ちます。

- RBSU（F8）

汎用的でシステムに依存しないRBSUを使用すればiLOをすばやく簡単に設定できます。

- シングル マウス カーソル モード

シングルカーソルモードでの動作には、Microsoft® Internet Explorerの場合は、Java™ 1.3.1_02 JVM以降、NetscapeおよびMozillaの場合は、Java™ 1.4.1 JVMが必要です。システム構成に合わせて推奨されるJVMをダウンロードするには、HPのWebサイト<http://www.hp.com/servers/manage/jvm/>（英語）を参照してください。

注：このサイトにアクセスすると、メイン サイトからjava.sun.comサイトに転送されます。JVMのバージョンについては、リモート コンソールのヘルプページで指定されているバージョンの使用をおすすめします。Internet Explorer用の指定されたバージョンは、java.sunサイトまたはマネジメントCDから入手できます。

- HP ProLiant BL p-Class

このタブの設定により、ラック、エンクロージャ（筐体）、およびベイ名を管理して、識別を容易にすることができ、電源オプションやラック アラート オプションの制御も可能になります。サーバ ブレード管理モジュールおよび電源管理モジュールの診断情報も利用できます。このタブは、サポートされているProLiant BL p-Classサーバを使用する場合にのみ表示されます。

iLOに初めてアクセスする方法

iLOは、デフォルトのユーザ名、パスワード、およびDNS名が事前に設定されています。この設定済みの値は、iLOマネジメント プロセッサを搭載するサーバに取り付けられているネットワーク設定タグに記載されています。これらの値を使用し、標準的なWebブラウザを使用して、ネットワーク クライアントからリモートでiLOにアクセスしてください。

重要：セキュリティ上の理由から、iLOに初めてアクセスした後は、デフォルトの設定値を変更することをおすすめします。

デフォルトの値は次のとおりです。

- ユーザ名：Administrator
- パスワード：無作為に選んだ英数字8文字による文字列
- DNS名：ILOXXXXXXXXXXXXX（12個のXは、サーバのシリアル番号）

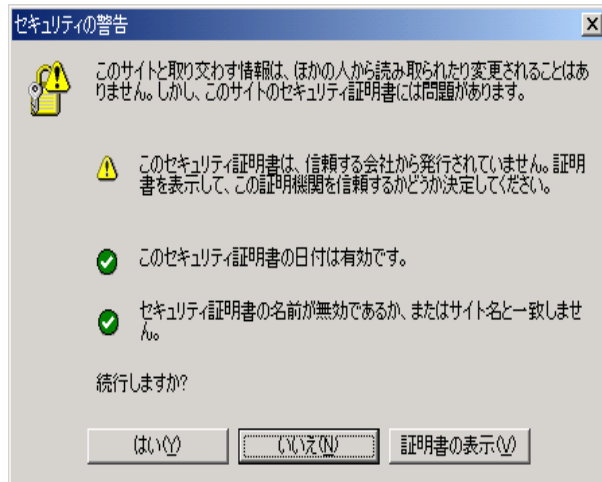
注：ユーザ名とパスワードでは、大文字と小文字が区別されます。

iLOに初めてアクセスする場合は、以下の手順に従ってください。

1. Webブラウザのアドレス入力ボックスに、iLOのIPアドレスまたはDNS名を入力します。

注：この手順は、ご使用のネットワークでDNS/DHCPをサポートしていることを前提としています。サポートしていない場合は、RBSUを使用してIPアドレスを設定しなければなりません。ProLiant BL p-Classサーバでは、iLOの診断ポートを使用してください。

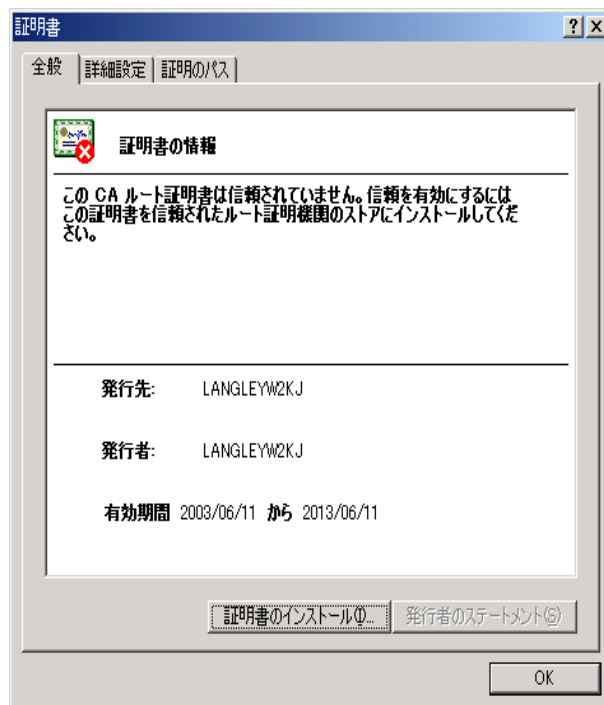
2. ブラウザを使用して初めてiLOに接続すると、図に示すようにセキュリティの警告が表示されます。



3. この警告メッセージは、iLOが動的に生成したデフォルトのSSL証明書をご使用のブラウザが認識しないために表示されるものです。証明書を表示してインストールすることができます。また、iLOにアクセスするたびに[はい]をクリックしてもかまいません。

注：CAの署名した証明書をインポートするには、97ページの「電子証明書」の項を参照してください。

4. **[はい]**をクリックすると、ブラウザは引き続きiLOのログイン画面に移動します。この警告メッセージは、ブラウザを使用してiLOマネジメント プロセッサにアクセスするたびに表示されます。
5. **[いいえ]**をクリックすると、iLOの初期画面に戻ります。
6. **[証明書の表示]**をクリックすると、図に示すようにポップアップ ウィンドウが表示され、証明書の情報を示します。デフォルトの証明書をブラウザにインストールすると、次からはセキュリティの警告メッセージが表示されなくなります。
7. 証明書をインストールする場合は、手順8に進んでください。証明書をインストールしない場合は、手順9に進んでください。



注：ブラウザから証明書を削除した場合、ファームウェアをアップグレードした場合、またはiLOを再起動した場合は、セキュリティの警告メッセージが再度表示されます。

8. ブラウザにデフォルトの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。

- a. [証明書のインストール]をクリックします。[証明書マネージャのインポートウィザード]が開始されます。
 - b. [次へ]をクリックします。
 - c. [次へ]をクリックして、[証明書の種類に基づいて、自動的に証明書ストアを選択する]を選択します。
 - d. [証明書マネージャのインポート ウィザードの完了]ウィンドウが表示されたら、[完了]をクリックします。
 - e. 確認ウィンドウが表示されたら、[はい]をクリックして、デフォルトの証明書のインストールを確認します。
 - f. [OK]をクリックして、証明書が正常にインポートされたことを確認します。
 - g. [証明書]ウィンドウで[OK]をクリックして、[セキュリティの警告]ウィンドウに戻ります。
 - h. [セキュリティの警告]ウィンドウで[はい]をクリックして、ログインします。
9. ブラウザによるiLOとのSSL接続が完了すると、[Account Login]画面で、ユーザ名とパスワードの入力を指示されます。ネットワーク設定タブに記されたデフォルトのユーザ名とパスワードを入力して[Log In]をクリックします。



Account Login

This is a private system. Do not attempt to login unless you are an authorized user.
Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.

Login Name:

Password:

Copyright © 2003 Hewlett-Packard Development Company, L.P.

Hewlett-Packard and the Hewlett-Packard logo are trademarks of Hewlett-Packard Development Company, L.P. in the U.S. and/or other countries.

Confidential computer software. Valid license from Hewlett-Packard required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Contains security software licensed from: RSA Data Security Inc.
Portions Copyright 1985, 1991, 1992 by Carnegie Mellon University
Derivative Work - 1996, 1998-2000 Copyright 1995, 1998-2000 The Regents of the University of California

10. デフォルトのユーザ名とパスワードが確認されると、[Status Summary]画面が表示されます。



注：これ以降のスクリーンショットには、[BL p-Class]タブを示していません。

iLOの[Status Summary]画面には、現在ログオンしているユーザ、サーバ名とステータス、iLOのIPアドレスと名前、最終ログ エントリのデータなどiLOについての概要情報が表示されます。[Status Summary]画面には、iLOがHPのWebベースのマネジメント エージェントおよびInsightマネジメントWebエージェントを使用するように設定されているかどうかについても表示されています。

失敗したブラウザ ログイン試行に対するプログレッシブ デイレイ

ログインの1回目の失敗に対して、iLOは5秒間の遅延時間を課します。ログインの2回目の失敗に対しては、10秒間の遅延時間が課せられます。3回目の失敗に対しては、60秒間の遅延時間が課せられます。別のユーザによる失敗に対しても、この遅延時間が繰り返されます。遅延時間が発生するたびに、情報ページが表示されます。この設定は、有効なログインが完了するまで続行されます。

この機能は、ブラウザのログイン ポートに対して実行される可能性のある辞書攻撃からの防御に役立ちます。

ヘルプ

iLOのすべてのオプションについての説明は、[iLO Help]オプションを選択して参照できます。これらのリンクを使用すると、iLOの機能についての概要、およびiLOの動作を最適化するために役に立つ情報が得られます。各ページに関するヘルプ情報にアクセスするには、ブラウザウィンドウの右側にある[?]をクリックします。

システム ステータス

[System Status]タブには、以下のオプションが用意されています。これらのオプションを使用して、サーバの一般的なステータス情報および詳細なステータス情報、イベント ログおよび管理ログ データ、ならびに診断データを見ることができます。

ステータスの概要

[Status Summary]画面には、現在のユーザ、サーバ名とステータス、iLOのIPアドレスと名前、最終ログ エントリのデータなどiLOについての概要情報が表示されます。

iLOステータス

[iLO Status]オプションは、次のような、iLOについての包括的なステータス情報を提供します。

- 現在のユーザ
- リモート コンソールのステータスと可用性
- iLOが現在使用している日付と時刻
- iLOファームウェアのリビジョン情報

- iLOの製品バージョン（iLO StandardまたはiLO Advanced）

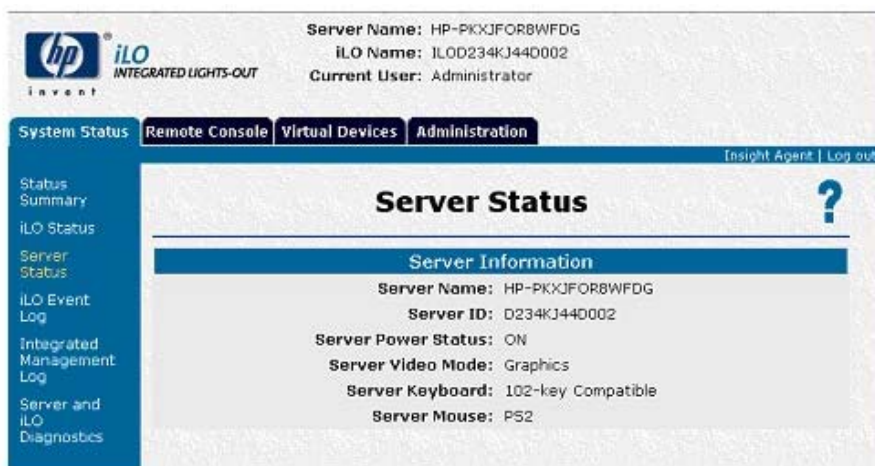


サーバステータス

[Server Status]オプションは、次のような、サーバについての包括的なステータス情報を提供します。

- iLOマネジメント プロセッサに対応するサーバ名
注：ホスト サーバにHPマネジメント エージェントがロードされていない場合、[Server Name]フィールドでは、ホストの名前が"unnamed"と報告されます。
- サーバの電源ステータス
- サーバのビデオ モード

- サーバのキーボードおよびマウスの種類



iLOのイベント ログ

iLOのイベント ログは、オペレーティング システムに依存しないログで、日付および時刻によってイベントの記録を維持管理しています。記録されるイベントには、サーバの電源障害やサーバのリセットなどのサーバの主要なイベントや無許可のログイン試行などのiLOイベントが含まれます。

記録されるイベントには、他に成功または失敗したブラウザ ログインおよびリモート コンソール ログイン、仮想電源および電源の再投入イベント、ならびにイベント ログのクリア操作が含まれます。ユーザの作成や削除などの一部のコンフィギュレーションの変更も記録されます。

[Clear Event Log]をクリックすると、以前に記録されたすべての情報を含むiLOのイベント ログがクリアされます。[OK]をクリックして、イベント ログをクリアすることを確認します。ログがクリアされたことを示す行が、ログに記録されます。

注：iLOファームウェアの新しいバージョンによって記録されたイベントが、それ以前のバージョンのファームウェアでサポートされない場合があります。サポートされていないファームウェアでイベントが記録されると、そのイベントは、UNKNOWN EVENT TYPEとしてリストに表示されます。この外観上の問題は、イベント ログをクリアしてこれらのエントリを削除するか、またはファームウェアをサポートされる最新バージョンにアップデートすることにより、解決できます。

インテグレートド マネジメント ログ

IMLにより、記録されたりモート サーバのイベントを表示できます。記録されるイベントには、オペレーティング システムの情報やROMベースのPOSTコードなど、システム ヘルス ドライバで記録されるサーバ固有のイベントがすべて含まれます。詳しくは、サーバのガイドを参照してください。

[Clear Event Log]をクリックすると、以前に記録されたすべての情報を含むIMLのイベント ログがクリアされます。[OK]をクリックして、イベント ログをクリアすることを確認します。ログがクリアされたことを示す行が、ログに記録されます。

サーバおよびiLOの診断

[Server and iLO Diagnostics]オプションは、以下の各項で示す、包括的な診断情報を提供します。

注：診断ポートを介して接続されている場合、ディレクトリ サーバを使用することはできません。ローカル アカウントでのみログインできます。

ホスト サーバのPOST診断の結果

iLOは、内蔵マネジメント プロセッサとして、サーバの起動プロセスの進行状況を監視します。ホスト サーバのROMは、起動時に、POSTコードを書き込みます。iLOは、これらのコードを記録し表示します。選択されたPOSTコードは、進行状況を示すコードとみなされ、これらのコードに関する説明が添えられます。これらのコードと説明を参照して、サーバの起動プロセスの開始から完了に至るまで進行状況を確認できます。

POSTコードは、ROM BIOSの起動プロセスを記録します。コードは、起動プロセスの特定の段階の開始を示します。POSTコードの結果を参照することにより、起動プロセスが停止したと考えられるおおまかな段階を確認できます。一般には、起動プロセス停止の実際の根本原因を診断するには、POSTコードを参照するだけでは不十分です。POSTコードを、IML、ローカル コンソールまたはiLOリモート コンソール、診断ユーティリティなどのツールと組み合わせて使用して、起動プロセス停止の根本原因を突き止めてください。

次の表に、ProLiantサーバの通常の起動シーケンスについて、iLOが追跡するホストサーバ用のすべてのPOSTコードと診断結果を示します。

コード	段階の開始
FE04	EISAの初期化
FE08	PCIの初期化
FE0C	プロセッサの初期化
FE10	ビデオの初期化
FE14	キャッシュの初期化
FE18	USBの初期化
FE1C	メモリ テスト
FE20	メモリの初期化
FE24	USBの起動
FE28	ディスクレット コントローラのテスト
FE2C	オプションROMの初期化
FE30	ATAPIオプションROMの初期化
FE34	BBSの初期化
FE38	起動プロセスの開始
FE3C	SCSI CDブートの試行
FE40	ディスクレット ブートの試行
FE44	HDブートの試行
FE48	CDブートの試行
FE4C	PXEブートの試行
FE50	ブート セクタのコードに制御を渡す
FE54	起動可能デバイスなし

NVRAM環境変数のリスト

HPでは、NVRAMにサーバの環境変数情報を格納しています。この情報は、HPのエンジニアやHPのシステム管理アーキテクチャについてよく理解されたお客様には役に立ちます。

仮想NMIボタン

仮想NMIボタンは、デバッグのためにオペレーティング システムを停止します。この機能は高度な機能です。この機能をカーネルのデバッグを行う担当者以外が使用することは避けてください。

iLOのセルフテストの結果

Webページのこのセクションには、iLOのセルフテストの結果が表示されます。正常な状態では、すべてのテスト済みサブシステムがPassedと表示されるはずです。

Server Name: HP-PKXJFOR9WFDG
iLO Name: ILOD234KJ44D002
Current User: Administrator

System Status | Remote Console | Virtual Devices | Administration

Insight Agent | Log out

Server and iLO Diagnostics

POST results for server | NVRAM environment variables | Virtual NMI Button | iLO self-test results

POST diagnostic results for the host server

Code	Description
FE1C	Memory Test
FE20	Memory Initialization
FE24	USB Startup
FE28	Floppy Controller Test
FE2C	Option ROM Initialization
FE30	ATAPI Option ROM Initialization
FE34	BBS Initialization
FE38	Begin BOOT Process
FE48	Attempting CD Boot
FE54	No bootable devices
FE40	Attempting Floppy Boot

リモート コンソール

[Remote Console]タブには、以下のオプションが用意されています。このタブを使用して、リモート コンソールのいろいろな表示にアクセスでき、ホット キーを押したときにリモートのホスト サーバに転送されるキーストロークのシーケンスを定義することができます。標準はテキスト モードです。グラフィック リモート コンソールは、iLO Advancedパックの使用許諾を受けることによって有効にすることができます。

リモート コンソール情報オプション

[Remote Console Information]オプションは、使用できるリモート コンソール オプションに関する情報、およびリモート コンソールでシングル カーソル オプション（48ページの「リモート コンソールでのシングル マウス ポインタ」を参照）を使用するために必要な最新のJava™ Runtime Environmentをダウンロードするためのリンクを表示します。

[Remote Console Information]オプションでは、リモート コンソールが使用中または使用可能のどちらであるかも表示します。iLOには、最大10のユーザが同時にログインできますが、リモート コンソールに一度にアクセスできるのは1ユーザだけです。他のユーザの使用中にアクセスを試みると、リモート コンソールがすでに使用中であることを示す警告メッセージが表示されます。

注： Telnetセッションとリモート コンソール セッションを同時に開くことはできません。両方のセッションを同時に行おうとすると、エラー メッセージが生成されます。

注： [Global Settings]タブでリモート コンソール ポートの設定が無効になっている場合、リモート コンソールは使用できません。

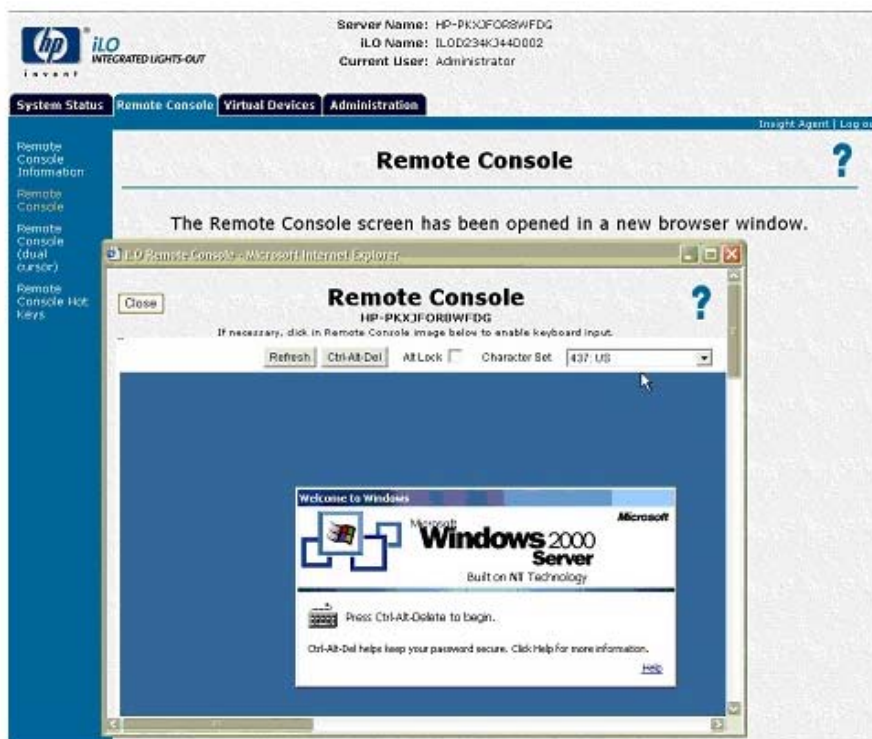
リモート コンソール オプション

[Remote Console]オプションにより、ホスト サーバのコンソールをネットワーク クライアントのブラウザに転送することができ、テキスト モード（標準）とグラフィックモードで、ビデオ、キーボード、およびマウスを利用したリモートのホスト サーバへの完全なアクセスができるようになります（iLO Advancedパックを使用して使用許諾されている場合）。

リモート コンソールを使用すれば、リモートのホスト サーバの前にいるかのようにサーバを完全に制御することができます。リモートのファイル システムとネットワーク ドライブにアクセスできます。リモート コンソールにより、リモートのホスト サーバのハードウェアとソフトウェアの設定、アプリケーションとドライバのインストール、リモート サーバの画面解像度の変更、およびリモート システムの適切なシャットダウンができます。

リモート コンソールを使用すれば、リモートのホスト サーバが再起動するときのPOSTブート メッセージを確認することができ、またROMベースのセットアップ ルーチンを起動してリモートのホスト サーバのハードウェアを設定することができます。オペレーティング システムをリモートでインストールする場合、グラフィック リモート コンソールにより（使用許諾されている場合）、インストール作業の全体をホスト サーバの画面に表示して、制御することができます。

最高のパフォーマンスを発揮するには、必ず、ホスト オペレーティング システムの画面を16ページの「グラフィック リモート コンソールのパフォーマンスの最適化」の項の説明に従って設定してください。



リモート コンソールの拡張機能

リモート コンソール アプレットには、iLOに拡張機能を提供する4つのボタンがあります。これらのボタンには、以下の機能があります。

- **Refresh** - [Remote Console]画面が最新のデータを表示していない場合があります。この場合、[Refresh]をクリックするとiLOの画面を更新することができます。
- **Ctrl-Alt-Del** - このボタンを使用して、**Ctrl+Alt+Del**のキー シーケンスをリモート コンソールに入力します。

- **Alt Lock** - [Alt Lock]ボックスを使用して、**Alt**で始まるキー シーケンスをリモート コンソール セッションからサーバに転送します。
- **Character Set** - このメニューを使用して、リモート コンソールで使用するデフォルトの文字セットを変更します。リモート コンソールの文字セットを変更することにより、文字が正しく表示されるようになります。

リモート コンソールでのシングル マウス ポインタ

リモート コンソールの機能の1つに、シングル マウス ポインタがあります。この機能は、マウス カーソルがリモート コンソール画面上にあるときは、ローカル カーソルが表示されないことを意味します。

この機能を正しく動作させるには、Internet ExplorerではJava™ 1.3.1 JVM以降、Linux ブラウザでは1.4.1 JVMをダウンロードしてクライアント マシンにインストールする必要があります。リモートのサーバでは、シングル マウス ポインタを使用するためのソフトウェアは必要ありません。Java™ 1.3.1 JVMは、HPのWebサイト<http://www.hp.com/servers/manage/jvm/>（英語）からダウンロードできます。

Linuxのユーザは、同じくHPのWebサイト<http://www.hp.com/servers/manage/jvm/>（英語）で提供される、1.4.1 Java2™ Runtime Environment, Standard Editionを使用する必要があります。

注：このサイトにアクセスすると、メイン サイトからjava.sun.comサイトに転送されます。JVMのバージョンについては、リモート コンソールのヘルプ ページで指定されているバージョンの使用をおすすめします。Internet Explorer用に指定されているバージョンは、java.sunサイトまたはマネジメントCDから入手できます。

[Remote Console Information]画面の必要なJVMをダウンロードするためのリンクも利用できます。

リモート コンソールのLinux用設定

Linuxでテキスト画面を表示するためにiLOのリモート コンソールを使用する場合、描線用の文字が正しく表示されない場合があります。

リモート コンソールのテキスト モード用の文字セットを正しく設定するには、以下の手順に従ってください。

- リモート コンソール アプレットで[Character Set]プルダウン メニューをクリックします。
- [Lat1-16]文字セットを選択します。

リモート コンソール (デュアル カーソル) モード

[Remote Console (dual cursor)]オプションを使用する場合、「リモート コンソール (45 ページ)」の項で説明したすべての機能を使用できます。このオプションを選択すると、画面上の[Remote Console (dual cursor)]フレーム内にメイン カーソルとセカンダリカーソルの2つのカーソルが表示されます。メイン カーソルがリモート コンソールのフレームを通過すると、セカンダリ カーソルはメイン カーソルの後を追います。

クライアント コンピュータのマウス カーソルは、リモート コンソール内では十字形で表示されます。iLOを使用する際に、クライアント コンピュータのマウス カーソルの位置を正確に確認するほうが好まれる場合もあります。最高のパフォーマンスを発揮するには、必ず、ホスト オペレーティング システムの画面を16ページの「グラフィック リモート コンソールのパフォーマンスの最適化」の項の説明に従って設定してください。

最新のJava™ Runtime Environmentをダウンロードしない場合は、リモート コンソールで利用できるのは[Remote Console (dual cursor)]オプションだけです。

リモート コンソール ホット キー

リモート コンソール ホット キー機能により、最大6つの複数のキーの組み合わせを定義して各ホット キーに割り当てることができます。クライアント システムのリモート コンソールでホット キーを押すと、ホット キーの代わりに、定義したキーの組み合わせ (同時に押したすべてのキー) がリモートのホスト サーバに転送されます。

リモート コンソール ホット キーを定義するには、以下の手順に従ってください。

1. [Remote Console]タブで、[Remote Console Hot Keys]をクリックします。
2. 定義したいホット キーを選択します。次に、ホット キーを押したときにホストサーバに送信されるキー シーケンスをドロップダウン ボックスを用いて選択します。
3. キー シーケンスの定義が完了したら、[Save Hot Keys]をクリックします。

[Remote Console Hot Keys]画面には、[Reset Hot Keys]オプションもあります。このオプションにより、ホット キー フィールドのすべてエントリをクリアできます。クリアされたフィールドを保存するには、[Save Hot Keys]をクリックしてください。

注：リモート コンソール ホット キーは、リモート コンソール アプレットを介したリモート コンソール セッションおよびTelnetクライアントを介したテキスト リモート コンソール セッションの実行中に使用できます。

リモート ホストのトラブルシューティング

リモートのホスト サーバの問題を解決するために、リモート システムを再起動しなければならない場合があります。[Virtual Devices]タブのオプションを使用することにより、リモートのホスト サーバを再起動できます。両方のオプションは、サーバの現在の電源ステータスを表示します。

仮想デバイス

[Remote Console]タブには、以下のオプションが用意されています。このタブを使用して、リモート仮想電源ボタン、仮想メディア、仮想インジケータの機能を実行できます。仮想メディアは、iLO Advancedパックの使用許諾を受けることによって、有効にすることができます。

仮想電源ボタン

仮想電源ボタンによって、リモート サーバの電源状態を制御できます。このボタンは、サーバ上で実際に電源ボタンを押す動作をシミュレートします。仮想電源ボタンを使用するには、使用したい電源オプションを選択して、[Virtual Power]ボタンをクリックし、電源オプションを起動します。



注：これらの機能の中には、オペレーティング システムを適切にシャットダウンしないものもあります。オペレーティング システムのシャットダウンを開始する場合は、仮想電源ボタンを使用する前に、リモート コンソールを使用してください。

ブラウザの更新機能を使用して、電源インジケータのステータスを常に最新のものにしてください。

使用できる電源オプションは、次のとおりです。

- **[Momentary Press]** - このオプションは、電源ボタンを瞬間的に押す動作をシミュレートします。現在電源が投入されているサーバの電源を切る場合や現在電源が切断されているサーバの電源を入れる場合は、通常、瞬間的に押す動作で十分です。このオプションを使用するには、**[Momentary Press]**を選択してから**[Virtual Power]**ボタンをクリックします。
- **[Press and Hold]** - このオプションにより、電源ボタンが6秒間押し続けられます。このオプションは、オペレーティング システムが瞬間的に押す動作に 응답しない場合、システムの電源を強制的に切るために役立ちます。システムを再起動するには、**[Cold Boot of system]**を選択してから**[Virtual Power]**ボタンをクリックします。これにより、システムの電源がただちに切断されます。システムは、約6秒後再起動します。サーバの電源がオフの場合、このオプションは表示されません。

注：このオプションを使用する場合、オペレーティング システムによる適切なシャットダウンは行われません。
- **[Cold Boot of system]** - このオプションは、サーバの電源を切ってから、再投入します。
- **[Warm Boot of system]** - このオプションは、サーバの電源を切らずに、サーバをリセットします。このオプションを使用するには、**[Warm Boot of system]**を選択してから、**[Virtual Power]**ボタンをクリックします。サーバの電源がオフの場合、このオプションは表示されません。

注：このオプションを使用する場合、オペレーティング システムによる適切なシャットダウンは行われません。
- **[Automatically Power On Server]** - このオプションで**[Yes]**を選択すると、AC電源が供給された時点で、サーバの電源が自動的に投入されます。サーバの電源コードをコンセントに接続したとき、あるいは停電の後UPSがアクティブになったとき、AC電源が供給されます。AC電源が供給されると、サーバの電源が自動的にオンになり、サーバの通常の起動プロセスが開始されます。

- **[Manual Override for BL p-Class]** - このオプションは、ProLiant BL p-Classサーバに接続されている場合のみ表示されます。このオプションによって、電源が不十分であることがラックから報告されている場合でも、サーバの電源を強制的に投入できます。ラックが正しく構成されていない場合やラックの通信に問題がある場合、十分な電源が供給されていてもサーバに電源が入らないことがあります。ラックに十分な電源容量があることが明らかな場合のみ、このオプションを使用してください。



注意：[Manual Override for BL p-Class]オプションを使用すると、パワー サプライから利用できる電力の制限値を超えているサーバに電源を入れることができます。利用できる電力の制限値を超えると、ラック内のすべてのサーバの電源の切断、サーバの障害、およびデータの消失または破壊が発生することがあります。構成や通信の問題を解決して、動作の信頼性を確保することをおすすめします。

仮想メディア

仮想メディアは、オプションのiLO Advanced/パックの使用許諾を受けることによって、有効にできる高度な機能です。使用許諾されていない場合は、iLO feature not licensed というメッセージが表示されます。

iLOの[Virtual Media]オプションにより、管理者は、仮想フロッピー ディスク ドライブおよび仮想CDドライブを使用できます。iLO仮想メディア デバイスは、USB技術を使用するホストサーバに接続されます。iLOの仮想メディア デバイスは、ホストシステムの起動時に使用できます。USBをサポートするオペレーティング システムに接続した場合、iLO仮想メディア デバイスはUSBを使用して新しい機能も実現できます。ホストのオペレーティング システムは、特別なHP製ドライバを実行することなく、USBをサポートするオペレーティング システム上で、iLO仮想メディア デバイスを使用できます。

オペレーティング システムの種類が異なると、USBサポートのレベルも異なります。iLO仮想メディアは、さまざまなサポート レベルに対応するように設定できます（52 ページの「オペレーティング システムのUSBサポート」を参照）。

オペレーティング システムのUSBサポート

オペレーティング システムの種類が異なると、USBサポートのレベルも異なります。iLOは、オペレーティング システムに組み込まれたUSBドライバを使用します。iLO仮想メディアのサポート レベルは、オペレーティング システムのUSBサポートのレベルの影響を受けます。一般に、物理USBディスク ドライブに影響を与えるオペレーティング システムの問題は、iLO仮想メディアにも影響します。

サーバ起動時の仮想フロッピーのサポートは、HP製サーバのROMにより提供されま
す。起動時には、サーバのオペレーティング システムとは関係なく、仮想フロッピー
を使用できます。

次のサーバ オペレーティング システムは、USBメディアをサポートしていないので、
オペレーティング システムの稼動中は仮想フロッピーにアクセスできません。

- Microsoft® Windows NT® 4.0
- Linux Red Hat (7.2より前のバージョン)
- SuSE Linux (7.0より前のバージョン)
- Novell NetWare 5.xおよび6

一部のLinuxオペレーティング システムは、オペレーティング システムのインストー
ル時にUSBの仮想フロッピー ドライブを正しくサポートしていません。次のLinuxオ
ペレーティング システムのインストール時に、iLOの仮想メディアは、使用しないで
ください。

- Linux Red Hat 7.2 Professional
- SuSE Linux 7.0

Windows® 95 OSR 1は、USBデバイスをサポートしません。このため、SmartStart 5.x
CDをiLO仮想メディアで使用することはできません。

次の表に、オペレーティング システムのUSB機能および対応するiLOの仮想メディア
機能を示します。

	NetWare	SuSE (7.0よ り前)	Red Hat (7.2よ り前)	Red Hat 7.2 SuSE 7.0	Windows NT®	Windows® 2000	Windows® Server 2003

	NetWare	SuSE (7.0より前)	Red Hat (7.2より前)	Red Hat 7.2 SuSE 7.0	Windows NT®	Windows® 2000	Windows® Server 2003
オペレーティング システム ロード前のサーバの起動時の USB ディスケットの使用	あり	あり	あり	あり	あり	あり	あり
USB ディスケットを使用したオペレー ティング システムのインス トール	なし	なし	なし	なし	なし	あり	あり
USB CDを使用したオペレー ティング システムのインス トール	なし	なし	なし	なし	なし	あり	あり
オペレーティング システム 稼働時のUSB ディスクの使用	なし、 NW6.5の場合 はあり	なし	なし	あり	なし	あり	あり

iLO仮想メディア デバイスの使用

iLO仮想メディア デバイスを使用するには、[Virtual Devices]タブの[Virtual Media]オプションを選択します。アプレットがロードされ、仮想フロッピーまたは仮想CD-ROMデバイスを選択できるようになります。

仮想メディア アプレットがサポートするモードは、4つあります。仮想メディア アプレットの[Configure]ボタンをクリックして、目的の動作モードを選択してください。4つのモードは、次のとおりです。

- フロッピーのみ - このモードでは、仮想フロッピー ディスクのみを使用できます。
- CD-ROMのみ - このモードでは、仮想CD-ROMディスクのみを使用できます。
- 自動 - 自動モードでは、最後に選択されたデバイスが使用できるデバイスになります。一度に、両方のデバイス（仮想フロッピーまたは仮想CD）を選択することはできません。

- コンボジット - コンボジット モードでは、一方または両方のデバイスを選択できます。両方のデバイスを選択すると、両方のデバイスを同時に使用できます。コンボジット モードでは、CD-ROMもディスクとも、クライアント マシン上でローカルで使用することはできません。一部のオペレーティング システムでは、コンボジット モードはサポートされません。
 - BIOSおよびDOS[®]は、コンボジット モードをサポートします。
 - Windows[®] 2000、Windows[®] 2000 SP1、SP2は、大容量記憶装置を対象にしたコンボジット モードをサポートしません。大容量記憶装置を含むコンボジット デバイス構成を使用すると、大容量記憶装置を使用できなくなります。
 - Windows[®] 2000 SP3は、コンボジット モードをサポートします。
 - Windows[®] Server 2003は、コンボジット モードをサポートします。
 - Linuxはコンボジット モードをサポートします。ただし、ご使用のコンボジット デバイスに複数の大容量記憶装置が含まれる場合は、サポートしません。複数の大容量記憶装置を含むコンボジット デバイスには、切断と再接続の問題が発生します。コンボジット モードは、キーボード、マウス、ディスクなどコンボジット デバイスとしてサポートします。

iLO仮想フロッピー

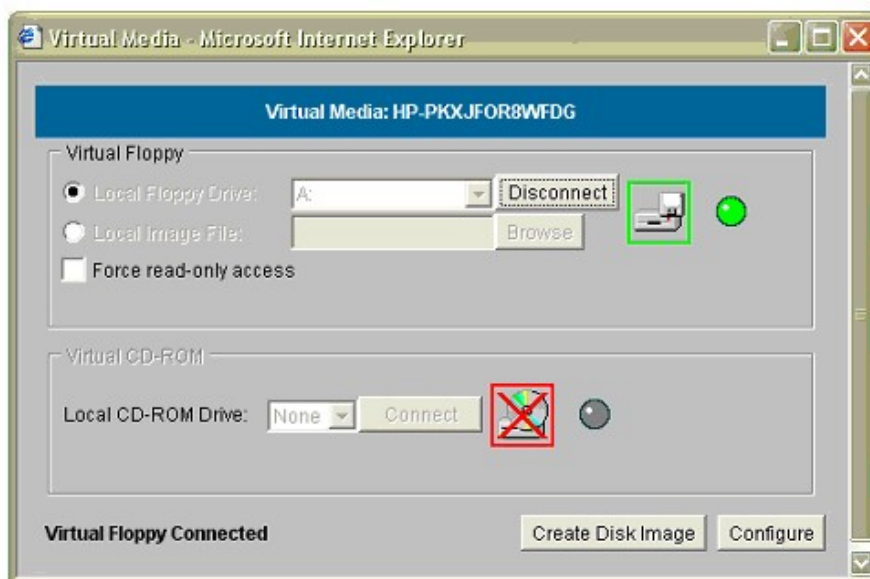
iLO仮想フロッピー ディスクは、すべてのオペレーティング システムで、サーバの起動時に使用できます。iLO仮想フロッピーから起動することにより、ホスト システムのROMのアップグレード、ネットワーク ドライブからのオペレーティング システムのインストール、障害の発生したオペレーティング システムのディザスタ リカバリなどの作業を実行できます。

ホスト サーバのオペレーティング システムがUSBの大容量記憶装置をサポートする場合、ホスト サーバのオペレーティング システムをロードした後にも、iLO仮想フロッピーを使用できます。iLO仮想フロッピーは、ホスト サーバのオペレーティング システムの実行中に、デバイス ドライバのアップグレード、緊急時修復ディスクの作成などの作業に使用できます。サーバの実行時に仮想フロッピーを使用できるようにしておくと、管理者がネットワーク インタフェース コントローラ ドライバを使用して診断を行い、問題を修復する必要がある場合に、特に役立てることができます。

仮想デバイスは、Webブラウザを実行しているマシン上の物理的なディスク ドライブである場合があります。また、仮想デバイスは、ローカルのハードディスク ドライブまたはネットワーク ドライブに保存されているイメージ ファイルの場合もあります。パフォーマンスを最高にするには、高速ネットワーク リンクを介してアクセスできるクライアントPCのハードディスク ドライブまたはネットワーク ドライブに格納されているローカルのイメージ ファイルの使用をおすすめします。

クライアントPCの物理ディスク ドライブを使用するには、以下の手順に従ってください。

1. **[Local Floppy Drive]**を選択します。
2. ドロップダウン メニューから、クライアントPC上の使用するディスク ドライブのドライブ文字を選択します。
3. **[Connect]**をクリックします。



イメージ ファイルを使用するには、以下の手順に従ってください。

1. **仮想メディア** アプレットの仮想フロッピー セクションで**[Local Image File]**を選択します。
2. テキスト ボックスにディスク イメージの名前を入力します。 **[Browse]**を使用して、イメージ ファイルを検索することもできます。
3. **[Connect]**をクリックします。

接続が完了したら、**仮想メディア** アプレットを閉じるまで、ホスト サーバは仮想デバイスを使用できます。仮想フロッピーの使用が終了したら、ホスト サーバからデバイスを切断するかまたはアプレットを終了することができます。

注：仮想メディア デバイスを継続して使用する場合は、ブラウザ上で仮想メディア アプレットを開いたままにする必要があります。

iLO仮想メディア フロッピーは、ホスト サーバのオペレーティング システムがUSBのディスク ドライブをサポートしている場合、稼働中のホスト サーバで使用できます。このガイドの発表時では、Windows® 2000およびLinuxオペレーティング システムがUSBのディスク ドライブをサポートしています。

図に示したように、オペレーティング システムからは、iLOの仮想フロッピーは別のディスク ドライブのように見えます。この例では、Bドライブとして接続されている仮想フロッピーを使用するiLOの例を示します。

注：iLO仮想メディア機能を初めて使用する場合、ホスト オペレーティング システムが、新しいハードウェアの検出ウィザードを実行するよう指示する場合があります。

注：iLO仮想メディア機能を切断するとき、ホスト オペレーティング システムからデバイスが安全に取り外されていないという警告メッセージを受け取る場合があります。仮想メディア機能からデバイスを切断する前に、デバイスを停止するためのオペレーティング システム提供の機能を使用することにより、この警告を避けることができます。

iLO仮想フロッピー イメージの作成

iLO仮想メディア機能を使用することにより、同じアプレット内でディスク イメージ ファイルを作成できます。ディスクからイメージ ファイルを作成することも、既存のイメージ ファイルからディスクを作成することもできます。iLO仮想フロッピーは、イメージ ファイルを使用するほうが高速に機能します。

仮想メディア イメージ ファイルを作成するには、以下の手順に従ってください。

1. **[Create Disk Image]**をクリックします。
2. ドライブ文字とイメージ ファイルの名前を選択します。**参照**機能を使用して、既存のイメージ ファイルを検索し選択することができます。また、イメージ ファイルが作成されるディレクトリを変更することもできます。
3. **[Create]**をクリックします。仮想メディア アプレットは、イメージ ファイルの作成プロセスを開始します。進行状況表示バーが100%になると、プロセスは完了します。

[Disk >> Image]をクリックすると、**[Image >> Disk]**に変わります。物理ディスクからイメージ ファイルを作成する手順をイメージ ファイルから物理ディスクを作成する手順に切り替えるには、このボタンを使用します。

LinuxでUSB仮想メディア フロッピーをマウントする

1. ブラウザを介してiLOにアクセスします。
2. **[Virtual Devices]**タブの**[Virtual Media]**をクリックします。
3. 使用するディスク ドライブまたはディスク イメージを選択して、**[Connect]**をクリックします。
4. 以下のコマンドを使用して、USBドライバをロードします。

```
modprobe usbcore  
modprobe usb-storage  
modprobe usb-ohci
```

5. 以下のコマンドを使用して、SCSI ディスク ドライバをロードします。

```
modprobe sd_mod
```
6. 以下のコマンドを使用して、ディスク ドライブをマウントします。

```
mount /dev/sda /mnt/floppy -t vfat
```

注：別の種類のファイル システムについては、`man mount`コマンドを使用してください。

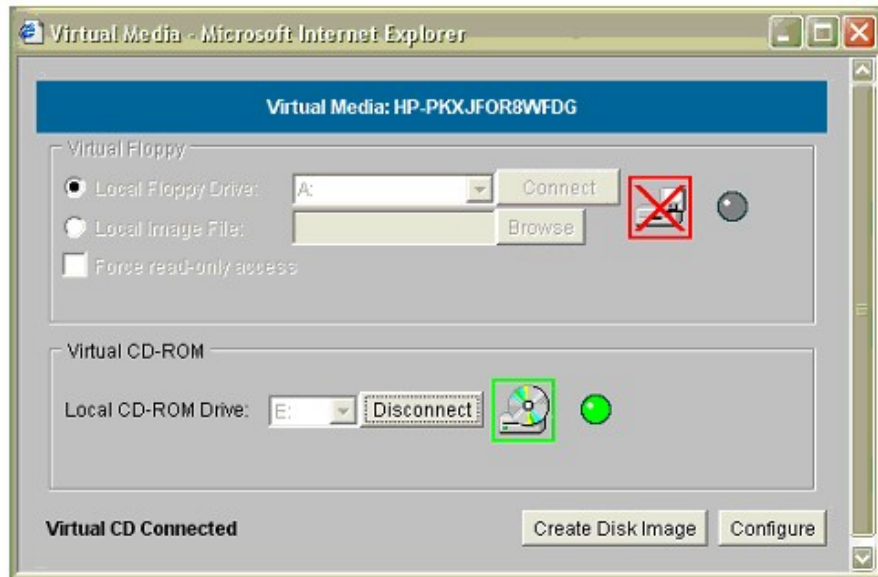
iLOの仮想CD-ROM

iLO仮想CDを使用するには、**[Virtual Devices]**タブの**[Virtual Media]**オプションを選択します。アプレットが仮想CD デバイスをロードします。

クライアントPCの物理ディスク ドライブを使用するには、以下の手順に従ってください。

1. **[Local CD-ROM Drive]**を選択します。
2. ドロップダウン メニューから、クライアントPC上の使用するCD-ROMドライブのドライブ文字を選択します。

3. [Connect]をクリックします。



LinuxでUSB仮想メディアCD-ROMをマウントする

1. ブラウザを介してiLOにアクセスします。
2. [Virtual Devices]タブの[Virtual Media]をクリックします。
3. 使用するCD-ROMを選択して、[Connect]をクリックします。
4. 以下のコマンドを使用して、USBドライバをロードします。

```
modprobe usbcore
modprobe usb-storage
modprobe usb-ohci
```
5. 以下のコマンドを使用して、SCSI CD-ROMディスクドライバをロードします。

```
modprobe sr_mod
```
6. 以下のコマンドを使用して、ディスクドライブをマウントします。

```
mount /dev/scd0 /mnt/cdrom -t iso9660
```

注：別の種類のファイル システムについては、`man mount`コマンドを使用してください。

仮想メディア アプレットのタイムアウト

仮想メディアがホスト サーバに接続されている場合、仮想メディア アプレットがタイムアウトすることはありません。ユーザがログアウトした場合でも、仮想メディア アプレットが接続を維持するため、ホスト サーバは仮想メディアにアクセスできます。ただし、仮想メディアが接続されていない場合は、仮想メディア アプレットはタイムアウトします。仮想メディアをホスト サーバに接続せずに仮想メディア アプレットを起動した場合またはアプレットの使用後に仮想メディアを切断した場合は、制限時間が経過する前に再接続しないと仮想メディア アプレットは終了します。タイムアウト値は、[Global Settings]画面の[Idle Connection Timeout (minutes)]フィールドで設定した値と同じ値になります。アイドル時の接続タイムアウトが起きると、仮想メディアが接続されていない場合は、ユーザはログアウトされ仮想メディア アプレットは閉じられます。

iLO仮想メディア権限

iLO仮想メディアを使用する機能は、iLOユーザ権限により制限されます。仮想メディア デバイスを選択してホスト サーバに接続するには、認証されたユーザが仮想メディアの権限を持つ必要があります。

重要： iLO仮想フロッピーを使用して、ROMPaqディスクットからiLOのファームウェアをアップグレードしないでください。iLOのファームウェアをリモートでアップグレードする場合は、[Administration]タブの[Upgrade iLO Firmware]オプションの使用をおすすめします。

仮想シリアル ポート

仮想シリアル ポートは、サーバのシリアル ポートへの接続を可能にするJava™アプレットを提供します。Java™アプレットにより、シリアル ポート用に設定されたアプリケーションへのアクセスを可能にするVT320端末エミュレーション機能を使用できるようになります。

Windows EMSコンソール

Windows® Server 2003の機能の1つがEMSです。一般には、EMSコンソールは、サーバにシリアル ケーブルを物理的に接続して使用します。ただし、iLOを使用すると、EMSをネットワーク経由でWebブラウザを介して使用できます。Microsoft® EMSにより、ユーザは、実行中のプロセスの表示、プロセスの優先順位の変更、およびプロセスの停止といった機能を使用できます。EMSコンソールとiLOのリモート コンソールは、同時に使用できます。

Windows® EMSコンソールが有効になっていると、ビデオ、デバイス ドライバなどオペレーティング システム機能が原因で通常の動作や通常の修正処置が実行できない場合に、この機能を使用してEMSを実行できます。

Windows® EMSシリアル ポートを、ホスト システムのRBSUを使用して有効にしておく必要があります。RBSUの設定では、EMSポートの有効化/無効化、およびCOMポートの選択を行うことができます。iLOシステムは、EMSポートの有効/無効、COMポートの選択を自動的に検出します。

SAC>プロンプトが表示されるようにするには、仮想シリアル ポート コンソールを介して接続した後で、Enterとタイプする必要がある場合があります。

EMSの機能の使用方法について詳しくは、Windows® Server 2003のマニュアルを参照してください。

セキュリティ情報

[Remote Console Data Configuration]を有効にすると、仮想シリアル ポートのデータがiLOシステムと表示用のアプレット間で転送される際に、データ ストリームが暗号化されます。

仮想インジケータ

iLOは、ユニットID LEDのステータスを監視して制御する機能を提供します。ユニットID LEDはHP製サーバの青色のLEDで、サーバを多数搭載したラック内でシステムを識別するために使用されます。iLOは、iLOのWebページを使用して、ユニットID LEDのステータスを表示し、ステータスを変更する機能を提供します。

また、ユニットID LEDは、サーバ上で重大なリモート管理タスクがアクティブになるといつでも点滅します。ユニットID LEDの点滅は、サーバが現在、中断してはならない動作の最中であることを示します。ユニットID LEDの点滅中は、絶対にサーバの電源を切らないでください。

ユニットID LEDは、iLOリモート コンソールによるサーバの制御がアクティブのとき、iLOの設定をXMLスクリプト機能を使用して変更しているとき、およびiLOのファームウェアの更新中に点滅します。

管理

[Administration]タブで使用できるオプションでは、ユーザの設定、Insightマネージャ7との統合によるSNMPアラートの通知、セキュリティ設定、およびネットワーク環境設定を管理できます。このセクションには、ファームウェア アップグレードのオプションも設けられているので、iLOを常に最新の状態にすることができます。

ユーザ管理

[User Administration]により、安全なiLOメモリにローカルで保存されているユーザ アカウントを管理できます。ディレクトリ ユーザのアカウントは、MMCまたはConsoleOneスナップインを使用して管理します。[User Administration]を使用して、新規ユーザの追加、既存のユーザ設定の表示や変更、またはユーザの削除を実行できます。

注：すべてのLights-Outマネジメント デバイス上で共通なディレクトリ サーバ アーキテクチャを実現するために、iLOファームウェア バージョン1.40は、以前のバージョンとは異なるユーザ権限を備えています。

新規ユーザの追加

重要：管理者ユーザ アカウント権限を持つユーザだけがiLO上の他のユーザを管理できます。

各ユーザに個別のアクセス権限を割り当てることができます。各ユーザは、ユーザが実行する必要のある作業用に指定された固有の権限セットを持つことができます。リモート コンソール、ユーザの管理、仮想電源ボタンなど、重大な機能へのアクセスは、拒否することができます。

iLOは、最大12ユーザの設定をサポートします。ログインはトラッキングされ、失敗したときはログに記録されます。ログインに失敗した場合にInsightマネージャ7を実行するリモート管理用PCにアラートを発生させるオプションを選択できます。iLOは、LAN用のすべてのセキュリティ機能およびパスワードの暗号化をサポートします。

iLO Advanced 1.40以降では、ディレクトリベースのユーザ アカウントとの統合が実現しているため、12を超えるユーザをサポートできます。これにより、ユーザ アカウント数の制限が実質的になくなります。

新しいユーザをiLOに追加するには、以下の手順に従ってください。

1. 管理者ユーザ アカウント権限を持つアカウントを使用して、iLOにログオンします。[Administration]をクリックします。

2. [User Administration]をクリックします。図に示すような画面が表示されます。



3. [Add]をクリックします。
4. 追加しようとするユーザについて必要な情報をフィールドに指定します。
5. ユーザのプロファイルの入力が完了したら、[Save User Information]をクリックして[User Administration]画面に戻ります。新しいユーザの指定中にユーザのプロファイルのフォームを消去するには、[Restore User Information]をクリックしてください。

既存のユーザ設定の表示または変更

重要：管理者ユーザ アカウント権限を持つユーザだけがiLO上の他のユーザを管理できます。すべてのユーザは、[View/Modify User]機能を使用して、自身のパスワードを変更できます。

既存ユーザの情報を表示または変更するには、以下の手順に従ってください。

1. 管理者ユーザ アカウント権限を持つアカウントを使用して、iLOにログオンします。[Administration]をクリックします。
2. [User Administration]をクリックし、情報を変更したいユーザ名をリストから選択します。
3. [View/Modify User]をクリックします。

4. 変更が必要なフィールドで、ユーザ情報を変更します。フィールドの変更が終了すると、[Save User Information]をクリックして[User Administration]画面に戻ります。元のユーザ情報を復元するには、[Restore User Information]をクリックしてください。プロファイルに対して行った変更はすべて破棄されます。

ユーザの削除

重要：管理者ユーザ アカウント権限を持つユーザだけがiLO上の他のユーザを管理できます。

既存のユーザ情報を削除するには、以下の手順に従ってください。

1. 管理者ユーザ アカウント権限を持つアカウントを使用して、iLOにログオンします。[Administration]をクリックします。
2. [User Administration]をクリックし、情報を変更したいユーザ名をリストから選択します。
3. [Delete User]をクリックします。ポップアップ ウィンドウが表示され、「Are you sure you want to delete the selected user?」というメッセージが表示されます。[OK]をクリックします。

ネットワーク設定

[Network Settings]オプションにより、NICの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て変更することができます。この画面から、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については、静的なIPアドレスを設定できます。

iLOのネットワーク設定を変更するには、以下の手順に従ってください。

1. iLOの設定権限を持つアカウントを使用してiLOにログオンします。[Administration]をクリックします。

重要：これらの設定を変更できるのは、iLOの設定権限を持つユーザだけです。iLOの設定権限を持たないユーザは、割り当てられた設定の表示だけが可能です。
2. [Network Settings]をクリックします。

3. 必要に応じてフィールドに選択内容を入力することにより、ネットワーク設定を変更します。パラメータ（216ページ「ネットワーク設定のパラメータ」を参照）の変更が終われば、[Apply]をクリックして変更を完了します。

The screenshot displays the HP iLO Network Settings interface. At the top, the HP iLO logo and 'INTEGRATED LIGHTS-OUT' text are visible. The page header shows the Server Name (HP-PKXJFOR8WFDG), iLO Name (ILOD234KJ44D002), and Current User (Administrator). The navigation bar includes tabs for System Status, Remote Console, Virtual Devices, and Administration. The left sidebar lists various settings categories: User Administration, Global Settings, Network Settings, iLO Manager Settings, Upgrade iLO, Firmware, Licensing, Certificate Administration, and Directory Settings. The main content area is titled 'Network Settings' and contains two sections: 'Standard Configuration Parameters' and 'Advanced Configuration Parameters'. The 'Standard' section includes radio button options for 'Enable NIC', 'Transceiver Speed Autoselect', 'Speed' (10 Mbps/s or 100 Mbps/s), 'Duplex' (Half or Full), 'Enable DHCP', and several 'Use DHCP Supplied' options for Gateway, DNS Servers, WINS Servers, Static Routes, Domain Name, Register With WINS Server, Register With DDNS Server, and Ping Gateway on Startup. The 'Advanced' section includes text input fields for 'IP Address' (16.100.241.130), 'Subnet Mask' (255.255.252.0), 'Gateway IP Address' (16.100.240.1), 'iLO Subsystem Name' (ILOD234KJ44D002), 'Domain Name' (americaes.cpqcorp.net), 'DHCP Server' (16.110.251.250), 'Primary DNS Server' (16.110.251.242), 'Secondary DNS Server' (16.110.251.243), and 'Tertiary DNS Server' (16.103.131.242).

[Apply]をクリックすると、iLOが再起動され、ブラウザからiLOへの接続が切断されます。接続を再確立するには、60秒待ってから、再びWebブラウザのセッションを立て上げてiLOにログインします。

iLO診断ポートの設定パラメータ

ProLiant BL p-Classサーバのフロント パネルのiLO診断ポートに診断ケーブルを接続することにより、サーバの問題にアクセスしてトラブルシューティングを実行できます。iLOの診断ポートは、静的IPアドレスを使用します。iLOの診断ポートは、IPアドレスの取得にDHCPを使用したり、WINSや動的DNSに登録したり、ゲートウェイを使用したりすることはありません。標準のiLOネットワーク ポートのネットワーク パフォーマンスの低下の原因となるため、ネットワーク接続を利用しないときは、診断ポートのケーブルは、必ず、抜き取ってください。

[Network Settings]では、特定の診断ポート情報を設定できます。診断ポートと診断ケーブルの使用法について詳しくは、ブレード サーバのセットアップ/インストール ション ガイドを参照してください。

診断ポート用に設定できるフィールドは、次のとおりです。

注：診断ポートを使用できるかどうかは、[Enable NIC]フィールドで制御します。[Enable NIC]をYesに設定すると、診断ポートは有効になります。

[Transceiver Speed Autoselect]

自動選択は、インタフェースの速度を検出して10Mbpsまたは100Mbpsで動作するようにインタフェースを設定し、さらに半二重/全二重を設定します。必要に応じて、このパラメータを手動選択に設定し、速度とデュプレックス（半二重/全二重）の設定を手動で調整するようにできます。

[Speed]

トランシーバ速度の自動選択が有効でない場合、この設定を使用して、10Mbpsまたは100Mbpsの接続速度を割り当てます。

[Duplex]

トランシーバ速度の自動選択が有効でない場合、この設定を使用して、デュプレックス（半二重/全二重）をNICに割り当てます。

[IP Address]

このパラメータを使用して、iLOの診断ポートにネットワーク上で静的IPアドレスを割り当てます。デフォルトでは、すべてのiLO診断ポートのIPアドレスは192.168.1.1です。

[Subnet Mask]

このサブネット マスク パラメータを使用して、iLOの診断ポートのサブネット マスクを割り当てます。デフォルトでは、すべてのiLOの診断ポートのサブネット マスクは255.255.255.0です。

有効なネットワーク ケーブルが診断ポートに接続されると、診断ポートが使用されることが自動的に検知されます。診断ポートとバック ポートの間の切り替えが行われる際、ネットワークの切り替えが完了するまで90秒の余裕をみておく必要があります。その後、Webブラウザを介した接続を試みてください。

注：リモート コンソール セッションがアクティブな場合やファームウェアの更新が行われているときは、診断ポートの切り替えは行われません。

グローバル設定

[Global Settings]オプションにより、iLOのセキュリティ設定を表示して変更することができます。この画面では、リモート コンソールのタイムアウト、iLO Webサーバで使用するiLOポート、リモート コンソール、および仮想メディアを設定できます。これらの設定は、個々のユーザの設定とは関係なく、グローバルに適用されます。

重要：これらの設定を変更できるのは、iLOの設定権限を持つユーザだけです。iLOの設定権限を持たないユーザは、割り当てられた設定の表示だけが可能です。

Server Name: HP-P100FOR8WFDG
iLO Name: ILOD234KJ44D002
Current User: Administrator

System Status Remote Console Virtual Devices Administration

User Administration
Global Settings
Network Settings
SNMP/Insight Manager Settings
Upgrade iLO Firmware
Licensing
Certificate Administration
Directory Settings

Global Settings

Security Settings

Idle Connection Timeout (minutes): 15

Enable Lights-Out Functionality: ☒ Yes ☐ No

Enable iLO ROM-Based Setup Utility: ☒ Yes ☐ No

Require Login for iLO RBSU: ☐ Yes ☒ No

Remote Console Port Configuration: ☐ Enabled ☐ Disabled ☒ Automatic

Remote Console Data Encryption: ☐ Yes ☒ No

SSL Encryption Strength: 128-bit

Current Cipher: RC4-MD5 with 128 bit encryption

Web Server Non-SSL Port: 80

Web Server SSL Port: 443

Virtual Media Port: 17988

Remote Console Port: 23

Minimum Password Length: 0

NOTE: The Integrated Lights-Out subsystem must be restarted before any port changes you make on this screen will take effect. Pressing the Apply button below terminates your browser connection and restarts Integrated Lights-Out if any changes have been made to port settings. In this case you must wait at least 30 seconds before attempting to reestablish a connection with Integrated Lights-Out.

Apply

[Global Settings]オプションにより、次の機能を定義できます。

[Idle Connection Timeout (Minutes)]

このオプションで指定した時間内（分単位）にユーザが操作を行わない場合、Webサーバセッションおよびリモートコンソールセッションは自動的に終了します。

[Enable Lights-Out Functionality]

このオプションにより、iLOに接続できます。無効にすると、iLOへのすべての接続が拒否されます。デフォルト設定は、Yesです。

- 内蔵Lights-Outの機能が無効になっている場合、iLOの10/100ネットワークおよびオペレーティングシステム ドライバとの通信は切断されます。ProLiant BL p-Class サーバ用のiLO診断ポートも無効になります。
- iLO診断ポートを含むiLOの機能が無効になっている場合、iLOの機能を有効にするには、サーバのセキュリティ オーバーライド スイッチを使用する必要があります。サーバのマニュアルに従って、セキュリティ オーバーライド スイッチの位置を確認し、スイッチをオーバーライド位置に設定します。サーバの電源を入れ、iLOのRBSUを使用して[Enable Lights-Out Functionality]を設定します。

[Enable iLO ROM-Based Setup Utility]

このオプションにより、ホストに物理アクセスまたは仮想アクセスするユーザは、そのシステムのiLOを、iLOのRBSUを使用して設定できます。RBSUは、ホストシステムが再起動して、POSTの実行中に起動されます。デフォルト設定は、Yesです。

[Require Login for iLO RBSU]設定を使用して、RBSUへのアクセスを許可されたユーザだけに限定することもできます。

注：セキュリティ用のジャンパが物理的に設定されている場合、再起動中に、RBSUのプロンプトが表示されます。

[Require Login for iLO RBSU]

このオプションは、ユーザがiLOのRBSUにアクセスする際に、ログイン名とパスワードの入力を求められるかどうかを指定します。デフォルト設定は、Noです。

[Remote Console Port Configuration]

このオプションにより、ポート アドレスの設定を有効または無効にします。このオプションを**Enabled**に設定すると、Telnetおよびリモート コンソール アプレットによるiLOへのアクセスが可能になります。**Disabled**に設定すると、Telnetおよびリモート コンソール アプレットによるiLOへのアクセスができなくなります。Telnetを使用してテキストベースのリモート コンソールにアクセスする場合は、[Remote Console Data Encryption]をNoに設定する必要があります。

[Remote Console Data Encryption]

このオプションにより、リモート コンソール データの暗号化を有効にします。標準的なTelnetクライアントを使用してiLOにアクセスする場合は、Noに設定する必要があります。

[SSL Encryption Strength]

このオプションは、現在の暗号化強度設定を表示します。最も安全な設定は、128-bit (High)です。

[Current Cipher]

このオプションは、ブラウザとiLOとの間でデータを転送する際に、データを保護するために現在使用されている暗号化アルゴリズムを表示します。

[Web Server Non-SSL Port]

デフォルトでは、iLOに内蔵のWebサーバは、非暗号化通信用にポート80を使用するように設定されています。このポートは、[Administration]タブの[Global Settings]オプションで設定できます。

[Web Server SSL Port]

デフォルトでは、iLOに内蔵のWebサーバは暗号化通信用にポート443を使用するように設定されています。このポートは、[Administration]タブの[Global Settings]オプションで設定できます。

[Virtual Media Port]

iLOの仮想メディア サポートは、通信用に設定可能なポートを使用します。このポートは、[Administration]タブの[Global Settings]オプションで設定できます。デフォルトでは、ポート17988を使用するように設定されています。

[Remote Console Port]

デフォルトでは、iLOのリモート コンソールは、リモート コンソール通信用にポート23を使用するように設定されています。このポートは、[Administration]タブの[Global Settings]オプションで設定できます。

[Minimum Password Length]

このオプションにより、ユーザ パスワードの設定または変更の際に許可される文字の最小数を指定します。文字数は、0 ~ 39の任意の値に設定できます。デフォルト設定は、8文字です。

SNMP/Insightマネージャの設定

[SNMP/Insight Manager Settings]オプションを使用して、SNMPアラートの設定、テストアラートの生成、およびInsightマネージャ7との統合の設定を実行できます。

SNMPアラートの有効化

iLOは、SNMPトラップを受信する最大3つのTCP/IPアドレスをサポートします。通常、このアドレスはInsightマネージャ7サーバ コンソールのTCP/IPアドレスと同じになります。

重要：これらの設定を変更できるのは、iLOの設定権限を持つユーザだけです。iLOの設定権限を持たないユーザは、割り当てられた設定の表示だけが可能です。

[SNMP/Insight Manager Settings]画面では、次の2つのアラート オプションを使用できます。

- **[Enable iLO SNMP Alerts]** - このSNMPアラートは、iLOによって生成されるもので、ホスト サーバのオペレーティング システムには依存しません。このアラートには、ホスト サーバの電源切断やホスト サーバのリセットなど、主要なイベントが含まれます。また、許可のないログイン試行など、iLOのイベントも含まれます。これらのアラートは、InsightマネージャのSNMPトラップの形式をとります。
- **[Forward Insight Manager Agent SNMP Alerts]** - このアラートは、サポートされている各ネットワーク オペレーティング システムに設けられたInsightマネジメントエージェントによって生成されます。アラートを受信するには、これらのエージェントをホスト サーバにインストールする必要があります。iLOは、アラートをInsightマネージャ7に転送します。

アラートを設定するには、以下の手順に従ってください。

1. iLOの設定権限を持つアカウントを使用してiLOにログオンします。

2. [Administration]タブにある[SNMP/Insight Manager Settings]をクリックします。
次のような画面が表示されます。

3. SNMPトラップを受信する最大3つのTCP/IPアドレスを入力します。
4. iLOがサポートするアラート オプションを選択します。
5. [Apply Settings]をクリックします。

テスト アラートの生成

テスト アラートは、iLOナビゲーション フレームの[Administration]セクションにある[SNMP/Insight Manager Settings]によって生成されます。このアラートには、InsightマネージャのSNMPトラップが含まれるので、Insightマネージャ7でiLOのネットワーク接続を確認するのに使用できます。iLOの設定権限を持つユーザだけが、テスト アラートを送信できます。

テスト アラートを送信する前に、[Apply Settings]をクリックして、[SNMP Alert Destination(s)]に対して行った変更を保存してください。

テスト アラートを送信するには、以下の手順に従ってください。

1. [Administration]タブにある[SNMP/Insight Manager Settings]をクリックします。

2. [Send Test Alert]をクリックしてテスト アラートを生成し、[SNMP Alert Destination(s)]フィールドに保存したTCP/IPアドレスに送信します。
3. アラートの生成後、確認の画面が表示されます。
4. Insightマネージャ7のコンソールを調べて、トラップの受信を確認します。

Insightマネージャ7の統合

iLOでは、InsightマネージャのWebエージェントが動作しているホスト サーバのURL（DNS名またはIPアドレス）を設定することができます。また、Insightマネージャ7の識別情報で返されるデータのレベルも設定することができます。

[Insight Manager Web Agent URL]フィールドでは、InsightマネージャのWebエージェントが動作しているホスト サーバのIPアドレスまたはDNS名を入力できます。このデータをフィールドに入力すると、iLOは、iLOのWebページからWebエージェントのページへのリンクを作成することができます。

注：[Insight Manager Web Agent URL]フィールドには、IPアドレスまたはDNS名だけを入力することをおすすめします。プロトコル（例：http://）やポートID（例：2301）は、入力しないでください。

Insight Webエージェントへのリンクは、青いヘッダー バーの'Log out'リンクの横にあります。

[Level of Data Returned]フィールドでは、Insightマネージャ7に返す情報の量を制御できます。この情報は、マネジメント プロセッサをサーバに対応させるために使用され、Insightマネージャ7のiLOの概要ページに表示されます。

iLOファームウェアのアップグレード

ファームウェアをアップグレードすると、iLOの機能が向上します。ファームウェアのアップグレードは、標準的なWebブラウザを使用して任意のネットワーク クライアントから実行できます。iLOファームウェアのアップグレード権限を持つユーザだけがiLOのファームウェアをアップグレードできます。iLOの最新のファームウェアは、HPのWebサイトから入手できます。標準的なWebブラウザを使用して、iLOのファームウェアをアップグレードするには、以下の手順に従ってください。

1. iLOファームウェアをアップグレードする権限を持つアカウントを使用してiLOにログインします。

2. [Administration]タブにある[Upgrade iLO Firmware]をクリックします。次のような画面が表示されます。



3. [New firmware image]フィールドにファイル名を入力するか、またはファイルを参照します。[Send firmware image]をクリックします。
4. ファームウェアのアップグレードは、数分かかります。進行状況バーには、ファームウェアの更新の進行状況が表示されます。

重要： iLOのファームウェア アップグレードを、実行中に中断しないでください。

ファームウェアが正常にアップグレードされると、iLOシステムは自動的にリセットされます。ホスト オペレーティング システムおよびサーバは、iLOシステムのリセットによる影響を受けません。



警告：バージョン1.40にアップグレードした後で以前のバージョンにダウングレードすると、設定データが失われる場合があります。ファームウェア バージョン1.40から他のバージョンにダウングレードする場合は、事前に、設定データのバックアップをとっておくことをおすすめします。

ファームウェアのアップグレードが中断された場合やアップグレードに失敗した場合は、ただちに、再度、アップグレードを試みてください。ファームウェア アップグレードを再度試みる前に、iLOシステムをリセットしないでください。iLOは、ファームウェアのアップグレードが中断された場合やアップグレードに失敗した場合、FTPベースのファームウェア アップグレードによるディザスタ リカバリ（239ページの「iLOのファームウェアをアップグレードできない」を参照）を提供します。

注：ディスク ドライブを搭載したシステムでは、ROMPaqディスクを使用してiLOのファームウェアを更新することもできます。仮想メディア フロッピー ディスクを使用したiLOファームウェアの更新はおすすめできません。

使用許諾

[iLO Advanced License Activation]ページは、iLO Advancedパックのライセンス アクティベーションを適用するために使用されます。アクティベーション キーを入力して高度な機能を有効にする手順については、18ページの「iLOの高度な機能の有効化」の項で説明しています。

証明書管理

[Certificate Information]には、保管された証明書に関する情報が表示されます。証明書上では、情報はCAによって暗号化されていますが、iLOによって取り出され表示されます。

- [Issued To]は、証明書の発行先を示します。
- [Issued By]は、証明書を発行したCAを示します。
- [Valid From]は、証明書の有効期限の開始日を示します。
- [Valid Until]は、証明書の有効期限の終了日を示します。
- [Serial Number]は、CAによって割り当てられた証明書のシリアル番号を示します。

[Importing a Certificate]は、証明書のインポート方法に関する情報を表示します。証明書のインポートについては、93ページの「内蔵Lights-Outのセキュリティ」の項の「電子証明書」（97ページ）を参照してください。

ディレクトリ設定

[Directory Settings]画面では、ディレクトリ サービスの設定およびテストを行えます。ディレクトリについて詳しくは、99ページの「ディレクトリ サービス」の項を参照してください。ディレクトリの設定パラメータについて詳しくは、135ページの「ディレクトリの設定」の項を参照してください。

ProLiant BL p-Class

[BL p-Class]タブでは、ProLiant BL p-Classブレード サーバのラックの特定の設定を制御できます。iLOは、ProLiant BL p-Classサーバ ラックのWebベースの診断機能も提供します。診断結果は、[BL p-Class]タブの下に表示される4つのWebページに示されます。

注：サーバの構成にリダンダント電源管理モジュールが含まれる場合は、4番目のWebページが表示されます。

ラックの設定

ブレード サーバは、電源の供給やラックの共有リソース（ファン、温度、パワー サプライ）の管理のためにラック環境と通信します。[Rack Settings]オプションにより、この通信を設定できます。

hp iLO INTEGRATED LIGHTS-OUT

Server Name: Administration
iLO Name: iLOB119JTM8089E
Logged in: Administrator

System Status Remote Console Virtual Devices Administration **BI, p-Class**

Rack Settings
Rack Topology
Server Blade Mgt. Module
Power Mgt. Module
Redundant Power Mgt. Module

Insight Agent | Log out

Rack Settings

Rack Information

Rack Name	North America	Rack Serial Number	2098DWA94E1
Enclosure Name	Accounting	Enclosure Serial Number	DY1962W40E88
Bay Name	Accounts Payable	Blade Serial Number	68D01YE10062
Bay #			

Power On Control

Power Source: ☒ Rack Provides Power ☐ Facility Provides 48V

Enable Automatic Power On: ☒ Yes ☐ No

Enable Rack Alert Logging (IML): ☒ Yes ☐ No

Apply

使用できるフィールドは、次のとおりです。

[Rack Name]

ラック名は、1つのラックを構成するコンポーネントを論理的なグループにまとめるために使用されます。[Rack Name]を変更すると、そのラック名はラックに接続されている他のすべてのコンポーネントに通知されます。この名前は、ログ記録やアラート生成の際に使用され、コンポーネントの識別に役立ちます。

[Enclosure Name]

エンクロージャ名は、1つのエンクロージャを構成するサーバ ブレードを論理的なグループにまとめるために使用されます。エンクロージャ名を変更すると、そのエンクロージャ名は同じエンクロージャに接続されている他のすべてのサーバ ブレードに通知されます。この名前は、ログ記録やアラート生成の際に使用され、コンポーネントの識別に役立ちます。

[Bay Name]

ベイ名は、ログ記録やアラート生成の際に使用され、コンポーネントやその機能の識別に役立ちます。

[Bay]

ProLiant BL p-Classエンクロージャは、1～8台のサーバ ブレードをサポートできます。ベイには、左から右に1～8までの番号が付けられます。ベイ番号は、障害の発生したサーバ ブレードや他のエラー状態の物理的識別に役立ちます。この情報は、表示のためにのみ提供されます。

[Rack Serial Number]

ラックのシリアル番号は、ラック内のコンポーネントを論理グループとして識別します。シリアル番号は、さまざまなコンポーネントの起動時に決定され、固有のラックシリアル番号が作成されます。コンポーネント（サーバ ブレード エンクロージャまたはパワー サプライ）を取り替えると、ラックのシリアル番号が変更されます。

[Enclosure Serial Number]

エンクロージャのシリアル番号は、表示されているサーバ ブレードが挿入されている特定のサーバ ブレード エンクロージャを識別します。

[Blade Serial Number]

ブレードのシリアル番号は、サーバ ブレード製品のシリアル番号を識別します。

[Power Source]

サーバ ブレード エンクロージャは、次に示す2つの構成のうちいずれかを使用してラックにインストールできます。

- サーバ ブレードのパワー サプライは、通常使用している既存のAC電源を48VDCに変換してラックに電源を供給するために使用できます。この構成では、電源の設定で**[Rack Provides Power]**を選択します。この設定により、電源障害の危険を伴うことなく適切な電力消費を確保できるように、各ブレード サーバ、エンクロージャ、およびパワー サプライが電源要求を伝達することができます。
- 付属のパワー サプライを使用しないで、既存の48VDC電源を直接供給できる場合は、**[Facility Provides 48V]**を選択します。電源投入または切断時に、各サーバ ブレードが、電源についてインフラストラクチャと通信する必要はなくなります。

注：ラック内のすべてのサーバ ブレードおよび他のコンポーネントに十分な電力を供給するには、適切な電源サイジング要件の実現は必須条件です。

[Enable Automatic Power On]

各サーバ ブレードをエンクロージャに挿入すると、サーバ ブレードに自動的に電源が入るように設定できます。電源設定によって異なりますが、サーバ ブレードは、ラックと通信して電源を投入するための十分な電源があるかどうかを確認します。電源を使用できる場合は、サーバ ブレードに自動的に電源が投入され、サーバの通常の起動プロセスが開始されます。

[Enable Rack Alert Logging]

サーバ ブレードがアラートを受信したときに、これらのイベントをIMLに記録できます。これらのイベントは、iLOの[System Status]タブのIMLを使用して、表示できます。IMLの表示のための別のツールを使用して、サーバ ブレードにインストールされているオペレーティングシステムからIMLを表示することもできます。

ラック トポロジ

[Rack Topology]画面では、次の機能を実行できます。

- ラック内で接続されているすべてのデバイスの検出
- エンクロージャの種類、名前、アドレス、およびシリアル番号の表示
- ラックの診断情報の表示

Server Name: Administration
iLO Name: iLOB1153TND009E
Logged in: Administrator

System Status Remote Console Virtual Devices Administration **Rack Topology**

Rack Settings
Rack Topology
Server Blade Mgt. Module
Power Mgt. Module
Redundant Power Mgt. Module

Rack Topology

Rack Infrastructure

Enclosure Type	Name	Address	Serial Number
Server Blade Enclosure	Accounting	305b	02173TK70015
Power Enclosure	67091phsNAJP	c9d4	67091phsNAJP
Power Enclosure	01403TK50003	453a	01403TK50003

[Return to top](#)

Diagnostic Information

Description	Count
IPMI Packets Lost	0

[Return to top](#)

サーバブレード管理モジュール

[Server Blade Management Module]画面では、次の機能を実行できます。

- BL p-Classエンクロージャ内で検出されたデバイスの表示
- ブレードサーバエンクロージャ用のコントローラの現在のファームウェアバージョンの読み取りと表示
- ブレードサーバのヒューズと電源の状態の検出と表示
- エンクロージャのLEDの有効化

The screenshot displays the HP iLO Server Blade Management Module interface. At the top, it shows the HP iLO logo and 'INTEGRATED LIGHTS-OUT'. The user is logged in as 'Administrator' with the iLO Name 'ILO019JTN009SE'. The interface has tabs for 'System Status', 'Remote Console', 'Virtual Devices', 'Administration', and 'BL p-Class'. The 'Administration' tab is selected, showing the 'Server Blade Management Module' page. The page contains two main sections: 'Enclosure Information' and 'Server Component Information'.

Enclosure Information

Name	Serial Number	Temp (°C)	FW Rev	HW Rev
Accounting	DY1962W40E00	32	0.92	4

[Return to top](#)

Server Component Information

Bay Number	Occupied	Fuse A	Fuse B	Power
1	Empty	Good	Open	Unknown
2	Empty	Good	Open	Unknown
3	Empty	Good	Open	Unknown
4	Empty	Good	Open	Unknown
5	Present	Good	Open	Unknown
6	Present	Good	Open	Unknown
7	Present	Good	Open	Unknown
8	Present	Good	Open	On

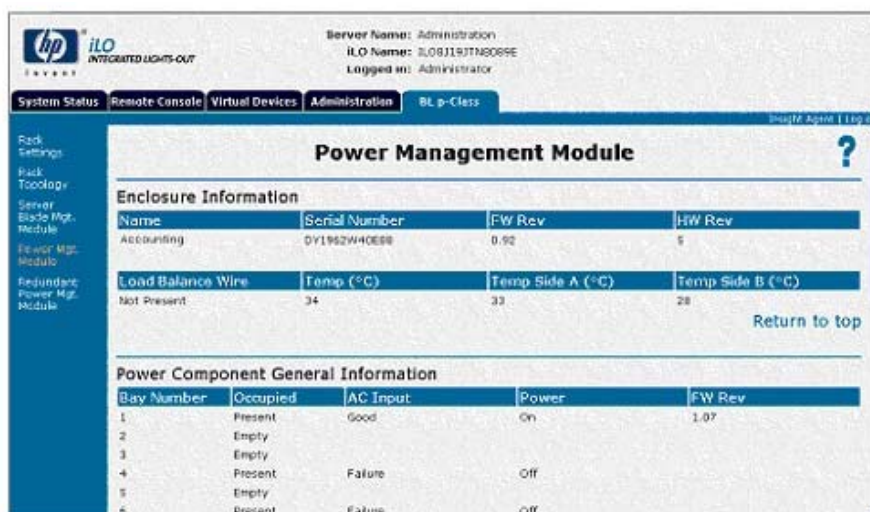
[Return to top](#)

電源管理モジュール

[Power Management Module]画面では、次の機能を実行できます。

- 主電源の検出と表示
- 電源エンクロージャ用のコントローラの現在のファームウェアバージョンの読み取りと表示
- パワーサプライの現在の電源出力、最大電源出力、および温度情報の表示

- この画面で、電源管理モジュールのLEDの有効化



リダンダント電源管理モジュール

ラック トポロジにリダンダント電源が含まれる場合は、[Redundant Power Management Module]画面を表示できます。[Redundant Power Management Module]画面では、[Power Management Module]画面が電源管理モジュールに提供しているものと同じ、リダンダント電源管理モジュールに関する情報が表示されます。

ProLiant BL p-ClassサーバのLEDのiLOによる制御

iLOは、POSTのトラッキングとサーバのヘルスLEDを利用してBL p-Classサーバを監視できます。

POSTのトラッキング

ProLiant BL p-Classサーバはヘッドレス サーバであるため、サーバの起動時に十分なフィードバックを提供できません。iLOは、サーバのPOST実行中、サーバのヘルスLEDを緑色で点滅させ、起動時のフィードバックを提供します。起動が正常に行われない場合、LEDは黄色で点灯します。起動が正常に完了すると、LEDは緑色で点灯します。

起動が正常に行われた後、サーバのヘルスLEDの制御は、サーバに返されます。サーバはLEDを消灯するか、またはサーバ ハードウェアの状態が正常であることを示すためにLEDを他の何らかの色で点灯します。

不十分な電源に関する通知

ラック インフラストラクチャが十分な電源を供給できないために、iLOがサーバの電源を投入できない場合、iLOは、サーバのヘルスLEDを赤色で点灯させます。

Telnetサポート

Telnetを使用してiLOにアクセスできるようになりました。Telnetを使用すると、テキストベースでリモート コンソールにアクセスできます。Telnetを使用するには、**[Global Settings]**画面の*[iLO Remote Console Port Configuration]*および*[Remote Console Data Encryption]*を、次のように設定する必要があります。

1. *[Remote Console Port Configuration]*を**Enabled**に設定
2. *[Remote Console Data Encryption]*を**No**に設定

Telnetを使用してiLOにアクセスするには、以下の手順に従ってください。

注： Telnetセッションとリモート コンソール セッションを同時に開くことはできません。両方のセッションを同時に行おうとすると、エラー メッセージが生成されます。

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

注：[Global Settings]タブのリモート コンソール ポートの設定が**Disabled**または**Automatic**に設定されている場合や、リモート コンソール データの暗号化が有効になっている場合は、Telnetを使用したアクセスは無効になります。

Telnetセッションを終了するには、以下の手順に従ってください。

1. **Ctrl+]キー**を押し、プロンプトで**Enterキー**を押します。
2. **Enterキー**を押すたびに不要な改行が行われる場合は、**Ctrl+]キー**を押して、プロンプトで**set crlf off**と入力します。

Insightマネージャ7との統合

この項の目次

機能の概要	85
識別と関連付け	85
アラート	87
ポートを一致させる	87
iLOの識別の設定	88
内蔵iLOとInsightマネージャ7との統合	89

機能の概要

Insightマネージャ7により、次の機能を実現できます。

- iLOプロセッサの識別
- iLOとそのサーバの関連付け
- iLOとそのサーバ間のリンクの作成
- iLOとサーバの情報およびステータスの表示
- iLOについて表示する詳細情報の量の制御
- ProLiant BL p-Classラック インフラストラクチャの図を表示

以下の各項では、各機能の概要を説明します。これらの利点やInsightマネージャ7の使用方法については、マネジメントCDに収録されているHP Insightマネージャ7のテクニカル リファレンス ガイドを参照してください。

識別と関連付け

Insightマネージャ7は、iLOプロセッサを識別し、iLOとサーバを関連付けます。iLOデバイスの管理者は、iLOをInsightマネージャ7の識別要求に対応するように設定できます。

ステータス

Insightマネージャ7では、iLOはマネジメント プロセッサとして識別されます。Insightマネージャ7は、デバイス リストにマネジメント プロセッサのステータスを表示します。

デバイス リストでは、iLOマネジメント プロセッサは、そのホスト サーバと同じ行にアイコンで表示されます。マネジメント プロセッサのステータスは、アイコンの色で示されます。

Actions View		HW Status	Mgmt Proc	SW Status	Device Name	Device Type	Device Addresses	Product Name
					R1003	Server	170.125.1.203	ProLiant DL380
					R1004	Server	170.125.1.204	ProLiant DL380
					R1005	Server	170.125.1.205	ProLiant DL380
					R1006	Server	170.125.1.206	ProLiant DL380
					r1016	Server	170.125.1.216	ProLiant DL380
					iLO-r1016 in r1016	Management Processor	170.125.1.217	Integrated Lights-Out
					r1019	Server	170.125.1.222	ProLiant DL380
					r1021	Server	170.125.1.226	ProLiant DL380
					iLO-r1021 in r1021	Management Processor	170.125.1.227	Integrated Lights-Out
					R1022	Server	170.125.1.228	ProLiant DL380
					nb123456789	Management Processor	170.125.1.229	ProLiant DL380
					r1023	Server	170.125.1.230	ProLiant DL380
					iLO-r1023 in r1023	Management Processor	170.125.1.231	Integrated Lights-Out
					r1024	Server	170.125.1.232	ProLiant DL380
					iLO-r1024 in r1024	Management Processor	170.125.1.233	Integrated Lights-Out
					r1025	Server	170.125.1.234	ProLiant DL380
					iLO-r1025 in r1025	Management Processor	170.125.1.235	Integrated Lights-Out
					r1026	Server	170.125.1.236	ProLiant DL380
					iLO-r1026 in r1026	Management Processor	170.125.1.237	Integrated Lights-Out

Devices in table: 14 Critical 32 Major 30 Minor 108 Normal 77 Unknown Total: 261

デバイスのステータスの詳細な一覧については、マネジメントCDに収録されているHP Insightマネージャ7のテクニカル リファレンス ガイドを参照してください。

クエリ

iLOマネジメント プロセッサは、Insightマネージャ7内で照会できます。管理者は、これらのクエリを保存して使用し、マネジメント プロセッサのグループを作成できます。詳しくは、HP Insightマネージャ7のテクニカル リファレンス ガイドを参照してください。

リンク

Insightマネージャ7は、管理を簡単にするために、次の位置へのリンクを作成します。

- Insightマネージャ7のホームページからiLOおよびホスト サーバへ
- クエリの結果ページからiLOへ
- クエリの結果ページからサーバへ
- iLOのデバイス概要ページからサーバへ
- サーバのデバイス概要ページからiLOへ

ホームページおよびクエリの結果ページには、iLO、サーバ、およびその関係が表示されます。たとえば、ページでは、サーバとその横にiLOの名前が表示され、iLOの[デバイス名]フィールドは「<iLO名> **サーバ内** <サーバ名>」という形式をとります。

iLOまたはサーバのデバイス ステータス アイコンをクリックすると、デバイスの概要ページに移動します。概要ページには、対応するデバイスのステータスとIPアドレスおよび対応するデバイスへのリンクがあります。

アラート

iLOマネジメント プロセッサは、Insightマネージャ7のコンソールにSNMPアラートを送信するように設定できます。iLOの[Administration]タブの[Management Integration]ページに、Insightマネージャ7コンソールのTCP/IPアドレスを入力して、SNMPアラートをコンソールに送信します。

iLOは、ホスト オペレーティング システムのマネジメント エージェントからアラートを送信するように設定できます。また、iLOが生成したアラートをInsightマネージャ7のコンソールに送信するようにも設定できます。

ポートを一致させる

Insightマネージャ7は、ポート80で、HTTPセッションを開始してiLOを確認するように設定されています。ポートは変更できます。ポート番号を変更する場合は、[Network Settings]とInsightマネージャ7で変更する必要があります。

Insight マネージャ7でポート番号を変更するには、ポートを¥ADDITIONALWSDISC.PROPSファイルに追加します。このpropsファイルには、ポート80のエントリは必要ありませんが、iLO用に指定された他のポートはすべて指定して、HTTP識別の際にInsight マネージャ7が使用できるようにしなければなりません。エントリの書式は、次のとおりです。

```
Port=Description,Reserved 1,Reserved 2,Reserved 3,Class  
Name
```

ここで、各項目は、次の情報を示します。

- Portは、検出に追加する別のHTTPポートの番号です。
- Descriptionは、デバイス ページのリンクのリストに表示するWebサーバの説明です。
- Reserved 1は、予約されており、スペースを入力する必要があります。
- Reserved 2は、予約されており、trueを入力する必要があります。
- Reserved 3は、予約されており、falseを入力する必要があります。
- Class Nameは、追加マネジメント プロセッサ ポートの処理を行うInsight マネージャ7 Javaクラスの名前を指定します。この情報は、変更しないでください。

例：

```
80=iLO, ,true,false,compaq.ID.MgmtProc.MgmtProcessorParser
```

iLOの識別の設定

iLOでは、Insight マネージャ7の詳細情報を求める要求に対して、どれだけのデータを返すかを設定できます。

返されるデータのレベルは、[SNMP/Insight Manager Settings]画面で制御します。選択できる識別データ レベルは、次のとおりです。

- **[High]** - 対応が存在し、すべてのデータが概要ページに表示されます。
- **[Medium]** - 対応は存在しますが、概要ページには、セキュリティ レベルの高い場合ほどの詳細なデータは表示されません。

- **[Low]** - SNMPのパススルーがサポートされる場合、対応は存在します。そうでない場合は、サーバとマネジメント プロセッサは、デバイス リストでは別のものとして扱われます。
- **[None]** - Insightマネージャ7にデータが返されません。

表示情報	Low	Medium	High	None
製品名	あり	あり	あり	
サーバのシリアル番号		あり	あり	
サーバの状態			あり	
マネジメント プロセッサのステータス	あり	あり	あり	
マネジメント プロセッサのシリアル番号		あり	あり	
iLO Advanced/バック ライセンスのステータスとデータ		あり	あり	
ハードウェアのリビジョン情報			あり	
ファームウェアのリビジョン情報			あり	
ラックのトポロジ		あり	あり	
シングル サイン オン*			あり	
セキュリティ保護されたタスクの実行*			あり	
CIMOM*			あり	
デバイス ホームページのURL			あり	
*将来のInsightマネージャ7との統合用に予約されています。				

内蔵iLOとInsightマネージャ7との統合

iLOは、主要な操作がInsightマネージャ7と完全に統合されていて、Insightマネジメント エージェントにアクセスでき、またインバンドでのSNMP管理をフルサポートすることができます。iLOは、InsightマネージャのコンソールへのSNMPトラップ配信をサポートしているので、このSNMPトラップをポケットベルや電子メールに転送するように設定することができます。

またInsightマネージャ7と完全に統合することにより、単一の管理コンソールを設定することが可能となり、標準的なWebブラウザを立ち上げてiLOにアクセスすることができます。さらにiLOの動作についての診断情報も入手することができます。オペレーティング システムの動作中、Insightマネージャ7を使用することでiLOへの接続を簡単に確立することができます。

Insightマネージャ7でSNMPアラートを受信

Insightマネージャ7は、完全なSNMP管理をサポートすることができ、またiLOは、Insightマネージャ7のコンソールへのSNMPトラップ配信をサポートしています。ユーザは、イベント ログを表示し、イベントを選択し、アラートについての詳細情報を表示できます。

Insightマネージャ7でのSNMPアラート受信の設定は、2段階の手順で行います。この手順では、Insightマネージャ7を設定して管理対象のiLOデバイスからのSNMPアラートを受信可能にすることと、iLOを設定してSNMPアラートを使用可能にすることが必要です。

Insightマネージャ7でSNMPアラートの受信を設定するには、以下の手順に従ってください。

1. iLOナビゲーション フレームの[Administration]タブにある[SNMP/Insight Manager Settings]オプションを使用してSNMPアラートを有効にし、SNMPトラップIPアドレスをiLOに設定します。このIPアドレスは、Insightマネージャ7が動作しているコンピュータのアドレスでなければなりません。詳しくは、「SNMPアラートの有効化」の項を参照してください。
2. iLOをInsightマネージャ7の管理対象デバイスとして設定します。iLOをInsightマネージャ7に追加すると、iLO上のNICインタフェースが専用の管理ポートとして機能するようになり、管理トラフィックはリモートのホスト サーバのNICインタフェースから分離されます。
 - a. Insightマネージャ7を起動して、**[設定]**をクリックします。デフォルトでは、**[自動検出]**画面が表示されます。この画面を使用して、Insightマネージャ7が管理するiLOを検出します。**[PING包括範囲]**セクションにIPアドレスが表示されていない場合は、IPアドレスを入力します。
 - b. **[検出の実行]**をクリックして、iLOをInsightマネージャ7に追加します。[ステータス]セクションに、更新中のシステムが表示されます。
 - c. 検出が完了したら、続いてクエリがデバイスをマネジメント プロセッサとして表示します。
 - d. **[検出]**タブから**[デバイスの編集]**を選択して、モニタ コミュニティ名を（たとえば、"public"に）変更する必要がある場合があります。これによって、iLOが監視対象デバイスの一覧に表示されます。
 - e. iLOトラップが主要な、クリアされていないイベントのクエリに表示されます。画面上部にあるオレンジ色のボタンを使用してこのクエリを実行することができます。イベントについて詳しくは、イベントの説明をクリックしてください。

注：各iLOについて内蔵Lights-Outマネジメントを可能にするには、内蔵Lights-Out用のHP Insightエージェントを、リモートのホストサーバにインストールする必要があります。エージェントのインストール手順と設定について詳しくは、iLOのマニュアルを参照してください。

Insightマネージャ7でのiLO Advancedパック ライセンス情報の確認

Insightマネージャ7は、iLOマネジメント プロセッサのライセンス状態を示すレポートを提供します。このレポートを使用して、iLO Advancedパックで使用許諾されているiLOデバイスとその数を確認できます。

このレポートを表示するには、以下の手順に従ってください。

1. **[デバイス]**をクリックします。
2. **[レポート]**をクリックします。
3. **[デバイス ライセンス情報-すべてのデバイス]**をクリックします。

マネジメント プロセッサのライセンス情報が表示されます。このデータを最新のものにするには、ご使用のマネジメント プロセッサのデバイス識別タスクを実行してください。タスクの開始手順について詳しくは、Insightマネージャ7のマニュアルを参照してください。

ProLiant BL p-Classラックの視覚化

Insightマネージャ7は、iLOからの情報を使用して、ProLiant BL p-Classラック、エンクロージャ（筐体）、およびサーバの図を表示できます。Insightマネージャ7が図を表示するには、返されるデータのレベルについてのSNMP/Insightマネージャの設定をMediumまたはHighにしなければなりません。



Device: 170.10.2.4

The following information is known about this device:
 ([Last Update:](#) Tuesday January 22, 2002 - 7:45:13 AM)

Device Information

Status: ■ Normal

Address: 170.10.2.4

Management Protocols: SNMP

Device Name: 170.10.2.4

SNMP Alias: Axx4

Contact: JP

Location: MIMIC1

Device Type: Server

Product Name: ProLiant BL20p

Description: Hardware: x86 Family 6 Model 11 Stepping 0 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)

Server Role: A Very Special Server

[Data Collection Report](#)

[SNMP Communications Settings](#)

[All Events For This Device](#)

Device Links

■ Normal [Compag Subsystem Status Information \(using SNMP\)](#)
[Legacy Version Control](#)
[SNMP Explorer](#)

Container Information

Rack Name: [IDFRack1](#)

Enclosure Name: [Enclosure2R1](#)

Slot Number: 4

Server Dimensions: 44mm x 257mm x 711mm



LEGEND:

-  Server
-  Current server
-  No server identified
-  Switch
-  Power supply enclosure

内蔵Lights-Outのセキュリティ

この項の目次

セキュリティに関する一般的なガイドライン.....	93
暗号化.....	93
iLOのセキュリティ オーバーライド スイッチによる管理.....	93
ユーザ アカウント.....	95
パスワード.....	96
電子証明書.....	97

セキュリティに関する一般的なガイドライン

iLOのセキュリティに関する一般的なガイドラインは、次のとおりです。

- セキュリティを最大限に高めるには、iLOは、独立した管理ネットワーク上でセットアップする必要があります。
- 内蔵Lights-Outは、インターネットに直接接続しないでください。
- 128ビットの暗号化強度を備えたブラウザを使用する必要があります。

暗号化

デフォルトでは、iLOのWebページはすべて、SSL（Secure Sockets Layer）を使用して暗号化されています。セキュリティ上の理由から、パスワードがネットワークを介して送信されるとき、クリア テキスト形式はとりません。ログイン シーケンスを自動化するために、パスワードはクリア テキストでは示されません。リモート コンソールのデータは、128ビットのRC4双方向暗号を使用して暗号化されています。

iLOのセキュリティ オーバーライド スイッチによる管理

iLOのセキュリティ オーバーライド スイッチにより、管理者は、iLOプロセッサにフル アクセスできます。次のいずれかのような状況では、このアクセスが必要な場合があります。

- iLOが無効になった後で、再度、有効にする必要がある。

- 管理者ユーザ アカウント権限を持つすべてのユーザ アカウントがロックアウトされた。
- 設定が正しくないため、iLOがネットワーク上に表示されず、RBSUが無効にされている。
- ブート ブロックをフラッシュする必要がある。

セキュリティ オーバーライド スイッチを設定すると、次のことが可能です。

- スイッチが設定されている間、セキュリティ認証チェックがすべて無効になる。
- ホスト サーバがリセットされると、iLOのRBSUが実行される。
- iLOが無効化されず、設定に従って、ネットワーク上で表示できる。
- セキュリティ オーバーライド スイッチが設定されている間にiLOが無効にされても、サーバの電源を切って再度投入するまで、iLOは、ユーザをログアウトしたり無効化プロセスを実行したりしない。
- iLOのファームウェアが実行されていない場合でも、iLOのOption ROMPkgは、iLOのROMを書き換えることができる。
- ブート ブロックをエクスポートして、書き換えることができる。

iLOのWebページに、iLOのセキュリティ オーバーライド スイッチが現在使用中であることを示す警告メッセージが表示されます。iLOのログに、iLOセキュリティ オーバーライド スイッチの使用を記録するエントリが追加されます。iLOセキュリティ オーバーライド スイッチを設定またはクリアしたとき、SNMPアラートを送信することもできます。

iLOセキュリティ オーバーライド スイッチを設定すると、iLOのブート ブロックをフラッシュすることもできます。HPは、お客様がiLOのブート ブロックを更新しなければならないような事態は発生しないと考えています。iLOのブート ブロックを更新しなければならないような事態が発生した場合、ブートブロックを書き換えiLOをリセットするには、サーバの設置場所に行き、サーバに付いていなければなりません。ブートブロックは、iLOがリセットされるまでエクスポートされます。セキュリティを最大限に高めるために、リセットが完了するまで、ネットワークからiLOを切断することをおすすめします。

iLOセキュリティ オーバーライド スイッチは、サーバ内部にあるため、サーバエンクロージャを開かないとアクセスできません。iLOセキュリティ オーバーライド スイッチを設定するには、サーバの電源を切る必要があります。スイッチを設定し、その後でサーバの電源を入れてください。iLOセキュリティ オーバーライド スイッチをクリアするには、逆の手順を実行してください。

サーバにより、iLOセキュリティ オーバーライド スイッチは、1つのジャンパの場合やディップ スイッチ パネルの特定のスイッチ位置にある場合があります。iLOセキュリティ オーバーライド スイッチにアクセスして位置を確認するには、サーバのマニュアルを参照してください。また、iLOセキュリティ オーバーライド スイッチの位置は、サーバのフード ラベルの図で確認することもできます。

ユーザ アカウント

iLOは、最大12のローカル ユーザ アカウントの設定をサポートします。これらのアカウントはそれぞれ、次の機能を使用して管理できます。

- 権限
- グローバル セキュリティ設定
- ログイン セキュリティ

権限

iLOでは、管理者は、権限を使用して、iLOの機能へのユーザ アカウント アクセスを制御できます。ユーザが機能の使用を試みると、iLOシステムは、ユーザが権限を持っているかどうかを確認してから、機能の実行を許可します。

iLOで利用できる各機能は、ユーザ アカウントの管理、リモート コンソールへのアクセス、仮想電源およびリセット、仮想メディア、iLOの設定などの権限を介して制御できます。各ユーザの権限は、[Administration]タブの[User Administration]ページで設定できます。

グローバル セキュリティ設定

グローバル セキュリティ設定により、機能へのアクセスを制御したり、グローバルに有効にされている機能の中の特別な操作を制御したりすることができます。たとえば、iLO RBSUに対するアクセスの制御、Lights-Out機能の有効化または無効化、リモート コンソールのタイムアウトの設定、WebサーバのSSLポートおよび非SSLポートの設定、仮想メディア ポートの設定、パスワードの最小長の設定などを行うことができます。

ログイン セキュリティ

iLOには、複数のログイン セキュリティ機能があります。ログインの1回目の失敗に対して、iLOは5秒間の遅延時間を課します。ログインの2回目の失敗に対しては、10秒間の遅延時間が課せられます。3回目以降の失敗に対しては、60秒間の遅延時間が課せられます。別のユーザによる失敗に対しても、この遅延時間が繰り返されます。遅延時間が発生するたびに、情報ページが表示されます。この設定は、有効なログインが完了するまで続行されます。この機能は、ブラウザのログイン ポートに対して実行される可能性のある辞書攻撃からの防御に役立ちます。

iLOは、失敗したログイン試行について詳細なログ エントリも保存します。これらのログ エントリを記録することにより、60秒の遅延時間が課せられます。

パスワード

次に、推奨されるパスワードのガイドラインを示します。

- パスワードを書き留めたり記録したりしないでください。
- パスワードを他のユーザと共有しないでください。
- 辞書によく出てくるような単語や、企業名、製品名、ユーザの名前、ユーザのユーザIDなど推測の容易な単語を、パスワードに使用しないでください。
- パスワードには、次の4つの文字のうち少なくとも3つを含むようにしてください。
- 少なくとも1つの数字
- 少なくとも1つの特殊文字
- 少なくとも1つの小文字
- 少なくとも1つの大文字

一時的なユーザID、パスワードの再設定、またはロックアウトされたユーザID用に発行されるパスワードも、これらの基準に従う必要があります。各パスワードは、0文字以上、39文字以下の長さでなければなりません。デフォルトでは最小の長さは、8文字に設定されています。保護されたデータ センタの外側に拡大されることのない物理的に安全な管理ネットワークがない場合は、パスワードの最小の長さを8文字未満に設定することはおすすめできません。

電子証明書

iLOは、SSL接続で使用するために「自己署名」の電子証明書をデフォルトで作成します。この電子証明書により、設定手順を追加することなく、iLOの動作を有効にすることができます。iLOのセキュリティ機能は、信頼済みの証明書をインポートすることにより強化することができます。

証明書のインポート

- **[Create Certificate Request]** - iLOは、CR (PKCS #10フォーマット) を作成して、CAに送信できます。この証明書要求は、base64でエンコードされます。CAは、この要求を処理して応答 (X.509証明書) を返します。このX.509証明書を内蔵Lights-Outにインポートできます。iLOの名前が同じ場合でも、**[Create Certificate Request]** ボタンをクリックするたびに、新しい証明書要求が生成されます。

CRには、公開鍵/秘密鍵ペアが含まれ、この鍵ペアを使用してクライアント ブラウザとiLO間の通信が正当なものであるかどうかを確認します。生成されたCRは、新しいCRが生成されるか、このプロセスを介して証明書がインポートされるか、またはiLOがリセットされるまで、メモリに格納されます。これにより、CRを生成し、CRをクライアントのクリップボードにコピーし、証明書を取得するためにiLOのWebサイトを離れ、その後で、証明書をインポートするためにサイトに戻ることができます。

CAに要求を送信する際は、必ず、次の手順を実行してください。

- サーバのURLとして[System Status]画面に示されているiLO名を使用してください。
- 証明書をRAWフォーマットで生成するように要求してください。
- 証明書のBegin行およびEnd行を含むようにしてください。
- **[Import Certificate]** - インポートする証明書を取得した後でこのページに戻る場合、**[Import Certificate]** ボタンをクリックすると、**[Certificate Import]** 画面に直接移動できます。この際、新しいCRは生成しません。これは重要です。というのは、ある証明書は、その証明書の生成元となったCRに含まれる鍵を使用する場合にのみ有効だからです。iLOがリセットされた場合や、その証明書の要求に使用されたCRの生成後に他のCRが生成された場合は、別のCRを生成してCAから新しい証明書を取得する必要があります。

ディレクトリ サービス

この項の目次

ディレクトリ サービスとは	99
スキーマに関する資料	99
ディレクトリ サービスのサポート	100
必要なソフトウェア	101
スキーマ インストーラ	101
マネジメント スナップイン インストーラ	104
Active Directoryのディレクトリ サービス	105
eDirectoryのディレクトリ サービス	122
ディレクトリの設定	135
iLOへのユーザ ログイン	138

ディレクトリ サービスとは

iLOのディレクトリ サービス機能は、ファームウェア バージョン1.40以降で利用できます。この機能には、次の特長があります。

- 統合されたスケーラブルな共有ユーザ データベースからユーザを認証します。
- ディレクトリ サービスを使用して、ユーザの権限を制御（権限付与）します。
- ディレクトリ サービスでは、iLOマネジメント プロセッサおよびiLOユーザのグループ レベルの管理にロールを使用します。

重要：内蔵Lights-Out用のディレクトリ サービスをインストールするには、ディレクトリのスキーマを拡張する必要があります。スキーマの拡張は、スキーマ管理者が行わなければなりません。

スキーマに関する資料

プランニングおよび認可プロセスに役立てるために、HPでは、スキーマのセットアップ プロセスでのスキーマの変更に最新の資料を用意しています。『HP Directory Services Schema Information Booklet』は、HPのWebサイト<http://www.hp.com/servers/lights-out/>（英語）で入手できます。

ディレクトリ サービスのサポート

iLOは、次のディレクトリ サービスをサポートします。

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Novell eDirectory 8.6.2
- Novell eDirectory 8.7

iLOソフトウェアは、Microsoft® Active Directory Users and ComputersおよびNovell ConsoleOne マネジメント ツール内で動作するように設計されており、ユーザは、Microsoft Active DirectoryまたはNovell eDirectory上でユーザ アカウントを管理できます。このソリューションでは、NetWare、Linux、またはWindows®上で実行されるeDirectory間での違いはありません。eDirectoryのスキーマ拡張を生成するには、SSL 認証用のJava 1.4.0以降が必要です。

iLOは、以下のいずれかのオペレーティング システム上で動作するMicrosoft® Active Directoryをサポートします。

- Windows® 2000
- Windows® 2000 Advanced Server
- Windows® Server 2003

iLOは、以下のいずれかのオペレーティング システム上で動作するeDirectory 8.6.2および8.7をサポートします。

- Windows® 2000
- Windows® 2000 Advanced Server
- Windows® Server 2003
- NetWare 5.x
- NetWare 6.x
- Red Hat Enterprise Linux AS 2.1

- Red Hat 7.3.x
- Red Hat 8.0.x

必要なソフトウェア

iLOでは、スキーマを拡張し、iLOネットワークを管理するためのスナップインを提供する固有のソフトウェアが必要です。スキーマ インストーラとマネジメント スナップイン インストーラを含むHP Smartコンポーネントは、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。

スキーマ インストーラ

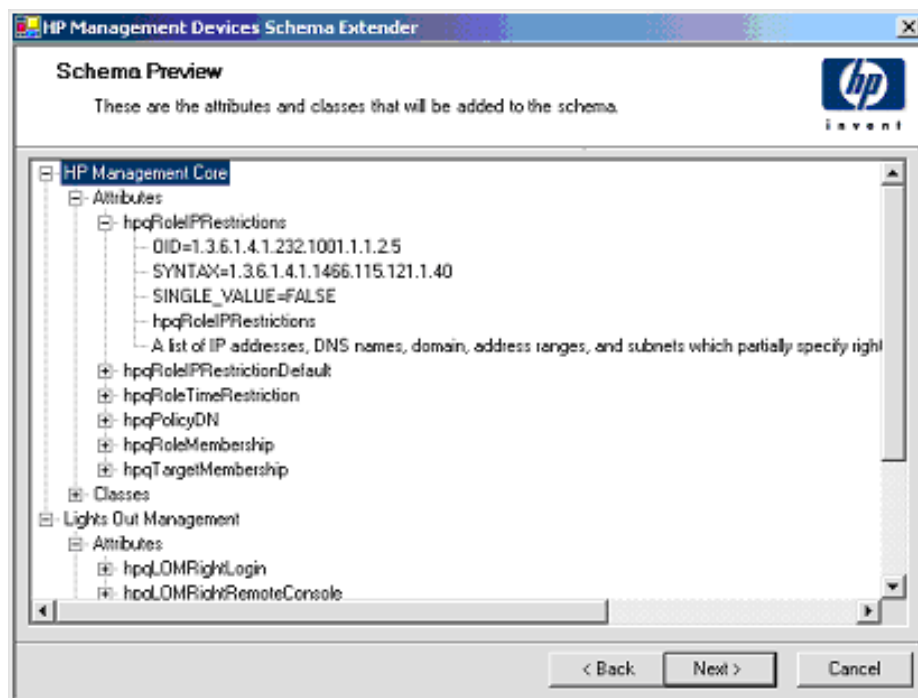
スキーマ インストーラには、1つ以上の.xmlファイルがバンドルされています。これらのファイルには、ディレクトリに追加されるスキーマが含まれています。通常、これらのファイルのうち1つに、サポートされているすべてのディレクトリ サービスに共通のコア スキーマが格納されます。他のファイルには、製品固有のスキーマだけが格納されます。スキーマ インストーラでは、.NET Frameworkを使用する必要があります。

インストーラには、次の3つの重要な画面があります。

- [Schema Preview]
- [Setup]
- [Results]

[Schema Preview]

[Schema Preview]画面では、提供されているスキーマ拡張を表示できます。この画面は、選択されたスキーマ ファイルを読み出し、XMLの構文を解析し、ツリー ビューの形式で表示します。また、インストールされる属性とクラスの詳細をすべて示します。



[Setup]

[Setup]画面は、スキーマを拡張する前に該当情報を入力するために使用します。

[Setup]画面の[Directory Server]セクションでは、Active DirectoryとeDirectoryのどちらを使用するかを選択や、LDAP通信に使用するコンピュータ名およびポートの設定を行うことができます。

重要：Active Directory上でスキーマを拡張するには、ユーザが認証されているスキーマ管理者でなければなりません。また、スキーマが書き込み禁止であってはなりません。さらに、そのディレクトリがツリー内でFSMO ロール オーナでなければなりません。インストーラは、ターゲット ディレクトリ サーバをフォレストのFSMOスキーマ マスタにしようとします。

Windows® 2000上でスキーマへの書き込みアクセス権限を得るには、レジストリのセーフティ インターロックを変更する必要があります。ユーザが[Active Directory]オプションを選択した場合、スキーマ エクステンダは、レジストリを変更しようとします。この試みは、ユーザにレジストリ変更の実行権限がある場合のみ、成功します。スキーマへの書き込みアクセス権限は、Windows® Server 2003では自動で有効になっています。

[Setup]画面の[Directory Login]セクションには、ログイン名とパスワードを入力できます。スキーマを拡張するには、ログイン名とパスワードが必要です。[Use SSL during authentication]オプションでは、安全な認証形式の使用を指定します。このオプションを選択しない場合、Active Directoryでは、NT認証が使用され、eDirectoryでは、認証が平文で行われます。

HP Management Devices Schema Extender

Setup

The wizard needs to know about the directory you will be accessing.

Directory Server

☒ Active Directory ☐ eDirectory

Name: compeq2loseval

Port: 636

Directory Login

Login Name: JPDMAIN_LAB\Administrator

Password:

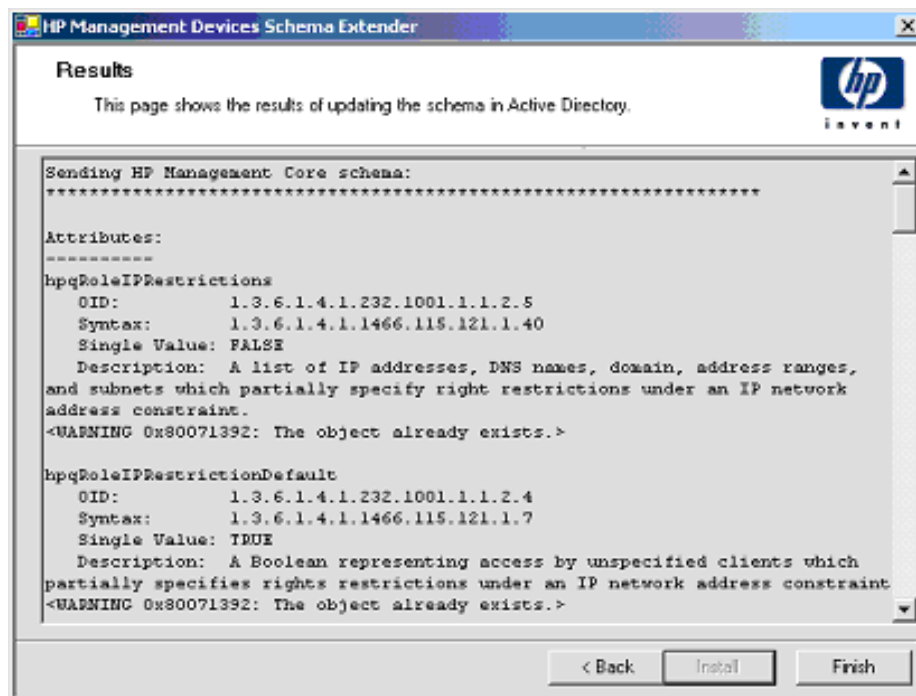
☐ Use SSL during authentication.

When you press the "Install" button, the wizard will begin extending the schema.

< Back Install Cancel

[Results]

[Results]画面には、スキーマを拡張できたかどうか、どの属性が変更されたかなど、インストールの結果が表示されます。



マネジメント スナップイン インストーラ

マネジメント スナップイン インストーラは、Microsoft® Active Directory Users and ComputersディレクトリまたはNovell ConsoleOneディレクトリで、iLOオブジェクトを管理するためのスナップインをインストールします。

iLOスナップインは、iLOディレクトリを作成する際に次のタスクを実行するために使用されます。

- iLOオブジェクトおよびロール オブジェクトを作成して管理する（ポリシー オブジェクトは将来サポートされます）。

- iLOオブジェクトとロール（またはポリシー）オブジェクトとの関連を作成する。

Active Directoryのディレクトリ サービス

以下の各項では、Active Directoryのディレクトリ サービスの、インストールの前提条件、準備、および作業例について説明します。

Active Directoryインストールの前提条件

iLO用のディレクトリ サービスは、SSL上のLDAPを使用してディレクトリ サーバとの通信を行います。Active Directory用のスナップインとスキーマをインストールする前に、次のマニュアルをよく読んでいつでも参照できるようにしておいてください。

重要：内蔵Lights-Out用のディレクトリ サービスをインストールするには、Active Directoryのスキーマを拡張する必要があります。スキーマの拡張は、Active Directoryスキーマ管理者が行われなければなりません。

- Microsoft社のWebサイト<http://msdn.microsoft.com/>で入手できるMicrosoft® Windows® 2000 Server Resource Kitの『Extending the Schema』
- Microsoft® Windows® 2000 Server Resource Kitの『Installing Active Directory』
- Microsoft® Knowledge Baseの次のArticle
 - 216999 『Installing the remote server administration tools in Windows® 2000』
 - 314978 『Using the Adminpak.msi to install a server administration tool in Windows® 2000』
 - 247078 『Enabling SSL communication over LDAP for Windows® 2000 domain controllers』
 - 321051 『Enabling LDAP over SSL with a third-party certificate authority』
 - 299687 『MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed』

Active Directoryでのディレクトリ サービスの準備

iLOマネジメント プロセッサで使用するディレクトリ サービスをセットアップするには、以下の手順に従ってください。

1. Active Directoryをインストールします。詳しくは、Microsoft® Windows® 2000 Server Resource Kitの『Installing Active Directory』を参照してください。
2. Microsoft® Admin Pack (Windows® 2000 Server CDまたはAdvance Server CDのi386サブディレクトリにあるADMINPAK.MSIファイル) をインストールします。詳しくは、Microsoft® Knowledge Base のArticle 216999を参照してください。
3. Windows® 2000では、誤ってスキーマに書き込みが行われないようにするためのセーフティ インターロックを一時的に無効にする必要があります。リモート レジストリ サービスが実行され、ユーザが該当する権限をもつ場合、スキーマ エクステンダ ユーティリティは、この操作を実行できます。この操作は、レジストリのHKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥ServicesParameters¥Schema Update Allowedをゼロ以外の値に設定することによっても実行できます (Windows® 2000 Server Resource Kitの『Installation of Schema Extensions』の「Order of Processing When Extending the Schema」の項を参照)。または、次の手順を実行してください。

重要：レジストリの設定を誤ると、システムに重大な影響を及ぼす可能性があります。レジストリを変更する前に、コンピュータ上の大切なデータのバックアップをとっておくことをおすすめします。

注：Windows® Server 2003を使用する場合は、この手順を実行する必要はありません。

- a. MMCを起動します。
 - b. Active Directory SchemaスナップインをMMCにインストールします。
 - c. [Active Directory Schema]を右クリックして、[Operations Master]を選択します。
 - d. [The Schema may be modified on this Domain Controller]を選択します。
 - e. [OK]をクリックします。
- 注：**[Active Directory Schema]フォルダを展開して、チェックボックスを使用できるようにする必要がある場合があります。
4. 証明書を作成するかまたは証明書サービスをインストールします。iLOはSSLを使用してActive Directoryと通信するため、証明書を作成するかまたは証明書サービスをインストールする必要があります。必ず、Active Directoryをインストールしてから、証明書サービスをインストールしてください。
 5. Active Directoryを実行するサーバに証明書が発行されたことを確認するには、以下の手順に従ってください。

- a. サーバ上でMicrosoft Management Consoleを起動して、デフォルト ドメイン ポリシー スナップインを追加します（グループ ポリシーを追加して、デフォルト ドメイン ポリシー オブジェクトにアクセスします）。
 - b. [Computer Configuration]、[Windows Settings]、[Security Settings]、[Public Key Policies]の順にクリックします。
 - c. [Automatic Certificate Requests Settings]を右クリックして、[new]、[automatic certificate request]の順に選択します。
 - d. ウィザードを使用して、ドメイン コントローラ テンプレートを選択し、使用する証明機関を選択します。
6. スキーマ エクステンダとスナップインのインストーラを含むSmartコンポーネントをダウンロードします。Smartコンポーネントは、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。
 7. スキーマ インストーラ アプリケーションを実行してスキーマを拡張します。インストーラは、適切なHPオブジェクトを使用してディレクトリ スキーマを拡張します。

注：スキーマ インストーラは、Active Directoryスナップインと新しいスキーマを関連付けます。スナップイン インストレーション セットアップ ユーティリティは、Windows MSIセットアップ スクリプトで、MSIがサポートされているどのシステム（Windows® XP、Windows® 2000、Windows® 98）でも実行されます。ただし、スキーマ エクステンション アプリケーションの一部では、.NET Frameworkが必要です。.NET Frameworkは、Microsoft社のWebサイト<http://www.microsoft.com/>からダウンロードできます。

スナップインのインストールとActive Directory用の初期設定

1. スナップイン インストレーション アプリケーションを実行して、スナップインをインストールします。
2. ディレクトリ サービスを設定して、ディレクトリ サービスがiLOマネジメント用の適切なオブジェクトおよび関連を所有するようにします。
 - a. HPが提供するマネジメント スナップインを使用して、iLOオブジェクト、Policyオブジェクト、Adminオブジェクト、およびUser Roleオブジェクトを作成します。
 - b. HPが提供するマネジメント スナップインを使用して、iLOオブジェクト、Policyオブジェクト、Roleオブジェクトの関連を作成します。
 - c. iLOオブジェクトがAdminオブジェクトとUser Roleオブジェクトを指し示すようにします（これにより、AdminオブジェクトとUser Roleオブジェクトは、自動的にiLOオブジェクトを指し示します）。

注：内蔵Lights-Outオブジェクトについて詳しくは、「ディレクトリ サービス オブジェクト」の項を参照してください。

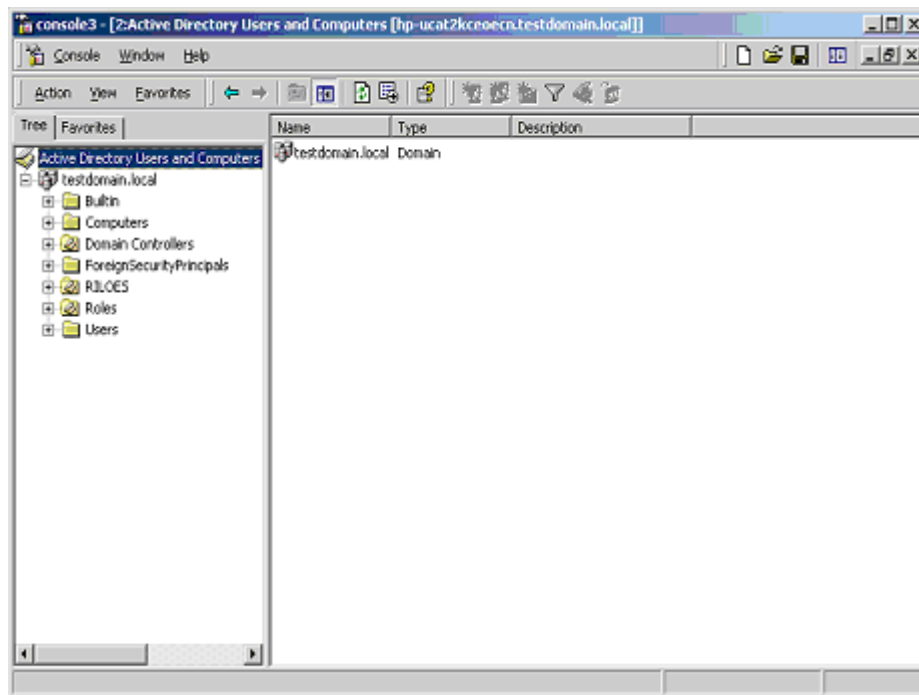
少なくとも、次のオブジェクトを作成する必要があります。

- 1人以上のユーザと1つ以上のiLOオブジェクトを含むRoleオブジェクトを1つ
- ディレクトリを使用するiLOマネジメント プロセッサごとに1つのiLOオブジェクト

例：Active Directory内で、iLOで使用するために、ディレクトリ オブジェクトを作成して設定する

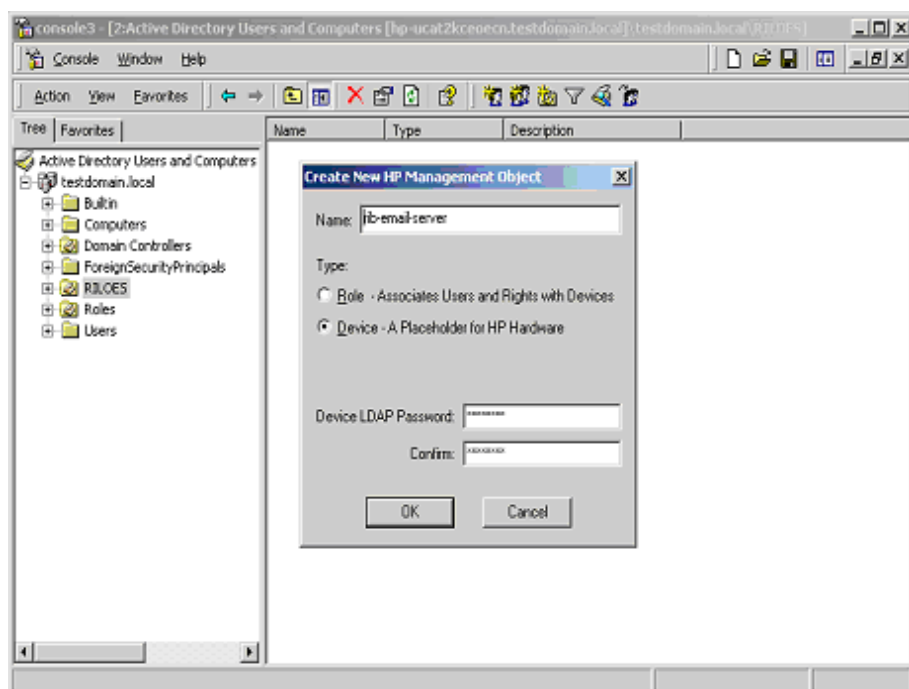
次の例は、testdomain.localドメインを含むエンタープライズ ディレクトリでロールとHPデバイスをセットアップする方法を示します。testdomain.localドメインは、2つの組織単位（RolesとRILOES）で構成されます。

ある企業が、次の画面のように編成されたtestdomain.localドメインを含むエンタープライズ ディレクトリを持っているとします。



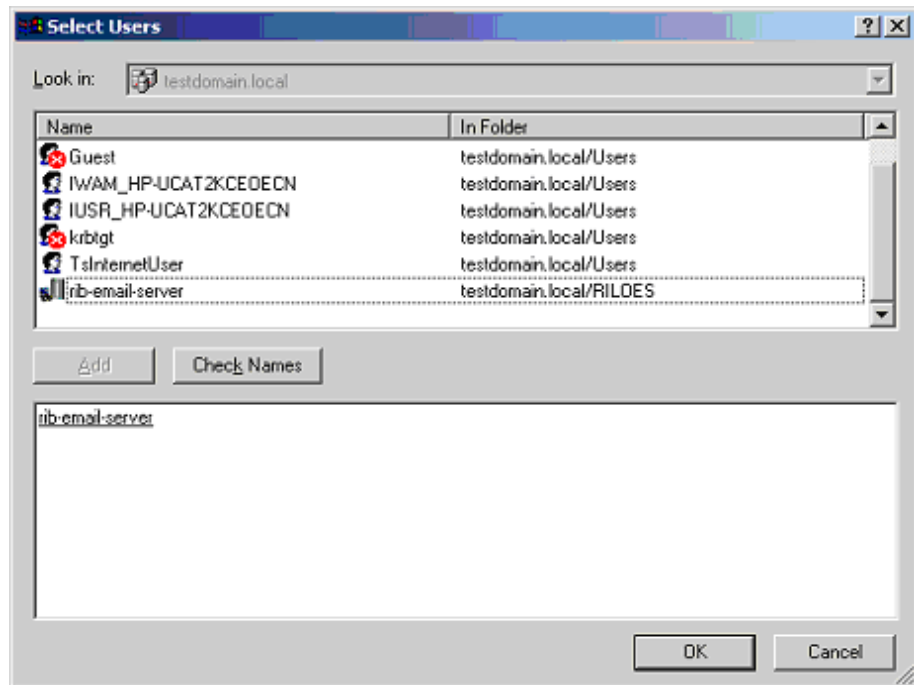
1. ドメインによって管理されるLights-Outデバイスを含む組織単位を作成します。この例では、2つの組織単位が作成され、RolesおよびRILOESと命名されます。
2. HPの提供するActive Directory Users and Computersスナップインを使用して、複数のiLOデバイスを対象に、組織単位RILOES内にLights-Out Managementオブジェクトを作成します。
 - a. testdomain.localドメイン内にある[RILOES]組織単位を右クリックして、[NewHPObject]を選択します。
 - b. [Create New HP Management Object]ダイアログ ボックスで、タイプとして[Device]を選択します。
 - c. ダイアログ ボックスの[Name]フィールドに、適切な名前を入力します。この例では、Lights-Out Managementオブジェクトの名前として、iLOデバイスのDNSホスト名rib-email-serverが使用されます。surnameはRILOEIIになります。
 - d. [Device LDAP Password]フィールドおよび[Confirm]フィールドにパスワードを入力して確認します。デバイスは、このパスワードを使用して、ディレクトリに対する認証を受けます。このパスワードはデバイスに対して固有でなければなりません。このパスワードは、iLOの[Directory Settings]画面で使用されるパスワードです。

- e. [OK]をクリックします。

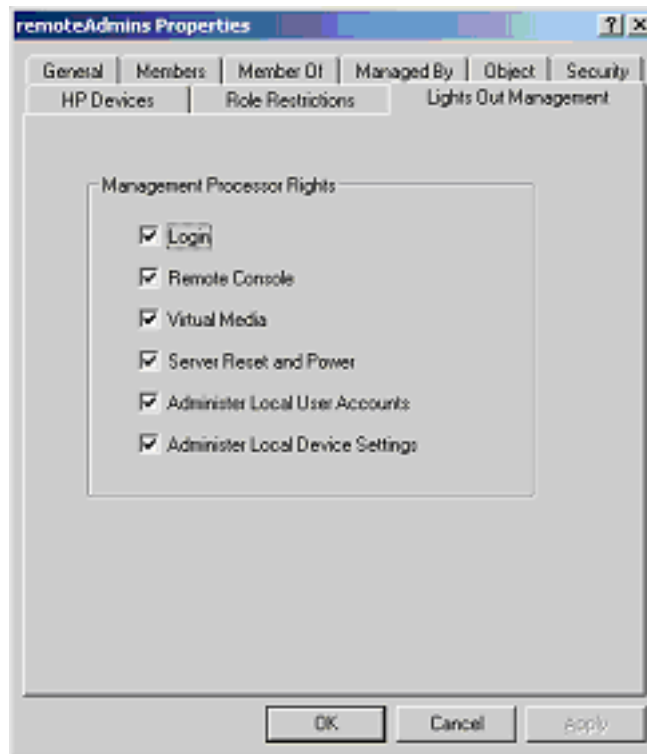


3. HPの提供するActive Directory Users and Computersスナップインを使用して、Roles組織単位内にHP Roleオブジェクトを作成します。
 - a. [Roles]組織単位を右クリックし、[New]、[Object]の順に選択します。
 - b. [Create New HP Management Object]ダイアログ ボックスのタイプ フィールドで[Role]を選択します。
 - c. [New HP Management Object]ダイアログ ボックスの[Name]フィールドに適切な名前を入力します。この例では、ロールには、リモート サーバの管理を行うことのできる信頼されるユーザを所属させるので、remoteAdminsと名付けます。[OK]をクリックします。
 - d. 手順を繰り返して、リモート サーバの監視を行うremoteMonitorsという名前のロールを作成します。
4. HPの提供するActive Directory Users and Computersスナップインを使用して、ロールに権限を割り当て、ロールをユーザおよびデバイスと関連付けます。

- a. testdomain.local ドメインの [Roles] 組織単位の **remoteAdmins** ロールを右クリックして、[Properties] を選択します。
- b. [HP Devices] タブを選択して、[Add] をクリックします。
- c. [Select Users] ダイアログ ボックスを使用して、手順2で、testdomain.local/RILOES フォルダに作成した Lights-Out Management オブジェクト **rib-email-server** を選択します。[OK] をクリックしてダイアログ ボックスを閉じ、次に [Apply] をクリックしてリストを保存します。



- d. ロールにユーザを追加します。[Members]タブをクリックし、[Add]ボタンと[Select Users]ダイアログ ボックスを使用してユーザを追加します。



5. これで、デバイスとユーザが関連付けられました。[Lights Out Management]タブを使用して、ロールの権限を設定します。ロールに所属するすべてのユーザとグループが、ロールによって管理されるすべてのiLOデバイス上でロールに割り当てられた権限を所有します。この例では、remoteAdminsロール内のユーザにiLOの機能へのフル アクセス権限が付与されます。各権限の横のボックスを選択して、[Apply]をクリックします。[OK]をクリックして、プロパティ シートを閉じます。
6. 手順4の手順を使用して、remoteMonitorsロールのプロパティを編集し、rib-email-serverデバイスを[HP Devices]タブの[Managed Devices]リストに追加し、さらに[Members]タブを使用してユーザをremoteMonitorsロールに追加します。次に、[Lights Out Management]タブで、[Login]の横のボックスを選択します。[Apply]をクリックしてから[OK]をクリックします。remoteMonitorsロールのメンバーは、サーバ ステータスへのアクセスの認証を受けることができ、サーバ ステータスを表示できるようになります。

内蔵Lights-Outデバイスに対するユーザ権限は、そのユーザがメンバーとして所属し、その内蔵Lights-Outデバイスが管理対象デバイスとなっているすべてのロールによって割り当てられたすべての権限の和とみなされます。上記の例では、あるユーザがremoteAdminsロールとremoteMonitorsロールの両方に所属する場合、remoteAdminsロールがすべての権限を持っているため、そのユーザはすべての権限を持つことになります。

内蔵Lights-Outデバイスを設定して、この例のLights-Out Managementオブジェクトと関連付けるには、**[Directory Settings]**画面で次のような設定を使用してください。

```
RIB Object DN =  
cn=rib-email-server,ou=RILOES,dc=testdomain,dc=local  
Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

たとえば、testdomain.localドメイン内の[Users]組織単位に所属する、固有のID、MooreMを持つユーザMel Mooreが、remoteAdminsロールまたはremoteMonitorsロールのうちのいずれかのメンバーでもある場合、Mel Mooreは、iLOにログインしてアクセスすることができます。このユーザは、iLOログイン画面の**[Login Name]**フィールドに、testdomain¥moorem、moorem@testdomain.local、またはMel Mooreとタイプし、同じ画面の**[Password]**フィールドにそのActive Directoryパスワードを入力することになります。

Active Directory用のディレクトリ サービス オブジェクト

ディレクトリ ベースの管理で大切なことの1つは、ディレクトリ サービス内の管理対象デバイスを正しく仮想化することです。この仮想化によって、管理者は、ディレクトリ サービス内にすでに存在する管理対象デバイスとユーザまたはグループとを関連付けることができます。内蔵Lights-Outのユーザ管理では、ディレクトリ サービス内に次の3つの基本オブジェクトが必要です。

- Lights-Out Managementオブジェクト
- Roleオブジェクト
- Userオブジェクト

各オブジェクトは、ディレクトリ ベースの管理に必要なデバイス、ユーザ、関連を意味します。

注：スナップインがインストールされた後、新しいエントリを表示するには、ConsoleOneおよびMMCを再起動する必要があります。

スナップインのインストール後、内蔵Lights-Outオブジェクトと内蔵Lights-Outロールを、ディレクトリ内で作成できます。ユーザは、Users and Computersツールを使用して次の作業を行います。

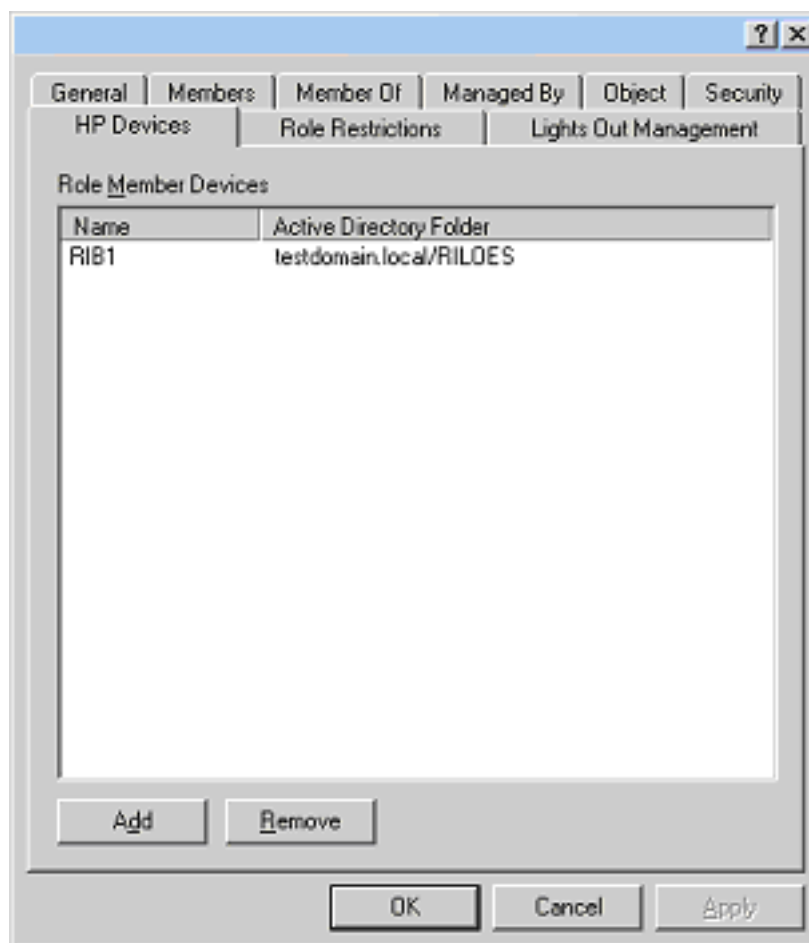
- 内蔵Lights-Outオブジェクトとロール オブジェクトの作成
- ロール オブジェクトへのユーザの追加
- ロール オブジェクトの権限と制限の設定

Active Directoryスナップイン

以下の各項では、HPスナップインがインストールされた後、Active Directory Users and Computers内で使用できるようになる管理オプションについて説明します。

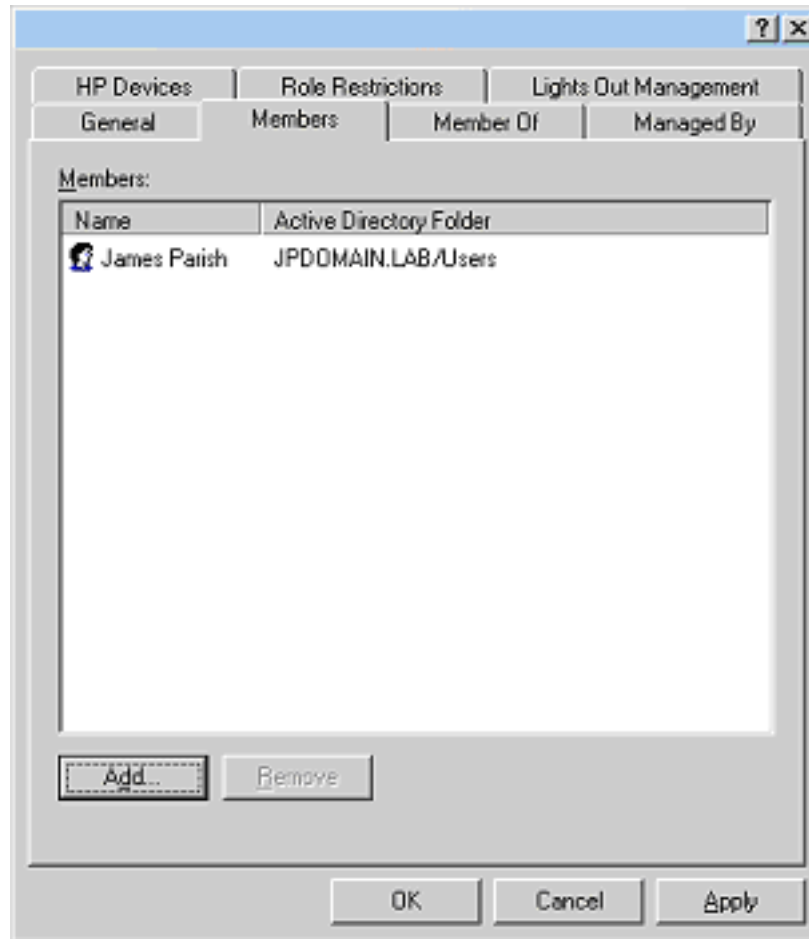
[HP Devices]

[HP Devices]タブは、管理対象となるHPデバイスをロール内で追加するために使用します。[Add]をクリックすると、特定のHPデバイスにアクセスして、そのデバイスをメンバー デバイスのリストに追加することができます。[Remove]をクリックすると、特定のHPデバイスにアクセスして、そのデバイスをメンバー デバイスのリストから削除することができます。



[Members]

ユーザ オブジェクトが作成された後、[Members]タブを使用してロール内でユーザを管理できます。[Add]をクリックすると、追加したいユーザにアクセスできます。既存のユーザを強調表示して、[Remove]をクリックすると、そのユーザは有効なメンバーのリストから削除されます。



[Role Restrictions]

[Role Restrictions]サブタブでは、ロールのログイン制限を設定できます。制限には次のものがあります。

- [Time Restrictions]
- [IP Network Address Restrictions]
 - [IP/Mask]
 - [IP Range]
 - [DNS Name]

The screenshot shows a Windows-style dialog box titled "HP Device" with a standard title bar (minimize, maximize, close buttons). The dialog has several tabs: "General", "Members", "Member Of", "Managed By", "HP Devices" (selected), "Role Restrictions", and "Lights Out Management".

Under the "Role Restrictions" tab, there are two main sections:

- Time Restrictions:** Contains a text box labeled "Effective Hours".
- IP Network Address Restrictions:** Includes a "By Default" dropdown menu currently set to "Grant". To the right of the dropdown is the text: "access from all clients, EXCEPT those listed below." Below this text is a large, empty rectangular list box.

At the bottom of the "IP Network Address Restrictions" section, there are three radio buttons: "IP/MASK" (selected), "IP Range", and "DNS Name". To the right of these radio buttons are two buttons: "Add" and "Remove".

At the very bottom of the dialog box are three buttons: "OK", "Cancel", and "Apply".

強制クライアントIPアドレスまたはDNS名アクセス

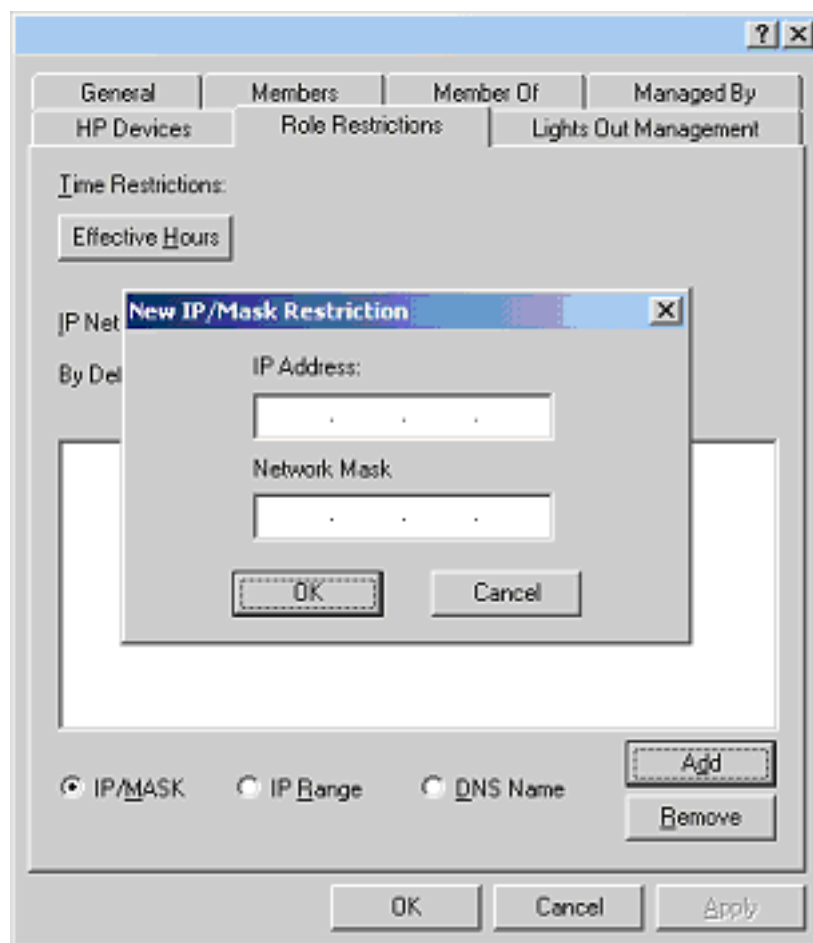
IPアドレス、IPアドレスの範囲、またはDNS名を対象にして、アクセス権限を付与または取り消すことができます。

1. **[By Default]**ドロップダウン メニューで、指定したIPアドレスを除くすべてのアドレス、IPアドレス範囲、およびDNS名からのアクセスを、**付与するか取り消すか**を選択します。
2. 追加するアドレスを選択し、制限の種類を選択してから、**[Add]**をクリックします。
3. 新しい制限ポップアップ ウィンドウで、情報を入力して、**[OK]**をクリックします。新しい制限ポップアップ ウィンドウが表示されます。

注：[DNS Name]オプションでは、単一のDNS名またはサブドメイン ベースでアクセスを制限できます。入力は、host.company.comまたは*.domain.company.comという形式で行います。

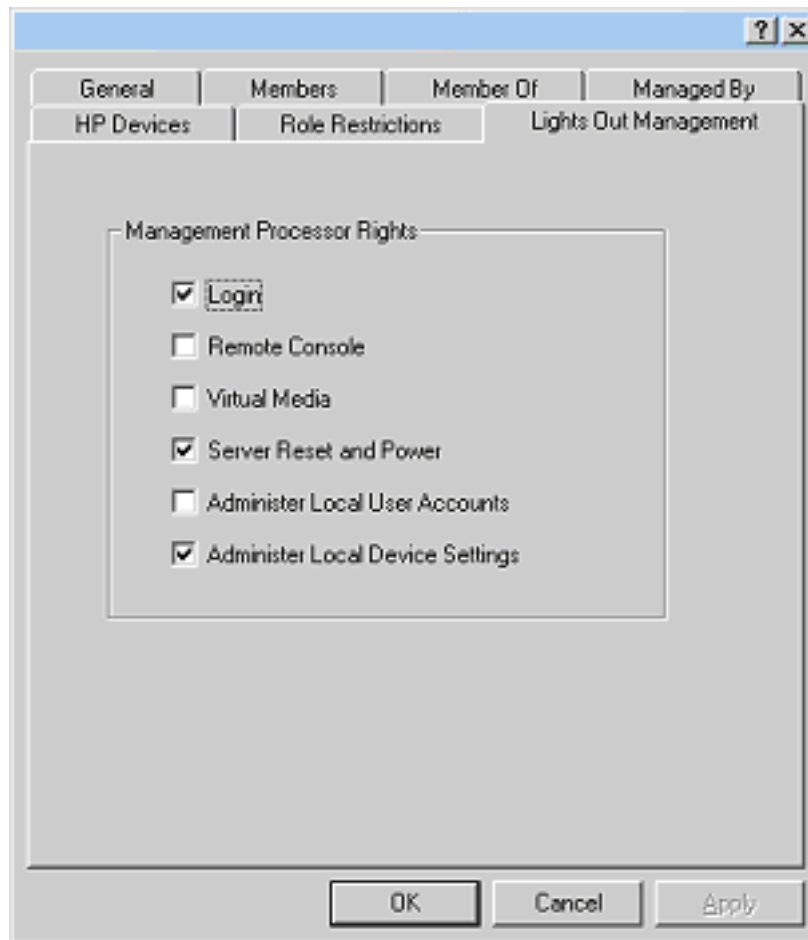
4. **[OK]**をクリックして、変更を保存します。

5. エントリのいずれかを削除するには、表示されているリストでエントリを強調表示してから、[Remove]をクリックします。



Active Directory Lights-Out Management

ロールを作成したら、そのロールの権限を選択できます。この時点で、ユーザ オブジェクトおよびグループ オブジェクトをロールのメンバーにすることにより、ユーザまたはユーザ グループにロールが付与する権限を与えることができます。権限は、[Lights Out Management]タブで管理されます。



使用できる権限は、次のとおりです。

- **[Login]** - このオプションは、関連付けられたデバイスにユーザがログインできるかどうかを制御します。

- **[Remote Console]** - このオプションは、ユーザによるリモート コンソールへのアクセスを許可します。
- **[Virtual Media]** - このオプションは、ユーザによるiLOの仮想メディア機能へのアクセスを許可します。
- **[Server Reset and Power]** - このオプションは、ユーザがiLOの仮想電源ボタンにアクセスできるようにします。仮想電源ボタンを使用すると、リモートからのサーバのリセットやサーバの電源切断が可能になります。
- **[Administer Local User Accounts]** - このオプションは、ユーザがアカウントを管理できるようにします。ユーザは、自身および他のユーザのアカウント設定の変更やユーザの追加と削除を行うことができます。
- **[Administer Local Device Settings]** - このオプションは、ユーザがiLOマネジメントプロセッサを設定できるようにします。設定には、iLO Webブラウザの**[Global Settings]**、**[Network Settings]**、**[SNMP Settings]**、および**[Directory Settings]**画面で利用できるオプションが含まれます。

eDirectoryのディレクトリ サービス

以下の各項では、eDirectoryのディレクトリ サービスの、インストールの前提条件、準備、および作業例について説明します。

eDirectoryインストールの前提条件

iLO用のディレクトリ サービスは、ディレクトリ サーバとの通信にSSL上のLDAPを使用します。iLOソフトウェアは、eDirectoryバージョン8.6.1（またはそれ以降）のツリーにインストールされるように設計されています。ご使用のeDirectoryサーバにバージョン8.6.1以前のeDirectoryがインストールされている場合、この製品のインストールはおすすめできません。eDirectory用のスナップインおよびスキーマ拡張をインストールする前に、Novell Support（<http://support.novell.com/>）で提供されている次の技術資料をよく読んでいつでも参照できるようにしておいてください。

重要：内蔵Lights-Out用のディレクトリ サービスをインストールするには、eDirectoryのスキーマを拡張する必要があります。スキーマの拡張は、スキーマ管理者が行わなければなりません。

- TID10066591 『Novell eDirectory 8.6 NDS compatibility』
- TID10057565 『Unknown objects in a mixed environment』
- TID10059954 『How to test whether LDAP is working correctly』

- TID10023209 『How to configure LDAP for SSL (secure) connections』
- TID10075010 『How to test LDAP authentication』

スナップインのインストールとeDirectory用の初期設定

1. スナップイン インストレーション アプリケーションを実行して、スナップインをインストールします。
2. ディレクトリ サービスを設定して、ディレクトリ サービスがiLOマネジメント用の適切なオブジェクトおよび関連を所有するようにします。
 - a. HPが提供するマネジメント スナップインを使用して、iLOオブジェクト、Policyオブジェクト、Adminオブジェクト、およびUser Roleオブジェクトを作成します。
 - b. HPが提供するマネジメント スナップインを使用して、iLOオブジェクト、Policyオブジェクト、Roleオブジェクトの関連を作成します。
 - c. iLOオブジェクトがAdminオブジェクトとUser Roleオブジェクトを指し示すようにします（これにより、AdminオブジェクトとUser Roleオブジェクトは、自動的にiLOオブジェクトを指し示します）。

注：内蔵Lights-Outオブジェクトについて詳しくは、「ディレクトリ サービス オブジェクト」の項を参照してください。

少なくとも、次のオブジェクトを作成する必要があります。

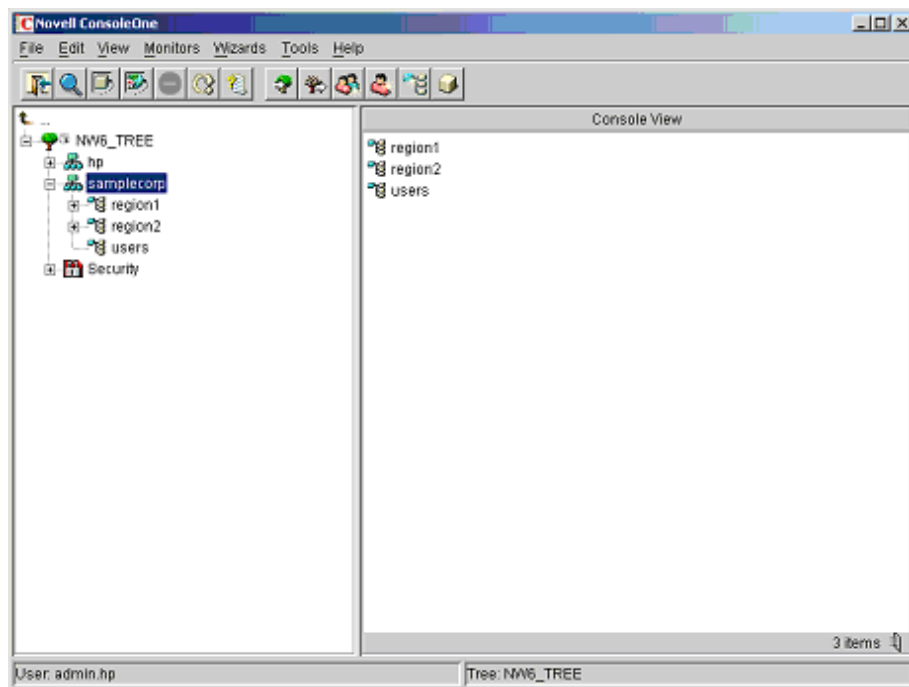
- 1人以上のユーザと1つ以上のiLOオブジェクトを含むRoleオブジェクトを1つ
- ディレクトリを使用するiLOマネジメント プロセッサごとに1つのiLOオブジェクト

注：スナップインがインストールされた後、新しいエントリを表示するには、ConsoleOneおよびMMCを再起動する必要があります。

例：eDirectory内で、iLOで使用するディレクトリ オブジェクトを作成して設定する

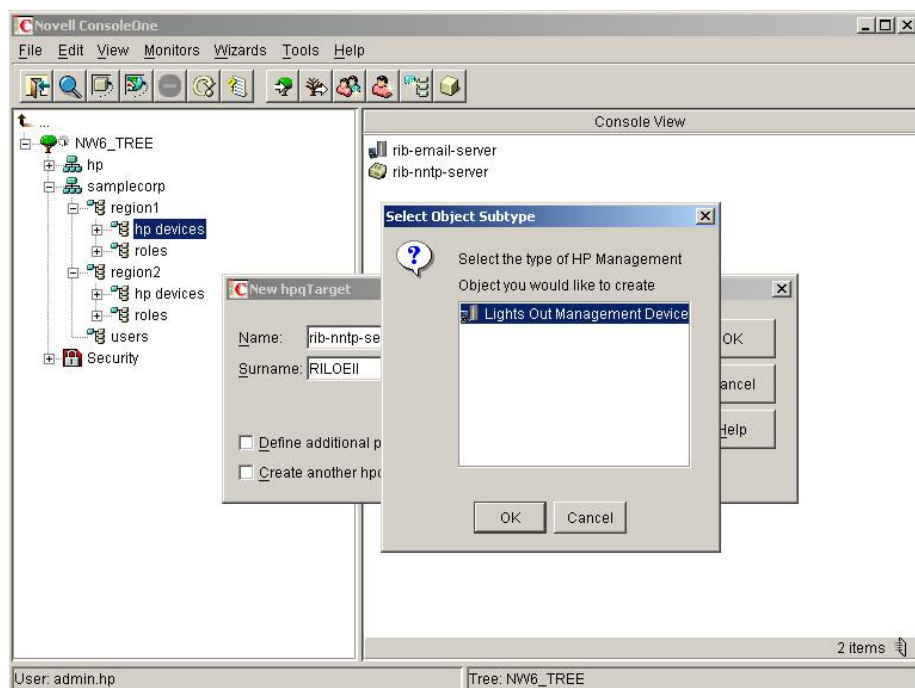
次の例では、2つの地域（region1およびregion2）から成り立つsamplecorpという名前の企業で、ロールとHPデバイスをセットアップする方法を示します。

samplecorpには、次の画面のように編成されたエンタープライズ ディレクトリがあります。



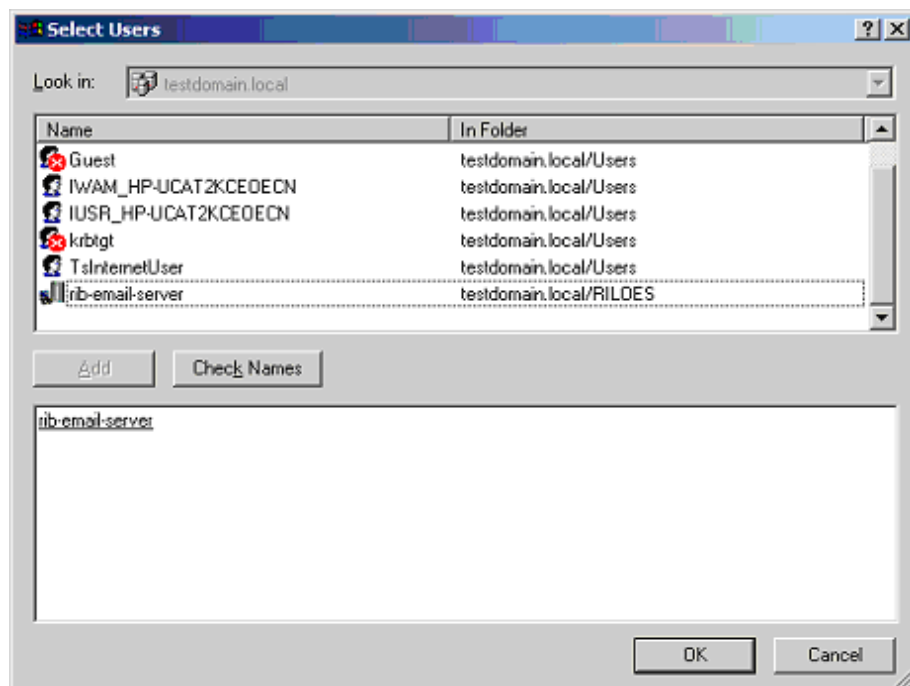
1. 各地域に組織単位を作成することから開始します。組織単位には、Lights-Out マネジメント デバイスを含み、地域固有のロールを持たせるようにします。この例では、組織単位region1とregion2に、rolesとhp devicesという名前の2つの組織単位が作成されます。
2. HP の提供する ConsoleOne スナップインを使用して、複数の iLO デバイスを対象に、組織単位hp devices内にLights-Out Managementオブジェクトを作成します。
 - a. [region1]組織単位内にある[hp devices]組織単位を右クリックして、[New]、[Object]の順に選択します。
 - b. クラスのリストから[hpqTarget]を選択して、[OK]をクリックします。
 - c. [New hpqTarget]ダイアログ ボックスに、適切な名前とsurnameを入力します。この例では、iLO デバイスのDNSホスト名rib-email-serverがLights-Out Management オブジェクト名として使用されます。surnameはRILOEIIになります。[OK]をクリックします。

- d. [Select Object Subtype]ダイアログ ボックスが表示されます。リストから[Lights Out Management Device]を選択して、[OK]をクリックします。
- e. [region1]の[hp devices]で、DNS名rib-nntp-serverとrib-file-server-users1のiLOデバイス、[region2]の[hp devices]で、DNS名rib-file-server-users2とrib-app-serverのiLOデバイスについて、手順を繰り返します。

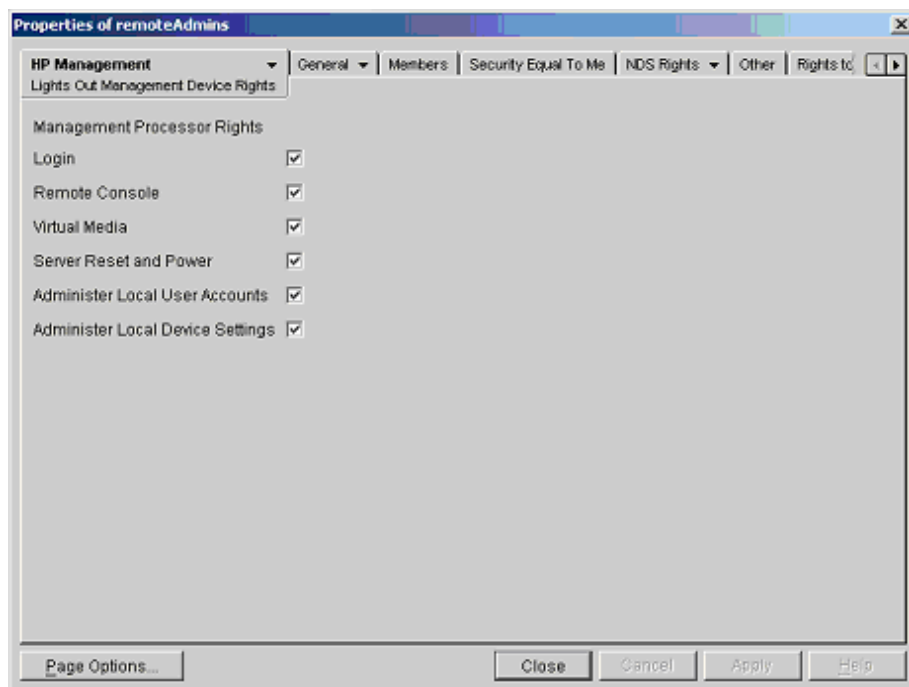


3. HPの提供するConsoleOneスナップインを使用して、[roles]組織単位内にHP Roleオブジェクトを作成します。
 - a. [region2]組織単位内にある[roles]組織単位を右クリックして、[New]、[Object]の順に選択します。
 - b. クラスのリストから[hpqRole]を選択して、[OK]をクリックします。
 - c. [New hpqRole]ダイアログ ボックスに、適切な名前を入力します。この例では、ロールには、リモート サーバの管理を行うことのできる信頼されるユーザを所属させるので、remoteAdminsと名付けます。[OK]をクリックします。

- d. [Select Object Subtype]ダイアログボックスが表示されます。このロールは、Lights-Outマネジメントデバイスに対する権限を管理するので、リストから[Lights Out Management Devices]を選択して、[OK]をクリックします。
 - e. 手順を繰り返して、[region1]の[roles]に、remoteMonitorsという名前のリモートサーバ監視用のロール、[region2]の[roles]にremoteAdminsロールとremoteMonitorsロールを作成します。
4. HPの提供するConsoleOneスナップインを使用して、ロールに権限を割り当て、ロールとユーザおよびデバイスと関連付けます。
 - a. [region1]組織単位の[roles]組織単位のremoteAdminsロールを右クリックして、[Properties]を選択します。
 - b. [HP Management]タブの[Role Managed Devices]サブタブを選択して、[Add]をクリックします。



- c. [Select Objects]ダイアログ ボックスで、[region1]組織単位の[hp devices]組織単位にアクセスします。手順2で作成した3つのLights-Out Managementオブジェクトを選択します。[OK]、[Apply]の順にクリックします。
- d. 次に、ロールにユーザを追加します。[Members]タブをクリックし、[Add]ボタンと[Select Object]ダイアログ ボックスを使用してユーザを追加します。
- e. これで、デバイスとユーザが関連付けられます。[HP Management]タブの[Lights Out Management Device Rights]サブタブを使用して、ロールの権限を設定します。ロールに所属するすべてのユーザが、ロールによって管理されるすべてのiLOデバイス上でロールに割り当てられた権限を持ちます。この例では、remoteAdminsロール内のユーザにiLOの機能へのフル アクセス権限が付与されます。各権限の横のボックスを選択して、[Apply]をクリックします。[Close]をクリックして、プロパティ シートを閉じます。



5. 手順4で説明した手順を参照して、remoteMonitorsロールのプロパティを編集します。

- a. [region1]の[hp devices]内にある3つのiLOデバイスを[HP Management]タブの[Role Managed Devices]サブタブ上の[Managed Devices]リストに追加します。
- b. [Members]タブを使用して、ユーザをremoteMonitorsロールに追加します。
- c. 次に、[HP Management]タブの[Lights Out Management Device Rights]サブタブで、[Login]の横のチェックボックスを選択し、[Apply]、[Close]の順にクリックします。remoteMonitorsロールのメンバーは、サーバステータスへのアクセスの認証を受けることができ、サーバステータスを表示できます。

内蔵Lights-Outデバイスに対するユーザ権限は、そのユーザがメンバーとして所属し、その内蔵Lights-Outデバイスが管理対象デバイスとなっているすべてのロールによって割り当てられたすべての権限の和とみなされます。上記の例では、あるユーザがremoteAdminロールとremoteMonitorsロールの両方に所属する場合、remoteAdminsロールがすべての権限を持っているため、そのユーザはすべての権限を持つことになります。

内蔵Lights-Outデバイスを設定して、この例のLights-Out Managementオブジェクトと関連付けるには、[Directory Settings]画面で次のような設定を使用してください。

注：LDAP識別名では、各コンポーネントを区切るのにピリオドではなくカンマを使用します。

```
RIB Object DN = cn=rib-email-server,ou=hp
devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

たとえば、samplecorp組織内のusers組織単位に所属するユーザCSmithが、remoteAdminsロールまたはremoteMonitorsロールのうちのいずれかのメンバーでもある場合、iLOにログインできます。この例では、iLOログイン画面の[Login Name]フィールドにcsmith（大文字と小文字は区別されません）、同じ画面の[Password]フィールドにそのeDirectoryパスワードをタイプしてアクセスすることになります。

eDirectory用のディレクトリ サービス オブジェクト

ディレクトリ ベースの管理で大切なことの1つは、ディレクトリ サービス内の管理対象デバイスを正しく仮想化することです。この仮想化によって、管理者は、ディレクトリ サービス内にすでに存在する管理対象デバイスとユーザまたはグループとを関連付けることができます。内蔵Lights-Outのユーザ管理では、ディレクトリ サービス内に次の3つの基本オブジェクトが必要です。

- Lights-Out Managementオブジェクト

- Roleオブジェクト
- Userオブジェクト

各オブジェクトは、ディレクトリ ベースの管理に必要なデバイス、ユーザ、関連を意味します。

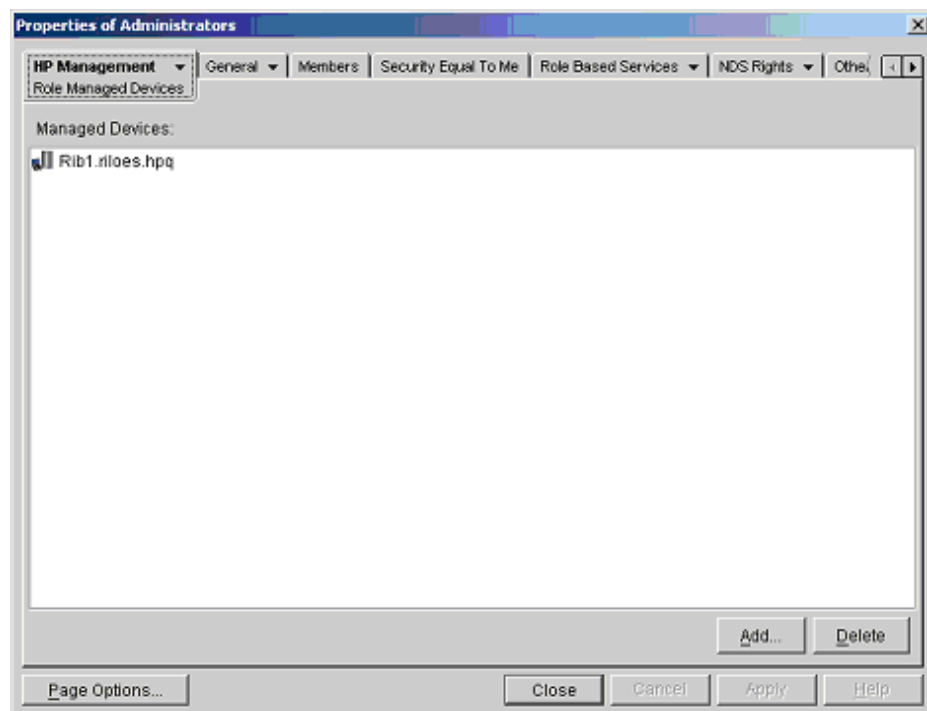
注：スナップインがインストールされた後、新しいエントリを表示するには、ConsoleOneおよびMMCを再起動する必要があります。

スナップインのインストール後、内蔵Lights-Outオブジェクトと内蔵Lights-Outロールを、ディレクトリ内で作成できます。ユーザは、Users and Computersツールを使用して次の作業を行います。

- 内蔵Lights-Outオブジェクトとロール オブジェクトの作成
- ロール オブジェクトへのユーザの追加
- ロール オブジェクトの権限と制限の設定

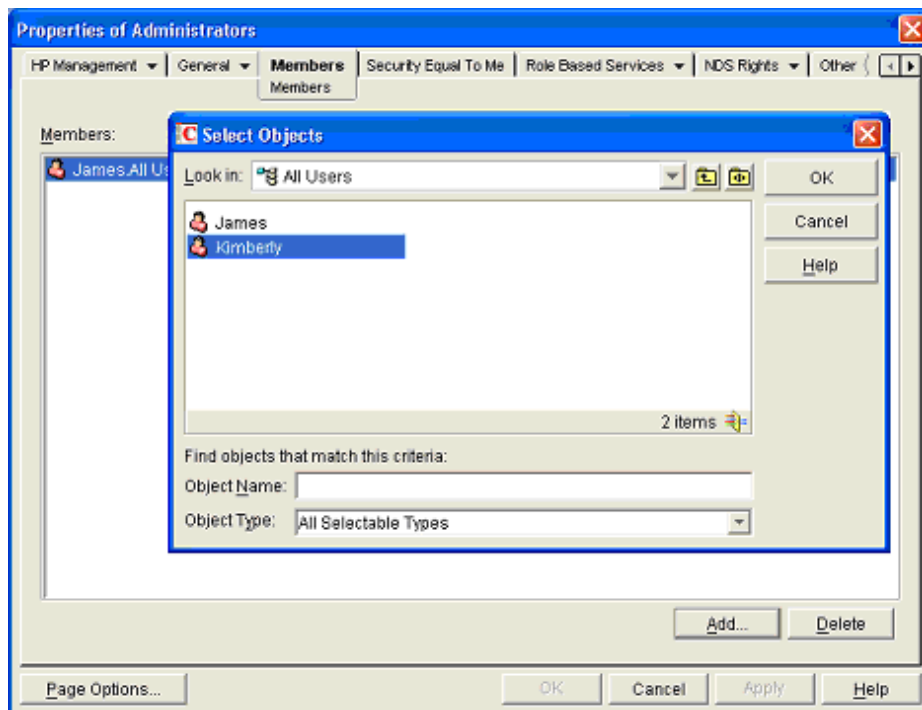
[Role Managed Devices]

[HP Management]タブの[Role Managed Devices]サブタブは、管理対象となるHPデバイスをロール内で追加するために使用します。[Add]をクリックすると、特定のHPデバイスにアクセスして、そのデバイスを管理対象デバイスとして追加できます。



[Members]

ユーザ オブジェクトが作成された後、[Members]タブを使用してロール内でユーザを管理できます。[Add]をクリックすると、追加したいユーザにアクセスできます。既存のユーザを強調表示して、[Delete]をクリックすると、そのユーザは有効なメンバーのリストから削除されます。

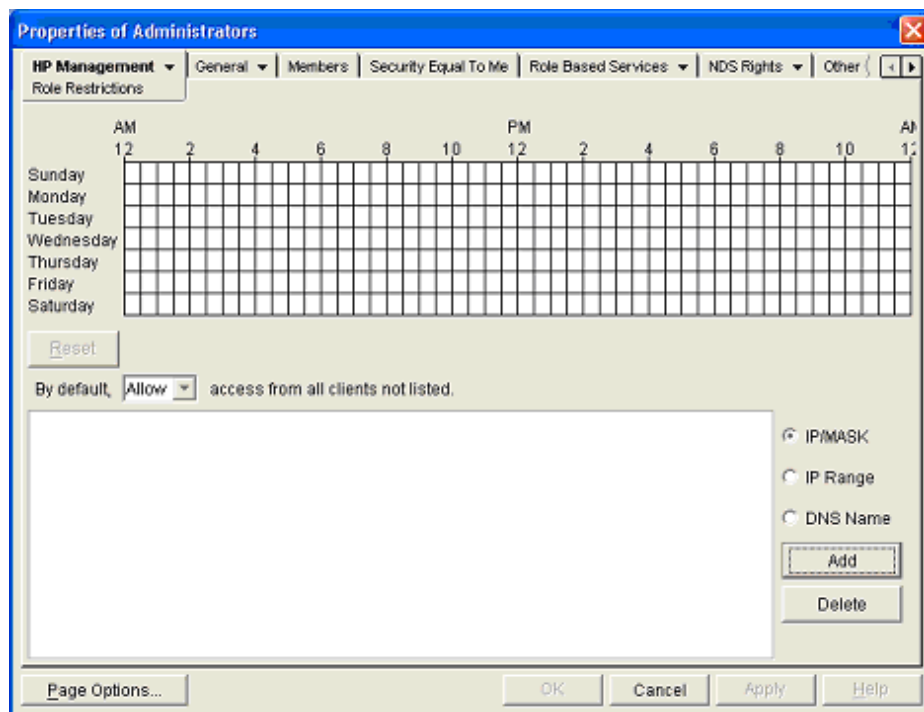


[Role Restrictions]

[Role Restrictions]サブタブでは、ロールのログイン制限を設定できます。制限には次のものがあります。

- [Time Restrictions]
- [IP Network Address Restrictions]
 - [IP/Mask]

- [IP Range]
- [DNS Name]



[Time Restrictions]

[Role Restrictions]サブタブに表示されるタイム グリッドを使用して、ロールのメンバーがログオンできる時間帯を管理できます。ログオンできる時間を、曜日ごとに30分単位で選択できます。四角形のボックスを1つだけ変更する場合は、そのボックスをクリックしてください。連続した四角形のボックスをまとめて変更するには、マウス ボタンを押したまま、変更する各ボックス上でカーソルをドラッグして、マウス ボタンを離してください。デフォルトでは、常時アクセスできるように設定されています。

強制クライアントIPアドレスまたはDNS名アクセス

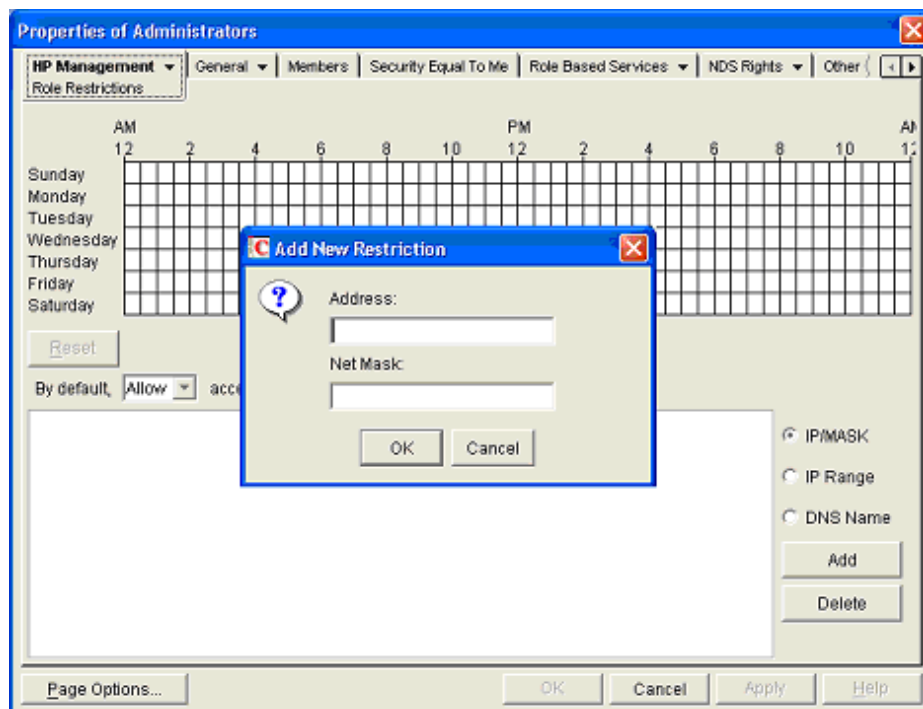
IPアドレス、IPアドレスの範囲、またはDNS名を対象にして、アクセス権限を付与または取り消すことができます。

1. **[By Default]**ドロップダウン メニューで、指定したIPアドレスを除くすべてのアドレス、IPアドレス範囲、およびDNS名からのアクセスを、許可するか取り消すかを選択します。
2. 追加するアドレスを選択し、制限の種類を選択してから、**[Add]**をクリックします。
3. **[Add New Restriction]**ポップアップ ウィンドウで情報を入力して、**[OK]**をクリックします。[IP/Mask]オプション用の**[Add New Restriction]**ポップアップ ウィンドウが表示されます。

注：[DNS Name]オプションでは、単一のDNS名またはサブドメイン ベースでアクセスを制限できます。入力は、host.company.comまたは*.domain.company.comという形式で行います。

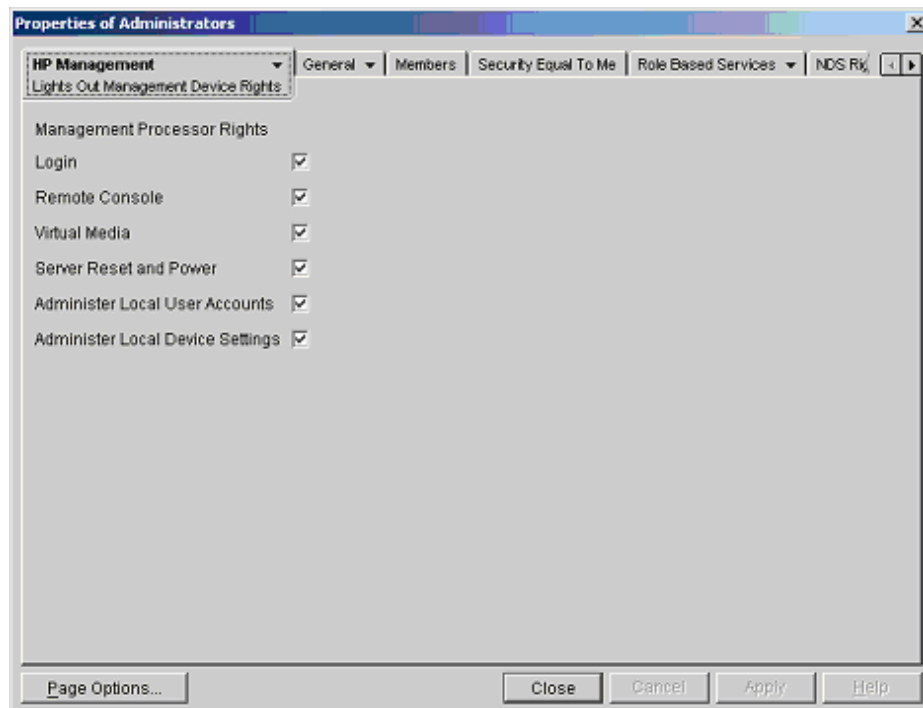
4. **[Apply]**をクリックして、変更を保存します。

エントリのいずれかを削除するには、表示されているフィールドでエントリを強調表示してから、**[Delete]**をクリックします。



Lights-Out Management

ロールを作成したら、そのロールの権限を選択できます。この時点で、ユーザ オブジェクトおよびグループ オブジェクトをロールのメンバーにすることにより、ユーザまたはユーザ グループにロールが付与する権限を与えることができます。権限は、[HP Management]タブの[Lights Out Management Device Rights]サブタブで管理されます。



使用できる権限は、次のとおりです。

- **[Login]** - このオプションは、関連付けられたデバイスにユーザがログインできるかどうかを制御します。
- **[Remote Console]** - このオプションは、ユーザによるリモート コンソールへのアクセスを許可します。
- **[Virtual Media]** - このオプションは、ユーザによるiLOの仮想メディア機能へのアクセスを許可します。

- [Server Reset and Power] - このオプションは、ユーザがiLOの仮想電源ボタンにアクセスできるようにします。仮想電源ボタンを使用すると、リモートからのサーバのリセットやサーバの電源切断が可能になります。
- [Administer Local User Accounts] - このオプションは、ユーザがアカウントを管理できるようにします。ユーザは、自身および他のユーザのアカウント設定の変更やユーザの追加と削除を行うことができます。
- [Administer Local Device Settings] - このオプションは、ユーザがiLOマネジメントプロセッサを設定できるようにします。設定には、iLO Webブラウザの[Global Settings]、[Network Settings]、[SNMP Settings]、および[Directory Settings]画面で利用できるオプションが含まれます。

ディレクトリの設定

The screenshot shows the HP iLO web interface for Directory Settings. The top header includes the HP iLO logo, server name (HP-PKXJFOR8WFDG), iLO name (ILOD234KJ440002), and current user (Administrator). The navigation bar has tabs for System Status, Remote Console, Virtual Devices, and Administration. The left sidebar lists various settings categories, with Directory Settings selected. The main content area is titled 'Directory Settings' and contains the following configuration options:

- Enable Directory Authentication: ☒ Yes ☐ No
- Enable Local User Accounts: ☐ Yes ☒ No
- Directory Server Address:
- Directory Server LDAP Port:
- LOM Object Distinguished Name:
- LOM Object Password:
- LOM Object Password Confirm:
- Directory User Context 1:
- Directory User Context 2:
- Directory User Context 3:

At the bottom of the form are two buttons: 'Test Settings' and 'Apply Settings'.

[Directory Settings]画面には、次の設定オプションがあります。

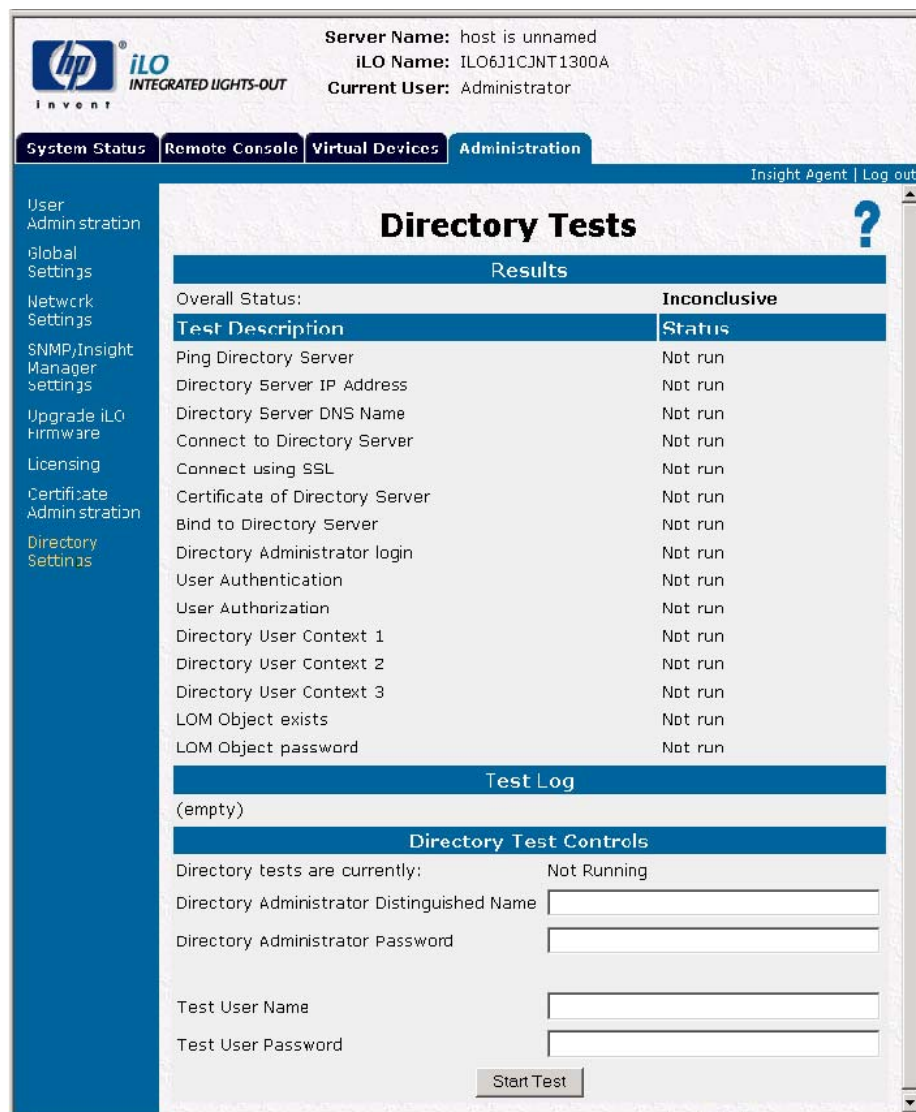
- **[Directory Authentication]** - ディレクトリ サーバがユーザ ログインの認証に使用されるかどうかを指定します。この設定は、デフォルトでは**[Disabled]**になっています。
- **[Local User Accounts]** - ユーザがディレクトリ アカウントではなくローカル ユーザ アカウントを使用してログインできるようにします。この設定は、デフォルトでは**[Enabled]**になっています。
- **[Directory Server Address]** - ディレクトリ サーバのIPアドレスまたはDNS名あるいはドメインの名前を指定します。ユーザ認証にディレクトリ サービスを使用する場合は、この設定が必要です。DNS名またはマルチホストDNS名の使用をおすすめします。IPアドレスを使用すると、そのサーバが停止したときディレクトリを使用できなくなります。
- **[Directory Server LDAP Port]** - LDAP通信に使用するポートを指定します。デフォルト設定は、セキュリティ保護されているLDAPのポート番号636です。LDAPポートを変更する場合は、SSLポート上のLDAPでなければなりません。
- **[LOM Object Distinguished Name]** - ディレクトリ サービス内のLights-Out Device オブジェクトの完全識別名を指定します（例：CN=RILOE2OBJECT,CN=Users, DC=HP,DC=com）。識別名は、256文字までに制限されています。
- **[LOM Object Password]** - ディレクトリ内の対応するオブジェクトにログインする際にLights-Out Deviceオブジェクトが使用するパスワードを指定します。パスワードは、iLOがディレクトリと通信するために使用されます。ディレクトリをユーザ認証とアクセスにのみ使用する場合は、このパスワードは不要です。パスワードは、39文字までに制限されています。

注：現時点では、[LOM Object Password]フィールドは使用されません。このフィールドは、将来のファームウェア リリースとの上位互換性を保つために提供されています。
- **[Directory User Context]** - ユーザを認証する際の検索コンテキストを指定します。これらの設定は、ディレクトリ サービス内でのユーザの位置を指し示します。これにより、ユーザはログインする際に、フル ツリー構造を入力する必要がなくなります（例：CN=Users,DC=HP,DC=com）。Directory User Contextは、それぞれ128文字までに制限されています。

画面の内容を変更する場合は、**[Apply Settings]**をクリックしてください。**[Test Settings]**を使用して、ディレクトリ サーバとiLOボード間の通信をテストすることができます。

ディレクトリ テスト

iLOに対する現在のディレクトリ設定の有効性を確認するには、[Directory Settings]ページの[Test Settings]ボタンをクリックします。[Directory Tests]ページが表示されます。



hp iLO INTEGRATED LIGHTS-OUT

Server Name: host is unnamed
iLO Name: ILO6J1CJNT1300A
Current User: Administrator

System Status Remote Console Virtual Devices Administration

Insight Agent | Log out

User Administration
Global Settings
Network Settings
SNMP/Insight Manager settings
Upgrade iLO firmware
Licensing
Certificate Administration
Directory Settings

Directory Tests ?

Results	
Test Description	Status
Overall Status:	Inconclusive
Ping Directory Server	Not run
Directory Server IP Address	Not run
Directory Server DNS Name	Not run
Connect to Directory Server	Not run
Connect using SSL	Not run
Certificate of Directory Server	Not run
Bind to Directory Server	Not run
Directory Administrator login	Not run
User Authentication	Not run
User Authorization	Not run
Directory User Context 1	Not run
Directory User Context 2	Not run
Directory User Context 3	Not run
LOM Object exists	Not run
LOM Object password	Not run

Test Log

(empty)

Directory Test Controls

Directory tests are currently: Not Running

Directory Administrator Distinguished Name

Directory Administrator Password

Test User Name

Test User Password

Start Test

テスト ページには、現在のディレクトリ設定の有効性を確認するために設計された一連の簡単なテストの結果が表示されます。また、このページには、テスト結果および検出された問題を示すテスト ログも表示されます。ディレクトリを正しく設定した後、これらのテストを再実行する必要はありません。[Directory Tests]画面には、ユーザがディレクトリ ユーザとしてログインする必要はありません。

ディレクトリ設定の有効性を確認するには、ディレクトリ管理者の識別名とパスワードを入力します。ディレクトリ内にiLOオブジェクトを作成する際に使用するものと同じ識別名とパスワードを使用することをおすすめします。これらの識別名とパスワードは、iLOによって保存されるものではなく、iLOオブジェクトとユーザ検索コンテキストを確認するために使用されます。

テスト用のユーザ名とパスワードも入力します。通常は、テスト対象のiLOへのアクセスに利用するアカウントを使用します。ディレクトリ管理者と同じアカウントでかまいませんが、テストは、"superuser"アカウントを使用してユーザ認証を確認することはできません。これらのユーザ名とパスワードは、iLOによって保存されるものではありません。

[Start Test]ボタンを押すと、複数のテストがバックグラウンドで開始されます。最初、ディレクトリ ユーザによるネットワークpingが実行され、次に、サーバへのSSL接続が確立され、通常のログインと同じようにユーザの権限が評価されます。

テストの実行中、ページは定期的に更新されます。テストの実行中にいつでも、テストを停止したり、手動でページを更新したりすることができます。

ページのヘルプ リンクを利用して、テストの詳細や問題が発生した場合の処置を確認してください。

iLOへのユーザ ログイン

iLOのログイン ページの[Login Name]フィールドは、次に示す項目をすべて受け入れます。

- ディレクトリ ユーザ
- LDAP完全識別名

例：CN=John Smith,CN=Users,DC=HP,DC=COM、または@HP.com

注：ログイン名だけの短い形式は、アクセスしようとしているドメインをディレクトリに通知しません。ドメイン名を入力するかまたはアカウントのLDAP識別名を使用する必要があります。

- ドメイン¥ユーザ名形式（Active Directoryのみ）

例：HP¥jsmith

- ユーザ名@ドメイン形式（Active Directoryのみ）

例：jsmith@hp.com

注：@検索可能形式を使用して指定されるディレクトリ ユーザは、3つの検索可能コンテキストのいずれかに配置できます。このコンテキストは、[Directory Settings]で設定されます。

- ユーザ名形式

例：John Smith

注：ユーザ名形式を使用して指定されるディレクトリ ユーザは、3つの検索可能コンテキストのいずれかに配置できます。このコンテキストは、[Directory Settings]で設定されます。

- ローカル ユーザ - ログインID

注：iLOのログイン ページでは、[Login Name]の最大長は、ローカル ユーザについては39文字、ディレクトリ サービス ユーザについては256文字です。

ローカル ユーザ データベースは、保持されます。ディレクトリを使用しないことも、ディレクトリとローカル アカウントを組み合わせ使用することも、認証用にのみディレクトリを使用することも可能です。

注：診断ポートを介して接続されている場合、ディレクトリ サーバは利用できません。ローカル アカウントを使用する場合のみ、ログインできます。

グループ管理と内蔵Lights-Outスクリプティング

この項の目次

Lights-Out設定ユーティリティの特長	141
Lights-Out設定ユーティリティおよびInsightマネージャ7を使用したグループ管理	142
Lights-Out設定ユーティリティを使用したバッチ処理	145

Lights-Out設定ユーティリティの特長

バージョン1.10のファームウェアでは、XMLベースのスクリプトによるiLOの設定のサポートが追加されます。ユーザ管理、グローバル設定、ネットワーク設定、SNMP/Insightマネージャ設定、iLOファームウェアの更新、ライセンス許諾、およびProLiant BL p-Classラックの設定を、iLOスクリプティングを使用して設定できます。

iLOで利用できるスクリプティング ユーティリティは、Lights-Out設定ユーティリティ（*CPQLOCFG.EXE*）です。このユーティリティは、ネットワーク経由のセキュリティ保護された接続を使用してiLOに接続する、Windowsベースのユーティリティです。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。

CPQLOCFGユーティリティは、Insightマネージャ7から起動してグループ管理に使用したり、コマンド プロンプトで個別に使用してバッチ処理に利用したりすることができます。

注：iLOのディレクトリ設定用XMLスクリプトを設定するには、*CPQLOCFG.EXE*のバージョン2.2が必要です。

Lights-Out設定ユーティリティは、以下の機能を実行できます。

- ユーザの追加、変更、または削除
- 個々のユーザやすべてのユーザの設定情報の表示
- ネットワーク設定の変更
- グローバル設定の変更

- ディレクトリ設定の変更
- iLOイベント ログのクリア
- iLOファームウェア バージョンの表示
- iLOファームウェアの更新
- リモート コンソール ホット キーの設定
- 仮想電源ボタンのステータスの表示と設定
- サーバの電源ステータスの表示
- サーバのリセット

Lights-Out設定ユーティリティおよび Insightマネージャ7を使用したグループ管理

ファームウェアの更新が完了したら、IT管理者はInsightマネージャ7を使用して複数のiLOプロセッサを管理できます。グループ管理の4つの構成要素は、RIBCL、Lights-Out設定ユーティリティ、Insightマネージャ7のクエリ定義、およびアプリケーション起動です。

Insightマネージャ7は、iLOデバイスをマネジメント プロセッサとして検出します。Insightマネージャ7は、Lights-Out設定ユーティリティを使用して、RIBCLファイルをiLOプロセッサのグループに送信し、これらのiLOプロセッサのユーザ アカウントを管理します。送信を受けると、iLOプロセッサは、RIBCLファイルで指定された処理を実行し、ログ ファイルに応答を送信します。

Lights-Out設定ユーティリティ

Lights-Out設定ユーティリティは、iLOボード上でRIBCLスクリプトを実行するために使用します。このユーティリティの実行ファイルは、*CPQLOCFG.EXE*です。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。

Lights-Out設定ユーティリティは、Insightマネージャ7と同じサーバに常駐していなければなりません。Lights-Out設定ユーティリティは、ランタイム エラーおよびシンタックス エラーの2種類のエラー メッセージを生成します。ランタイム エラーは、不正な操作が要求されたときに発生します。

注：ランタイム エラーは、次のディレクトリにログとして記録されます。
C:\PROGRAM FILES\INSIGHT MANAGER 7

無効なXMLタグが検出された場合、シンタックス エラーが発生します。シンタックス エラーが発生すると、Lights-Out設定ユーティリティは、実行を停止してランタイム スクリプトと出力ログ ファイルにエラーを記録します。

注：シンタックス エラーは、次の例に示すように "Syntax error: expected 'x' but found 'y' " の書式をとります。
Syntax error: expected USER_LOGIN=userlogin but found USER_NAME=username

エラーの詳細なリストについては、RIBCLの項（159ページの「リモートInsightボード コマンド言語」）を参照してください。

Insightマネージャ7のクエリ定義

すべてのiLOボードをグループ化するには、Insightマネージャ7にログインして、クエリを作成してください。

クエリを作成するには、以下の手順に従ってください。

1. Insightマネージャ7にログインします。
2. 画面左上のナビゲーション バーの[デバイス]をクリックします。
3. [クエリ]をクリックしたあと、[デバイス]をクリックします。
4. メイン ウィンドウの[パーソナル クエリ]セクションを確認します。クエリ カテゴリが存在する場合は、手順7に進みます。そうでない場合は、手順5に進みます。
5. [新規]をクリックして、新しいカテゴリを作成します。たとえば、新しいカテゴリの名前を "RIB Cards" とします。[カテゴリの作成]をクリックします。
6. [クエリ]をクリックして、[デバイス クエリ]画面に戻ります。
7. 該当するクエリ カテゴリ内で[新規]をクリックして、[クエリの作成/編集]画面を開きます。ここで、クエリ定義を作成します。
8. クエリ名を定義します。たとえば、 "Mgmt Processors" とします。
9. [デバイスの種類]、[製品名別デバイス]の順に選択します。条件ウィンドウで、製品名を "Integrated Lights-Out" に設定します。
10. [クエリ説明]フィールドで[種類]をクリックします。これによりポップアップウィンドウが開き、ここでデバイスの種類を定義します。

11. **[マネジメント プロセッサ]**を選択して、**[OK]**をクリックします。
12. **[保存]**をクリックして、**[デバイス クエリ]**画面に戻ります。
13. 該当するクエリ カテゴリ内で新しく作成したクエリを見つけて、クエリ名をクリックし、確認のために実行します。
14. 確認が実行されたら、画面左側の**[概要]**をクリックします。デバイスの初期ページが開きます。

Insightマネージャ7を使用したアプリケーション起動

アプリケーション起動は、RIBCL、Lights-Out設定ユーティリティ、およびクエリ定義を結合して、iLOマネジメント プロセッサのグループ管理機能を管理します。

アプリケーション起動タスクを作成するには、以下の手順に従ってください。

1. 画面左上のナビゲーション バーの**[デバイス]**をクリックします。
2. **[タスク]**をクリックして、**[タスク]**画面を開きます。
3. **[新規制御タスクの作成]**をクリックします。ドロップダウン メニューが表示されます。
4. ドロップダウン メニューから**[アプリケーション起動]**をクリックして、**[タスクの作成/編集]**画面を開きます。
5. 提供される領域にLights-Out設定ユーティリティのフル パスと名前を入力します。CPQLOCFG.EXEファイルがC:¥ドライブのルート ディレクトリにある場合は、パスは次のようになります。C:¥cpqlcfg.exe.
6. 表示されるエリアにパラメータを入力します。Insightマネージャ7は、Lights-Out設定ユーティリティ用に次のパラメータを要求します。

-F - RIBCLファイル名のフル パス

-V - verboseメッセージ (オプション)

RIBCLファイルがC:¥ドライブのルート ディレクトリにある場合は、パラメータは次のようになります。

-F C:¥MANAGEUSERS.xml -V

注：Insightマネージャ7では、-Lパラメータで出力ログ ファイルを指定することはできません。DNS名またはIPアドレス名が付けられたデフォルトのログ ファイルは、CPQLOCFGが起動している場所と同じディレクトリに作成されます。

7. **[次へ]**をクリックします。タスクの命名、クエリの関連付けの定義、およびタスクの予定を設定するためのオプションを示した画面が表示されます。
8. **[このタスクの名前]**フィールドにタスク名を入力します。
9. 初めに作成したクエリを選択します。たとえば、"Mgmt Processors"です。
10. **[予定]**をクリックして、アプリケーション起動タスクを実行する時期を定義します。[スケジュール設定]ウィンドウが表示されます。
11. **[OK]**をクリックして、スケジュールを設定します。

注：制御タスクのデフォルトスケジュールは、**[今すぐ実行]**です。
12. **[完了]**をクリックして、アプリケーション起動タスクを保存します。
13. **[タスクの実行]**アイコン（緑色の三角形のマーク）をクリックして、グループ管理を実行します。

注：Insightマネージャ7では、-Lパラメータで出力ログ ファイルを指定することはできません。DNS名またはIPアドレス名が付けられたデフォルトのログ ファイルは、CPQLOCFGが起動している場所と同じディレクトリに作成されます。

注：シンタックス エラーは、次の例に示すように"Syntax error: expected 'x' but found 'y' "の書式をとります。
Syntax error: expected USER_LOGIN=userlogin but found USER_NAME=username

Lights-Out設定ユーティリティを使用したバッチ処理

バッチ処理を使用して、iLOのグループ管理を実行することもできます。バッチ処理で使用する構成要素は、Lights-Out設定ユーティリティ、RIBCLファイル、およびバッチ ファイルです。

Lights-Out設定ユーティリティのパラメータ

Lights-Out設定ユーティリティは、内蔵Lights-Out上でRIBCL（159ページの「リモートInsightボード コマンド言語」）を実行するために使用します。Lights-Out設定ユーティリティの実行可能なファイルは、*CPQLOCFG.EXE*です。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。

次に、内蔵Lights-Outのグループ管理に使用できるバッチ ファイルの例を示します。

```
REM Updating the Integrated Lights-Out board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\¥...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\¥...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\¥...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
CPQLOCFG -S RIBN -F C:\¥...SCRIPT.XML -L LOGFILE.TXT -V
```

- -Sは、更新される内蔵Lights-Outを確認するスイッチです。このスイッチでは、ターゲット サーバのDNS名またはIPアドレスを指定します。

iLOから起動する場合は、このスイッチを使用しないでください。Insightマネージャ7は、*CPQLOCFG.EXE*の起動時に、Insightマネージャ7のアドレスを提示します。

- -Fは、RIBCLファイルの絶対パスで示した位置と名前を指定するスイッチです。このファイルには、iLOボード上で実行される処理が記載されています。
- -Lは、ログ ファイルの生成される位置とファイル名を定義するスイッチです。このスイッチを省略すると、DNS名またはIPアドレスを使用したファイル名が付けられたデフォルトのログ ファイルが、CPQLOCFGが起動したディレクトリに作成されます。

Insightマネージャ7から起動する場合は、このスイッチを使用しないでください。

- -Vは、オプション スイッチで、verboseメッセージの返送をオンにします。結果として生成されるログ ファイルには、リモートInsightボードに送信されたすべてのコマンド、リモートInsightボードからのすべての応答、およびすべてのエラーが記録されます。このスイッチを設定しない場合、デフォルトで、エラーとGETコマンドの応答だけがログに記録されます。

- -Cを設定すると、CPQLOCFGは、XMLの書式をチェックしますが、リモートInsightボードへの接続は開きません。

スイッチ-Lおよび-Vは、IT管理者の好みによって設定される場合とされない場合があります。

同じディレクトリにない場合は、必ずLights-Out設定ユーティリティをPATH環境変数で参照されるディレクトリに配置してください。生成されるログ ファイルは、Lights-Out設定ユーティリティの実行可能プログラムと同じディレクトリに配置してください。

注：Lights-Out設定ユーティリティは、既存のログ ファイルに上書きします。

Lights-Out DOSユーティリティ

この項の目次

Lights-Out DOSユーティリティの概要	149
CPQLODOSの一般的なガイドライン	150
コマンドライン引数	150
CPQLODOS	152
MOD_NETWORK_SETTINGS	152
MOD_DIR_CONFIG	155
ADD_USER	157

Lights-Out DOSユーティリティの概要

CPQLODOSは、SmartStart Scripting Toolkitに含まれるコマンドラインユーティリティです。このユーティリティは、iLOの必須の設定項目だけをセットアップするための初期設定プログラムです。この必須の設定項目は、全機能を備えた他の設定方法のいずれかを使用するために必要です。このように利用方法が限定されているため、CPQLODOSは、iLOスクリプティング言語のごく一部だけを処理します。

注：CPQLODOSは、DOS専用のツールであり、MS-DOS® 6.0以降を必要とします。Lights-Outスクリプティングは、Linuxオペレーティングシステムではサポートされていません。また、Novell NetWareクライアントを使用する場合もサポートされません。

CPQLODOSを使用すると、F8起動またはグラフィカルユーザインタフェースを介して表示される機能を設定できます。このユーティリティは、継続的な管理には使用しません。サーバ上で、ユーザの権限やネットワーク機能を管理するには、RIBCLを使用してください。

注：このユーティリティは、基本的には再設定ツールです。既存の設定がある場合は、削除されます。

CPQLODOSの一般的なガイドライン

この項では、すべてのコマンドが機能ごとにグループ分けされています。ユーザ情報を処理するすべてのコマンドは、1つのグループにまとめられます。コマンドをグループ化することにより、ファームウェアは処理されるデータを、テキスト文書と同様の情報ブロックとみなすことができ、異なる種類の情報へのマルチスレッド アクセスが可能になります。

開始コマンドによりデータベースが開かれます。このデータベースは、対応する終了コマンドが送信されるまで開いたままです。1つのコマンド ブロック内で実行されたすべての変更は、データベースの終了時に、同時に適用されます。コマンド ブロック内にエラーがある場合は、ブロック内の変更は放棄されます。

次に、開始コマンドと対応する終了コマンドの例を示します。

```
<USER_INFO>  
</USER_INFO>
```

以下の各項では、すべての例で、開始コマンドと終了コマンドを示します。

コマンド ライン引数

次の表に、CPQLODOSが認識する引数を示します。

コマンドライン引数	説明
/HELPまたは/?	簡単なヘルプメッセージを表示します。
/RESET_RILOE	iLOマネジメント プロセッサを工場出荷時のデフォルト設定にリセットします。
/DETECT	ターゲット サーバ上でiLOマネジメント プロセッサを検出します。
/RESET_RILOE	iLOマネジメント プロセッサをリセットします。
/VIRT_FLOPPY	仮想フロッピー挿入エラーを無視します。
/MIN_FW-xxx	最小ファームウェア バージョンを設定できるようにします。このファームウェアに基づいてiLOマネジメント プロセッサは稼働します。
/GET_STATUS	iLOマネジメント プロセッサのステータスを返します。
/GET_HOSTINFO	iLOマネジメント プロセッサ上の最新のホスト サーバ情報を取得して表示し、サーバ名と番号を表示します。
/GET_USERINFO	iLOマネジメント プロセッサ ボードに格納されている最新のユーザ情報を取得して、名前、ログイン名、およびセキュリティ マスク情報を表示します。
/GET_NICCONFIG	iLOマネジメント プロセッサに格納されているNIC設定情報を取得して表示します。
/GET_DHCPCONFIG	iLOマネジメント プロセッサに格納されているDHCP設定情報を取得して表示します。
/GET_DIRCONFIG	iLOマネジメント プロセッサに格納されているディレクトリ設定情報を取得して表示します。
/WRITE_XML=A:¥DL360.RLO	iLOマネジメント プロセッサ上の設定を読み出し、NIC、DHCP、ディレクトリ、およびユーザ設定をXMLハードウェア コンフィギュレーション スクリプト ファイルに書き込みます。
/LOAD_XML=A:¥DL360.RLO	スクリプト ファイルをロードして、その変更点をiLOマネジメント プロセッサの現在のコンフィギュレーションに適用します。
/VERIFY_XML	スクリプト ファイルに間違いがないかを調べて、誤ったデータがある場合は、エラー メッセージを生成します。

CPQLODOSは、<CPQLODOS>、<MOD_NETWORK_SETTINGS>、<MOD_DIR_CONFIG>、および<ADD_USER>XMLスクリプティング言語ブロックを処理します。以下の各項で説明するパラメータのみがサポートされます。

CPQLODOS

このコマンドは、CPQLODOSセッションを開始して終了するために使用されます。このコマンドは、1回だけ使用でき、必ず、XMLスクリプトの最初と最後に配置されます。

例：

```
<CPQLODOS VERSION="2.0">
</CPQLODOS>
```

CPQLODOSのパラメータ

VERSIONは、このスクリプトを処理するのに必要なCPQLODOSのバージョンを示す、数字で表示される文字列です。VERSION文字列は、CPQLODOSが処理できるバージョンと比較されます。CPQLODOSのバージョンとスクリプトのバージョンが一致しない場合は、エラーが返されます。VERSIONパラメータをブランクにすることはできません。

CPQLODOSのランタイム エラー

表示される可能性のあるCPQLODOSのエラー メッセージには、「バージョンをブランクにすることはできません」があります。

MOD_NETWORK_SETTINGS

このコマンドは、特定のネットワーク設定を変更します。すべてのエレメントがオプションであり、指定されないオプションは、工場出荷時のデフォルト値に設定されます。

例：

```
<MOD_NETWORK_SETTINGS>
  <SPEED_AUTOSELECT VALUE = "N"/>
  <NIC_SPEED VALUE = "10"/>
```

```

<FULL_DUPLEX VALUE = "N"/>
<IP_ADDRESS VALUE = "192.168.1.2"/>
<SUBNET_MASK VALUE = "255.255.255.0"/>
<GATEWAY_IP_ADDRESS VALUE = "192.168.1.222"/>
<DNS_NAME VALUE = "RIB0002A5617D3B"/>
<PRIM_DNS_SERVER value = "192.168.2.200"/>
<DOMAIN_NAME VALUE = "riloe.mgmt.net"/>
<DHCP_ENABLE VALUE = "Y"/>
<DHCP_GATEWAY VALUE = "Y"/>
<DHCP_DNS_SERVER VALUE = "Y"/>
<DHCP_STATIC_ROUTE VALUE = "Y"/>
<DHCP_WINS_SERVER VALUE = "Y"/>
<REG_WINS_SERVER VALUE = "Y"/>
<PRIM_WINS_SERVER VALUE = "192.168.2.220"/>
<STATIC_ROUTE_1 DEST = "192.168.5.1" GATEWAY =
"192.168.5.200"/>
<STATIC_ROUTE_2 DEST = "192.168.5.2" GATEWAY =
"192.168.5.200"/>
<STATIC_ROUTE_3 DEST = "192.168.5.3" GATEWAY =
"192.168.5.200"/>
</MOD_NETWORK_SETTINGS>

```

MOD_NETWORK_SETTINGSのパラメータ

SPEED_AUTOSELECTは、トランシーバの速度を自動的に選択するために使用します。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されません。

FULL_DUPLEXは、iLOが全二重モードと半二重モードのどちらをサポートするかを決定するために使用します。このパラメータは、SPEED_AUTOSELECTを"No"に設定した場合にのみ、適用できます。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されません。

NIC_SPEEDは、SPEED_AUTOSELECTを"NO"に設定した場合に、トランシーバ速度を設定するために使用します。値として"10"または"100"を指定できます。これ以外の値を指定するとシンタックス エラーが発生します。

DHCP_ENABLEは、DHCPを有効にするために使用します。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されません。

IP_ADDRESSは、DHCPが有効ではない場合に、iLOのIPアドレスを選択するために使用します。空白文字列を入力すると、現在の値は削除されます。

SUBNET_MASKは、DHCPが有効ではない場合に、iLOのサブネット マスクを選択するために使用します。空白文字列を入力すると、現在の値は削除されます。

GATEWAY_IP_ADDRESSは、DHCPが有効ではない場合に、iLOのデフォルト ゲートウェイIPアドレスを選択するために使用します。空白文字列を入力すると、現在の値は削除されます。

DNS_NAMEは、iLOのDNS名を指定するために使用します。空白文字列を入力すると、現在の値は削除されます。

DOMAIN_NAMEは、iLOがインストールされているネットワークのドメイン名を指定するために使用します。空白文字列を入力すると、現在の値は削除されます。

DHCP_GATEWAYは、DHCP割り当てゲートウェイ アドレスを使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されます。この選択は、DHCPが使用できる場合にのみ有効です。

DHCP_DNS_SERVERは、DHCP割り当てDNSサーバを使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されます。この選択は、DHCPが使用できる場合にのみ有効です。

DHCP_WINS_SERVERは、DHCP割り当てWINSサーバを使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されます。この選択は、DHCPが使用できる場合にのみ有効です。

DHCP_STATIC_ROUTEは、DHCP割り当て静的経路を使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されます。この選択は、DHCPが使用できる場合にのみ有効です。

REG_WINS_SERVERは、iLOをWINSサーバに登録する必要があるかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータでは、大文字と小文字が区別されます。この選択は、DHCPが使用できる場合にのみ有効です。

PRIM_DNS_SERVERは、プライマリDNSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てDNSサーバ アドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

SEC_DNS_SERVERは、セカンダリDNSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てDNSサーバ アドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

TER_DNS_SERVERは、ターシャリDNSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てDNSサーバ アドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

PRIM_WINS_SERVERは、プライマリWINSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てWINSサーバ アドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

SEC_WINS_SERVERは、セカンダリWINSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てWINSサーバ アドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

STATIC_ROUTE_1、STATIC_ROUTE_2、およびSTATIC_ROUTE_3は、静的経路の宛先とゲートウェイのIPアドレスを指定するために使用します。静的経路のコマンド内では、次の2つのパラメータが使用されます。空白文字列を入力すると、現在の値は削除されます。

- DESTは、静的経路の宛先のIPアドレスを指定します。このパラメータは、DHCP割り当て静的経路機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。
- GATEWAYは、静的経路のゲートウェイのIPアドレスを指定します。このパラメータは、DHCP割り当て静的経路機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

注：MOD_NETWORK_SETTINGSの終了後、iLOは再起動して変更を適用します。

MOD_DIR_CONFIG

このコマンドは、特定のディレクトリ サービス設定を変更します。ディレクトリ サービスを有効にする場合、必須パラメータをすべて入力して、ディレクトリ サービスによる認証と権限付与が正しく行われるようにする必要があります

例：

```
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE = " YES"/>
<DIR_LOCAL_USER_ACCT VALUE = "YES"/>
<DIR_SERVER_ADDRESS VALUE = ¥"directory.corp.net"/>
<DIR_SERVER_PORT VALUE = "636"/>
```

```
<DIR_OBJECT_DN VALUE = "CN=RIL0E2-JJ, OU=RIL0ES,  
DC=RIL0EII, DC=HP"/>  
<DIR_OBJECT_PASSWORD VALUE = "wingsauce"/>  
<DIR_USER_CONTEXT_1 VALUE = "CN=Users, DC=RIL0EII,  
DC=HP"/>  
<DIR_USER_CONTEXT_2 VALUE = "CN=Mgmt, DC=RIL0EII,  
DC=HP"/>  
<DIR_USER_CONTEXT_3 VALUE = "CN=Admins, DC=RIL0EII,  
DC=HP"/>  
</MOD_DIR_CONFIG>
```

MOD_DIR_CONFIGパラメータ

DIR_AUTHENTICATION_ENABLEDは、iLOに対する認証とiLOについての権限付与の決定にディレクトリ サービスを使用するかどうかを示します。値として、"Y"、"Yes"、"N"、または"No"を指定できます。デフォルト値は、"No"で、このパラメータはオプションです。

DIR_LOCAL_USER_ACCTは、ディレクトリ サービス ユーザ アカウントの使用に加えてローカル ユーザ アカウントを使用するかどうかを示します。値として、"Y"、"Yes"、"N"、または"No"を指定できます。このパラメータは、DIR_AUTHENTICATION_ENABLEDが"Yes"に設定されている場合にのみ有効です。デフォルト値は、"Yes"です。このパラメータは、オプションです。

DIR_SERVER_ADDRESSは、iLOがディレクトリ サービス操作に使用するコンピュータのIPアドレスまたはDNS名を指定します。値として、文字列またはIPアドレスを指定できます。DIR_AUTHENTICATION_ENABLEDが"Yes"に設定されている場合は、このパラメータを必ず指定してください。

DIR_SERVER_PORTは、iLOが通信に使用する、ディレクトリ サービス サーバ上のポート番号を指定します。値として、数字で表示される有効な任意のIPポート番号を指定できます。デフォルト値は636です。このデフォルト値は、オプション パラメータです。

DIR_OBJECT_DN_VALUEは、ディレクトリ内でのiLOオブジェクトのディレクトリ サービス識別名を指定します。値として、iLOに適用される識別名を示す文字列を指定できます。DIR_AUTHENTICATION_ENABLEDを"Yes"に設定する場合は、このパラメータを必ず指定してください。

DIR_OBJECT_PASSWORDは、iLOオブジェクトへのアクセスに使用するiLOのパスワードを指定します。このパスワードは現在使用されていませんが、将来のファームウェアバージョンで使用されます。

DIR_USER_CONTEXT_1、DIR_USER_CONTEXT_2、およびDIR_USER_CONTEXT_3は、認証および権限付与プロセスで検索されるディレクトリ サービス コンテキストを指定します。ディレクトリ サービスへのアクセスを試みるとき、各コンテキストストリングの前にユーザ名が追加され、ディレクトリ サービスで認証される完全なユーザ名が作成されます。値として、有効なディレクトリ サービス コンテキストストリングを指定できます。これらのパラメータは、オプションです。

ADD_USER

このコマンドは、iLOにユーザを追加するために使用します。XMLスクリプト内に複数のADD_USERコマンドがある場合、CPQLODOSは、最後のコマンドからの設定のみを使用します。

例：

```
<ADD_USER
  USER_NAME = "James Madison"
  USER_LOGIN = "jmadison"
  PASSWORD = "president">
</ADD_USER>
```

ADD_USERのパラメータ

USER_NAMEは、追加するユーザの実際の名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。この文字列は表示用にだけ使用されます。このパラメータをブランクにすることはできません。

USER_LOGINは、ユーザがiLOにログインするためにタイプする名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。このストリングをブランクにすることはできません。

PASSWORDは、ユーザに関連付けられるパスワードです。このパラメータは0文字以上、39文字以下でなければなりません。パスワードの最小文字数は、[Global Settings]画面での設定によって変わります。パスワードには、印刷可能文字の任意の組み合わせで構成されるASCII文字列を使用します。PASSWORDパラメータには単一引用符および二重引用符は使用できません。このパラメータには、大文字と小文字の区別があります。

リモートInsightボード コマンド言語

この項の目次

リモートInsightボード コマンド言語の概要	160
RIBCLのサンプル スクリプト	160
RIBCLの一般的なガイドライン	160
XMLヘッダ	161
データタイプ	161
応答の定義	162
RIBCL	162
LOGIN	163
USER_INFO	164
ADD_USER	165
DELETE_USER	168
GET_USER	169
MOD_USER	171
GET_ALL_USERS	173
GET_ALL_USER_INFO	175
RIB_INFO	176
RESET_RIB	177
GET_NETWORK_SETTINGS	177
MOD_NETWORK_SETTINGS	179
MOD_DIAGPORT_SETTINGS	183
DIR_INFO	184
GET_DIR_CONFIG	185
MOD_DIR_CONFIG	186
GET_GLOBAL_SETTINGS	188
MOD_GLOBAL_SETTINGS	189
MOD_SNMP_IM_SETTINGS	190
CLEAR_EVENTLOG	192
UPDATE_RIB_FIRMWARE	193
GET_FW_VERSION	194
HOTKEY_CONFIG	195
LICENSE	197
RACK_INFO	198
MOD_BLADE_RACK	199
GET_TOPOLOGY	200

SERVER_INFO	201
GET_HOST_POWER_STATUS	202
SET_HOST_POWER	203
RESET_SERVER	204
GET_UID_STATUS	205
UID_CONTROL	205

リモートInsightボード コマンド言語の概要

リモートInsightボード コマンド言語を使用すると、スクリプトを作成して、ユーザ アカウントを管理したり、設定を行ったりすることができます。

重要：コメントが、コマンドを中断しないようにしてください。コメントでコマンドが中断されると、エラー メッセージが生成されます。

RIBCLのサンプル スクリプト

この項で説明するすべてのiLOコマンドのサンプルスクリプトは、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。

RIBCLの一般的なガイドライン

この項では、すべてのコマンドは、機能ごとにグループ分けされています。ユーザ情報を処理するすべてのコマンドは、1つのグループにまとめられます。コマンドをグループ化することにより、ファームウェアは処理されるデータを、テキスト文書と同様の情報ブロックとみなすことができ、異なる種類の情報へのマルチスレッド アクセスが可能になります。

開始コマンドによりデータベースが開かれます。このデータベースは、対応する終了コマンドが送信されるまで開いたままです。1つのコマンド ブロック内で実行されたすべての変更は、データベースの終了時に、同時に適用されます。コマンド ブロック内にエラーがある場合は、ブロック内の変更は放棄されます。

次に、開始コマンドと対応する終了コマンドの例を示します。

```
<USER_INFO>
```

```
</USER_INFO>
```

以下の各項では、すべての例で開始コマンドと終了コマンドを示します。

XMLヘッダ

XMLヘッダにより、接続がHTTP接続ではなく、XML接続であることが保証されます。XMLヘッダは、cpqlcfgユーティリティに組み込まれ、次の書式を備えています。

```
<?xml version="1.0"?>
```

データ タイプ

パラメータ内で許可されるデータ タイプは、次の3つです。

- スtring
- 特殊String
- BooleanString

String

Stringは、引用符で囲まれた任意のテキストです。Stringは、スペースや数字、その他の印刷可能な文字で構成できます。Stringは、単一引用符と二重引用符のどちらで始めることもできますが、同じ種類の引用符で終わらなければなりません。区切りの引用符と異なるものであれば、String内に引用符を含むことができます。

たとえば、Stringが二重引用符で始まる場合、単一引用符をString内で使用することができますが、Stringの終わりは二重引用符でなければなりません。

特殊String

特殊Stringは、特定の文字で構成する必要のあるStringで、通常、ユーザが正しい構文として受け入れられる単語から選択します。それ以外の単語が入力された場合はすべてエラーが返されます。

Booleanストリング

Booleanストリングは、「はい」または「いいえ」の状態を指定する特殊ストリングです。受け入れられるBooleanストリングは、"yes"、"y"、"no"、"n"、"true"、"t"、"false"、および"f"です。これらのストリングに、大文字と小文字の区別はありません。

応答の定義

iLOに送信されるすべてのコマンドが、応答を生成します。応答は、コマンドの成功/失敗を示します。コマンドの中には、追加情報を生成するものもあります。エラーが発生しなければ、追加情報は実行シーケンスで表示されます。

例：

```
<RESPONSE
  STATUS="0x0001"
  MSG="There has been a severe error."
/>
```

- RESPONSE

このタグ名は、iLOが前のコマンドに対する応答を、クライアントアプリケーションに返して、iLOに送信されたコマンドの成功/失敗を示すことを表します。

- STATUS

このパラメータは、エラー番号を示します。番号"0x0000"は、エラーが発生していないことを示しています。

- MSG

このエレメントは、発生したエラーを説明するメッセージで構成されます。エラーが発生していない場合、"No error"と表示されます。

RIBCL

このコマンドは、RIBCLセッションを開始して終了するために使用されます。このコマンドは、RIBCLセッションを開始するために1回だけ使用でき、スクリプトに表示される最初のコマンドでなければなりません。RIBCLタグは、RIBCLドキュメントの最初と終わりをマークするために必要です。

例：

```
<RIBCL VERSION="2.0">  
</RIBCL>
```

RIBCLのパラメータ

VERSIONは、クライアント アプリケーションが使用を予測しているRIBCLのバージョンを示す文字列です。VERSION文字列は、使用が予測されているRIBCLのバージョンと比較され、文字列とバージョンが一致しない場合は、エラーが返されます。VERSIONパラメータの標準値は、"2.0"です。VERSIONパラメータについては、正確に一致しているかどうかのチェックは行われなくなりましたが、このパラメータをブランクにすることはできません。

RIBCLのランタイム エラー

表示される可能性のあるRIBCLのエラー メッセージは次のとおりです。

バージョンをブランクにすることはできません。

LOGIN

RIBCL処理は、各ユーザの権限レベルを使用して実行されます。LOGINコマンドの提供する情報により、各ユーザの権限レベルがチェックされユーザが認証されます。RIBCLコマンドの実行を可能にするには、指定されたユーザが少なくともログイン権限を持っていない限りなりません。ユーザの権限は、そのコマンドの実行に必要な権限と照合され、権限レベルが一致しない場合は、エラーが返されます。

例：

```
<LOGIN USER_LOGIN="username" PASSWORD="password">  
</LOGIN>
```

注：管理権限のないユーザでも、自身のパスワード設定は変更できます。

LOGINのパラメータ

USER_LOGINは、ユーザがiLOにログインするためにタイプする名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。このストリングをブランクにすることはできません。

PASSWORDは、ユーザに関連付けられるパスワードです。このパラメータは0文字以上、39文字以下でなければなりません。パスワードの最小文字数は、[Global Settings]画面での設定によって変わります。パスワードには、印刷可能文字の任意の組み合わせで構成されるASCII文字列を使用します。PASSWORDパラメータには単一引用符および二重引用符は使用できません。このパラメータには、大文字と小文字の区別があります。

LOGINのランタイム エラー

表示される可能性のあるランタイム エラー メッセージは次のとおりです。

- ユーザのログイン名が見つかりません。
- パスワードをブランクにすることはできません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

USER_INFO

USER_INFOコマンドは、LOGINコマンド内にのみ示すことができます。このコマンドは、構文解析されると、ユーザ情報のローカル データベースをメモリに読み出し、編集の準備をします。USER_INFOブロックの内側で有効なコマンドは、USER_INFOタイプのコマンドだけです。USER_INFOコマンドは、ユーザ情報の読み出しに成功したかどうかをホスト アプリケーションに示す応答を生成します。別のアプリケーションでユーザ情報が書き込み用に開かれている場合、このコールは失敗します。

例：

```
<USER_INFO MODE="write">
</USER_INFO>
```

USER_INFOのパラメータ

MODEは、最大長10文字の特殊ストリング パラメータです。このパラメータは、ユーザ情報を使用して何をしようとしているのかを示します。有効な引数は、"read"および"write"です。

パラメータが、"write"モードで開かれている場合、読み出しと書き込みが有効になり他のユーザがユーザ情報を開くことはできません。"read"モードで開かれた場合は、ユーザ データの変更はできません。引数に、大文字と小文字の区別はありません。このパラメータをブランクにすることはできません。

USER_INFOのランタイム エラー

表示される可能性のあるランタイム エラー メッセージは次のとおりです。MODEパラメータをブランクにすることはできません。

ADD_USER

ADD_USERコマンドは、ローカル ユーザを追加するために使用します。ユーザ関連の属性はすべて、次に説明するパラメータを使用して設定します。ユーザがすでに存在する場合は、このコマンドは機能しません。既存のユーザの情報を変更するには、MOD_USERコマンドを使用します。ADD_USERコマンドは、USER_INFOエレメント内に示す必要があり、USER_INFOは"write"モードでなければなりません。他のユーザを追加するには、管理権限を持つユーザがログインする必要があります。

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="loginname" PASSWORD="password">
    <USER_INFO MODE="write">
      <ADD_USER
        USER_NAME="User"
        USER_LOGIN="username" PASSWORD="password">
        <ADMIN_PRIV value ="No"/>
        <REMOTE_CONS_PRIV value ="Yes"/>
        <RESET_SERVER_PRIV value ="No"/>
        <VIRTUAL_MEDIA_PRIV value ="No"/>
        <CONFIG_ILO_PRIV value ="No"/>
      </ADD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

ADD_USERのパラメータ

USER_NAMEは、追加するユーザの実際の名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。この文字列は表示用にだけ使用されます。このパラメータをブランクにすることはできません。

USER_LOGINは、ユーザがiLOにログインするためにタイプする名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。このストリングをブランクにすることはできません。

PASSWORDは、ユーザに関連付けられるパスワードです。このパラメータは0文字以上、39文字以下でなければなりません。パスワードの最小文字数は、[Global Settings]画面での設定によって変わります。パスワードには、印刷可能文字の任意の組み合わせで構成されるASCII文字列を使用します。PASSWORDパラメータには単一引用符および二重引用符は使用できません。このパラメータには、大文字と小文字の区別があります。

以下のパラメータは、ユーザの権限を制御します。これらのパラメータはオプションで、権限を許可または拒否する"Yes"または"No"のBooleanストリングを指定する必要があります。新しく追加されたユーザ アカウントには、デフォルトでは、権限は許可されません。パラメータが省略されている場合、その権限は拒否されます。

ADMIN_PRIVは、ユーザがユーザ アカウントを管理できるようにするBooleanパラメータです。ユーザは、自身および他のユーザのアカウント設定の変更、ユーザの追加と削除を行うことができます。このパラメータを省略すると、ユーザはアカウントを追加、削除、または設定できません。

REMOTE_CONS_PRIVは、リモート コンソール機能にアクセスする権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザにリモート コンソールの権限を与える必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。この権限を省略すると、ユーザはリモート コンソールの機能にアクセスできません。

RESET_SERVER_PRIVは、サーバをリモートからリセットしたり電源を切断したりする権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザがサーバの電源を変更できるようにする場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。このパラメータを省略すると、ユーザにサーバ リセット権限は与えられません。

VIRTUAL_MEDIA_PRIVは、仮想フロッピー機能にアクセスする権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザに仮想フロッピーの権限を与える必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。このパラメータを省略すると、ユーザに仮想フロッピーの権限は与えられません。

CONFIG_ILO_PRIVは、ユーザがiLOを設定できるようにするBooleanパラメータです。この権限を持つユーザは、ネットワーク設定、グローバル設定、Insightマネージャ設定、およびSNMP設定などを行えます。このパラメータはオプションで、ユーザがiLOを設定できるようにする必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

注：iLOファームウェア バージョン1.40以降では、以下の各パラメータはユーザ権限に適用されません。パラメータは正しく構文解析されますが、ユーザの権限には影響しません。

VIEW_LOGS_PRIVは、iLOシステムのログを表示する権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザがログを表示できるようにする必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

CLEAR_LOGS_PRIVは、イベント ログをクリアする権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザがiLOのイベント ログをクリアできるようにする必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

EMS_PRIVは、Windows® Server 2003のEMSサービスを使用する権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザがEMSサービスを使用できるようにする必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

UPDATE_ILO_PRIVは、ユーザが新しいファームウェア イメージをiLOのシステムROMにコピーできるようにするBooleanパラメータです。このパラメータはオプションで、ユーザがiLOをアップデートできるようにする必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

CONFIG_RACK_PRIVは、サーバのラック リソースを設定および管理する権限をユーザに与えるBooleanパラメータです。このパラメータはProLiant BL p-Classサーバにのみ適用できます。このパラメータはオプションで、ユーザがラック リソースを管理または設定できるようにする必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

DIAG_PRIVは、iLOの診断情報を表示する権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザに診断権限を与える必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

ADD_USERのランタイム エラー

表示される可能性のあるADD_USERのエラー メッセージは次のとおりです。

- ログイン名が長すぎます。最大長は39文字です。
- パスワードが短すぎます。パスワードは8文字以上でなければなりません。
- パスワードが長すぎます。最大長は39文字です。
- ユーザ テーブルに空きがないため、新規ユーザ用のスペースがありません。
- そのユーザ名は既に存在しているため、ユーザを追加することはできません。
- ユーザ情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- ユーザ名をブランクにすることはできません。
- ユーザのログインIDをブランクにすることはできません。
- パスワードをブランクにすることはできません。
- Boolean値が指定されていません。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

DELETE_USER

DELETE_USERコマンドは、既存のローカル ユーザ情報を削除するために使用します。このコマンドを使用する前に、USER_INFOコマンドを"write"モードで発行しておかなければなりません。他のユーザのアカウントを削除するには、管理権限を持つユーザがログインする必要があります。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname"
    PASSWORD="password">
    <USER_INFO MODE="write">
      <DELETE_USER USER_LOGIN="username"/>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

DELETE_USERのパラメータ

USER_LOGINは、削除するユーザのログイン名です。USER_LOGINパラメータの最大長は39文字で、印刷可能文字の任意の組み合わせで構成されるASCII文字列を使用できます。また、このパラメータでは、大文字と小文字が区別されます。USER_LOGINパラメータをブランクにすることはできません。

DELETE_USERのランタイム エラー

表示される可能性のあるDELETE_USERのエラーは、次のとおりです。

- ユーザ情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- 現在ログイン中のユーザのユーザ情報は削除できません。
- ユーザのログイン名が見つかりません。
- ユーザのログイン名をブランクにすることはできません。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_USER

GET_USERコマンドは、パスワードを除くローカル ユーザ情報を返します。このコマンドを実行するには、ログイン権限を持つユーザがログインする必要があります。ログインしたユーザが管理権限を持たない場合は、そのユーザの情報だけを取得できます。

例：

```
<RIBCL VERSION="2.0">
```

```
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<USER_INFO MODE="read">
<GET_USER USER_LOGIN="username"/>
</USER_INFO>
</LOGIN>
</RIBCL>
```

GET_USERのパラメータ

USER_LOGINは、ユーザがiLOにログインするためにタイプする名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。このストリングをブランクにすることはできません。

他のユーザのアカウントを取得するには、ユーザがユーザ アカウントの管理権限を持たなければなりません。管理権限のないユーザが表示できるのは、自身のアカウント情報だけです。

GET_USERのランタイム エラー

表示される可能性のあるGET_USERのエラー メッセージは次のとおりです。

- ユーザのログインIDをブランクにすることはできません。
- ユーザのログイン名が見つかりません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_USERが返すメッセージ

GET_USERは、次のようなメッセージを返します。

```
<RESPONSE
  STATUS="0x0000"
  MSG="No Errors"
/>
<GET_USER
  USER_NAME="Admin User"
  USER_LOGIN= "username"
  ADMIN_PRIV="N"
  REMOTE_CONS_PRIV="Y"
  RESET_SERVER_PRIV="N"
```

```

        VIRTUAL_MEDIA_PRIV="N"
        CONFIG_ILO_PRIV value ="No"
    />

```

MOD_USER

MOD_USERコマンド、既存のローカル ユーザの情報を変更するために使用します。変更するユーザを指定する最初のフィールドは必ず入力しなければなりませんが、それ以外のフィールドは、必ず入力しなければいけないわけではありません。変更する必要のないパラメータは、省略してください。MOD_USERコマンドは、USER_INFOパラメータ内に示す必要があり、USER_INFOは"write"モードでなければなりません。アクセスに使用されるユーザのログイン名は変更できません。

ユーザ名、ユーザのパスワード、またはユーザの権限を変更するには、管理権限を持つユーザがログインしなければなりません。管理権限のないユーザが変更できるのは、自身のアカウントのパスワードだけです。

例：

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="write">
      <MOD_USER USER_LOGIN="loginname">
        <USER_NAME value="username"/>
        <PASSWORD value="password"/>
        <ADMIN_PRIV value="No"/>
        <REMOTE_CONS_PRIV value="Yes"/>
        <RESET_SERVER_PRIV value="No"/>
        <CONFIG_ILO_PRIV value="Yes"/>
        <VIRTUAL_MEDIA_PRIV value="No"/>
      </MOD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>

```

MOD_USERのパラメータ

USER_LOGINは、ユーザがiLOにログインするためにタイプする名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。このストリングをブランクにすることはできません。

注：以下の各パラメータを指定しない場合、指定したユーザのパラメータ値は変更されません。

USER_NAMEは、追加するユーザの実際の名前です。このパラメータには、大文字と小文字の区別があり、有効な任意の文字列を使用できます。最大長は39文字です。この文字列は表示用にだけ使用されます。このパラメータをブランクにすることはできません。

PASSWORDは、ユーザに関連付けられるパスワードです。このパラメータは0文字以上、39文字以下でなければなりません。パスワードの最小文字数は、[Global Settings]画面での設定によって変わります。パスワードには、印刷可能文字の任意の組み合わせで構成されるASCII文字列を使用します。PASSWORDパラメータには単一引用符および二重引用符は使用できません。このパラメータには、大文字と小文字の区別があります。

ADMIN_PRIVは、ユーザがユーザ アカウントを管理できるようにするBooleanパラメータです。ユーザは、自身および他のユーザのアカウント設定の変更、ユーザの追加と削除を行うことができます。このパラメータをブランクにすると、ユーザはアカウントを追加することも、削除することも、設定することもできなくなります。

REMOTE_CONS_PRIVは、リモート コンソール機能にアクセスする権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザにリモート コンソールの権限を与える必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。この権限をブランクにすると、ユーザはリモート コンソールの機能にアクセスできなくなります。

RESET_SERVER_PRIVは、サーバをリモートからリセットしたり電源を切断したりする権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザがサーバの電源を変更できるようにする場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。このパラメータをブランクにすると、ユーザにサーバリセット権限は与えられなくなります。

CONFIG_ILO_PRIVは、ユーザがiLOを設定できるようにするBooleanパラメータです。この権限を持つユーザは、ネットワーク設定、グローバル設定、Insightマネージャ設定、およびSNMP設定などを行えます。このパラメータはオプションで、ユーザがiLOを設定できるようにする必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。

VIRTUAL_MEDIA_PRIVは、仮想フロッピー機能にアクセスする権限をユーザに与えるBooleanパラメータです。このパラメータはオプションで、ユーザに仮想フロッピーの権限を与える必要がある場合は、Booleanストリングを"Yes"に設定しなければなりません。このパラメータを使用する場合、Booleanストリング値をブランクにしてはなりません。このパラメータをブランクにすると、ユーザに仮想フロッピーの権限は与えられなくなります。

MOD_USERのランタイム エラー

表示される可能性のあるMOD_USER のエラー メッセージは次のとおりです。

- ログイン名が長すぎます。最大長は39文字です。
- パスワードが短すぎます。パスワードは8文字以上でなければなりません。
- パスワードが長すぎます。最大長は39文字です。
- ユーザ情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- ユーザのログインIDをブランクにすることはできません。
- 現在ログイン中のユーザのユーザ情報は変更できません。
- このユーザはログインしていません。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_ALL_USERS

GET_ALL_USERSコマンドは、現在のローカル ユーザ データベースに存在するすべての有効なユーザ名の一覧を要求します。このコマンドが機能するには、ユーザ データベースがUSER_INFOコマンドを使用して"read"または"write"モードで正常に開かれていなければなりません。このコマンドを実行するには、管理権限を持つユーザがログインする必要があります。

例：

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">  
    <USER_INFO MODE="read">  
      <GET_ALL_USERS />
```

```
</USER_INFO>
</LOGIN>
</RIBCL>
```

GET_ALL_USERSのランタイム エラー

ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_ALL_USERSが返すメッセージ

GET_ALL_USERSは、次のようなメッセージを返します。

```
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No Error '
/>
  USER_LOGIN="username"
  USER_LOGIN="user2"
  USER_LOGIN="user3"
  USER_LOGIN="user4"
  USER_LOGIN="user5"
  USER_LOGIN="user6"
  USER_LOGIN="user7"
  USER_LOGIN="user8"
  USER_LOGIN="user9"
  USER_LOGIN="user10"
  USER_LOGIN="user11"
  USER_LOGIN="user12"
/>
```

要求が成功しなかった場合、次のように表示されます。

```
<RESPONSE
  STATUS = "0x0001"
  MSG = "Error Message"/>
```

GET_ALL_USER_INFO

GET_ALL_USERS_INFOコマンドは、現在のローカル ユーザ データベースを返すことを要求します。このコマンドは、ユーザのログイン名だけでなく、各ユーザの詳細な情報を返します。このコマンドが機能するには、ユーザ データベースがUSER_INFOコマンドを使用して正常に開かれていなければなりません。USER_INFOコマンドは、"read"または"write"モードのどちらで開いてもかまいません。GET_ALL_USERS_INFOを使用するには、管理権限を持つユーザがログインする必要があります。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
      <GET_ALL_USER_INFO />
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

GET_ALL_USER_INFOのパラメータ

このコマンドにはパラメータはありません。

GET_ALL_USER_INFOのランタイム エラー

表示される可能性のあるGET_ALL_USERS_INFOのエラー メッセージは次のとおりです。ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_ALL_USER_INFO

GET_ALL_USERS_INFOは、次のようなメッセージを返します。

```
<RESPONSE
  STATUS="0x0000"
  MSG="No Errors"
/>
<GET_USER
  USER_NAME="Admin"
  USER_LOGIN="Admin"
  ADMIN_PRIV="Y"
```

```
CONFIG_RILO_PRIV="Y"  
LOGIN_PRIV="Y"  
REMOTE_CONS_PRIV="Y"  
RESET_SERVER_PRIV="Y"  
VIRTUAL_MEDIA_PRIV="Y"  
/> .....
```

すべてのユーザについて同じ情報が繰り返されます。

要求が成功しなかった場合のメッセージは、次のとおりです。

```
<RESPONSE  
  STATUS = "0x0001"  
MSG = "Error Message"/>
```

RIB_INFO

RIB_INFOコマンドは、iLOの設定をこれから変更することをファームウェアに通知するために使用されます。

例：

```
<RIB_INFO MODE="write">  
..... RIB_INFO commands .....  
</RIB_INFO>
```

RIB_INFOのパラメータ

MODEは、最大長10文字の特殊ストリング パラメータです。このパラメータは、ユーザ情報を使用して何をしようとしているのかを示します。有効な引数は、"read"および"write"です。

"write"モードでは、読み出しと書き込みの両方が有効になり、他のユーザはiLOの情報を開くことはできません。"read"モードでは、ユーザはiLOのデータの変更ができません。モード属性を省略すると、"read"モードが設定されているものとみなされます。

RIB_INFOのランタイム エラー

RIB_INFOエラーはありません。

RESET_RIB

このコマンドは、ユーザがiLOをリセットできるようにします。RESET_RIBは"write"モードのRIB_INFOブロックの内側に示さなければなりません。このコマンドを実行するには、iLOの設定権限を持つユーザがログインしなければなりません。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Admin" PASSWORD="Password">
    <RIB_INFO MODE = "write">
      <RESET_RIB/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

RESET_RIBのパラメータ

このコマンドにはパラメータはありません。

RESET_RIBのランタイム エラー

このコマンドにはエラーはありません。

GET_NETWORK_SETTINGS

GET_NETWORK_SETTINGSコマンドによって、ユーザは、ネットワーク設定情報を取得できます。GET_NETWORK_SETTINGSは、RIB_INFOブロックの内側に示さなければなりません。このコマンドを実行するには、ユーザがログイン権限を持つ必要があります。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_NETWORK_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_NETWORK_SETTINGSのパラメータ

このコマンドにはパラメータはありません。

GET_NETWORK_SETTINGSのランタイム エラー

このコマンドにはエラーはありません。

GET_NETWORK_SETTINGSが返すメッセージ

GET_NETWORK_SETTINGSは、次のようなメッセージを返します。

```
<GET_NETWORK_SETTINGS
  SPEED_AUTOSELECT="YES"
  NIC_SPEED="100"
  FULL_DUPLEX="NO"
  DHCP_ENABLE="YES"
  DHCP_GATEWAY="YES"
  DHCP_DNS_SERVER="YES"
  DHCP_STATIC_ROUTE="YES"
  DHCP_WINS_SERVER="YES"
  REG_WINS_SERVER="YES"
  IP_ADDRESS="111.111.111.111"
  SUBNET_MASK="255.255.255.0"
  GATEWAY_IP_ADDRESS="111.111.111.1"
  DNS_NAME="test"
  DOMAIN_NAME="test.com"
  PRIM_DNS_SERVER="111.111.111.242"
  SEC_DNS_SERVER="111.111.111.242"
  TER_DNS_SERVER="111.111.111.242"
  PRIM_WINS_SERVER="111.111.111.246"
  SEC_WINS_SERVER="111.111.111.247"
  STATIC_ROUTE_1 DEST="0.0.0.0" GATEWAY="0.0.0.0"
  STATIC_ROUTE_2 DEST="0.0.0.0" GATEWAY="0.0.0.0"
  STATIC_ROUTE_3 DEST="0.0.0.0" GATEWAY="0.0.0.0"
  WEB_AGENT_IP_ADDRESS=""
/>
```

要求が成功しなかった場合のメッセージは、次のとおりです。

```
<RESPONSE
  STATUS = "0x0001"
```

```
MSG = "Error Message"/>
```

MOD_NETWORK_SETTINGS

MOD_NETWORK_SETTINGSコマンドは、特定のネットワーク設定を変更するために使用します。このコマンドは、RIB_INFOブロックの内側でのみ有効です。ログインユーザは、iLOの設定権限を持つ必要があり、このコマンドを含むRIB_INFOブロックのモードは"write"でなければなりません。次のエレメントはすべて、オプションで省略することができます。エレメントを省略すると、現在の設定が維持されます。MOD_NETWORK_SETTINGSコマンドの終了後、iLOマネジメント プロセッサは再起動して、変更を適用します。

ネットワーク設定を変更する場合、ユーザは、マネジメント プロセッサ用のネットワーク コマンドをよく知っておく必要があります。マネジメント プロセッサがコマンドを無視し、エラーも返されない場合もあります。たとえば、スクリプトにDHCPを有効にするコマンドとIPアドレスを変更するコマンドが含まれている場合、IPアドレスは無視されます。ネットワークに適合しない値にネットワーク設定を変更すると、iLOに接続できなくなることがあります。iLOのスクリプティング ファームウェアは、変更される設定が、ネットワーク設定に適合するかどうかを判定しません。

iLOに接続できなくなった場合、RBSUを使用して、ネットワーク設定を、ネットワークと互換性のある値に再設定しなければなりません。詳しくは、「iLO RBSU (14 ページ)」の項を参照してください。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_NETWORK_SETTINGS>
        <ENABLE_NIC value="Yes"/>
        <SPEED_AUTOSELECT value="No"/>
        <NIC_SPEED value="100"/>
        <FULL_DUPLEX value="Yes"/>
        <DHCP_ENABLE value="Yes"/>
        <IP_ADDRESS value="192.168.132.25"/>
        <SUBNET_MASK value="255.255.0.0"/>
        <GATEWAY_IP_ADDRESS value="192.168.132.2"/>
        <DNS_NAME value="demorib"/>
        <DOMAIN_NAME value="internal.net"/>
        <DHCP_GATEWAY value="No"/>
```

```
<DHCP_DNS_SERVER value="No"/>
<DHCP_WINS_SERVER value="No"/>
<DHCP_STATIC_ROUTE value="No"/>
<REG_WINS_SERVER value="No"/>
<REG_DDNS_SERVER value="No"/>
<PING_GATEWAY value="Yes"/>
<PRIM_DNS_SERVER value="192.168.12.14"/>
<SEC_DNS_SERVER value="192.168.12.15"/>
<TER_DNS_SERVER value="192.168.12.16"/>
<PRIM_WINS_SERVER value="192.168.145.1"/>
<SEC_WINS_SERVER value="192.168.145.2"/>
<STATIC_ROUTE_1 DEST="192.168.129.144"
GATEWAY="192.168.129.1"/>
<STATIC_ROUTE_2 DEST="192.168.129.145"
GATEWAY="192.168.129.2"/>
<STATIC_ROUTE_3 DEST="192.168.129.146"
GATEWAY="192.168.129.3"/>
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

MOD_NETWORK_SETTINGSのパラメータ

SPEED_AUTOSELECTは、トランシーバの速度を自動的に選択するために使用します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別はありません。

FULL_DUPLEXは、iLOが全二重モードと半二重モードのどちらをサポートするかを決定するために使用します。このパラメータは、SPEED_AUTOSELECTを"No"に設定した場合にのみ、適用できます。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別はありません。

NIC_SPEEDは、SPEED_AUTOSELECTを"No"に設定した場合に、トランシーバ速度を設定するために使用します。値として"10"または"100"を指定できます。これ以外の値を指定するとシンタックス エラーが発生します。

DHCP_ENABLEは、DHCPを有効にするために使用します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別はありません。

IP_ADDRESSは、DHCPが有効ではない場合に、iLOのIPアドレスを選択するために使用します。空白文字列を入力すると、現在の値は削除されます。

SUBNET_MASKは、DHCPが有効ではない場合に、iLOのサブネット マスクを選択するために使用します。空白文字列を入力すると、現在の値は削除されます。

GATEWAY_IP_ADDRESSは、DHCPが有効ではない場合に、iLOのデフォルト ゲートウェイIPアドレスを選択するために使用します。空白文字列を入力すると、現在の値は削除されます。

DNS_NAMEは、iLOのDNS名を指定するために使用します。空白文字列を入力すると、現在の値は削除されます。

DOMAIN_NAMEは、iLOがインストールされているネットワークのドメイン名を指定するために使用します。空白文字列を入力すると、現在の値は削除されます。

DHCP_GATEWAYは、DHCP割り当てゲートウェイ アドレスを使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別があります。この選択は、DHCPが有効である場合にのみ有効です。

DHCP_DNS_SERVERは、DHCP割り当てDNSサーバを使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別があります。この選択は、DHCPが有効である場合にのみ有効です。

DHCP_WINS_SERVERは、DHCP割り当てWINSサーバを使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別があります。この選択は、DHCPが有効である場合にのみ有効です。

DHCP_STATIC_ROUTEは、DHCP割り当て静的経路を使用するかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別があります。この選択は、DHCPが有効である場合にのみ有効です。

REG_WINS_SERVERは、iLOをWINSサーバに登録する必要があるかどうかを指定します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別があります。この選択は、DHCPが有効である場合にのみ有効です。

PRIM_DNS_SERVERは、プライマリDNSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てDNSサーバ アドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

SEC_DNS_SERVERは、セカンダリDNSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てDNSサーバ アドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

TER_DNS_SERVERは、ターシャリDNSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てDNSサーバアドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

PRIM_WINS_SERVERは、プライマリWINSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てWINSサーバアドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

SEC_WINS_SERVERは、セカンダリWINSサーバのIPアドレスを指定します。このパラメータは、DHCP割り当てWINSサーバアドレス機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

STATIC_ROUTE_1、STATIC_ROUTE_2、およびSTATIC_ROUTE_3は、静的経路の宛先とゲートウェイのIPアドレスを指定するために使用します。静的経路のコマンド内では、次の2つのパラメータが使用されます。空白文字列を入力すると、現在の値は削除されます。

- DESTは、静的経路の宛先のIPアドレスを指定します。このパラメータは、DHCP割り当て静的経路機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。
- GATEWAYは、静的経路のゲートウェイのIPアドレスを指定します。このパラメータは、DHCP割り当て静的経路機能が無効な場合にのみ適用されます。空白文字列を入力すると、現在の値は削除されます。

WEB_AGENT_IP_ADDRESSは、Web対応エージェントのアドレスを指定します。空白文字列を入力すると、現在の値は削除されます。

注：MOD_NETWORK_SETTINGSの終了後、iLOは再起動して変更を適用します。

MOD_NETWORK_SETTINGSのランタイム エラー

表示される可能性のあるMOD_NETWORK_SETTINGSのエラー メッセージは次のとおりです。

- RIB情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

MOD_DIAGPORT_SETTINGS

このコマンドは、iLOの診断ポートで特定のネットワーク設定を変更するために使用します。このコマンドは、ProLiant BL p-Classシリーズ サーバについてのRACK_INFOブロックの内側でのみ有効です。ログイン ユーザは、iLOの設定権限を持つ必要があり、このコマンドを含むRACK_INFOブロックのモードは"write"でなければなりません。DP_IP_ADDRESSおよびDP_SUBNET_MASKを空白にすることはできません。これら2つのパラメータでは、空白文字列を入力すると現在のアドレスが削除されます。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="username" PASSWORD="password">
    <RACK_INFO MODE="write">
      <MOD_DIAGPORT_SETTINGS>
        <DP_SPEED_AUTOSELECT value="No"/>
        <DP_NIC_SPEED value="100"/>
        <DP_FULL_DUPLEX value="Yes"/>
        <DP_IP_ADDRESS value="192.168.142.56"/>
        <DP_SUBNET_MASK value="255.255.0.0"/>
      </MOD_DIAGPORT_SETTINGS>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

MOD_DIAGPORT_SETTINGSのパラメータ

DP_SPEED_AUTOSELECTは、トランシーバの速度を自動的に選択するために使用します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別はありません。

DP_NIC_SPEEDは、DP_SPEED_AUTOSELECTを"No"に設定した場合に、トランシーバ速度を設定するために使用します。値として"10"または"100"を指定できます。これ以外の値を指定するとシンタックス エラーが発生します。

DP_FULL_DUPLEXは、iLO診断ポートが全二重モードと半二重モードのどちらをサポートするかを決定するために使用します。このパラメータは、DP_SPEED_AUTOSELECTを"No"に設定した場合にのみ、適用できます。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別はありません。

DP_IP_ADDRESSは、iLO診断ポートのIPアドレスを選択するために使用します。空白文字列を入力すると、現在のアドレスは変更されません。書式は、XXX.XXX.XXX.XXXです。

DP_SUBNET_MASKは、iLO診断ポートのサブネット マスクを選択するために使用します。空白文字列を入力すると、現在のアドレスは変更されません。書式は、XXX.XXX.XXX.XXXです。

注：MOD_DIAGPORT_SETTINGSが終了されると、iLOは変更を適用するために再起動します。ランタイム エラーが発生している場合は、内蔵Lights-Outは再起動しません。

MOD_DIAGPORT_SETTINGSのランタイム エラー

表示される可能性のあるMOD_DIAGPORT_SETTINGSのエラー メッセージは、次のとおりです。

- iLO情報は、読み出し専用アクセス用にかかれています。この操作では、書き込みアクセスが必要です。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

DIR_INFO

DIR_INFOコマンドは、サーバに関する情報を表示するために使用されます。DIR_INFOブロックの内側で有効なコマンドは、DIR_INFOタイプのコマンドだけです。

```
<DIR_INFO MODE="read">
</DIR_INFO>
```

DIR_INFOのパラメータ

MODEは、最大長10文字の特殊ストリング パラメータで、ユーザ情報を使用して何をしようとしているのかを示します。有効な引数は、"read"および"write"です。

DIR_INFO のランタイム エラー

- MODEパラメータをブランクにすることはできません。

- ユーザは、この操作を行うための適切な権限を持っていません。

GET_DIR_CONFIG

GET_DIR_CONFIGコマンドは、iLOのディレクトリ設定を取得します。このコマンドは、DIR_INFOブロックの内側に示さなければなりません。すべてのパラメータは、オプションです。このコマンドを実行するには、ログイン権限を持つユーザがログインする必要があります。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <DIR_INFO MODE="read">
      <GET_DIR_CONFIG/>
    </DIR_INFO>
  </LOGIN>
</RIBCL>
```

GET_DIR_CONFIGのパラメータ

このコマンドにはパラメータはありません。

GET_DIR_CONFIGのランタイム エラー

このコマンドにはエラーはありません。

GET_DIR_CONFIGが返すメッセージ

GET_DIR_CONFIGは、次のようなメッセージを返します。

```
<RESPONSE
STATUS="0x0000"
MSG = 'No Error'
/>
<GET_DIR_CONFIG
DIR_AUTHENTICATION_ENABLED = "YES"
DIR_LOCAL_USER_ACCT = "YES"
DIR_SERVER_ADDRESS = "server1.hprib.labs"
DIR_SERVER_PORT = "636"
```

```
DIR_OBJECT_DN = "CN=SERVER1_RIB, OU=RIB, DC=HPRIB, DC=LABS"
DIR_USER_CONTEXT1 = "CN=Users0, DC=HPRIB0, DC=LABS"
DIR_USER_CONTEXT2 = "CN=Users1, DC=HPRIB1, DC=LABS"
DIR_USER_CONTEXT3 = ""
/>
```

要求が成功しなかった場合のメッセージは、次のとおりです。

```
<RESPONSE
  STATUS = "0x0001"
  MSG = "Error Message"/>
```

MOD_DIR_CONFIG

MOD_DIR_CONFIGコマンドは、特定のディレクトリ設定を変更します。ディレクトリは、ユーザ認証に使用されます。このコマンドは、DIR_INFOブロックの内側でのみ有効です。ログイン ユーザは、iLOの設定権限を持つ必要があり、このコマンドを含むDIR_INFOブロックのモードは"write"でなければなりません。次のパラメータはすべて、オプションで省略することができます。パラメータを省略すると、現在の設定が維持されます。値に空白文字列を設定すると、以前の値が消去されます。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <DIR_INFO MODE="write">
      <MOD_DIR_CONFIG>
        <DIR_AUTHENTICATION_ENABLED value="Yes"/>
        <DIR_LOCAL_USER_ACCT value="Yes"/>
        <DIR_SERVER_ADDRESS value="16.141.100.44"/>
        <DIR_SERVER_PORT value="636"/>
        <DIR_OBJECT_DN value="CN=server1_rib, OU=RIB, DC=HPRIB,
          DC=LABS"/>
        <DIR_OBJECT_PASSWORD value="password"/>
        <DIR_USER_CONTEXT_1 value="CN=Users, DC=HPRIB, DC=LABS"/>
      </MOD_DIR_CONFIG>
    </DIR_INFO>
  </LOGIN>
</RIBCL>
```

MOD_DIR_CONFIGのパラメータ

DIR_AUTHENTICATION_ENABLEDは、ディレクトリ認証を有効または無効にします。値として"Yes"または"No"を指定できます。

DIR_LOCAL_USER_ACCTは、ローカル ユーザ アカウントを有効または無効にします。

DIR_SERVER_ADDRESSは、ディレクトリ サーバの位置を示します。ディレクトリ サーバの位置は、IPアドレスまたはDNS名で指定します。

DIR_SERVER_PORTは、ディレクトリ サーバとの接続に使用するポート番号を示します。この値は、ディレクトリ管理者から入手してください。セキュリティ保護されているLDAPポートの番号は636ですが、ディレクトリ サーバを設定して別のポート番号を指定することもできます。

DIR_OBJECT_DNは、ディレクトリ サーバ内でのiLOボードの固有名を指定します。この値は、ディレクトリ管理者から入手してください。識別名は、256文字までに制限されています。

DIR_OBJECT_PASSWORDは、ディレクトリ サーバ内でiLOオブジェクトに関連付けられるパスワードを指定します。パスワードは、39文字までに制限されています。

DIR_USER_CONTEXT_1、DIR_USER_CONTEXT_2、およびDIR_USER_CONTEXT_3は、ユーザがディレクトリを使用して認証を受けようとしているときに、ユーザの位置を確認するために使用する検索可能なコンテキストを指定します。最初のパスでユーザの位置を確認できない場合、2番目、3番目のパスで指定されたパラメータが使用されます。これらのパラメータの値は、ディレクトリ管理者から入手してください。Directory User Contextは、それぞれ128文字までに制限されています。

MOD_DIR_CONFIGのランタイム エラー

表示される可能性のあるMOD_DIR_CONFIGのエラー メッセージは次のとおりです。

- ディレクトリ情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_GLOBAL_SETTINGS

GET_GLOBAL_SETTINGSコマンドによって、グローバル設定を取得できます。GET_GLOBAL_SETTINGSは、RIB_INFOブロックの内側に示さなければなりません。このコマンドを実行するには、ログイン権限を持つユーザがログインする必要があります。このコマンドによって返される情報は、MOD_GLOBAL_SETTINGSコマンドで変更できます。

GET_GLOBAL_SETTINGSのパラメータ

このコマンドにはパラメータはありません。

GET_GLOBAL_SETTINGSのランタイム エラー

このコマンドにはエラーはありません。

GET_GLOBAL_SETTINGSが返すメッセージ

GET_GLOBAL_SETTINGSは、次のようなメッセージを返します。

```
<GET_GLOBAL_SETTINGS
  SESSION_TIMEOUT="120"
  F8_PROMPT_ENABLED="YES"
  REMOTE_CONSOLE_PORT_STATUS ="ENABLED"
  HTTPS_PORT ="443"
  HTTP_PORT ="80"
  REMOTE_CONSOLE_PORT ="23"
  VIRTUAL_MEDIA_PORT = "17988"
  SNMP_ADDRESS_1 =""
  SNMP_ADDRESS_2 =""
  SNMP_ADDRESS_3 =""
  OS_TRAPS ="NO"
  RIB_TRAPS ="NO"
  CIM_SECURITY_MASK ="MEDIUM"
/>
```

成功しなかった要求の例を次に示します。

```
<RESPONSE
  STATUS = "0x0001"
```

```
MSG = "Error Message"/>
```

MOD_GLOBAL_SETTINGS

このコマンドは、特定のグローバル設定を変更するために使用します。MOD_GLOBAL_SETTINGSコマンドは、RIB_INFOエレメント内に示す必要があり、RIB_INFOは"write"モードでなければなりません。ログインするユーザは、iLOの設定権限を持たなければなりません。次のエレメントはすべて、オプションで省略することができます。エレメントを省略すると、現在の設定が維持されます。このコマンドは、特定のグローバル設定を変更します。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_GLOBAL_SETTINGS>
        <SESSION_TIMEOUT value="60"/>
        <ILO_FUNCT_ENABLED value="Yes"/>
        <F8_PROMPT_ENABLED value="Yes"/>
        <HTTPS_PORT value="443"/>
        <HTTP_PORT value="80"/>
        <REMOTE_CONSOLE_PORT value="23"/>
        <VIRTUAL_MEDIA_PORT value="17988"/>
      </MOD_GLOBAL_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

MOD_GLOBAL_SETTINGSのパラメータ

SESSION_TIMEOUTは、セッション タイムアウトの最大値を分単位で決定します。値として、15、30、60、および120が許可されます。120を超える値を指定すると、SESSION_TIMEOUTがエラーを返します。

ILO_FUNCT_ENABLEDは、iLOのLights-Out機能を有効にするかどうかを決定します。値として"Yes"または"No"を指定できます。このパラメータには、大文字と小文字の区別はありません。

F8_PROMPT_ENABLEDは、POSTの実行中に、ROMベースのコンフィギュレーション用のF8プロンプトを表示するかどうかを決定します。値として、"Yes"または"No"を指定できます。

HTTPS_PORTは、<LOM_short-name>のHTTPS（SSL）ポートの番号を指定します。この値を変更する場合は、iLOをリセットする必要があります。

HTTP_PORTは、iLOのHTTPポートの番号を指定します。この値を変更する場合は、iLOをリセットする必要があります。

REMOTE_CONSOLE_PORTは、iLOのリモート コンソール ポートを指定します。この値を変更する場合は、iLOをリセットする必要があります。

REMOTE_CONSOLE_ENCRYPTIONは、リモート コンソール データの暗号化を有効にするかどうかを決定します。値として、"Yes"および"No"を指定できます。

VIRTUAL_MEDIA_PORTは、iLOの仮想メディア用に使用するポートを指定します。この値を変更する場合は、iLOをリセットする必要があります。

注：ポートの変更を適用するために、iLOは再起動します。ランタイム エラーが発生している場合は、iLOは再起動しません。

MIN_PASSWORDコマンドは、すべてのユーザ パスワードに必要な文字数を指定します。0～39の値を指定できます。

MOD_GLOBAL_SETTINGSのランタイム エラー

表示される可能性のあるMOD_GLOBAL_SETTINGSのエラー メッセージは次のとおりです。

- RIB情報は、読み出し専用アクセス用にかかれています。この操作では、書き込みアクセスが必要です。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。
- パスワードの最大長が満たされていません。

MOD_SNMP_IM_SETTINGS

このコマンドにより、特定のSNMP設定およびInsightマネージャ設定を変更できます。MOD_SNMP_IM_SETTINGSコマンドは、RIB_INFOエレメント内に示す必要があり、RIB_INFOは"write"モードでなければなりません。ログインするユーザは、iLOの設定権限を持たなければなりません。次のエレメントはすべて、オプションで省略することができます。エレメントを省略すると、現在の設定が維持されます。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="write">
  <MOD_SNMP_IM_SETTINGS>
    <WEB_AGENT_IP_ADDRESS value="192.168.125.120"/>
    <SNMP_ADDRESS_1 value="192.168.125.121"/>
    <SNMP_ADDRESS_2 value="192.168.125.122"/>
    <SNMP_ADDRESS_3 value="192.168.125.123"/>
    <OS_TRAPS value="Yes"/>
    <RIB_TRAPS value="No"/>
    <CIM_SECURITY_MASK value="3"/>
  </MOD_SNMP_IM_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

MOD_SNMP_IM_SETTINGSのパラメータ

WEB_AGENT_IP_ADDRESSは、Web対応エージェントのアドレスです。このエレメントの値の最大長は、50文字です。有効な任意のIPアドレスまたはDNS名を指定できます。空白文字列を入力すると、現在の値は削除されます。

SNMP_ADDRESS_1、SNMP_ADDRESS_2、およびSNMP_ADDRESS_3は、ユーザに送信されるトラップを受け取るアドレスです。これらのパラメータの最大長は、それぞれ50文字で、有効なIPアドレスまたはDNS名を指定できます。

OS_TRAPSは、オペレーティング システムが生成したSNMPトラップをユーザが受信する必要があることを示します。値として"Yes"および"No"を指定できます。この値を設定しない場合、デフォルトの"No"とみなされ、トラップは送信されません。

RIB_TRAPSは、RIBが生成したSNMPトラップをユーザが受信する必要があることを示します。値として"Yes"および"No"を指定できます。この値を設定しない場合、デフォルトの"No"とみなされ、トラップは送信されません。

CIM_SECURITY_MASKは、0～4の整数を受け入れます。設定できる値は、次のとおりです。

- 0 - 変更なし
- 1 - None (Insightマネージャ7にデータが返されません)

- 2 - Low (名前とステータス データを返します。SNMPのパススルーがサポートされる場合、対応は存在します。サポートされない場合は、サーバとマネジメントプロセッサは、デバイス リストでは別のものとして扱われます)
- 3 - Medium (iLOとサーバの対応は存在しますが、概要ページには、セキュリティレベルの高い場合ほど詳細なデータは表示されません)
- 4 - High (対応が存在し、すべてのデータが概要ページに表示されます)

各値は、Insightマネージャ7の要求に対して返送するデータのレベルを示します。

MOD_SNMP_IM_SETTINGSのランタイム エラー

- ユーザは、この操作を行うための適切な権限を持っていません。
- RIB情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。

CLEAR_EVENTLOG

CLEAR_EVENTLOGコマンドは、iLOのイベント ログをクリアします。CLEAR_EVENTLOGコマンドは、RIB_INFOブロック内に示す必要があり、RIB_INFOは"write"モードでなければなりません。イベント ログをクリアするには、iLOの設定権限を持つユーザがログインしなければなりません。

例：

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">  
    <RIB_INFO MODE="write">  
      <CLEAR_EVENTLOG/>  
    </RIB_INFO>  
  </LOGIN>  
</RIBCL>
```

CLEAR_EVENTLOGのパラメータ

このコマンドにはパラメータはありません。

CLEAR_EVENTLOGのランタイム エラー

表示される可能性のあるCLEAR_EVENTLOGのエラー メッセージは次のとおりです。

- RIB情報は、読み出し専用アクセス用にかかれています。この操作では、書き込みアクセスが必要です。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

UPDATE_RIB_FIRMWARE

UPDATE_RIB_FIRMWAREコマンドは、ファームウェアのアップグレード ファイルをiLOにコピーし、アップグレード プロセスを開始し、イメージが正しくフラッシュされたらボードを再起動します。UPDATE_RIB_FIRMWAREコマンドは、RIB_INFOブロック内に示す必要があり、RIB_INFOは"write"モードでなければなりません。ファームウェアのアップグレードが完了した後、iLOはリセットされます。ファームウェアをアップデートするには、iLOの設定権限を持つユーザがログインしなければなりません。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:¥ILO140.BIN"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

UPDATE_RIB_FIRMWAREパラメータ

IMAGE_LOCATIONは、ファームウェア アップグレード ファイルの絶対パスで示されたファイル名を受け取ります。

UPDATE_RIB_FIRMWAREのランタイム エラー

表示される可能性のあるUPDATE_RIB_FIRMWAREのエラー メッセージは、次のとおりです。

- RIB情報は、読み出し専用アクセス用にかかれています。この操作では、書き込みアクセスが必要です。

- ファームウェア イメージ アップデート ファイルを開くことができません。
- ファームウェア イメージ アップデート ファイルを読み取ることができません。
- そのファームウェア アップグレード ファイルのサイズは大きすぎます。
- そのファームウェア イメージ ファイルは、無効です。
- 有効なファームウェア イメージがロードされていません。
- フラッシュ プロセスを開始できませんでした。
- IMAGE_LOCATIONをブランクにすることはできません。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_FW_VERSION

GET_FW_VERSIONコマンドは、iLOのファームウェアのバージョンと日付を返します。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_FW_VERSION/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_FW_VERSIONのパラメータ

このコマンドにはパラメータはありません。

GET_FW_VERSIONのランタイム エラー

このコマンドにはエラーはありません。

GET_FW_VERSIONが返すメッセージ

返される応答には、次の情報が含まれます。

```
<GET_FW_VERSION
  FIRMWARE_VERSION = <firmware version>
  FIRMWARE_DATE = <firmware date>
  MANAGEMENT_PROCESSOR = <management processor type>
/>
```

HOTKEY_CONFIG

HOTKEY_CONFIGコマンドは、iLOのリモート コンソールのホット キーを設定します。HOTKEY_CONFIGコマンドは、RIB_INFOエレメント内に示す必要があり、RIB_INFOは"write"モードでなければなりません。このコマンドのサブエレメントは、すべてオプションです。このコマンドを実行するには、iLOの設定権限を持つユーザがログインしなければなりません。

大文字はサポートされておらず、自動的に小文字に変換されます。二重引用符または単一引用符のいずれかを使用する場合、必ず、区切り記号とは異なるものを使用してください。入力されないCTRLサブエレメントは、変更されません。空白文字列を指定すると、現在の値は削除されます。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <HOTKEY_CONFIG>
        <CTRL_T value="CTRL,ALT,ESC"/>
        <CTRL_U value="L_SHIFT,F10,F12"/>
        <CTRL_V value=""/>
        <CTRL_Y value=""/>
        <CTRL_X value=""/>
        <CTRL_Z value=""/>
      </HOTKEY_CONFIG>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

HOTKEY_CONFIGのパラメータ

CTRL_Tは、CTRL_Tホット キーの設定を指定します。設定は、カンマで区切る必要があります（例：CTRL_T="CTRL,ALT,ESC"）。ホット キーごとに、最大5つのキーストロークを設定できます。

CTRL_Uは、CTRL_Uホット キーの設定を指定します。設定は、カンマで区切る必要があります（例：CTRL_U="CTRL,ALT,ESC"）。ホット キーごとに、最大5つのキーストロークを設定できます。

CTRL_Vは、CTRL_Vホット キーの設定を指定します。設定は、カンマで区切る必要があります（例：CTRL_V="CTRL,ALT,ESC"）。ホット キーごとに、最大5つのキーストロークを設定できます。

CTRL_Wは、CTRL_Wホット キーの設定を指定します。設定は、カンマで区切る必要があります（例：CTRL_W="CTRL,ALT,ESC"）。ホット キーごとに、最大5つのキーストロークを設定できます。

CTRL_Xは、CTRL_Xホット キーの設定を指定します。設定は、カンマで区切る必要があります（例：CTRL_X="CTRL,ALT,ESC"）。ホット キーごとに、最大5つのキーストロークを設定できます。

CTRL_Yは、CTRL_Yホット キーの設定を指定します。設定は、カンマで区切る必要があります（例：CTRL_Y="CTRL,ALT,ESC"）。ホット キーごとに、最大5つのキーストロークを設定できます。

HOTKEY_CONFIGのランタイム エラー

表示される可能性のあるHOTKEY_CONFIGのエラー メッセージは次のとおりです。

- RIB情報は、読み出し専用アクセス用にかかれています。この操作では、書き込みアクセスが必要です。
- 指定されているホット キーのパラメータは、無効です。
- ホット キーに割り当てられているキーストロークの数が無効です。許可される最大数は、5です。
- ユーザは、この操作を行うための適切な権限を持っていません。

LICENSE

LICENSEコマンドは、iLOの高度な機能を有効または無効にします。ProLiant BL p-Class サーバの場合、高度な機能が出荷時に有効になっているので、アクティベーション キーは必要ありません。

LICENSEコマンドは、RIB_INFOエレメント内に示す必要があり、RIB_INFOは"write"モードでなければなりません。iLOの設定権限を持つユーザがログインしなければなりません。このコマンドのサブエレメントは、すべてオプションです。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <LICENSE>
        <ACTIVATE KEY="111112222233334444455555"/>
      </LICENSE>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

LICENSEのパラメータ

ACTIVATEの後に有効なKEY値を記載し、iLOのAdvancedパックのライセンスを有効にすることを示します。

KEYには、アクティベーション キーの値を指定します。キーは、連続した1つのストリングとして入力してください。カンマ、ピリオド、またはその他の文字を、キー値の間にはさまないでください。キーは、25桁でのみ受け付けられます。キー値の間に他の文字をはさむと、キーの一部とみなされ不正なキーを入力したことになります。

DEACTIVATEは、iLO Advancedパックのライセンスを無効にすることを示します。

LICENSEのランタイム エラー

表示される可能性のあるLICENSEのエラー メッセージは次のとおりです。

- アクティベーション キー エラー

- ライセンスは、すでに有効です。
- ユーザは、この操作を行うための適切な権限を持っていません。

RACK_INFO

RACK_INFOコマンドは、ProLiant BL p-Classラックの情報をこれから変更することをファームウェアに通知するために使用します。このコマンド ブロックは、ラック サーバ上でのみ有効です。iLOの設定権限を持つユーザがログインしなければなりません。

例：

```
<RACK_INFO MODE="read">
..... RACK_INFO commands .....
</RACK_INFO>
```

RACK_INFOのパラメータ

MODEは、最大長10文字の特殊ストリング パラメータです。このパラメータは、ユーザ情報を使用して何をしようとしているのかを示します。有効な引数は、"read"および"write"です。

"write"モードで開かれた場合、読み出しと書き込みが有効になります。"read"モードで開かれた場合は、ラックの変更はできません。このパラメータでは、大文字と小文字は区別されません。このパラメータをブランクにすることはできません。

RACK_INFOのランタイム エラー

表示される可能性のあるRACK_INFOのエラー メッセージは次のとおりです。

- モードが無効です。
- このサーバはラック サーバではありません。ラック コマンドは適用されません。

MOD_BLADE_RACK

MOD_BLADE_RACKは、ProLiant BL p-Classラックの特定の設定を変更するために使用されます。MOD_BLADE_RACKコマンドは、RACK_INFOエレメント内に示す必要があり、RACK_INFOは"write"モードでなければなりません。ラックの設定権限を持つユーザがログインしなければなりません。サブエレメントは、すべてオプションです。サブエレメントを省略すると、現在の設定が維持されます。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="userlogin" PASSWORD="password">
    <RACK_INFO MODE="write">
      <MOD_BLADE_RACK>
        <RACK_NAME value="CPQ_Rack_1"/>
        <ENCLOSURE_NAME value="CPQ_Enclosure_1"/>
        <BAY_NAME value="CPQ_Bay_5"/>
        <FACILITY_PWR_SOURCE value="Yes"/>
        <RACK_AUTO_PWR value="Yes"/>
        <LOG_RACK_ALERTS value="Yes"/>
      </MOD_BLADE_RACK>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

MOD_BLADE_RACKのパラメータ

RACK_NAMEは、1つのラックを構成するコンポーネントを論理的なグループにまとめるために使用されます。RACK_NAMEを変更すると、そのラック名はラックに接続されている他のすべてのコンポーネントに通知されます。この名前は、ログ記録やアラート生成の際に使用され、コンポーネントの識別に役立ちます。RACK_NAMEには、最大31文字を使用できます。

ENCLOSURE_NAMEは、1つのエンクロージャ（筐体）を構成するProLiant BL p-Classサーバを論理的なグループにまとめるために使用します。ENCLOSURE_NAMEを変更すると、そのエンクロージャ名は同じエンクロージャに接続されている他のすべてのブレードサーバに通知されます。この名前は、ログ記録やアラート生成の際に使用され、コンポーネントの識別に役立ちます。ENCLOSURE_NAMEには、最大31文字を使用できます。

BAY_NAMEは、コンポーネントまたはコンポーネントの機能の識別に役立てるために使用されます。この名前は、ログ記録やアラート生成の際に使用され、コンポーネントの識別に役立ちます。BAY_NAMEには、最大31文字を使用できます。

FACILITY_PWR_SOURCEは、ブレード サーバの電源を決定します。"Yes"を指定すると既存の電源、"No"を指定するとサーバ ブレードのパワー サプライを使用するようにサーバに指示できます。

RACK_AUTO_PWRは、ブレード サーバに自動的に電源投入するかどうかを決定します。"Yes"を指定すると、ブレード サーバに自動的に電源が投入され通常の起動プロセスが開始されます（電源を供給できる場合）。"No"を指定すると、ブレード サーバに手動で電源を入れなければなりません。

LOG_RACK_ALERTSは、ラック インフラストラクチャからのアラートをログに記録するかどうかを決定します。"Yes"を指定すると、ラック アラートはIMLのログに記録されます。"No"を指定すると、ラック アラートは、IMLのログに記録されません。

MOD_BLADE_RACKのランタイム エラー

表示される可能性のあるMOD_BLADE_RACK のエラー メッセージは次のとおりです。

- ラック情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- ラック名が長すぎます。
- エンクロージャ名が長すぎます。
- ベイ名が長すぎます。
- ユーザは、この操作を行うための適切な権限を持っていません。

GET_TOPOLOGY

GET_TOPOLOGYコマンドは、iLOが現在のラックのラック トポロジを返すことを要求します。GET_TOPOLOGYコマンドは、RACK_INFOエレメント内に示す必要があります。

例：

```
<RIBCL VERSION="2.0">
```

```
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RACK_INFO MODE="read">
  <GET_TOPOLOGY/>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

GET_TOPOLOGYのパラメータ

このコマンドにはパラメータはありません。

GET_TOPOLOGYが返すメッセージ

成功した要求の例を次に示します。

```
<RK_TPLGY CNT="3">
<RUID>xxxxxx</RUID>
<ICMB ADDR="0xAA55" MFG="232" PROD_ID="NNN" SER="123"
NAME="Power_1">
<LEFT/>
<RIGHT ADDR="0xAB66" SER="123" NAME="Server_1"/>
</ICMB>
<ICMB ADDR="0xAB66" MFG="232" PROD_ID="NNN" SER="456"
NAME="Server_1">
<LEFT ADDR="0xAA55" SER="123" NAME="Power_1"/>
<RIGHT ADDR="0xAC77" SER="123" NAME="Power_2"/>
</ICMB>
<ICMB ADDR="0xAC77" MFG="232" PROD_ID="NNN" SER="789"
NAME="Power_2">
<RIGHT/>
</ICMB>
</RK_TPLGY>
```

SERVER_INFO

SERVER_INFOコマンドは、iLOの設定をこれから変更することをファームウェアに通知します。

例：

```
<SERVER_INFO MODE="read">
```

```
..... SERVER_INFO commands .....  
</SERVER_INFO>
```

SERVER_INFOのパラメータ

MODEは、最大長10文字の特殊ストリング パラメータです。このパラメータは、サーバ情報を使用して何をしようとしているのかをiLOに通知します。有効な引数は、"read"および"write"です。"write"モードで開いた場合は、読み出しと書き込みが有効になります。"read"モードで開いた場合は、サーバについての操作は行うことができません。このパラメータを指定しない場合、"read"とみなされます。

SERVER_INFOのランタイム エラー

表示される可能性のあるSERVER_INFOのエラー メッセージは次のとおりです。MODEパラメータをブランクにすることはできません。

GET_HOST_POWER_STATUS

GET_HOST_POWER_STATUSコマンドは、仮想電源ボタン ケーブルからサーバの電源状態を表示します。GET_HOST_POWER_STATUSコマンドは、SERVER_INFOエレメント内に示す必要があり、SERVER_INFOは"write"モードでなければなりません。

例：

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">  
    <SERVER_INFO MODE="write">  
      <GET_HOST_POWER_STATUS/>  
    </SERVER_INFO>  
  </LOGIN>  
</RIBCL>
```

GET_HOST_POWER_STATUSのパラメータ

このコマンドにはパラメータはありません。

GET_HOST_POWER_STATUSのランタイム エラー

表示される可能性のあるGET_HOST_POWER_STATUSのエラー メッセージは次のとおりです。

- ホストの電源は、オフです。
- ホストの電源は、オンです。

GET_HOST_POWER_STATUSが返すメッセージ

返される応答には、次の情報が含まれます。

```
<GET_HOST_POWER
  HOST_POWER="OFF"
/>
```

SET_HOST_POWER

SET_HOST_POWERコマンドは、仮想電源ボタン機能を設定します。この機能がサポートされている場合、この機能により、サーバの電源を投入/切断します。SET_HOST_POWERコマンドは、SERVER_INFOエレメント内に示す必要があり、SERVER_INFOは"write"モードでなければなりません。このコマンドを実行するには、サーバのリセット権限を持つユーザがログインしなければなりません。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <SET_HOST_POWER HOST_POWER="Yes"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

SET_HOST_POWERのパラメータ

HOST_POWERは、仮想電源ボタンを有効または無効にします値として、"Yes"または"No"を指定できます。

SET_HOST_POWERのランタイム エラー

表示される可能性のあるSET_HOST_POWERのエラー メッセージは次のとおりです。

- サーバ情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- このサーバでは仮想電源ボタン機能はサポートされていません。
- ホストの電源は、すでにオンです。
- ホストの電源は、すでにオフです。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

RESET_SERVER

RESET_SERVERコマンドは、サーバの電源が入っている場合に、サーバをリセットします。RESET_SERVERコマンドは、SERVER_INFOエレメント内に示す必要があり、SERVER_INFOは"write"モードでなければなりません。このコマンドを実行するには、サーバのリセット権限を持つユーザがログインしなければなりません。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <RESET_SERVER/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

RESET_SERVERのパラメータ

このコマンドにはパラメータはありません。

RESET_SERVERのエラー

表示される可能性のあるRESET_SERVERのエラー メッセージは次のとおりです。

- サーバ情報は、読み出し専用アクセス用に開かれています。この操作では、書き込みアクセスが必要です。
- 現在サーバの電源は切断されています。
- ユーザは、この操作を行うための適切な権限を持っていません。
- ログインしたユーザは、このコマンドの実行に必要な権限を持っていません。

GET_UID_STATUS

UID_STATUSコマンドは、サーバのUID LEDのステータスを提供します。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <GET_UID_STATUS />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

GET_UID_STATUSのパラメータ

このコマンドにはパラメータはありません。

GET_UID_STATUSの応答

返される応答には、次の情報が含まれます。

```
<GET_UID_STATUS
  UID="OFF"
/>
```

UID_CONTROL

UID_CONTROLコマンドは、サーバのUID LEDを点灯または消灯させます。UID_CONTROLコマンドは、SERVER_INFOエレメント内に示す必要があり、SERVER_INFOは"write"モードでなければなりません。

例：

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <UID_CONTROL UID="Yes"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

UID_CONTROLのパラメータ

UIDは、UIDのステータスを決定します。値を"Yes"に設定するとUID LEDは点灯し、"No"に設定すると消灯します。

UID_CONTROLのエラー

表示される可能性のあるUID_CONTROLのエラー メッセージは、次のとおりです。

- UIDはすでに点灯しています。
- UIDはすでに消灯しています。

内蔵Lights-Outのパラメータ

この項の目次

内蔵Lights-Outのパラメータに関する表	207
サーバの識別パラメータ	211
ユーザ管理のパラメータ	212
グローバル設定のパラメータ	214
ネットワーク設定のパラメータ	216
ディレクトリ設定のパラメータ	219
SNMP/Insightマネージャの設定のパラメータ	221
ProLiant BL p-Classのパラメータ	223
iLO Advancedライセンス アクティベーション設定	225

内蔵Lights-Outのパラメータに関する表

表の「使用する値」の欄に実際に使用する値をメモすることができます。

パラメータ	デフォルト値または設定	使用する値
サーバの識別		
PCIリソース	BIOSにより設定	
サーバ名		
サーバID		
シリアル番号	iLOXXXXXXXXXXXX	
ファームウェアのバージョン	XX.XX	
ファームウェアの日付	mm/dd/yyyy	
ユーザ管理		
ユーザ名	Administrator	
ログイン名	Administrator	
パスワード	無作為に選択した8文字の英数字文字列（工場出荷時に設定）	
ユーザ アカウントの管理	Yes（有効）	
リモート コンソールへのアクセス	Yes（有効）	
仮想電源およびリセット	Yes（有効）	
仮想メディア	Yes（有効）	
iLOの設定	Yes（有効）	
グローバル設定		
Lights-Out機能の有効化	Yes（有効）	
アイドル時の接続タイムアウト（分単位）	30分	
Webサーバの非SSLポート	80	
WebサーバのSSLポート	443	
仮想メディア ポート	17988	
リモート コンソール ポート	23	
iLOのROMベース セットアップユーティリティを有効にする	Yes（有効）	

パラメータ	デフォルト値または設定	使用する値
iLO RBSUへのログインを要求	なし	
パスワードの最小長	8	
ネットワーク設定		
NICの有効化	Yes (有効)	
トランシーバ速度の自動選択	Yes (有効)	
速度	適用なし (自動選択)	
デュプレックス	適用なし (自動選択)	
DHCPの有効化	Yes (有効)	
DHCPのゲートウェイの使用	Yes (有効)	
DHCPのDNSサーバの使用	Yes (有効)	
DHCPのWINSサーバの使用	Yes (有効)	
DHCPの静的経路の使用	Yes (有効)	
DHCPのドメイン名の使用	Yes (有効)	
WINSサーバの登録	適用なし (DHCP)	
DNSサーバの登録	適用なし (DHCP)	
起動時にゲートウェイにpingを送信	No (無効)	
iLOのIPアドレス	適用なし (DHCP)	
iLOのサブネット マスク	適用なし (DHCP)	
iLOゲートウェイのIPアドレス	適用なし (DHCP)	
iLOサブシステムの名前	iLOXXXXXXXXXXXXX (12個のXはサーバのシリアル番号、工場出荷時に割り当て)	
ドメイン名	適用なし (DHCP)	
DHCPサーバ	適用なし (DHCP)	

パラメータ	デフォルト値または設定	使用する値
プライマリ、セカンダリおよびターシャリDNSサーバ	適用なし (DHCP)	
プライマリおよびセカンダリWINSサーバ	適用なし (DHCP)	
静的経路#1、#2、#3	宛先とゲートウェイ アドレスについて、適用なし (DHCP)	
SNMP/Insightマネージャの設定		
SNMPアラートの通知先	No (無効)	
iLO SNMPアラートを有効にする	No (無効)	
InsightマネージャのエージェントからのSNMPアラートを転送する	No (無効)	
InsightマネージャのWebエージェントのURL		
返すデータのレベル	Medium	
<LOM_short_name>の高度な機能の使用許諾の有効化		
iLO Advancedバック アクティベーション キー	No (無効)	
BL p-Class		
ラック名	ラックにより提供	
エンクロージャ名	ラックにより提供	
ベイ名	ベイX (Xは、ブレード サーバが挿入されるベイの番号)	
ベイ	ラックにより提供	
ラックのシリアル番号	ラックにより提供	
エンクロージャのシリアル番号	ラックにより提供	
ブレードのシリアル番号	ブレード サーバにより提供	
電源	ラックにより提供	
自動電源投入の有効化	オン	

パラメータ	デフォルト値または設定	使用する値
ラック アラートの転送の有効化	オン	
ラック アラートのログ記録 (IML)の有効化	オン	
ディレクトリ設定		
ディレクトリ サービスによる 認証	無効	
ディレクトリ サーバのアドレス	0.0.0.0	
ディレクトリ サーバのLDAP ポート	636	
LOMオブジェクトの識別名		
LOMオブジェクトのパスワード		
ディレクトリ ユーザ コンテキスト1		
ディレクトリ ユーザ コンテキスト2		
ディレクトリ ユーザ コンテキスト3		

サーバの識別パラメータ

以下のパラメータは、ホスト サーバに関する情報を提供します。

PCIリソース

このフィールドには、PCIリソース用に予約された割り込みが表示されます。値は、BIOSによって設定されます。

サーバ名

ホスト サーバのオペレーティング システムでInsightマネジメント エージェントを使用している場合、エージェントは、サーバ名をiLOに提供します。

シリアル番号

この番号は、iLOのシリアル番号です。この番号は、情報として表示されるだけです。この番号を変更することはできません。

ファームウェアのバージョン

この番号は、iLOのファームウェアのバージョン番号です。この値を変更することはできません。

ファームウェアの日付

iLOに搭載されているバージョンのファームウェアの日付で、mm/dd/yyyyのフォーマットで表示されます。これは情報として表示されるだけで、変更することはできません。

ユーザ管理のパラメータ

ユーザの管理セクションを使用して、ユーザがiLOにアクセスできるように設定できます。最大12ユーザを指定できます。Webインタフェースを使用して、ユーザ設定を追加、削除または変更できます。

ユーザ名

このパラメータは、ユーザ リストやイベント ログに表示されるユーザの実際の名前です。これは、ログインに使用される名前ではありません。ユーザ名の最大長は39文字です。

ログイン名

ユーザがiLOにログインする際に提供しなければならない名前で、大文字と小文字が区別されます。

パスワード

ユーザがiLOにログインする際に提供しなければならないパスワードで、大文字と小文字が区別されます。[Security Options]で、パスワードの最小長を割り当てることができます。パスワードの最小長は、0～39文字の間で設定できます。デフォルトでは、パスワードの最小長は、8文字です。パスワードは確認のため、2回入力する必要があります。

ユーザ アカウントの管理

この権限により、ユーザ アカウントを追加、変更、および削除できます。また、すべてのユーザの権限を変更することも可能です。たとえば、1人のユーザにすべての権限を与えることもできます。

リモート コンソールへのアクセス

この権限により、管理対象システムの、モニタ、キーボード、およびマウス制御を含むリモート コンソールをリモートで管理できます。

仮想電源およびリセット

この権限により、ホスト プラットフォームの電源を再投入したり、ホスト プラットフォームをリセットしたりすることができます。

仮想メディア

この権限により、ホスト プラットフォーム上で仮想メディアを使用できます。

iLOの設定

この権限により、セキュリティ設定を含む、ほとんどのiLOの設定を行うことができます。この権限には、ユーザ アカウントの管理は含まれません。

iLOが正しく設定されたら、すべてのユーザからこの権限を取り消して、再設定を防止します。ユーザ アカウントの管理権限を持つユーザは、この権限を有効にしたり無効にしたりすることができます。iLOのRBSUを有効にしている場合も、iLOを再設定できます。

グローバル設定のパラメータ

グローバル設定セクションでは、iLOの全体的なセキュリティ レベルを定義できます。これらの設定は、個々のユーザの設定とは関係なく、グローバルに適用されます。

アイドル時の接続タイムアウト（分単位）

このオプションで指定した時間内（分単位）にユーザが操作を行わない場合、Webサーバセッションおよびリモート コンソール セッションは自動的に終了します。

Lights-Out機能の有効化

このオプションにより、iLOに接続できます。無効にすると、iLOへのすべての接続が拒否されます。デフォルト設定は、Yesです。

iLOのROMベース セットアップ ユーティリティを有効にする

このオプションにより、ホストに物理アクセスまたは仮想アクセスするユーザは、そのシステムのiLOを、iLOのRBSUを使用して設定できます。RBSUは、ホストシステムが再起動し、POSTの実行中に起動されます。デフォルト設定は、Yesです。**[Require Login for iLO RBSU]**設定を使用して、RBSUへのアクセスを許可されたユーザだけに限定することができます。

注：セキュリティ用のジャンパが物理的に設定されている場合、再起動中に、RBSUのプロンプトが表示されます。

iLO RBSUへのログインを要求

このオプションは、ユーザがiLOのRBSUにアクセスする際に、ログイン名とパスワードの入力を要求されるかどうかを指定します。デフォルト設定は、Noです。

リモート コンソール ポートの設定

このオプションにより、ポート アドレスの設定を有効または無効にします。このオプションを**Enabled**に設定すると、Telnetおよびリモート コンソール アプレットによるiLOへのアクセスが可能になります。**Disabled**に設定すると、Telnetによるアクセスもリモート コンソール アプレットによるアクセスもできなくなります。Telnetを使用してテキストベースのリモート コンソールにアクセスする場合は、**[Remote Console Data Encryption]**を**No**に設定する必要があります。

リモート コンソール データの暗号化

このオプションにより、リモート コンソール データの暗号化を有効にします。標準的なTelnetクライアントを使用してiLOにアクセスする場合は、**No**に設定する必要があります。

SSL暗号化強度

このオプションは、現在の暗号化強度設定を表示します。最も安全な設定は、128-bit（High）です。

現在の暗号化アルゴリズム

このオプションは、ブラウザとiLOとの間で転送中のデータを保護するために現在使用されている暗号化アルゴリズムを表示します。

Webサーバの非SSLポート

デフォルトでは、iLOに内蔵のWebサーバは、非暗号化通信用にポート80を使用するように設定されています。このポートは、**[Administration]**タブの**[Global Settings]**オプションで設定できます。

WebサーバのSSLポート

デフォルトでは、iLOに内蔵のWebサーバは暗号化通信用にポート443を使用するように設定されています。このポートは、**[Administration]**タブの**[Global Settings]**オプションで設定できます。

仮想メディア ポート

iLOの仮想メディア サポートは、通信用に設定可能なポートを使用します。このポートは、[Administration]タブの[Global Settings]オプションで設定できます。デフォルトでは、ポート17988を使用するように設定されています。

リモート コンソール ポート

デフォルトでは、iLOのリモート コンソールは、リモート コンソール通信用にポート23を使用するように設定されています。このポートは、[Administration]タブの[Global Settings]オプションで設定できます。

パスワードの最小長

このオプションにより、ユーザ パスワードの設定または変更の際に許可される文字の最小数を指定します。文字数は、0～39の任意の値に設定できます。デフォルト設定は、8文字です。

ネットワーク設定のパラメータ

以下のパラメータは、iLOのネットワークの設定に関する情報を提供します。

NICの有効化

このパラメータは、NICがiLOの状態を反映できるようにします。NICのデフォルト設定は、Yes（有効）になっています。DHCPを無効にした場合、静的なIPアドレスをiLOに割り当てする必要があります。このセクションで説明されているiLOのIPアドレスのパラメータを用いてIPアドレスを割り当てます。

トランシーバ速度の自動選択

自動選択は、インタフェースの速度を検出して10Mbpsまたは100Mbpsで動作するようにインタフェースを設定し、さらに半二重/全二重を設定します。必要に応じて、このパラメータを手動選択に設定し、速度とデュプレックス（半二重/全二重）の設定を手動で調整するようにできます。

速度

トランシーバ速度の自動選択が有効でない場合、この設定を使用して、10Mbpsまたは100Mbpsの接続速度を割り当てます。

デュプレックス

トランシーバ速度の自動選択が有効でない場合、この設定を使用して、デュプレックス（半二重/全二重）をNICに割り当てます。

DNS/DHCP

iLOは、DNS/DHCPが有効に設定された状態でHPから出荷されます。DHCPを無効にするには、iLOのRBSUを使用しなければなりません。

注：DHCPを無効にする場合、iLOのRBSUでIPアドレスとサブネット マスクを手動で設定する必要があります。

DHCPを有効にすると、次の設定も有効になります。

- DHCPのゲートウェイの使用
- DHCPのDNSサーバの使用
- DHCPのWINSサーバの使用
- DHCPの静的経路の使用
- DHCPのDNS名の使用

DHCPが無効の場合は、これらの設定を割り当てなければなりません。

WINSサーバの登録

iLOは、自動的にWINSサーバに登録されます。デフォルト設定は、Yesです。デフォルトでは、WINSサーバのアドレスは、DHCPが割り当てます。

DNSサーバの登録

iLOは、自動的にDNSサーバに登録されます。デフォルト設定は、Yesです。デフォルトでは、DNSサーバのアドレスは、DHCPが割り当てます。

起動時にゲートウェイにpingを送信

このオプションにより、iLOは、初期化中に4つのICMPエコー要求パケットをゲートウェイに送信します。このオプションにより、iLOとの間でパケットをルーティングするルータ上で、ARPキャッシュのiLOのエントリが最新のものになります。

iLOのIPアドレス

このパラメータを使用して、iLOにネットワーク上で静的IPアドレスを割り当てます。デフォルトでは、IPアドレスはDHCPが割り当てます。

iLOのサブネット マスク

このサブネット マスク パラメータを使用して、デフォルト ゲートウェイのサブネット マスクを割り当てます。デフォルトでは、サブネット マスクはDHCPが割り当てます。

iLOゲートウェイのIPアドレス

ゲートウェイ パラメータを使用して、ネットワーク ルータのIPアドレスを割り当てます。このルータは、iLOサブネットを管理コンソールが常駐する別のサブネットに接続します。デフォルト ゲートウェイは、DHCPが割り当てます。

iLOサブシステムの名前

iLOは、DNS/WINS名が設定された状態で出荷されます。DNS/WINS名は、"iLO"の後にサーバのシリアル番号を追加したものです。この名前は、iLOのブラケットに付けられているタグにも表示されています。この値は変更できます。

ドメイン名

iLOが属しているドメイン名を入力します。デフォルトでは、ドメイン名はDHCPが割り当てます。

DHCPサーバ

この設定は、DHCPが有効に設定されていれば自動的に検出されます。この設定を変更することはできません。

プライマリ、セカンダリおよびターシャリDNSサーバ

このパラメータを使用して、ネットワーク上で固有のDNSサーバのIPアドレスを割り当てます。デフォルトでは、プライマリ、セカンダリ、およびターシャリDNSサーバは、DHCPが割り当てます。

プライマリおよびセカンダリWINSサーバ

このパラメータを使用して、ネットワーク上で固有のWINSサーバのIPアドレスを割り当てます。デフォルトでは、プライマリおよびセカンダリWINSサーバは、DHCPが割り当てます。

静的経路#1、#2、#3

このパラメータを使用して、ネットワーク上で静的経路の宛先とゲートウェイのIPアドレスの固有のペアを割り当てます。最大3つの静的経路ペアを割り当てることができます。デフォルトでは、静的経路は、DHCPが割り当てます。

ディレクトリ設定のパラメータ

以下のパラメータは、ディレクトリ設定に関する情報を提供します。

ディレクトリ サービスによる認証

このパラメータは、ディレクトリ サービスによる認証を有効または無効にします。ディレクトリのサポートが正しく設定されている場合、この設定により、ユーザはディレクトリ用のユーザ名とパスワードを使用して、iLOにログインできます。

ディレクトリ サーバのアドレス

このパラメータは、ディレクトリ サーバのDNS名またはIPアドレスを指定します。DNS名またはマルチホストDNS名の使用をおすすめします。IPアドレスを使用する場合、そのサーバが停止するとディレクトリを使用できなくなります。

ディレクトリ サーバのLDAPポート

このオプションは、ディレクトリ サーバへの接続に使用するポート番号を設定します。SSLによりセキュリティ保護されているLDAPのポート番号は、636です。

LOMオブジェクトの識別名

このオプションは、ディレクトリ内でのiLOの固有名を指定します。LOMオブジェクトの識別名は、256文字までに制限されています。

LOMオブジェクトのパスワード

このパラメータは、iLOオブジェクトがディレクトリにアクセスするためのパスワードを指定します。LOMオブジェクトのパスワードは、39文字までに制限されています。

注：現時点では、LOMオブジェクトのパスワード フィールドは使用しません。このフィールドは、将来のファームウェア リリースとの上位互換性を保つために用意されます。

ディレクトリ ユーザ コンテキスト1、ディレクトリ ユーザ コンテキスト2、ディレクトリ ユーザ コンテキスト3

このパラメータにより、ユーザがディレクトリ サービスを使用して認証を受けようとするとき、そのユーザの位置を確認するために使用される最大3つの検索可能コンテキストを指定できます。ディレクトリ ユーザ コンテキストは、それぞれ128文字までに制限されています。ディレクトリ ユーザ コンテキストによりディレクトリ ユーザのコンテナを指定できます。このコンテナは、iLOへのログインが試みられたとき、自動的に検索されます。これにより、ログイン画面に、ユーザの完全な識別名を入力する必要がなくなります。たとえば、検索コンテキスト"ou=lights out devices,o=corp"により、ユーザ"cn=manager,ou=lights out devices,o=corp"は、"manager"と入力するだけでiLOにログインできます。Active Directoryでは、他に、検索コンテキスト フォーマット"@hostname"が提供されます（例："@directory.corp"）。

ディレクトリ設定のテスト

ディレクトリ設定の更新後、[Apply Settings]ボタンをクリックして設定を保存します。
[Test Settings]ボタンを有効にすると、現在のディレクトリ設定が有効かどうかを確認
できます。設定をテストするには、以下の手順に従ってください。

1. [Enable Directory Authentication]設定が有効になっていることを確認します。
2. [Test Settings]ボタンをクリックします。
3. [Directory Administrator Distinguished Name]フィールドと[Directory Administrator Password]フィールドに、iLOをディレクトリ サーバに追加したとき使用したユーザの完全識別名とパスワードを入力します。
4. [Test User Name]フィールドと[Test User Password]フィールドに、ディレクトリベースでiLOにログインすることが予想されるユーザ アカウントのユーザ名とパスワードを入力します。
5. [Start Test]ボタンをクリックします。

一連のテストが開始され、テストの進行とともにページが自動的に更新されます。テストの状態を参照して、結果を診断します。特定のテスト結果について詳しくは、ヘルプ ページを参照してください。ディレクトリ設定を変更した場合、iLOがリセットされた場合、またはテストが再開された場合、テスト結果はクリアされます。

SNMP/Insightマネージャの設定のパラメータ

iLOは、デバイス レベルでのSNMP設定をサポートします。このパラメータは、ユーザ単位で設定するものではなく、iLO固有のものです。

SNMPアラートの通知先

iLOからのSNMPトラップ アラートを受信するリモートの管理PCのIPアドレスを入力します。最大3つのIPアドレスを指定して、SNMPアラートを受信できます。

iLO SNMPアラートを有効にする

このアラート状態は、iLOによって検出されるもので、ホスト サーバのオペレーティング システムには依存しません。InsightマネージャのSNMPトラップもこのアラートで通知することができます。このアラートには、リモート サーバの電源切断やサーバのリセットなど、主要なイベントも含まれます。また、セキュリティの無効化やログイン試行の失敗など、iLOのイベントも含まれます。アラートは、iLOによって、指定された通知先を使用してInsightマネージャ7のコンソールに転送されます。デフォルト設定は、Yesです。

InsightマネージャのエージェントからのSNMPアラートを転送する

このアラートは、サポートされる各ネットワーク オペレーティング システム用のInsight マネジメント エージェントによって生成されます。これらのアラートを受信するには、ホスト サーバにエージェントをインストールしていなければなりません。このアラートは、ネットワーク上のInsightマネージャ7クライアントに送信された後、iLOによって、これらのアラートを受信するように設定されているIPアドレスに、非同期で転送されます。デフォルト設定は、Yesです。

InsightマネージャのWebエージェントのURL

[Insight Manager Web Agent URL]オプションにより、InsightマネージャのWebエージェントが動作しているホスト サーバのIPアドレスまたはDNS名を入力できます。このデータをフィールドに入力すると、iLOは、iLOのWebページからWebエージェントのページへのリンクを作成することができます。

返すデータのレベル

[Level of Data Returned]オプションにより、Insightマネージャ7からのiLO情報の匿名要求に対して返すデータの量を規定できます。[None]データ レベルを除くすべての設定では、Insightマネージャ7との統合を実現する十分なデータが提供されます。[Medium]および[High]に設定すると、Insightマネージャ7は、マネジメント プロセッサをホストサーバに関連付けることができます。[None]データ レベルに設定すると、iLOは、Insightマネージャ7の要求に回答しません。デフォルト設定は、[Medium]です。

ProLiant BL p-Classのパラメータ

以下のパラメータは、ProLiant BL p-Classの設定に関する情報を提供します。

ラック名

ラック名は、1つのラックを構成するコンポーネントを論理的なグループにまとめるために使用されます。ラック名を変更すると、そのラック名はラックに接続されている他のすべてのコンポーネントに通知されます。この名前は、ログ記録やアラート生成の際に使用され、コンポーネントの識別に役立ちます。

エンクロージャ名

エンクロージャ（筐体）名は、1つのエンクロージャを構成するサーバ ブレードを論理的なグループにまとめるために使用されます。エンクロージャ名を変更すると、そのエンクロージャ名は同じエンクロージャに接続されている他のすべてのサーバ ブレードに通知されます。この名前は、ログ記録やアラート生成の際に使用され、コンポーネントの識別に役立ちます。

ベイ名

ベイ名は、ログ記録やアラート生成の際に使用され、コンポーネントやその機能の識別に役立ちます。

ベイ

ProLiant BL p-Classエンクロージャは、1～8台のサーバ ブレードをサポートできます。ベイには、左から右に1～8までの番号が付けられます。ベイ番号は、障害の発生したサーバ ブレードや他のエラー状態の物理的識別に役立ちます。この情報は、表示のためにのみ提供されます。

ラックのシリアル番号

ラックのシリアル番号は、ラック内のコンポーネントを論理グループとして識別します。シリアル番号は、さまざまなコンポーネントの起動時に決定され、固有のラックシリアル番号が作成されます。コンポーネント（サーバ ブレード エンクロージャまたはパワー サプライ）を取り替えると、ラック シリアル番号が変更されます。

エンクロージャのシリアル番号

エンクロージャのシリアル番号は、表示されているサーバ ブレードが挿入されている特定のサーバ ブレード エンクロージャを識別します。

ブレードのシリアル番号

ブレードのシリアル番号は、サーバ ブレード製品のシリアル番号を識別します。

電源

サーバ ブレード エンクロージャは、次に示す2つの構成のうちいずれかを使用してラックにインストールできます。

- サーバ ブレードのパワー サプライは、通常使用している既存のAC電源を48VDCに変換してラックに電源を供給するために使用できます。この構成では、電源の設定で[Rack Provides Power]を選択します。この設定により、電源障害の危険を伴うことなく適切な電力消費を確保できるように、各ブレード サーバ、エンクロージャ、およびパワー サプライが電源要求を伝達することができます。
- 付属のパワー サプライを使用しないで、既存の48VDC電源を直接供給できる場合は、[Facility Provides 48V]を選択します。電源投入または切断時に、各サーバ ブレードが、電源についてインフラストラクチャと通信する必要はなくなります。

注：ラック内のすべてのサーバ ブレードおよび他のコンポーネントに十分な電力を供給するには、適切な電源サイジング要件の実現は必須条件です。

自動電源投入の有効化

各サーバ ブレードをエンクロージャに挿入すると、サーバ ブレードに自動的に電源が入るように設定できます。電源設定によって異なりますが、サーバ ブレードは、ラックと通信して電源を投入するための十分な電源があるかどうかを確認します。電源を使用できる場合は、サーバ ブレードに自動的に電源が投入され、サーバの通常の起動プロセスが開始されます。

iLO Advancedライセンス アクティベーション設定

次のパラメータは、iLOの高度な機能の使用許諾に関する情報を提供します。

iLO Advancedパック アクティベーション キー

[iLO Advanced Pack License Key]オプションは、グラフィック リモート コンソール、仮想メディア（フロッピーおよびCD-ROM）、ディレクトリ サポートなど、iLOの高度な機能を有効にするために使用します。このフィールドに25文字のキーを入力して、機能を有効にしてください。

内蔵Lights-Outのトラブルシューティング

この項の目次

最小要件	227
アラートおよびトラップの問題のトラブルシューティング	228
iLOのPOST LEDインジケータ	229
ハードウェアおよびソフトウェア リンクに関連する問題	231

最小要件

iLOの最小構成要件は、次のとおりです。

- Windows[®]クライアント
 - Windows[®] 2000
 - Microsoft[®] Internet Explorer 5.5 SP2、128ビット暗号化
 - Java 1.3.1 JVM以降
- Linuxクライアント
 - Red Hat 7.3
 - Netscape 7.xまたはMozilla 1.2.1、128ビット暗号化
 - Java 1.4.1 JVM以降

システム構成に合わせて推奨されるJVMをダウンロードするには、HPのWebサイト <http://www.hp.com/servers/manage/jvm/>（英語）を参照してください。

注：このサイトにアクセスすると、メイン サイトからjava.sun.comサイトに転送されます。JVMのバージョンについては、リモート コンソールのヘルプ ページで指定されているバージョンの使用をおすすめします。Internet Explorer用に指定されているバージョンは、java.sunサイトまたはマネジメントCDから入手できます。

アラートおよびトラップの問題のトラブルシューティング

アラート	説明
テストトラップ	このトラップは、ユーザがWebの設定ページを介して生成します。
サーバの電源障害	サーバに電源が入っていません。
サーバのリセット	サーバはリセットされました。
ログインの失敗	ユーザによるリモートログインが失敗しました。
一般エラー	ハードコード化されたMIBであらかじめ定義されていないエラー状態です。
ログ	循環式のログがオーバーラン状態になりました。
セキュリティ オーバーライド スイッチの変更：On/Off	セキュリティ オーバーライド スイッチの状態が変更されました（On/Off）。
ラック サーバの電源投入の失敗	BL p-Classラックがサーバに電源を投入するには十分な電源を供給できないことを報告したため、サーバに電源を投入できませんでした。
ラック サーバの電源投入の手動によるオーバーライド	BL p-Classラックが十分な電源を供給できないことを報告したのに、サーバに手動で強制的に電源が投入されました。
ラック名の変更	ProLiant BL p-Classラックの名前が変更されました。

iLOからInsightマネージャ7のアラート（SNMPトラップ）を受信できない

iLOの設定権限を持つユーザがiLOに接続して、SNMPトラップのパラメータを設定しなければなりません。iLOに接続したら、iLOのコンソール アプリケーションの[SNMP/Insight Manager Settings]画面で正しいアラートの種類とトラップの送付先が有効になっていることを確認してください。

iLOのセキュリティ オーバーライド スイッチ

iLOのセキュリティ オーバーライド スイッチにより、管理者は、サーバのシステムボードを物理的に制御して、緊急時にアクセスすることができます。iLOセキュリティ オーバーライド スイッチを設定することにより、ユーザIDやパスワードを使わずに、すべての権限を使用してログイン アクセスできます。

iLOセキュリティ オーバーライド スイッチは、サーバ内部にあるため、サーバエンクロージャ（筐体）を開かないとアクセスできません。iLOセキュリティ オーバーライド スイッチを設定するには、サーバの電源を切り、コンセントから電源コードを抜き取る必要があります。スイッチを設定し、その後でサーバの電源を入れてください。iLOセキュリティ オーバーライド スイッチをクリアするには、逆の手順を実行してください。

iLOのWebページに、iLOのセキュリティ オーバーライド スイッチを現在使用中であることを示す警告メッセージが表示されます。iLOのログに、iLOセキュリティ オーバーライド スイッチの使用を記録するエントリが追加されます。iLOセキュリティ オーバーライド スイッチを設定またはクリアしたとき、SNMPアラートを送信することもできます。

万一の場合、必要な処置として、iLOセキュリティ オーバーライド スイッチを設定して、iLOのブート ブロックをフラッシュすることもできます。ブート ブロックは、iLOがリセットされるまでエクスポートされます。リセットが完了するまで、ネットワークからiLOを切断することをおすすめします。

サーバにより、iLOセキュリティ オーバーライド スイッチは、1つのジャンパの場合やディップ スイッチ パネルの特定のスイッチ位置にある場合があります。iLOセキュリティ オーバーライド スイッチにアクセスする方法については、サーバのマニュアルを参照してください。

iLOのPOST LEDインジケータ

iLOの初期起動中には、iLOの起動プロセスの全過程で、POST LEDインジケータが点滅して進行を示します。起動プロセスが完了すると、ハートビート（HB）LEDが1秒に1回点滅します。正常な動作が行われている間、LED 7も、断続的に点滅します。

システムの起動後にLEDインジケータ（1～6）が点灯する場合は、ハードウェアの障害を示しています。ハードウェアの障害が検出された場合は、iLOをリセットしてください。LEDインジケータの位置については、サーバのマニュアルを参照してください。

iLOの稼働時の障害は、HBおよびLED 7が点灯したままになるか消灯したままになることにより示されます。また、8つのLEDすべてが点滅することによって、iLOの稼働時の障害が示される場合もあります。稼働時の障害が発生した場合は、iLOをリセットしてください。

LEDインジケータは、次のように割り当てられています。

HB	7	6	5	4	3	2	1
----	---	---	---	---	---	---	---

LEDインジケータ	POSTコード (処理の完了)	説明	障害の意味
なし	00	チップ セレクトの設定	
1または2	02- 通常動作	プラットフォームの判別	
2および1	03	RUNMAPビットの設定	
3	04	SDRAMコントローラの初期化	
3および2	06	Iキャッシュのアクティブ化	
3、2、および1	07	Dキャッシュ (のみ) の初期化	
4	08	セカンダリ ロードのRAMへのコピー	セカンダリ ロードをコピーできませんでした。
4および1	09	セカンダリ ロードの確認	セカンダリ ロードが実行されませんでした。
4および2	0a	セカンダリ ロードの開始	SDRAMメモリのテストに失敗しました。
4、2、および1	0b	ROMのRAMへのコピー	ブート ブロックをコピーできませんでした。
4および3	0c	RAM内のROMイメージの確認	ブート ブロックを実行できませんでした。
4、3、および1	0d	ブート ブロックMainの開始	ブート ブロックは、有効なイメージを検出できませんでした。
なし		Cラン タイム初期化の開始	
4、3、および2	0e	Main() による制御の受け取り	Mainセルフテストの失敗
可変	可変	各サブシステムのセルフテスト	
4、3、2、および1	0f	ThreadXの開始	RTOSの起動に失敗しました。
なし	00	Main_init() の完了	サブシステムの起動に失敗しました。
HBおよび7		iLOプロセッサがファームウェア コードを実行する際に点滅します。下側の6つのLEDの値は変更されません。	

iLOのマイクロプロセッサのファームウェアには、整合性チェックを行うコードが内蔵されています。整合性チェックのいずれかが失敗すると、マイクロプロセッサは、FEHを実行します。FEHは、iLOのPOST LEDインジケータを使用して情報を提供します。FEHコードは、99とそれ以外の部分から成るエラー コードの点滅パターンを繰り返すことで区別されます。

FEHコード	整合性チェック	説明
9902	TXAPICLK	RTOSの機能が不適切な値でコールされたかまたは不適切な呼び出し側からコールされました。
9903	TXCONTEXT	1つ以上のスレッドの保存されているコンテキストが壊れました。
9905	TRAP	スタック プローブが失敗したか、返されたアドレスが無効か、不正なトラップ命令が検出されました。
9966	NMIWR	容量の少ないメモリに予期しない書き込みが発生しました。
99C1	CHKNUL	リセット ベクタが変更されました。

ハードウェアおよびソフトウェア リンクに関連する問題

以下の各項では、ハードウェアまたはソフトウェア リンクに関連する問題を解決する場合に、注意すべき事項について説明します。

ハードウェア

iLOは、標準Ethernetケーブル（RJ-45コネクタの付いたCAT5 UTPケーブルなど）を使用します。標準的なEthernet/ハブへのハードウェア リンクを確立するには、ストレートケーブルが必要です。クロスオーバー ケーブルは、直接PCに接続する場合に使用してください。

ソフトウェア

iLOマネジメント ポートは、DHCPサーバに接続されたネットワークに接続する必要があります。また、iLOをネットワークに接続してから電源を入れなければなりません。DHCPは、電源が投入されるとただちに要求を送信します。iLOが最初に起動したときにDHCPの要求に対する回答がない場合、DHCPは、90秒間隔で要求を再発行します。

DHCPサーバは、DNSおよびWINS名前解決を提供するように設定しなければなりません。iLOは、**F8**キーによるオプションROMセットアップまたは[Network Settings]Webページから、静的IPアドレスで動作するように設定できます。

ネットワーク設定タグには、デフォルトのDNS名が記載されているため、割り当てられたIPアドレスを知らなくても、このDNS名を使用してiLOの位置を確認できます。

PCへの直接接続を使用する場合、リンク上にDHCPサーバがないので、静的IPアドレスを使用しなければなりません。

iLOのRBSUでは、高度なオプションに関するDNS/DHCPページで**F1**キーを押してiLOのDHCP要求のステータスを確認することができます。

ログイン時の問題

ログイン時の問題を解決するには、以下の情報を参照してください。

- デフォルトのログインはネットワークの設定タグに記載されています。
- ユーザがパスワードを忘れた場合、管理者ユーザ アカウント権限のある管理者は、そのユーザのパスワードを再設定できます。
- 管理者がパスワードを忘れた場合、管理者は、セキュリティ オーバーライド スイッチを使用しなければなりません。
- 次のような一般的な問題を確認してください。
 - パスワードは、パスワードの制限に従っていますか。たとえば、パスワード内に大文字と小文字の区別の必要な文字はありますか。
 - サポートされていないブラウザを使用していないですか。

ログイン名とパスワードが受け付けられない

iLOに接続したがログイン名とパスワードが受け付けられない場合、ログイン情報が正しく設定されていることを確認する必要があります。管理者ユーザ アカウント権限のあるユーザに、ログインしてパスワードを変更してもらってください。それでも接続できない場合は、そのユーザに再度ログインしてもらい、ユーザ アカウントを削除した上で追加しなおしてもらってください。

注：RBSUを使って、ログイン時の問題を修正することもできます。

ログイン ページにアクセスできない

ログイン ページにアクセスできない場合は、ブラウザとiLOのSSL暗号化レベルを確認する必要があります。ブラウザとiLOの暗号化レベルは、一致していなければなりません。

128ビットの高度暗号化パックの使用をおすすめします。

Telnetを使用してiLOにアクセスできない

Telnetを使用してiLOにアクセスできない場合は、**[Global Settings]**画面の**[Remote Console Port Configuration]**および**[Remote Console Data Encryption]**の設定を確認する必要があります。**[Remote Console Port Configuration]**の設定が**Automatic**になっている場合、リモート コンソール アプレットはポート23を有効にしてセッションを開始し、セッションが完了するとポート23を閉じます。Telnetは、自動的にポート23を有効にすることはできないので、Telnetセッションは失敗します。Telnetの設定について詳しくは、82ページの「Telnetサポート」を参照してください。

プロキシ サーバの問題

Webブラウザ ソフトウェアをプロキシ サーバを使用するように設定している場合、iLOのIPアドレスに接続できません。この問題を解決するには、ブラウザを設定して、iLOのIPアドレスについてはプロキシ サーバを使用しないようにしてください。たとえば、Internet Explorerでは、**[ツール]**、**[インターネット オプション]**、**[接続]**、**[LANの設定]**、**[詳細]**の順に選択し、**[例外]**フィールドにiLOのIPアドレスまたはDNS名を入力してください。

ファイアウォールの問題

iLOは、設定可能な複数のTCP/IPポートを介して通信を行います。これらのポートが使用できない場合、管理者は、ファイアウォールを設定して、これらのポート上の通信を許可しなければなりません。ポートの設定を表示または変更するには、[Administration] タブの[Global Settings]オプションを参照してください。

仮想メディアまたはグラフィック リモート コンソールにアクセスできない

仮想メディアとグラフィック リモート コンソールは、オプションのiLO Advancedパックの使用許諾を受けることによってのみ、有効になります。ライセンスがない場合は、この機能を使用できないことを示すメッセージが表示されます。iLOには、最大10のユーザが同時にログインできますが、リモート コンソールにアクセスできるのは1ユーザのみです。リモート コンソールがすでに使用中であることを示す警告メッセージが表示されます。

内蔵Lights-Outのリセット

まれに、iLOをリセットしなければならない場合があります。たとえば、iLOがブラウザに応答しない場合などです。iLOをリセットするには、サーバの電源を切り、電源を完全に切断しなければなりません。

特定の状況で、iLO自体がリセットされる場合があります。たとえば、ファームウェアがiLOの問題を検出するとiLOの内部ウォッチドッグ タイマがリセットされます。ファームウェアのアップグレードが完了した場合やネットワーク設定が変更された場合も、iLOはリセットされます。

HPマネジメント エージェント5.40以降には、iLOをリセットする機能があります。iLOをリセットするには、HPマネジメント エージェントのWebページのiLOセクションの下に[Reset iLO]オプションを使用します。

[Network Settings]ページの[Apply]をクリックすることにより、iLOマネジメント プロセッサを手動で強制的にリセットすることもできます。[Apply]をクリックする前に、パラメータを変更する必要はありません。

ビデオおよびモニタの問題のトラブルシューティング

以下の各項では、ビデオおよびモニタに関連する問題を解決する場合に、注意すべき事項について説明します。

一般的なガイドライン

- クライアントの画面解像度は、リモート サーバの画面解像度より高くする必要があります。
- iLOのリモート コンソールは、システムに内蔵されたATI Rage XLビデオ チップだけをサポートします。プラグインのビデオ カードをインストールしている場合、iLOのリモート コンソール機能は動作しません。iLOの他の機能はすべて、プラグインのビデオ カードを使用する場合でも使用できます。
- リモート コンソールにアクセスできるのは一度に1ユーザのみです。別のユーザがiLOにログインしているかどうか確認してください。

リモート コンソールのシングル カーソルをリモート コンソール ウィンドウの隅に移動できない

リモート コンソール ウィンドウの隅にマウス カーソルを移動できないケースがあります。その場合、マウス カーソルを右クリックしてリモート コンソール ウィンドウの外側にドラッグしてから、内側に戻してください。

それでもマウスが正常に動作しない場合やこの状態が頻繁に発生する場合は、マウスの設定が16ページの「グラフィック リモート コンソールのパフォーマンスの最適化」の項で推奨されている設定と一致していることを確認してください。

リモート コンソールのテキスト ウィンドウが正しく更新されない

リモート コンソールで表示したテキスト ウィンドウ内を高速でスクロールする場合、テキスト ウィンドウが正しく更新されないことがあります。この問題は、iLOのファームウェアの検出/表示速度よりもビデオの更新速度のほうが速いために発生します。通常、テキスト ウィンドウの左上隅だけが更新され、残りの部分の表示は更新されません。スクロールが完了した後、[Refresh]をクリックしてテキスト ウィンドウを正しく更新してください。

この問題の既知の例として、Linuxの起動およびPOST実行時に発生する問題があります。この問題が発生すると、一部のPOSTメッセージが表示されないことがあります。そのため、起動プロセスによってキーボードによる応答が要求され、すぐに表示されなくなることがあります。この問題を防止するには、Linuxの起動スクリプトを書き換えて、起動およびPOSTの進行速度を遅くして、キーボードで応答するための時間を確保する必要があります。

DOSでTelnetが正しく表示されない

iLOのTelnetセッションを使用して最大化されたDOSウィンドウを含むテキスト画面を表示するとき、サーバの画面が80×25より大きい場合、Telnetセッションが、画面の上部を除いて何も表示できないことがあります。

この問題を解決するには、DOS®ウィンドウのプロパティを調整して、そのサイズを80×25に限定してから、DOSウィンドウを最大化してください。

- DOS®ウィンドウのタイトル バーで、マウスを右クリックして、**[プロパティ]**、**[レイアウト]**の順に選択します。
- **[レイアウト]**タブで、**[画面バッファのサイズ]**の高さを25に変更します。

リモート コンソールにビデオ アプリケーションが表示されない

Microsoft® Media Playerなどの一部のビデオ アプリケーションは、リモート コンソールに表示されないかまたは正しく表示されません。この問題は、ビデオ オーバーレイ用のレジスタを使用するアプリケーションで最も多く発生します。通常、ビデオをストリーミングするアプリケーションは、ビデオ オーバーレイ用のレジスタを使用しません。iLOは、この種類のアプリケーションでの使用には適していません。

その他の問題のトラブルシューティング

以下の各項では、ハードウェアやソフトウェアに関するその他の問題のトラブルシューティングについて説明します。

リモート コンソールのマウスの制御の問題

Microsoft® Windows® Server 2003を実行するサーバでリモート コンソールを使用する際、マウスの動きが非常に緩慢になり、画面の四隅に移動することが困難になることがあります。画面の反対側の隅に移動しようとする、カーソルが完全に表示されなくなる場合があります。

注：マウスのこのような動作が明確に見られるのは、リモート コンソールセッションがサーバの画面よりも小さいサイズのブラウザ アプレットのウィンドウで実行されているとき、および画面内の表示されていない内容をすべて見るためにスクロールしなければならないときです。

この問題を解決するには、次のように設定を変更してください。

1. Windows® Server 2003デスクトップ アプレットから、[スタート]、[コントロールパネル]、[マウスのプロパティ]の順にクリックします。
2. [ポインタの精度を高める]パラメータを無効にします。

ヘッドレス サーバ環境でのPS/2キーボードのエミュレーション

iLOは、ヘッドレス サーバ環境でPS/2キーボードをエミュレートします。サーバがPOST実行中であることを検出すると、iLOは、PS/2キーボードをスキャンします。ローカルのPS/2キーボードが検出されない場合、iLOがサーバのPS/2キーボードの機能を実行します。

PS/2キーボードのスキャンがサーバのPOST実行時にのみ行われるため、iLOはPS/2キーボードのホットプラグ対応機能は実装しません。サーバのPOST終了後にPS/2キーボードを接続しても、キーボードは検出されないため機能することはありません。サーバのPOST完了後、オペレーティング システムがロードされるまでの間に、PS/2キーボードが抜き取られると、オペレーティング システムは、リモート コンソールからのキーストロークを受信できなくなります。この場合、サーバを再起動してiLOがPS/2キーボードを再スキャンするにしなければなりません。

iLOおよびサーバのリセット後、iLOのRBSUを使用できない

iLOプロセッサがリセットされた直後にサーバがリセットされた場合、サーバが初期化を実行しiLOのRBSUを起動しようとする際に、iLOファームウェアが完全には初期化されないことがまれにあります。この場合、iLOのRBSUを使用できなくなるかまたはiLOのオプションROMのコードが完全にスキップされます。この問題が発生した場合は、サーバをもう一度リセットしてください。この問題の発生を防止するには、iLOプロセッサをリセットした後、数秒待ってからサーバをリセットしてください。

NICを用いてiLOプロセッサに接続できない

NICを用いてiLOプロセッサに接続できない場合は、以下のトラブルシューティング方法のいずれかまたはすべてを試してください。

- iLOのRJ-45コネクタの緑のLEDインジケータ（リンク ステータス）が点灯していることを確認します。点灯している場合、PCI NICとネットワーク ハブ間の接続は問題ありません。
- 緑のLEDインジケータが断続的に点滅することを確認します。断続的に点滅する場合、ネットワーク トラフィックは正常です。
- iLOのRBSUを実行して、NICが有効であることを確認し、割り当てられたIPアドレスとサブネット マスクを確認します。

- iLOのRBSUを実行して、DHCP要求のステータスを確認するためにDNS/DHCPページ内の[F1 - Advanced]タブを使用します。
- ネットワーク上の別のワークステーションから、そのNICのIPアドレスをpingします。
- ブラウザ ソフトウェアで、NICのIPアドレスをURLとしてタイプして、NICとの接続を試みます。このアドレスで、iLOのホームページを表示できます。
- iLOをリセットします。

注：ネットワーク接続が確立した場合、DHCPサーバ要求を最大90秒待つ必要がある場合があります。

ProLiant BL p-Classサーバでは、診断ポートを使用できます。診断ポートに有効なネットワーク ケーブルを接続すると、iLOは自動的にiLOポートから診断ポートへの切り替えを行います。診断ポートとバック ポートの間の切り替えが行われる際、ネットワークの切り替えが完了するまで1分の余裕をみておく必要があります。その後、Webブラウザを介して接続してください。

iLOの診断ポートに接続できない

NICを介してiLOの診断ポートにアクセスできない場合、次の点に注してください。

- 有効なネットワーク ケーブルが診断ポートに接続されると、診断ポートが使用されることが自動的に検知されます。診断ポートとバック ポートの間の切り替えが行われる際、ネットワークの切り替えが完了するまで1分の余裕をみておく必要があります。その後、Webブラウザを介して接続してください。
 - 重大な動作が進行中の場合、その動作が完了するまで診断ポートは使用できません。重大な動作には、次の動作があります。
 - ファームウェアのアップグレード
 - リモート コンソール セッション
 - SSLの初期化
 - 複数の有効なNIC（無線カード、ネットワーク カードなど）を搭載するクライアント ワークステーションの使用で、配線の問題により、診断ポートにアクセスできないことがあります。この問題を解決するには、以下の手順に従ってください。
1. クライアント ワークステーションに搭載するアクティブなNICを1枚だけにします。たとえば、無線ネットワーク カードを無効にします。

2. クライアント ワークステーション ネットワークのIPアドレス（ネットワーク アドレス）を、iLOの診断ポート ネットワークと一致するように設定します。
 - a. 設定するIPアドレスは、192.168.1.Xにする必要があります。診断ポートのIP アドレスが192.168.1.1に設定されているため、Xは、1以外の任意の番号に設定してください。
 - b. サブネット マスクは、255.255.255.0に設定する必要があります。

Insightマネージャ7からSNMP情報を取得できない

管理対象サーバで動作するエージェントは、Insightマネージャ7にSNMP情報を提供します。エージェントが、iLOを介して情報を転送するには、iLO用のデバイス ドライバがインストールされている必要があります。インストール方法については、「iLOデバイス ドライバのインストール」の項を参照してください。

iLO用のドライバとエージェントをすでにインストールしている場合、iLOと管理PCが同じサブネット上にあることを確認してください。これは、管理用PCからiLOをpingすることで、すぐに確認できます。iLOのネットワーク インタフェースにアクセスする正しい経路については、ネットワーク管理者に確認してください。

ネットワーク設定の変更後iLOに接続できなくなった

接続の両端（NICおよびスイッチ）で、トランシーバ速度の自動選択、速度、およびデュプレックスについて同じ設定が行われていることを確認してください。たとえば、一方の側で接続が自動選択されるように設定されている場合、もう一方の側も同様に設定してください。iLO NICの設定は、[Network Settings]画面で制御します。

イベント ログ エントリの日付や時刻が正しくない

RBSUを実行してiLOの日付と時刻を更新できます。このユーティリティは、サーバの時刻と日付を使用して、自動的にプロセッサの日付と時刻を設定します。サポートされるネットワーク オペレーティング システム用のInsightマネージメント エージェントによって日付と時刻を更新することもできます。

iLOのファームウェアをアップグレードできない

iLOのファームウェアをアップグレードしようとしたが、iLOが応答しないかファームウェアのアップグレードを受け入れない場合、またはアップグレードが正常に完了する前に終了する場合は、次のオプションを使用できます。

- iLOのネットワーク フラッシュ リカバリ
- ROMPaq

iLOのネットワーク フラッシュ リカバリ

iLOのネットワーク フラッシュ リカバリ ペイロードにより、ファームウェア アップグレードの失敗から復旧できます。フラッシュ リカバリ ペイロードは、フラッシュ リカバリ ペイロードがアクティブな場合だけ使用できるFTPを使用して、ファームウェア イメージをiLOに転送します。フラッシュ リカバリ ペイロードは、次の場合にのみ使用してください。

- ファームウェア アップグレードを試みて失敗した場合
- Webブラウザに接続できない場合
- 他に使用できるファームウェア アップグレード オプションがない場合。ディスク ケット ドライブのあるサーバは、ROMPaqオプションを使用できます。ProLiant BL p-Classサーバは、フラッシュ リカバリ ペイロードを使用しなければなりません。

iLOのファームウェア イメージが損傷している場合や、ファームウェア イメージがない場合、または他の何らかの形で壊れている場合、iLOをフラッシュしなおすには、iLOフラッシュ リカバリ プロセスを使用してください。フラッシュ リカバリ プロセスは、システムを再フラッシュするためにだけ使用してください。リカバリ プロセスが完了するまで、他のプロセスを実行することはできません。

診断手順

ファームウェアのフラッシュ リカバリを試みる前に、次の診断手順を用いてフラッシュ リカバリが必要かどうかを確認してください。

1. iLOにWebブラウザ経由で接続を試みます。接続できない場合は、通信に問題があることがわかります。
2. iLOにpingを通してみます。pingが通る場合は、ネットワークが機能していることがわかります。
3. iLOのIPアドレスまたはDNS名に対して、FTPセッションを開いてみます。セッションを開くことができる場合は、フラッシュ リカバリ ペイロードがアクティブで、フラッシュ リカバリ プロセスを使用してファームウェアをアップグレードする必要があることがわかります。
4. FTPセッションを開くことができない場合は、システムはリカバリ モードになっていません。iLOのリセット (234ページの「内蔵Lights-Outのリセット」) の項の手順で、iLOをリセットしてみてください。

フラッシュ リカバリ プロセス

診断手順の結果、フラッシュ リカバリ プロセスが必要と確認された場合、以下の手順に従ってください。

1. iLOのIPアドレスまたはDNS名に対して、FTPセッションを開きます。
2. 固定ユーザ名flashとパスワードrecoveryを使用してiLOにログインします。ユーザ名とパスワードでは、大文字と小文字が区別されます。
3. FTPプロンプトで、putコマンドとファームウェア イメージのファイル名を入力します。

フラッシュ リカバリ プロセスで使用するエントリの例を次に示します。

```
ftp 192.168.177.142
login: flash
password: recovery
put ¥iLO140.bin
```

- ファイルが検出された場合、putコマンドによりファイルがiLOに転送され、イメージが検証され、フラッシュ プロセスが開始されます。
- ファイルが検出されない場合、putコマンドの一部のバージョンはエラー メッセージを報告しません。
- ディレクトリ パスにスペースが含まれる場合は、パスおよびファイル名を引用符で囲ってください。

ファームウェア イメージが転送された後、リカバリ ペイロードは、チェックサムを計算し、電子署名を検証し、イメージが有効だったかどうかを報告します。イメージが有効で、フラッシュ プロセスがクライアントに報告されると、フラッシュの書き換えを開始します。

注：リカバリ ペイロードが保存されているハッシュを解読し、イメージのハッシュを計算して比較するプロセスは、数秒かかります。イメージが有効な場合、FTPサーバは、イメージの書き換えを開始しフラッシュ部分を書き換え、ステータスを更新します。

フラッシュ リカバリ プロセスが完了すると、フラッシュ リカバリ ペイロード モジュールの接続が切断され、iLOプロセッサが再起動されます。フラッシュ リカバリ プロセスが失敗した場合、プロセスを再度繰り返し、進行状況を参照してエラーが発生していないかどうかを確認します。プロセスを実行するために、別のファームウェア イメージを使用しなければならない場合があります。

ROMPaq

ROMPaqを使用してiLOのファームウェアをアップグレードするには、2つの手順があります。最初の手順は任意のコンピュータで実行できますが、2番目の手順はiLOのホスト サーバで実行しなければなりません。

1. 任意のコンピュータで以下の手順を実行します。
 - a. 最新のiLOファームウェアのSoftPaqをダウンロードします。ディスクett用のSoftPaqイメージを選択して、ハードディスク ドライブに保存します。このSoftPaqは、HPのWebサイト<http://www.hp.com/servers/lights-out/>（英語）でダウンロードできます。
 - b. SoftPaqを実行して、ディスクettを作成します。
2. 以下の手順は、iLOのホスト サーバだけで実行してください。
 - a. ROMPaqディスクettからシステムを起動します。
 - b. A:¥プロンプトで、次のように入力します。
rompaq
 - c. ROMPaqの初期画面で、**Enter**キーを押します。画面に、コンピュータ上のアップグレード可能なデバイスが表示されます。
 - d. カーソルを使用して、**[iLO Management]**を選択して**Enter**キーを押します。画面に、ROMPaqでインストールできるファームウェア イメージが表示されます。
 - e. カーソルを使用して該当するイメージを強調表示し、**Enter**キーを押します。
 - f. **Enter**キーをもう一度押します。ROMPaqは、ファームウェア イメージを読み取ります。ファイルが複数のディスクettにコピーされているため、別のディスクettの挿入を指示するメッセージが表示されます。このメッセージが表示されたら、該当するディスクettを挿入して**Enter**キーを押します。
 - g. **Enter**キーをもう一度押して、ROMの更新を開始します。このプロセスの進行中は、システムの電源を切って入れなおしたり、再起動したり、電源を切ったりしないでください。
 - h. ROMの更新が正常に完了したというメッセージが表示されたら、**Enter**キーを押します。
 - i. **Enter**キーを押して別のデバイスを更新するかまたは**Esc**キーを押してA:¥プロンプトに戻ります。

注：ROMPaqによるアップグレードを実行するには、セキュリティ オーバーライド スイッチを設定しなければならない場合があります。ROMPaqプログラムは、セキュリティ オーバーライド スイッチを設定する必要があるかどうかをユーザに通知します。

名前を使用してiLOマネジメント ポートにアクセスできない

iLOマネジメント ポートは、WINSサーバまたはDynamic DNS (DDNS) サーバを使用して、iLOマネジメント ポートに名前でアクセスするために必要な名前-IPアドレス解決を提供することができます。iLOマネジメント ポートの電源を入れる前に、WINSサーバまたはDDNSサーバが稼動していなければなりません。また、iLOマネジメント ポートは、WINSサーバまたはDDNSサーバへの有効な経路を持つ必要があります。

さらに、iLOマネジメント ポートを、WINSサーバまたはDDNSサーバのIPアドレスを使用して設定しなければなりません。DHCPを使用して、必要なIPアドレスでDHCPサーバを設定してください。また、RBSUまたは[Administration]タブの[Network Settings]オプションを使用して、IPアドレスを入力することもできます。

iLOマネジメント ポートは、WINSサーバまたはDDNSサーバに登録するように設定しなければなりません。これらのオプションは、工場出荷時のデフォルト設定で、オンになっており、RBSUまたは[Administration]タブの[Network Settings]オプションを使用して変更できます。

iLOマネジメント ポートにアクセスするために使用するクライアントは、iLOマネジメント ポートに登録されたWINSサーバ、またはiLOマネジメント ポートのIPアドレスが登録されたDDNSサーバを使用するように設定しなければなりません。

WINSサーバと動的でないDNSサーバを使用する場合は、DNSサーバが名前解決用にWINSサーバを使用するように設定すると、iLOマネジメント ポートへのアクセスを大幅に高速化させることができます。詳しくは、該当するMicrosoft®社のマニュアルを参照してください。

イベント ログのエントリ

イベント ログの表示	イベント ログの説明
Server power failed	サーバの電源障害が発生したときに表示されます。
Browser login: IP address	ログインしたブラウザのIPアドレスを表示します。
Server power restored	サーバの電源が復旧したときに表示されます。
Browser logout: IP address	ログアウトしたブラウザのIPアドレスを表示します。
Server reset	サーバがリセットされたときに表示されます。
Failed Browser login - IP Address: IP address	ブラウザ ログインが失敗したときに表示されます。
iLO Self Test Error: #	iLOが内部テストに失敗したときに表示されます。考えられる原因は、重要なコンポーネントの故障です。このサーバでiLOを継続して使用することはお勧めできません。
iLO reset	iLOがリセットされたときに表示されます。
On-board clock set; was #:#:#:#:#	オンボード クロックが設定されたときに表示されます。
Server logged critical error(s)	サーバが重大なエラーを記録したときに表示されます。
Event log cleared by: User	ユーザがイベント ログをクリアしたときに表示されます。
iLO reset to factory defaults	iLOがデフォルト設定にリセットされたときに表示されます。
iLO ROM upgrade to #	ROMがアップグレードされたときに表示されます。
iLO reset for ROM upgrade	iLOがROMのアップグレードのためにリセットされたときに表示されます。
iLO reset by user diagnostics	iLOがユーザDiagnosticsによりリセットされたときに表示されます。
Power restored to iLO	iLOの電源が復旧したときに表示されます。
iLO reset by watchdog	iLOでエラーが発生し、iLO自体がリセットされたときに表示されます。この問題が続く場合は、HPのサービス窓口に連絡してください。
iLO reset by host	iLOがサーバによってリセットされたときに表示されます。
Recoverable iLO error, code #	iLOで重要でないエラーが発生し、iLO自体がリセットされたときに表示されます。この問題が続く場合は、HPのサービス窓口に連絡してください。
SNMP trap delivery failure: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。

イベント ログの表示	イベント ログの説明
Test SNMP trap alert failed for: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。
Power outage SNMP trap alert failed for: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。
Server reset SNMP trap alert failed for: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。
Illegal login SNMP trap alert failed for: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。
Diagnostic error SNMP trap alert failed for: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。
Host generated SNMP trap alert failed for: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。
Network resource shortage SNMP trap alert failed for: IP address	SNMPトラップが指定されたIPアドレスに送信されないときに表示されます。
iLO network link up	iLOへのネットワーク リンクが確立されたときに表示されます。
iLO network link down	iLOへのネットワーク リンクが切断されたときに表示されます。
iLO Firmware upgrade started by: User	ユーザがファームウェアのアップグレードを開始したときに表示されます。
Host server reset by: User	ユーザがホスト サーバをリセットしたときに表示されます。
Host server powered OFF by: User	ユーザがホスト サーバの電源を切ったときに表示されます。
Host server powered ON by: User	ユーザがホスト サーバの電源を入れたときに表示されます。
Virtual Floppy in use by: User	ユーザが仮想フロッピーの使用を開始したときに表示されます。
Remote Console login: User	ユーザがリモート コンソール セッションにログオンしたときに表示されます。
Remote Console Closed	リモート コンソール セッションがクローズされたときに表示されます。
Failed Console login - IP Address: IP address	コンソール ログインの失敗とそのIPアドレスを表示します。
Added User: User	ローカル ユーザが追加されたときに表示されます。
User Deleted by: User	ローカル ユーザが削除されたときに表示されます。
Modified User: User	ローカル ユーザが変更されたときに表示されます。

イベント ログの表示	イベント ログの説明
Browser login: User	インターネット ブラウザを使用してiLOに有効なユーザ ログインが行われたときに表示されます。
Browser logout: User	インターネット ブラウザを使用してiLOから有効なユーザ ログアウトが行われたときに表示されます。
Failed Browser login - IP Address: IP address	ブラウザ ログイン試行が失敗したときに表示されます。
Remote Console login: User	リモート コンソールのポートを使用して許可されたユーザがログインしたときに表示されます。
Remote Console Closed	許可されたリモート コンソール ユーザがログアウトしたとき、または失敗したログイン試行に続いてリモート コンソールのポートがクローズされたときに表示されます。
Failed Console login - IP Address: IP address	許可されないユーザが、リモート コンソールのポートを使用してログイン試行に3回失敗したときに表示されます。
Added User: User	許可されたユーザのリストに新しいエントリが作成されたときに表示されます。
User Deleted by: User	許可されたユーザのリストからエントリが削除されたときに表示されます。Userセクションには、削除を要求されているユーザが表示されます。
Event Log Cleared: User	Userがイベント ログをクリアしたときに表示されます。
Power Cycle (Reset): User	電源がリセットされたときに表示されます。
Virtual Power Event: User	仮想電源ボタンが使用されたときに表示されます。
Security Override Switch Setting is On	セキュリティ オーバーライド スイッチをオンに設定してシステムを起動したときに表示されます。
Security Override Switch Setting Changed to Off	セキュリティ オーバーライド スイッチをオンからオフに変更してシステムを起動したときに表示されます。
On-board clock set; was previously [NOT SET]"	オンボード クロックが設定されたときに表示されます。以前の時刻を表示します。以前に時刻が設定されていなかった場合は"NOT SET"と表示されます。
Logs full SNMP trap alert failed for: IP address	ログに空きがないとき、指定されたIPアドレスへのSNMPトラップ アラートが失敗した場合に表示されます。
Security disabled SNMP trap alert failed for: IP address	セキュリティが無効にされたとき、指定されたIPアドレスへのSNMPトラップ アラートが失敗した場合に表示されます。

イベント ログの表示	イベント ログの説明
Security enabled SNMP trap alert failed for: IP address	セキュリティが有効にされたとき、指定されたIPアドレスへのSNMPトラップ アラートが失敗した場合に表示されます。
Virtual Floppy connected by User	許可されたユーザが仮想フロッピーに接続したときに表示されます。
Virtual Floppy disconnected by User	許可されたユーザが仮想フロッピーを切断したときに表示されます。
License added by: User	許可されたユーザがライセンスを追加したときに表示されます。
License removed by: User	許可されたユーザがライセンスを削除したときに表示されます。
License activation error by: User	ライセンスを有効にする際にエラーが発生したときに表示されます。
iLO RBSU user login: User	許可されたユーザがiLO RBSUにログインしたときに表示されます。
Power on request received by: Type	次のいずれかのタイプの電源要求が受信されました。 電源ボタン Wake On LAN 自動電源投入
Virtual NMI selected by: User	許可されたユーザが仮想NMIボタンを選択したときに表示されます。
Virtual Serial Port session started by: User	仮想シリアル ポート セッションが開始されたときに表示されます。
Virtual Serial Port session stopped by: User	仮想シリアル ポート セッションが終了したときに表示されます。
Virtual Serial Port session login failure from: User	仮想シリアル ポート セッションに対するログインが失敗したときに表示されます。

頭字語と略語

ACPI

Advanced Configuration and Power Interface

ARP

Address Resolution Protocol

ASCII

American Standard Code for Information Interchange

CA

certificate authority。認証機関

CR

Certificate Request。証明書要求

DHCP

Dynamic Host Configuration Protocol

DNS

Domain Name System

EMS

Emergency Management Services

FEH

fatal exception handler

FSMO

Flexible Single-Master Operation

HB

heartbeat

ICMP

Internet Control Message Protocol

iLO

Integrated Lights-Out。内蔵Lights-Out

IML

Integrated Management Log。インテグレートッド マネジメント ログ

IP

Internet Protocol

LDAP

Lightweight Directory Access Protocol

LED

light-emitting diode。発光ダイオード

LOM

Lights-Out Management。Lights-Outマネジメント

MMC

Microsoft® Management Console。Microsoft®マネジメント コンソール

NIC

network interface controller。ネットワーク インタフェース コントローラ

NVRAM

non-volatile memory。不揮発性メモリ

POST

Power-On Self-Test。電源投入時セルフテスト

PSP

ProLiant Support Pack

RAS

remote access service

RBSU

ROM-Based Setup Utility。ROMベース セットアップ ユーティリティ

RIBCL

Remote Insight Board Command Language。リモートInsightボード コマンド言語

RILOE

Remote Insight Lights-Out Edition。リモートInsightボードLights-Out Edition

RILOE II

Remote Insight Lights-Out Edition II。リモートInsightボードLights-Out Edition II

SNMP

Simple Network Management Protocol。簡易ネットワーク管理プロトコル

SSL

Secure Sockets Layer

UID

unit identification

USB

universal serial bus

VM

Virtual Machine

VPN

virtual private networking

XML

extensible markup language

索引

A

Active Directory
 インストールの前提条件 105
 ディレクトリ サービス 105
 オブジェクト 113
Active Directory Lights-Out
 Management 121
ADD_USER 157、165
[Administration] 62、64

C

CLEAR_EVENTLOG 192
CPQLODOS 150、152
 コマンド ライン引数 150

D

DELETE_USER 168

E

eDirectory
 インストールの前提条件 122
 ディレクトリ サービス 122
 オブジェクト 128

G

GET_ALL_USERS 173
GET_DIR_CONFIG 185
GET_FW_VERSION 194
GET_GLOBAL_SETTINGS 188
GET_HOST_POWER_STATUS 202
GET_NETWORK_SETTINGS 177
GET_TOPOLOGY 200
GET_UID_STATUS 205

GET_USER 169

H

HOTKEY_CONFIG 195

I

iLO
 Insightマネージャ7との
 統合 89
 イベント ログ 42
 最小要件 227
 設定オプション 13
 動作の概要 30
iLO Advanced/バック
 機能 15、18、50
[iLO Status] 40
iLO仮想メディア デバイス
 使用 54
iLOデバイス ドライバ
 インストール 19、20、21
Insightマネージャ7 85
 アラート 87
 設定
 iLO、識別 88
 ポート 87

L

LDAP 122
LEDインジケータ 229
LICENSE 197
Lights-Out DOSユーティ
 リティ 149
Lights-Out Management 134
LOGIN 163

M

MOD_BLADE_RACK 199
MOD_DIR_CONFIG 155、186

MOD_GLOBAL_SETTINGS 189
MOD_NETWORK_SETTINGS 152
MOD_SNMP_IM_SETTINGS 190

N

Novell NetWareサーバドライバ
サポート 21

P

ProLiant BL p-Class 76

R

RACK_INFO 198
RBSU 14
[Remote Console (dual cursor)] 49
[Remote Console Information] 46
RESET_RIB 177
RESET_SERVER 204
RIBCL 159、160
一般的なガイドライン 160
RIB_INFO 176

S

[Server and iLO Diagnostics] 43
SERVER_INFO 201
[Server Status] 41
SET_HOST_POWER 203
SNMP/Insightマネージャ
設定 71
SNMPアラート設定 15
[Status Summary] 40
[System Status] 40

T

Telnet 82

U

UID_CONTROL 205

UPDATE_RIB_FIRMWARE 193
USER_INFO 164

W

Windows NT、Windows 2000、およ
びWindows Server 2003ドライバ
のサポート 20

X

XMLヘッダ 161

あ

アクセス
iLO 35
ヘルプ情報 40
アラート
Insightマネージャ7 87

い

インストール
ディレクトリ サービス 99
インテグレートド マネジメント
ログ (IML) 43

え

エラー メッセージ
MOD_DIR_CONFIG 187

か

カーソル モード 27
シングル カーソル 27
概要
リモートInsightボード コマン
ド言語 160
仮想CDドライブ 52
仮想インジケータ 61
仮想シリアルポート 60

仮想デバイス 50、52、54、60
仮想電源ボタン 50
仮想フロッピー 52
仮想メディア 52、54、57、58、59

き

機能

概要 85
ディレクトリ サービス 99
共通利用モデル 28

く

クエリ定義 143
グラフィック リモート コンソール
のパフォーマンスの最適化 16
グループ管理 141、142
グローバル設定 67

こ

コマンド

ADD_USER 165
CLEAR_EVENTLOG 192
DELETE_USER 168
GET_ALL_USER_INFO 175
GET_ALL_USERS 173
GET_DIR_CONFIG 185
GET_FW_VERSION 194
GET_GLOBAL_SETTINGS
188
GET_HOST_POWER_STATUS
202
GET_NETWORK_SETTINGS
177
GET_TOPOLOGY 200
GET_UID_STATUS 205
GET_USER 169
HOTKEY_CONFIG 195
LICENSE 197
LOGIN 163
MOD_BLADE_RACK 199
MOD_DIAGPORT_SETTINGS
183

MOD_DIR_CONFIG 186
MOD_GLOBAL_SETTINGS
189
MOD_NETWORK_SETTINGS
179
MOD_SNMP_IM_SETTINGS
190
MOD_USER 171
RACK_INFO 198
RESET_RIB 177
RESET_SERVER 204
RIB_INFO 176
SERVER_INFO 201
SET_HOST_POWER 203
UID_CONTROL 205
USER_INFO 164

さ

サーバ

識別パラメータ 211

サポートされるソフト

ウェア 25、26

す

スキーマ インストーラ 101
スキーマに関する資料 99
スクリプト 160

せ

接続

概要 29
企業ネットワーク 29
内蔵Lights-Outネット
ワーク 30

設定

iLO 13
iLO、識別 88
LinuxおよびSuSE Linux
Server 18
NetWare 18

Windows NT® 4.0および
Windows® 2000 17
Windows Server 2003 17
サーバ 17
ラック 76

そ

ソフトウェア
サポート 100
必要 101
問題を解決 231

て

定義
クエリ 143
ディレクトリ サービス 99、101、
122
Active Directory 105
eDirectory 122
設定 155
ディレクトリ設定 135
パラメータ 219
データ タイプ 161
[デバイス クエリ] 143

と

統合
Insightマネージャ7 85
トラブルシューティング
アラートおよびトラップの
問題 228

に

認証
ユーザ 99

ね

ネットワーク設定 64

は

ハードウェア
問題を解決 231
バッチ処理 145
パラメータ
iLO Advancedライセンス アク
ティベーション設定 225
LOMオブジェクト
識別名 220
パスワード 220
MOD_DIR_CONFIG 187
ProLiant BL p-Class 223
SNMP/Insightマネージャ
設定 221
グローバル設定 214
ディレクトリ サーバ
LDAPポート 220
アドレス 220
ディレクトリ サービスによる
認証 219
ディレクトリ設定 219
ディレクトリ ユーザ コンテ
キスト 220
ネットワーク設定 216
ユーザ管理 212

ひ

必要なソフトウェア 101

ふ

ファームウェア
アップグレード 73
ブラウザベースのセット
アップ 15

ほ

ポート
変更

Insightマネージャ7 87

ま

マネジメント スナップイン インス
トラ 104

ゆ

ユーザ
追加、新規 62
ログイン 138
ユーザ管理 62
ユーティリティ
Lights-Out DOSユーティ
リティ 149

り

リモートInsightボード コマンド
言語 159
一般的なガイドライン 160
概要 160
リモート コンソール 46
デュアル カーソル 27

ろ

ログイン
遅延時間 39