

管理者ガイド

HP BladeSystem PC Blade Enclosure Integrated
Administrator バージョン 4.30



© Copyright 2008 Hewlett-Packard Development Company, L.P. 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。

Microsoft および Windows 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。

HP 製品およびサービスに対する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られません。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書に記載されている製品情報は、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。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。

本書には、著作権によって保護された所有権に関する情報が掲載されています。本書のいかなる部分も、Hewlett-Packard Company の書面による承諾なしに複写、複製、あるいは他言語へ翻訳することはできません。

ユーザ ガイド

HP BladeSystem PC Blade Enclosure Integrated Administrator バージョン 4.30

改訂第 3 版：2009 年 1 月

改訂第 2 版：2008 年 2 月

初版：2007 年 5 月

製品番号：449377-293

このガイドについて

- △ **警告！** その指示に従わないと、人体への傷害や生命の危険を引き起こすおそれがあるという警告事項を表します。
 - △ **注意：** その指示に従わないと、装置の損傷やデータの損失を引き起こすおそれがあるという注意事項を表します。
 - ☞ **注記：** 重要な補足情報です。
-

目次

1 このガイドについて

対象読者	1
安全に使用していただくために	1
装置の記号	1
参考資料	2
お問い合わせ先	2
HP へのお問い合わせ	2
サポートおよびトラブルシューティング	2
HP の Web サイト	3

2 HP PC Blade エンクロージャ システム ソフトウェアの機能

HP PC Blade Enclosure Integrated Administrator	4
Integrated Administrator の機能	4
専用 LAN (Local Area Network) 接続	4
Integrated Administrator から管理コンソールへの SNMP (Simple Network Management Protocol) アラート送信	5
Integrated Administrator から電子メール アカウントへの電子メール アラート送信 (AlertMail)	5
リモート アクセスおよびリモート コントロール	5
ユーザ管理およびセキュリティ	5
自動ネットワーク設定	6
ネットワーク タイム プロトコル (NTP)	6
SOAP インタフェース	6
電力消費量のレポート	6
エンクロージャの電源管理および電源冗長機能	6
[HP Systems Insight Manager]ユーティリティとの統合	7
HP SAM (Session Allocation Manager) ユーティリティとの統合	7
イベント通知	7
HP BladeSystem ソフトウェア ツールの概要	8
ブレード ROM ベース セットアップ ユーティリティ (RBSU)	8
ヘッドレス操作	8
ProLiant Essentials Rapid Deployment Pack	8
HP Systems Insight Manager	8
ESR (Enclosure Self Recovery)	8

3 概要

設定ツールと情報の確認	10
Integrated Administrator の各部の確認	11
Integrated Administrator の初期 IP アドレスの決定	11
ローカル クライアント デバイスの要件	11
Integrated Administrator の初期値	12
ローカル コンソールを使用した IP アドレスの決定	13
Web ベースのユーザ インタフェースの設定	14
追加の手順	16

4 Web ブラウザ インタフェース

Web ベースのユーザ インタフェースへのアクセス	17
Web ベースのユーザ インタフェース内の移動	18
トップ パネル	18
左パネル	19
デッキ パネル	19
[Enclosure]タブ	20
Enclosure Information	21
Network Configuration	26
SNMP Configuration	29
Power Readings	31
Virtual Buttons	32
System Log	33
System Log Policy	33
[Enclosure Power Management]タブ	35
[Bays]タブ	36
Bay List	36
Bay Power Consumption	38
Bay Temperature	39
Bay Information	40
Remote Console	43
Virtual Buttons	44
Console Log	45
[Administration]タブ	46
User List	46
Group List	47
Add User	48
Add Group	50
View/Modify User	52
View/Modify Group	52
IA ファームウェアの更新	52

Configuration Scripts	53
[Event List]タブ	55
Event Log Policy	58
[Interconnect]タブ	58
5 コマンド ライン インタフェース	
コマンド ライン インタフェースへのアクセス	62
管理コネクタを介したリモート アクセス	62
コンソール コネクタを介したローカル アクセス	62
コマンド ライン インタフェースの操作	63
一般的なコマンド	63
一般的な管理コマンド	63
ユーザ アカウント コマンド	66
エンクロージャのネットワーク設定コマンド	70
エンクロージャの管理コマンド	72
Blade PC ベイの管理コマンド	77
コマンド ライン イベント メッセージ	80
コマンド ライン インタフェース特有の機能	83
6 システムの設定	
ユーザ アクセス権	89
エンクロージャ設定のカスタマイズ	90
エンクロージャ名およびラック名の変更	91
アセット タグ番号の変更	93
日付と時刻の変更	94
ユーザ アカウントの設定	95
グループの追加	95
ユーザの追加	98
Blade PC へのリモート コンソール セッションの有効化	101
AlertMail の設定	101
電子メール アラート	102
IP セキュリティの設定	103
自動ネットワーク タイム プロトコル (NTP) の設定	104
SNMP サポートの設定	105
コミュニティ名の入力	105
システムの位置の変更	106
システム連絡先情報の変更	106
トラップ送信先の追加	106
トラップ送信先の削除	107
トラップ ポリシーの変更	107
7 SOAP サポート タスクの設定	
SOAP インタフェースの有効化	108

SOAP インタフェースの無効化	108
サポートされている SOAP インタフェース コマンド	109

8 一般的な管理タスクの実行

Blade PC ベイの管理	111
Blade PC へのリモート コンソール セッションの開始	111
Blade PC の[ROM ベース セットアップ ユーティリティ]へのアクセス	112
Blade PC の動作の確認	114
Blade PC の電源の切断	114
ユニット確認ランプによる Blade PC の確認	116
エンクロージャの管理	117
エンクロージャの動作の確認	117
ユニット確認ランプによるエンクロージャの確認	119
エンクロージャ概要の生成	120
問題コンポーネントの特定	121
ユーザの管理	126
Blade PC ベイへのユーザのアクセス権の変更	126
アクセス権を更新した新しいグループの作成	126
Blade PC ベイへのグループ アクセス権の変更	126
ユーザ アカウントの無効化と削除	128
ユーザ アカウントの削除	130
グループ アカウントの削除	130

9 高度な機能の実行

Integrated Administrator の設定の複製	133
セキュリティ証明書の管理	134
証明書要求の作成	134
セキュリティ証明書のダウンロード	134
キーベースの SSH 認証	134
Blade PC の起動順序の設定	135
エンクロージャの電源切断	136
ネットワーク タイム プロトコルの無効化	137
Integrated Administrator のファームウェアのアップグレード	139
アップデート機能の設定	139
消失した管理者パスワードの復元	139
Flash Disaster Recovery の起動	140

付録 A コマンド ラインの規則

付録 B エラー メッセージ

警告メッセージ	144
エンクロージャの警告メッセージ	144

Blade PC の警告メッセージ	145
管理警告メッセージ	145
エラー メッセージ	146
エンクロージャのエラー メッセージ	146
Blade PC ベイのエラー メッセージ	146
管理エラー メッセージ	146

付録 C Blade PC の診断メッセージ

付録 D マスク可能なエンクロージャのシステム ログ メッセージ

付録 E マスク可能なエンクロージャのイベント メッセージ

付録 F トラブルシューティング

付録 G イベントのアイコンと詳細

付録 H 電源管理およびリダンダント電源装置

付録 I 出荷時の設定

エンクロージャ	167
ユーザ	168
グループ	168
ネットワーク	168
プロトコル	168

付録 J タイム ゾーンの設定

Universal	170
アフリカ	171
アジア	171
ヨーロッパ	172
オセアニア	173
極地	174
南北アメリカ	174

付録 K オープン ソースの利用

付録 L サポートされる SNMP トラップ

索引	180
----------	-----

1 このガイドについて

対象読者

このガイドは、HP Blade PC ソリューションのインストール、管理、およびトラブルシューティングを行うユーザを対象にしています。このガイドでは、ユーザがコンピュータ機器のサービスに関する資格を有し、エネルギーが危険なレベルに達する製品での危険を認識するためのトレーニングを受けていることを前提としています。

安全に使用していただくために

△ **警告！** システムに付属の『安全に使用していただくために』をよく読んでから、製品のインストールを開始してください。

装置の記号

安全上の注意が必要な装置の各部には、以下の記号が表示されています。



この記号は、以下の記号と組み合わせて使用され、危険があることを示します。警告事項に従わないと、けがをすることがあります。詳しくは、説明書を参照してください



この記号は、装置に高電圧が発生する回路があることや、装置の表面または内部部品に触れると感電の危険があることを示します。修理はすべて、資格のある担当者に依頼してください

警告： 感電、火傷、火災などの危険がありますので、絶対にこの筐体を開けないでください。保守、アップグレード、および修理はすべて、資格のある担当者に依頼してください



この記号は、装置の表面または内部部品に触れると感電の危険があることを示します。カバー内には、ユーザや使用現場の担当者が修理できる部品はありません。カバーは、絶対に開けないでください

警告： 感電、火傷、火災などの危険がありますので、絶対にこの筐体を開けないでください



RJ-45 ソケットに貼付されたこの警告記号は、ネットワーク インタフェース接続を示します

警告： 感電や火災が発生したり、装置を損傷したりする場合がありますので、電話回線のモジュラ コネクタをこのソケットに接続しないでください



この警告記号は、装置の表面または内部部品の温度が非常に高くなる可能性があることを示します。装置の表面に手を触れると、火傷をする場合があります

警告： 火傷の危険がありますので、必ず、表面の温度が十分に下がっていることを確認してから、次の手順に進んでください



これらの記号が電源装置またはシステムに貼付されている場合、装置の電源が複数あることを示します

警告：感電の危険がありますので、すべての電源コードを取り外し、システムの電源を完全に切ってください



Weight in kg
Weight in lb

製品や機械にこの記号が貼付されている場合、装置が1人で安全に取り扱うことのできる重量を超えていることを示します

警告：負傷したり、装置を損傷したりする場合がありますので、地域の労働安全衛生に関する条件および手作業による資材運搬に関するガイドラインを遵守してください

参考資料

このガイドで説明する項目について詳しくは、以下の資料を参照してください。

- 『White paper: Network Considerations Guide』（英語版）
- 『QuickSpecs』（英語版）
- 『セットアップおよびインストール ガイド HP BladeSystem bc2000/bc2500 Blade PC および PC Blade エンクロージャ』
- 『セットアップおよびインストール ガイド HP BladeSystem bc2200/bc2800 PC Blade および HP Bladesystem PC Blade エンクロージャ G2』
- 『White paper: HP Rack 9000 and 10000 Series installation and best practices』（英語版）
- 『インストール ガイド HP BladeSystem PC Blade スイッチ』
- 『コマンド ライン インタフェース リファレンス ガイド HP BladeSystem PC Blade スイッチ』
- 『内蔵 Web システム ユーザ ガイド HP BladeSystem PC Blade スイッチ』

お問い合わせ先

HP PC Blade エンクロージャについて質問があり、このガイドに記載されているすべての情報を使用しても解決できない場合は、以下の方法で追加情報を入手したり、その他のサポートを受けたりすることができます。

HP へのお問い合わせ

HP のお問い合わせ用 Web サイトには、オンライン チャット、電子メール、および電話を含むさまざまな問い合わせ方法が掲載されています。この Web サイトは、http://welcome.hp.com/country/jp/ja/contact_us.html からアクセスできます。

サポートおよびトラブルシューティング

HP のサポートおよびトラブルシューティングの Web サイトにアクセスすると、ソフトウェアおよびドライバをダウンロードしたり、特定の製品のサポートおよびトラブルシューティングについての情報を検索したりできます。この Web サイトは、<http://welcome.hp.com/country/jp/ja/support.html> からアクセスできます。

HP の Web サイト

最新のドライバやフラッシュ ROM イメージに関する情報については、<http://www.hp.com/jp/>を参照してください。

2 HP PC Blade エンクロージャ システム ソフトウェアの機能

HP BladeSystem は、効率的な Blade PC 管理およびソフトウェア導入をサポートするための多様な機能とオプション ツールを提供します。この章では、HP PC Blade Enclosure Integrated Administrator について説明するとともに、このシステムに関連したソフトウェアの概要についても簡単に説明します。

HP PC Blade Enclosure Integrated Administrator

HP PC Blade Enclosure Integrated Administrator は、HP PC Blade エンクロージャ（筐体）と Blade PC の集中管理および監視を行うシステムです。Integrated Administrator は、コンソール サーバおよびリモート電源コントローラの組み合わせとして機能するため、エンクロージャ内のすべての Blade PC に対する、セキュリティ保護されたインバンド（初期設定）またはアウトバンドのシリアル コンソール接続を可能にします。

Integrated Administrator は、エンクロージャおよびブレードの状態通知機能を提供し、リモート ブレード管理を可能にします。Integrated Administrator の機能は、ネットワーク ベースの任意のクライアントからアクセスできます。Integrated Administrator は、許可された任意のネットワーク クライアントへのリモート アクセスの提供やアラートの送信のほか、その他の多くの Blade PC 管理機能を提供できます。

Integrated Administrator サブシステムは、各インターコネクト トレイに付属のモジュールに内蔵され、高性能のマイクロプロセッサ、セキュリティ保護されたメモリ、およびインバンド（初期設定）またはアウトバンドのリモート アクセス用に構成可能な専用のネットワーク インタフェースを搭載しています。この設計のために、Integrated Administrator は、ホスト Blade PC やそのオペレーティング システムから独立しています。

Integrated Administrator の機能

以下のサブセクションでは、エンクロージャと Blade PC を管理するための Integrated Administrator の機能について説明します。

専用 LAN（Local Area Network）接続

各 Integrated Administrator は、専用のネットワーク接続を提供しています。アップリンク ポート 42 は、10 Mbps と 100 Mbps の速度を自動選択できます。PC Blade スイッチ（オプション）が取り付けられている場合は、初期設定で、仮想 LAN（VLAN）を使用してギガビット アップリンク コネクタ経由でルーティングするように Integrated Administrator が構成されているため、管理ネットワークを別に設ける必要がありません。

 **注記：** HP BladeSystem PC Blade スイッチ オプションの初期の構成には、同じ VLAN 内に専用の IA ポートおよびアップリンク ポート 45 と 46 の両方があります。

Integrated Administrator から管理コンソールへの SNMP (Simple Network Management Protocol) アラート送信

Integrated Administrator は、エンクロージャの問題を通知します。管理コンソールを使用すると、SNMP トラップを介して、許可されていないアクセスの試みやネットワーク接続の失敗などの各種のアラートにアクセスできます。

CPQRACK.MIB ファイルには、エンクロージャのインフラストラクチャとブレードを管理するための、HP 固有の SNMP オブジェクト識別子 (OID) およびトラップが含まれています。Integrated Administrator 4.3 には、CPQRACK バージョン 1.10 のサポートが実装されています。

Integrated Administrator から電子メール アカウントへの電子メール アラート送信 (AlertMail)

AlertMail を使用すると、Integrated Administrator は SNMP トラップを使用しないで、電子メールによってシステム イベントを送信できます。AlertMail は SNMP にまったく依存しておらず、この両方を同時に有効にすることができます。AlertMail は標準の SMTP コマンドを使用して、SMTP (Simple Mail Transfer Protocol) リレー エージェントの他に、任意の SMTP 対応メール サーバと通信します。

リモート アクセスおよびリモート コントロール

Integrated Administrator を使用すると、ホスト Blade PC の一部のテキストのみのコンソールにリモート アクセスしたり、エンクロージャまたはその任意の Blade PC 上のユニット確認ランプの状態をリモートで変更したりできます。また、単体またはグループとしての Blade PC の電源投入、電源切断、または再起動などをリモートで実行できます。

Integrated Administrator は、Blade PC の状態には関係なくアラートを表示します。また、SNMP バージョン 1 を使用して [HP Systems Insight Manager] などの業界標準の SNMP 管理ツールと統合することによって、システムのアラートおよび診断機能を提供できます。

Blade PC が応答しない場合、管理者はこの機能を使用し、コールド リブートを開始して Blade PC をオンラインに戻すことができます。Integrated Administrator を使用すると、エンクロージャ内の任意の Blade PC の電源ボタンまたはユニット確認ランプ (UID) をリモートで操作できます。

Integrated Administrator のすべての機能に一般的な Web ブラウザを使用してアクセスできます。また、Integrated Administrator は、暗号化された Secure Shell または暗号化されていない Telnet プロトコルを使用してアクセス可能なコマンド ライン インタフェース (CLI) も備えているため、リモート ネットワーク ユーザに広範囲の管理機能が提供されます。ローカル ユーザは、Integrated Administrator のコンソール (RS-232 シリアル) ポートにクライアント コンピュータ (端末エミュレータを使用) を接続することによって、CLI にアクセスできます。

 **注記：** Telnet セッションでは、パスワードを含むすべてのデータが通常のテキストとして送信されます。

ユーザ管理およびセキュリティ

Integrated Administrator は、最大 25 ユーザをサポートし、ユーザのアクセス権とログイン名はカスタマイズ可能です。最初にグループにベイが割り当てられ、次にそれらのグループのメンバシップがユーザに割り当てられます。このグループ中心の方式によって、複数の Blade PC にまたがるユーザ管理が容易になります。

Integrated Administrator は、ネットワーク内で転送される HTTP データに対して業界標準の SSL (Secure Sockets Layer) 暗号化を使用することによって、分散 IT 環境でのリモート管理に強力なセキュリティを提供します。SSL 暗号化 (最大 128 ビット) によって、ネットワーク内で転送される HTTP 情報の安全性が保証されます。また、すべてのリモート コンソール データも暗号化できます。

Integrated Administrator は、すべてのログインの試みを追跡し、すべてのログイン失敗のレコードを管理し、さらに安全なパスワード暗号化を提供します。また、Integrated Administrator には以下のようなセキュリティ機能もあります。

- Integrated Administrator システム ログへのユーザ操作の記録
- ログイン リーガル警告

IP セキュリティを使用すると、管理者は提供されているサービス (SSH (Secure Shell)、HTTP、HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)、TELNET (Telecommunications network)、SNMP) への接続を許可された唯一の IP アドレスである一連の IP アドレスを定義できます。つまり、管理者は、特定のシステム一式のみを Integrated Administrator にアクセス可能な状態にできます。

自動ネットワーク設定

Integrated Administrator は、DHCP (Dynamic Host Configuration Protocol) および動的 DNS/WINS を使用して、IP アドレスとホスト名の自動ネットワーク設定機能を提供します。Integrated Administrator の出荷時には、初期名と DHCP クライアントが設定されており、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。DHCP を使用しないネットワークの場合、Integrated Administrator は静的 IP 設定を使用できます。

ネットワーク タイム プロトコル (NTP)

自動時間設定を使用すると、Integrated Administrator は、システムの日付と時刻を、互換性のあるネットワーク タイム プロトコル (NTP) タイム サーバと同期させることができます。

SOAP インタフェース

Integrated Administrator は、SOAP (Simple Object Access Protocol) を使用する管理ツール用に、SOAP インタフェースを介していくつかのコマンドを提供します。このインタフェースは、IA によって管理されるエンクロージャとブレードの、インベントリおよび電力管理のためのコマンドをいくつか提供します。すべての管理者アクセス レベルのアカウントが、SOAP インタフェースを使用できます。SOAP インタフェースは、コマンド ライン (CLI) コマンドまたはグラフィカル ユーザ インタフェース (GUI) を使用して有効にします。

電力消費量のレポート

Integrated Administrator は、bc2000、bc2200、bc2500、および bc2800 ブレードから電力消費量の測定結果を収集し、CLI および GUI を介してそれらをレポートします。これらの、ハードウェア測定コンポーネントを使用したブレードの自己測定は、bc2000、bc2200、bc2500、および bc2800 ブレードに特有のものです。これらの測定結果を使用して、エンクロージャの電力消費量の推定値 ($\pm 10\%$) が計算されます。エンクロージャ全体の電力消費量の推定値を、CLI、GUI、および SOAP インタフェースによって収集できます。

エンクロージャの電源管理および電源冗長機能

電源装置の 1 つが停止した場合、IA は、ブレードの種類にかかわらず、すべてのブレードが完全に電力を供給された状態で動作を継続できるようにします。

200 V 以上の AC 電圧で動作する PC Blade エンクロージャ G2 のエンクロージャでは、AC 電源の冗長性が常に確保されています。

200 V 未満で動作する PC Blade エンクロージャまたは PC Blade エンクロージャ G2 のエンクロージャの場合、IA は、ブレードの数がリダンダント電源の割り当て最大容量を超えない限り、電源装置の 1 つが停止した後も通常で引き続きブレードを実行できるようにします。IA は、最大リダンダント、レジリエント、および総容量の値をレポートし、その値をエンクロージャの電源管理に利用します。これらの値が、(エンクロージャの電源冗長性を確保するための適切な動作を決定するブレード設定に基づいて) 割り当てられている電源容量と比較されます。

詳しくは、[164 ページの「電源管理およびリダンダント電源装置」](#)を参照してください。

[HP Systems Insight Manager]ユーティリティとの統合

Integrated Administrator は、主要な動作環境の下で、[HP Systems Insight Manager]ユーティリティと完全に統合されています。この統合によって、以下のことが可能になります。

- SNMP 管理のサポート : [HP Systems Insight Manager]コンソールへの SNMP トラップ配信のサポート。
- 管理プロセッサ : [HP Systems Insight Manager]ユーティリティでは、新しいデバイスの種類である管理プロセッサに対するサポートが追加されています。ネットワーク上の (HP PC Blade エンクロージャ内の) すべての Integrated Administrator は、[HP Systems Insight Manager]ユーティリティ内で管理プロセッサとして検出されます。管理プロセッサは、管理対象の Blade PC に関連付けられます。
- Integrated Administrator のハイパーリンク : [HP Systems Insight Manager]ユーティリティの Blade PC デバイス ページには、Integrated Administrator を起動し、そこに接続するためのハイパーリンクが用意されています。
- Integrated Administrator プロセッサのグループ化 : すべての Integrated Administrator 管理プロセッサを論理的にグループ化して、[HP Systems Insight Manager]の 1 つのページに表示することができます。この機能によって、[HP Systems Insight Manager]内の 1 か所から、ネットワーク上のすべての Integrated Administrator にアクセスできるようになります。

[HP Systems Insight Manager]ユーティリティについて詳しくは、<http://h50146.www5.hp.com/products/software/management/hpsim/>を参照してください。SNMP 用の配信設定について詳しくは、ホワイト ペーパー、『Network Considerations』(英語版)を参照してください。

HP SAM (Session Allocation Manager) ユーティリティとの統合

Integrated Administrator には、ハードウェアを管理し、レポートするための[HP Session Allocation Manager]ソフトウェア用の機能が備えられています。HP SAM では、SOAP インタフェースを利用して、電力消費量に関するレポート データを収集したり、エンクロージャ内のブレードの電源を入れ直したりすることができます。Integrated Administrator には、HP SAM を使用する展開内での実装を容易にするために提供されている、組み込みのアカウントがあります。このアカウントは、初期設定では無効になっています。

イベント通知

Integrated Administrator は、エンクロージャに関するリアルタイムのイベント通知を提供します。イベントが発生すると、Integrated Administrator は接続されているユーザに対し、コマンド ライン インタフェース (CLI) でイベント テキスト メッセージを生成して通知するか、GUI でユーザがクリックすることによって詳細を表示できる、選択可能なアイコンおよびテキストで通知します。

HP BladeSystem ソフトウェア ツールの概要

以下のサブセクションでは、エンクロージャの監視および管理を容易にするために HP BladeSystem Blade PC システムでサポートされているツールとユーティリティについて説明します。

ブレード ROM ベース セットアップ ユーティリティ (RBSU)

[Blade RBSU (F10)]を使用すると、さまざまな設定操作を実行したり、システム デバイスの設定、オペレーティング システムの選択、ブート コントローラの順序などの多くの設定にアクセスしたりすることができます。[RBSU (F10)]はまた、Integrated Administrator を使用するリモート シリアル コンソール モードとも完全な互換性があります。

ヘッドレス操作

HP bc シリーズ Blade PC には、VGA (Video Graphics Array)、キーボード、マウス、および USB (Universal Serial Bus) インタフェースを搭載していますが、本来は、キーボードやモニタを接続しないヘッドレス操作および管理用に設計されています。

ProLiant Essentials Rapid Deployment Pack

[ProLiant Essentials Rapid Deployment Pack]は、グラフィカルな導入コンソールを備えています。このコンソールによって、スクリプトやイメージなどの直感的なドラッグ アンド ドロップ イベントが提供され、エンクロージャに取り付けられた Blade PC の任意の組み合わせにオペレーティング システムとアプリケーションを配備できます。

[ProLiant Essentials Rapid Deployment Pack]を使用すると、ユーザは、新しく取り付けられた Blade PC に定義済みの設定を自動的にインストールできます。[ProLiant Essentials Rapid Deployment Pack]について詳しくは、HP 製品販売店に問い合わせるか、エンクロージャに付属している Rapid Deployment CD または以下の Web サイトを参照してください。
<http://h50146.www5.hp.com/products/servers/proliant/essentials/rdp/>

HP Systems Insight Manager

[HP Systems Insight Manager]は、障害状態、性能、セキュリティ、リモート管理、復旧サービスなどの Blade PC 情報を収集するために設計されたソフトウェア ユーティリティです。HP BladeSystem は、[HP Systems Insight Manager]ユーティリティと完全に互換性があります。

ESR (Enclosure Self Recovery)

[ESR]は、[Integrated Administrator]の自己監視による信頼性機能です。[Integrated Administrator]が起動しなかったり動作中にハングしたりすると、ESR は自己復旧を試みるために Integrated Administrator を自動的にリセットします。Blade PC とインターコネクト トレイは、ESR の影響を受けません。

HP PC Blade エンクロージャ管理システムおよびユーティリティ

HP PC Blade エンクロージャ管理システムおよびユーティリティは、HP PC Blade エンクロージャ (オプション) のための一連の設定/管理インタフェースおよびツールを提供します。インターコネクト スイッチおよびエンクロージャの管理用に、Web インタフェースおよびコンソール インタフェースの両方が用意されています。

どちらのインタフェースも、認証のために有効なユーザ名とパスワードを要求するように設定できます。スイッチ用の RMON (Remote Network Monitoring) および SNMP 管理機能がサポートされて

います。また、インターコネクト スイッチの設定をバックアップとして、または他のスイッチの事前設定用のテンプレートとして TFTP (Trivial File Transfer Protocol) サーバに保存することもできます。

3 概要

HP PC Blade Enclosure Integrated Administrator を使用すると、エンクロージャ内に収納された Blade PC 固有の機能を含む、エンクロージャ内のすべての機能を監視および管理することができます。Integrated Administrator を設定した後は、これらの機能が Web ベースのユーザ インタフェースと CLI の両方を介して提供されます。

この章では、エンクロージャをラックに搭載して電源を入れた後で、Integrated Administrator を初めて設定する場合の方法について説明します。

- 設定ツールと情報の確認
- Integrated Administrator コネクタの確認
- Integrated Administrator 初期 IP アドレスの決定
- Web ベースのユーザ インタフェースの設定
- 追加の手順
- ヘルプ

設定ツールと情報の確認

Integrated Administrator は、電源を入れるとすぐに使用できるようになります。Integrated Administrator の設定と管理を容易にするために、以下の機能と情報が用意されています。

- 各 Integrated Administrator の出荷時には、一意の管理者パスワードとホスト名がすでに設定されています。
- ネットワークで動的 DNS (Dynamic Domain Name System) または WINS (Windows® Internet Name Service) が使用されている場合は、工場出荷時に設定されているホスト名を使用して Integrated Administrator にアクセスできます。

 **注記：** 事前に設定された管理者パスワードとホスト名は、インターコネクト トレイに貼付された Integrated Administrator のネットワーク初期設定タグ (設定タグ) に記載されています。

- ネットワークで DHCP (Dynamic Host Configuration Protocol) を使用している場合は、Integrated Administrator に IP アドレスを自動的に割り当てることができます。
- Blade PC のヘルス サービス (ブレードにインストールされている場合) は、Integrated Administrator に、Blade PC のオペレーティング システム内で定義されている名前および各 Blade PC のオペレーティング システムの種類などの情報を提供します。

 **注意：** ACPI (Advanced Configuration and Power Interface) 準拠のオペレーティング システムがないと、Integrated Administrator は Blade PC を正しくシャットダウンできません。この状態が発生すると、重要なデータが永久に失われる場合があります。

Integrated Administrator の各部の確認

各 HP PC Blade エンクロージャ インターコネクト トレイの出荷時には、Integrated Administrator モジュールがすでに搭載されており、リア パネルにある 2 つのコネクタを介して外部接続が提供されます。

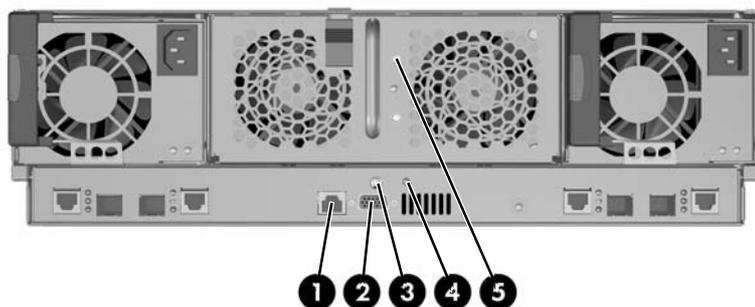


表 3-1 Integrated Administrator のリア パネルの各部

参照番号	説明
1	Web ベースのユーザ インタフェース、Telnet、または Secure Shell を介したリモート アクセス用の管理 (10/100 Ethernet) コネクタ
2	ラップトップ コンピュータを使用したコマンド ライン インタフェースへのローカル アクセス用のコンソール (シリアル) コネクタ
3	Integrated Administrator のリセット ボタン
4	Integrated Administrator のヘルス ランプ
5	エンクロージャ ユニット確認ボタン/ランプ

Integrated Administrator の初期 IP アドレスの決定

ネットワークが Integrated Administrator を認識するために使用する初期 IP アドレスを決定するために、ラップトップ コンピュータなどのローカル クライアント デバイスをコンソール (シリアル) コネクタに接続することをおすすめします。その IP アドレスを使用して、コンソール (シリアル) コネクタを介してローカルに Integrated Administrator にアクセスした後、Integrated Administrator の初期値を使用して初期設定を完了できます。

この項では、以下の内容について説明します。

- ローカル クライアント デバイスの要件
- Integrated Administrator の初期値
- ローカル コンソールを使用した IP アドレスの決定

ローカル クライアント デバイスの要件

ラップトップ コンピュータなどのローカル クライアント デバイスを使用して、エンクロージャのリア パネルにあるシリアル コネクタを介して Integrated Administrator にローカルにアクセスできま

す。ローカル クライアント デバイスでは、Windows システム用のハイパーターミナルや Linux システムの Kermit などの端末エミュレータを実行する必要があります。

端末エミュレータで、以下の設定で動作させる必要があります。

- 通信速度 : 9600 bps
- ビット数 : 8
- パリティ : なし
- ストップ ビット : 1
- フロー制御 : なし
- エミュレーション : VT100
- Backspace キーで Ctrl + H キーと同じ処理を行う

Integrated Administrator の初期値

Integrated Administrator には、初期設定のユーザ名、パスワード、および DNS 名が設定されています。これらの事前に設定された値が記載された設定タグは、Integrated Administrator モジュールを搭載したインターコネクト トレイに貼付されています。SOAP アクセス用の組み込みの管理者アカウントもあります。これは初期設定では無効になっています。

ユーザー名 : SAM

初期設定のパスワード : SamUser123

 **注記 :** この管理者アカウントは、初期設定では無効になっています。SAM アカウントを有効にするまで、このアカウントを使用してログインすることはできません。

アカウントを有効にする場合、HP SAM で通常の使用を開始する前に、初期設定のアカウント パスワードを変更することが重要です。最後に、SOAP インタフェースは、その他すべてのアカウントについては初期設定で無効になっていますが、SAM アカウントについては常に有効になっています。

 **注記 :** セキュリティ上の理由から、Integrated Administrator に初めてアクセスした後に管理者パスワードを変更することをおすすめします。

選択できるパスワードは 8 文字以内に制限されているため、パスワードを変更すると、コマンドによって初期設定のパスワードに戻すことはできなくなります。

ローカル コンソールを使用した IP アドレスの決定

ローカル コンソールを使用して Integrated Administrator の IP アドレスを決定するには、以下の操作を行います。

1. Integrated Administrator コンソールにアクセスします。
 - a. ヌル モデム シリアル ケーブルを使用して、VT100 端末エミュレーション ソフトウェアを搭載したローカル クライアント デバイス（ラップトップ コンピュータなど）を Integrated Administrator のコンソール（シリアル）コネクタに接続します。
 - b. 9600 bps、8 データ ビット、パリティなし、1 ストップ ビットに設定された端末エミュレーション セッションを開きます。
 - c. インターコネクト トレイに貼付された設定タグに記載されているパスワードを使用して、Integrated Administrator にログインします。
2. Integrated Administrator の IP アドレスを確立します。

このガイドで使用されているコマンド ラインの規則について詳しくは、[143 ページの「コマンド ラインの規則」](#)を参照してください。

ネットワークに DHCP サーバが接続されている場合は、Integrated Administrator の IP アドレスを決定します。コマンド ライン インタフェースで、以下のコマンドを入力します。

```
SHOW NETWORK
```

ネットワークに DHCP サーバが接続されていない場合は、以下のコマンドを順番に入力して、Integrated Administrator に静的 IP アドレスを割り当てます。

```
SET IPCONFIG STATIC <IP アドレス><サブネット マスク>
```

```
SET GATEWAY <IP アドレス>
```

```
SET DNS <プライマリ アドレス> {<セカンダリ アドレス>}
```

これで、Web ブラウザ、Secure Shell、Telnet、または SNMP を使用して Integrated Administrator にアクセスできます。

△ **注意：** すべての設定は、すぐに有効になります。また、手動でしか復元できません。

Web ベースのユーザ インタフェースの設定

Web ベースのユーザ インタフェースを設定するには、以下の操作を行います。

1. Web ブラウザのアドレス バーに、Integrated Administrator の IP アドレスまたは DNS 名を入力します。以下に示すセキュリティの警告が表示されます。



[Yes]をクリックすると、ブラウザは Integrated Administrator の [Login] ウィンドウに進みます。この警告メッセージは、ブラウザで Integrated Administrator 管理プロセッサにアクセスするたびに表示されます。

[No]をクリックすると、以前のブラウザ表示に戻ります。

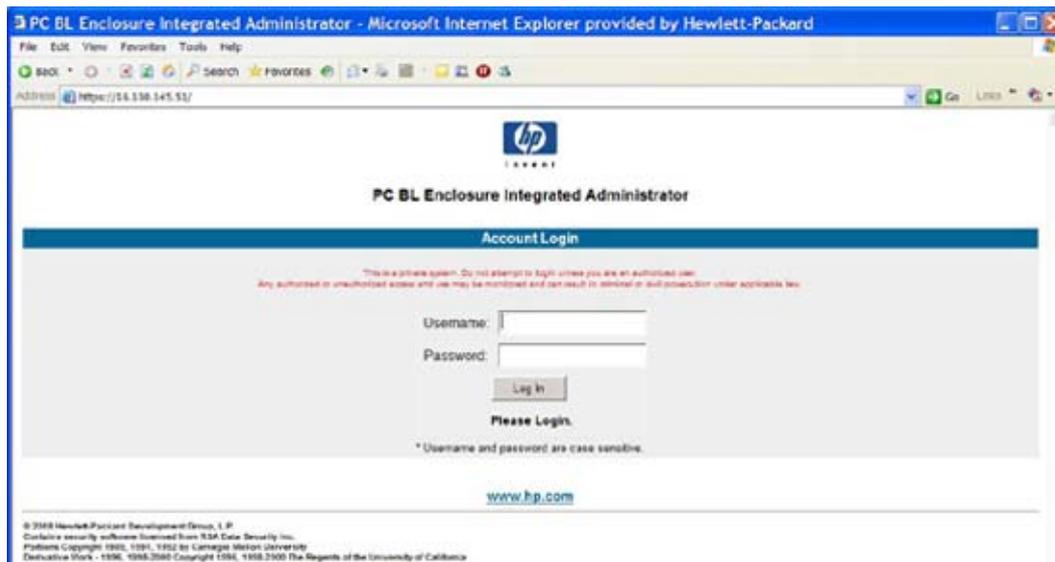
[View Certificate]をクリックすると、ポップアップ ウィンドウに証明書情報が表示されます。ブラウザに証明書をインストールすると、それ以降はセキュリティの警告メッセージが表示されなくなります。

 **注記：** 自動的に生成された証明書ではなく、独自の証明書を Integrated Administrator にインストールするには、[134 ページの「セキュリティ証明書の管理」](#)の証明書関連のコマンドに関する情報を参照してください。

ブラウザから証明書が削除されると、セキュリティの警告メッセージが再び表示されます。

2. ブラウザに証明書をインストールするには、以下の操作を行います。
 - a. [Install Certificate] をクリックします。[Certificate Manager Import Wizard] が起動します。
 - b. [Next] をクリックします。
 - c. [Next] をクリックして、[Certificate Store] ウィンドウが表示されたときにブラウザが証明書ストアを自動的に選択するようにします。
 - d. [Completing the Certificate Manager Import Manager Wizard] ウィンドウが表示されたら、[Finish] をクリックします。
 - e. 確認ウィンドウが表示されたら、[Yes] をクリックして証明書のインストールを確認します。

3. [Account Login]画面（以下の図を参照）にユーザ名とパスワードを入力するよう求められます。インターコネクト トレイに貼付された設定タグに記載されている初期設定のユーザ名とパスワードを入力してから、[Log In]をクリックします。



初期設定のユーザ名とパスワードが確認されると、概要ウィンドウが表示されます。



Integrated Administrator の概要ウィンドウには、現在ログオンしているユーザ、エンクロージャの名前とステータス、Integrated Administrator の IP アドレスと名前など、Integrated Administrator に関する一般的な情報が表示されます。

追加の手順

以下のタスクを実行することをおすすめします。

- 管理者パスワードの変更
- 日付と時刻の設定
- エンクロージャとラックの名前の設定
- グループ、ユーザ、およびアクセス権の設定

これらのタスクを実行する詳しい手順については、[88 ページの「システムの設定」](#)の該当する項を参照してください。

4 Web ブラウザ インタフェース

この章では、Integrated Administrator の Web ベースのユーザ インタフェースの使用方法について説明します。

 **注記：** この章の画面に表示されている値は、説明のみを目的としています。

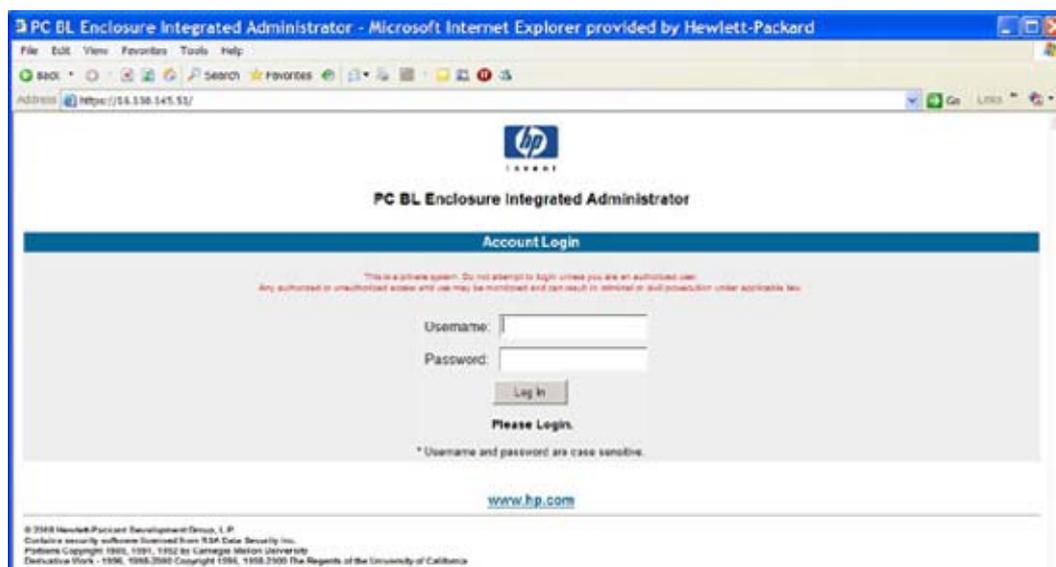
Web ベースのユーザ インタフェースへのアクセス

Web ベースのユーザ インタフェースへのコンソール（シリアル）コネクタからのアクセスはサポートされていません。

HTTP を使用して Integrated Administrator の Web ベースのユーザ インタフェースにアクセスするには、以下の操作を行います。

1. インターコネクト トレイに貼付された設定タグから、DNS 名を取得します。
2. Web ブラウザを開き、アクセスするエンクロージャの IP アドレスまたは DNS 名を入力します。

△ **注意：** ネットワークで DHCP と、動的 DNS または WINS のどちらかのサービスが提供されていない場合は、静的 IP アドレスを設定する必要があります。[13 ページの「ローカル コンソールを使用した IP アドレスの決定」](#)を参照してください。



3. [Login] プロンプトで、ユーザ名とパスワードを入力します。

Web ベースのユーザ インタフェース内の移動

Web ベースのユーザ インタフェースには情報が表示され、以下の領域で入力を受け付けます。

- トップ パネル
- 左パネル
- デッキ パネル

トップ パネル

以下の図は、トップ パネルの位置を示しています。



トップ パネルの情報は常に表示され、以下の項目が含まれています。

- エンクロージャ名
- 現在のユーザ
- タブ

Integrated Administrator のトップ パネルには、「Caution（注意）」および「Critical（重大）」という 2つのカテゴリに従って、エンクロージャに関するリアルタイムのイベント通知が表示されます。イベントが発生すると、Integrated Administrator は、クリックすると詳細が表示されるアイコンを生成してユーザに通知します。

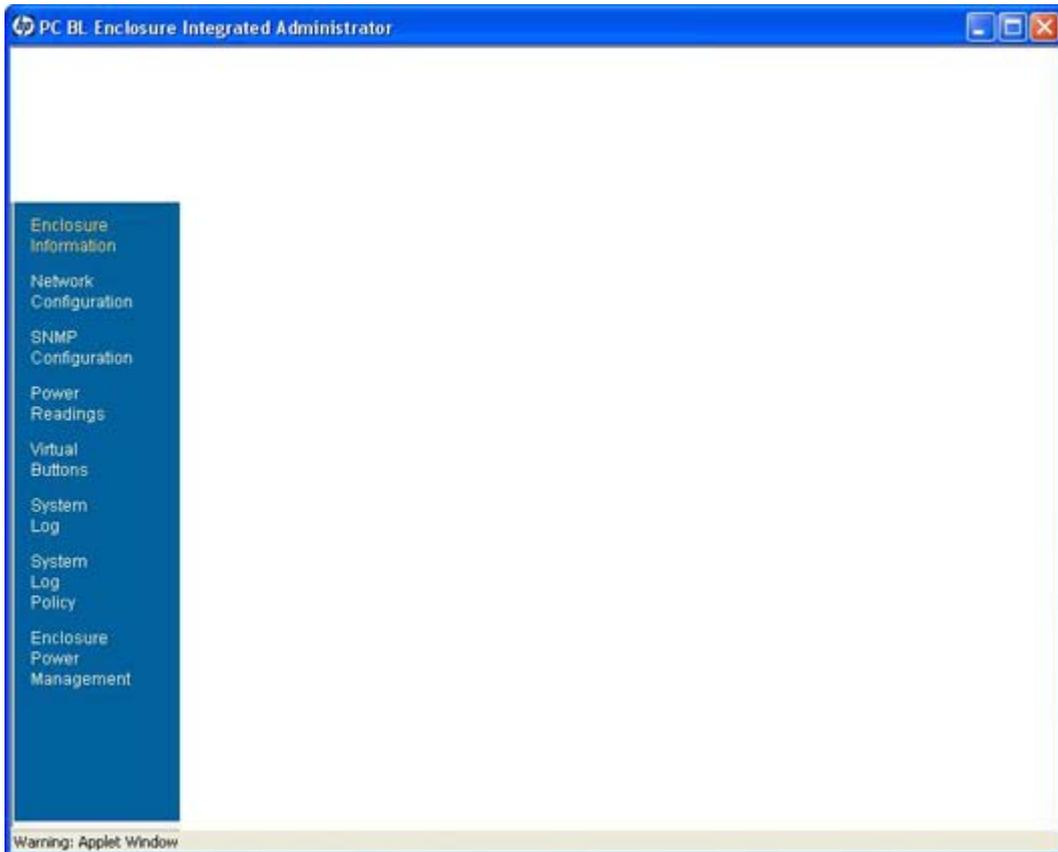
アイコン	説明
	Unknown Event (不明イベント)
	Informational (情報)
	Minor Event (マイナー イベント)
	Caution (注意)
	Warning (警告)
	Critical (重大)

トップ パネルには、以下の 2 つのボタンが表示されます。

- **[Summary View]** : 切り取りや貼り付けのためのエンクロージャ ステータスおよび設定情報を表示する別のウィンドウを開きます。
- **[Log Out]** : Web ベースのユーザ インタフェースからログアウトします。

左パネル

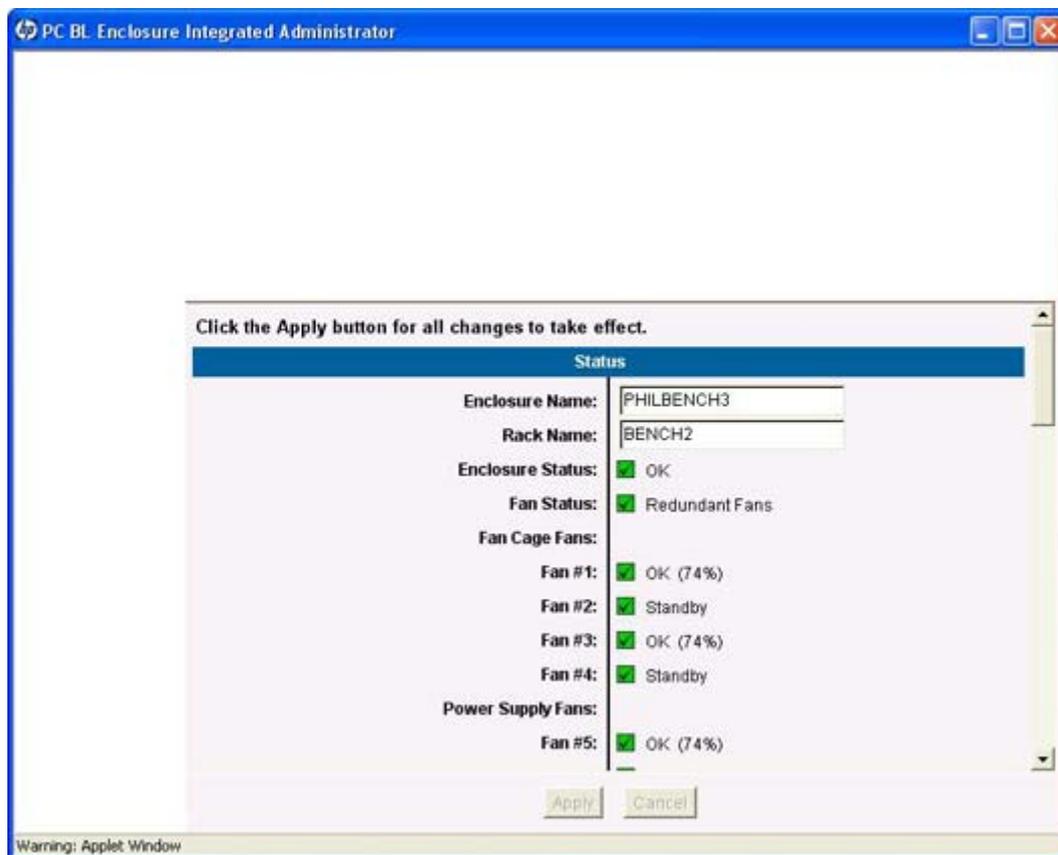
以下の図は、左パネルの位置を示しています。



左パネルには、各タブによってどの画面が使用できるかが表示されます。左パネルに表示される情報は、ユーザがトップ パネルから選択したタブによって異なります。

デッキ パネル

以下の図は、デッキ パネルの位置を示しています。



デッキ パネルには、各タブによって使用可能な画面に表示される情報の領域が表示されます。デッキ パネルに表示される情報は、ユーザがトップ パネルと左パネルから選択したオプションによって異なります。

[Enclosure]タブ

[Enclosure]タブからは、以下の画面にアクセスできます。

- Enclosure Information
- Network Configuration
- SNMP Configuration
- Power Readings
- Virtual Buttons
- System Log
- System Log Policy
- Enclosure Power Management

Enclosure Information

すべてのユーザは、以下の画面の情報への読み取りアクセス権を持っています。

- Status
- Temperature
- Power
- General
- Integrated Administrator
- Network
- Date and Time

以下の図は、[Enclosure Information]画面に表示される情報（[Status]領域）を示しています。

The screenshot shows the 'PC BL Enclosure Integrated Administrator' interface. The main content area is titled 'Enclosure Information' and contains a 'Status' section. The status section lists the following information:

Status	
Enclosure Name:	PHILBENCH3
Rack Name:	UnnamedRack
Enclosure Status:	<input checked="" type="checkbox"/> OK
Fan Status:	<input checked="" type="checkbox"/> Redundant Fans
Fan Cage Fans:	
Fan #1:	<input checked="" type="checkbox"/> OK (58%)
Fan #2:	<input checked="" type="checkbox"/> Standby
Fan #3:	<input checked="" type="checkbox"/> OK (58%)
Fan #4:	<input checked="" type="checkbox"/> Standby
Power Supply Fans:	
Fan #5:	<input checked="" type="checkbox"/> OK (58%)
Fan #6:	<input checked="" type="checkbox"/> OK (58%)
Fan Spare Number:	417425-001

At the bottom of the status section, there are 'Apply' and 'Cancel' buttons. The interface also includes a navigation menu on the left and a top header with the HP logo and enclosure details.

[Enclosure Information]画面を使用すると、エンクロージャ管理者は、ラック名、エンクロージャ名、アセット タグ、タイム ゾーン、日付、および時間を更新したり、エンクロージャ内のすべてのコンポーネントのステータスや一般的な情報を確認したりすることができます。

[Enclosure Information]画面には、以下の2つのボタンが表示されます。

- **[Apply]** : この画面に加えた変更を保存します。
- **[Cancel]** : この画面のすべてのフィールドを元の値に戻します。

以下の表では、[Enclosure Information]画面の各領域に表示される情報について説明します。

表 4-1 [Enclosure Information]画面のフィールドの説明 : [Status]領域

フィールド	可能な値	説明
[Status]領域		
Enclosure Name	すべての英数字、ハイフン、およびアンダースコアを含む最大 32 文字	エンクロージャの名前 エンクロージャ管理者だけが、このフィールドへの書き込みアクセス権を持ちます 初期設定のエンクロージャ名については、 167 ページの「出荷時の設定」 を参照してください
Rack Name	すべての英数字、ハイフン、およびアンダースコアを含む最大 32 文字	ラックの名前 エンクロージャ管理者だけが、このフィールドへの書き込みアクセス権を持ちます 初期設定のラック名については、 167 ページの「出荷時の設定」 を参照してください
Enclosure Status	OK、劣化、または障害	エンクロージャのステータス
Fan Status	リダンダントまたは非リダンダント	リダンダント : すべてのファンが動作しています。非リダンダント : 少なくとも1つのファンが動作していません
Fan #1 ~ Fan #4	OK、スタンバイ、劣化、障害、またはテスト中。最大速度に対するファン速度の比率 (%)	ファン1 ~ 4のステータス
Fan Spare Number		エンクロージャに取り付けられているファンのスペア番号
Fan #5 ~ Fan #6		電源装置ファン5および6のステータス
Power Supply Fans		
注記 : HP BladeSystem PC Blade エンクロージャ G2 のエンクロージャのみ		
Power Supply Fan Spare Number		電源装置に取り付けられているファンのスペア番号
Temperature	OK、温度上昇、注意、または重大	エンクロージャ コンポーネントの温度センサ

表 4-2 [Enclosure Information]画面のフィールドの説明 : [Power]領域

フィールド	可能な値	説明
-------	------	----

表 4-2 [Enclosure Information]画面のフィールドの説明 : [Power]領域 (続き)

[Power]領域		
Power Subsystem Status	リダンダント、レジリエント、レジリエント (スロットリング)、非リダンダント、非リダンダント (スロットリング)	<p>リダンダント：両方の電源供給装置が動作しています</p> <p>レジリエント：電源装置の障害または停止のため、ブレードのパフォーマンスが低下している可能性があります</p> <p>レジリエント (スロットリング)：電源装置の停止によってエンクロージャまたはブレードがシャットダウンするのを防止するために、すべての Blade PC のパフォーマンスを事前に低下させた結果、ブレードの総数が耐障害性電源の容量を超えています</p> <p>非リダンダント：電源装置の1つが機能していないか、割り当てられた容量がレジリエント電源の容量を超えています</p> <p>非リダンダント (スロットリング)：電源装置の停止によって、1つの電源装置に対して割り当てられている電源容量に合わせてすべてのブレードのパフォーマンスを低下させたため、ブレードの総数がリダンダント電源の容量を超えています</p>
Total Capacity	ワット数	電源供給装置の総容量
Power Supply #1 and #2 Status	OK、劣化、または障害	電源供給装置#1 と電源供給装置#2 のステータス
AC Input #1 and #2 Status	OK、劣化、または障害	電源供給装置#1 への AC 入力と電源供給装置#2 への AC 入力のステータス
Power Supply Spare Number		エンクロージャに取り付けられている電源供給装置のスペア番号

表 4-3 [Enclosure Information]画面のフィールドの説明 : [General]領域

フィールド	可能な値	説明
[General]領域		
Enclosure Type		エンクロージャの製品の種類
Part Number		エンクロージャの製品番号
Serial Number		エンクロージャのシリアル番号
Asset Tag	すべての英数字、ハイフン、およびアンダースコアを含む最大 31 文字	<p>アセット タグ</p> <p>エンクロージャ管理者だけが、このフィールドへの書き込みアクセス権を持ちます</p> <p>アセット タグの初期値については、167 ページの「出荷時の設定」を参照してください</p>
Interconnect Tray Type	HP PC Blade エンクロージャ インターコネクト スイッチ	インターコネクト トレイの種類

表 4-3 [Enclosure Information]画面のフィールドの説明 : [General]領域 (続き)

HP PC Blade エンクロージャ RJ-45 インターコネクト パッチ パネル		
Interconnect Tray Part Number		インターコネクト トレイの製品番号
Interconnect Tray Spare Number		インターコネクト トレイのスペア番号
Interconnect Tray Serial Number		インターコネクト トレイのシリアル番号
Blade Auto Power On Feature	有効または無効	有効になっている場合は、ブレードが取り付けられたか外部電源サイクルがエンクロージャに適用されたときに、エンクロージャ IA が自動的にブレードの電源を入れます。無効になっている場合は、ブレードが取り付けられても電源が自動的に入りません 初期設定では有効になっています

表 4-4 [Enclosure Information]画面のフィールドの説明 : [Integrated Administrator]領域

フィールド	可能な値	説明
[Integrated Administrator]領域		
Hardware Version		エンクロージャの Integrated Administrator のハードウェア バージョン
Software Version		エンクロージャの Integrated Administrator のソフトウェア バージョン。ビルド バージョンも表示されます

表 4-5 [Enclosure Information]画面のフィールドの説明 : [Network]領域

フィールド	可能な値	説明
[Network]領域		
IP Address	###.###.###.### (###は 0 ~ 255)	Integrated Administrator の IP アドレス
DHCP	有効または無効	動的 DNS のステータスを示します このフィールドは、DHCP が有効になっている場合だけ表示されます
MAC Address	##.##.##.##.##.## (##は 00 ~ FF)	Integrated Administrator の MAC アドレス

表 4-6 [Enclosure Information]画面のフィールドの説明 : [Date and Time]領域

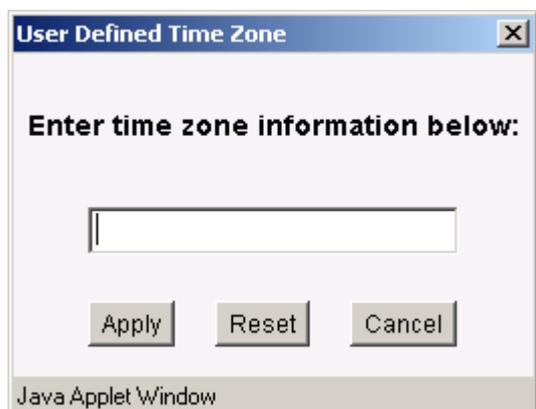
フィールド	可能な値	説明
[Date and Time]領域		
Time Zone	標準のタイムゾーンを一覧表示するドロップダウン ボックス	エンクロージャに割り当てられているタイムゾーン

表 4-6 [Enclosure Information]画面のフィールドの説明 : [Date and Time]領域 (続き)

		<p>初期設定のタイムゾーンについては、167 ページの「出荷時の設定」を参照してください</p> <p>サポートされているすべてのタイムゾーンの一覧については、170 ページの「タイムゾーンの設定」を参照してください</p> <p>エンクロージャのタイムゾーンをドロップダウンボックスにはない値に設定する方法の詳細な説明を表示するには、[Other]を選択します</p> <p>詳細については、159 ページの「トラブルシューティング」を参照してください</p>
Date	mm/dd/yy	エンクロージャに割り当てられている日付
Time	hh:mm (24 時間制)	エンクロージャに割り当てられている時間

エンクロージャ管理者だけが、**[Date and Time]**の情報にアクセスできます。これらのフィールドは、変更されている途中でなければ、Integrated Administratorによって20秒ごとに更新されます。自動時間設定が有効になっていると、日付と時間のフィールドはグレー表示になり、変更できません。

タイムゾーンの**[Other]**を選択した場合は、以下のウィンドウを使用してユーザ定義のタイムゾーンを設定します。



このウィンドウには、以下の3つのボタンが表示されます。

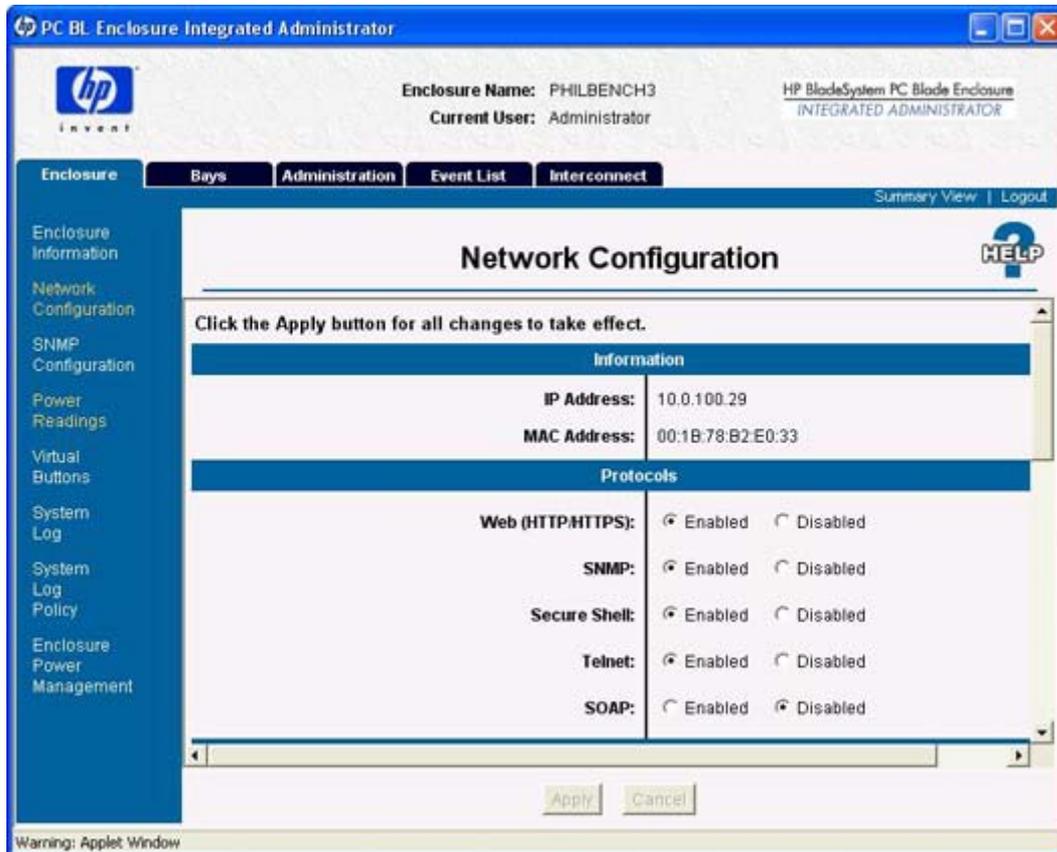
- **[Apply]** : 新しいタイムゾーンを適用します。
- **[Reset]** : タイムゾーンのテキストボックスを消去します。
- **[Cancel]** : すべての変更を取り消し、ウィンドウを閉じます。

使用可能なタイムゾーンについて詳しくは、[170 ページの「タイムゾーンの設定」](#)を参照してください。

Network Configuration

 **注記：** エンクロージャ管理者だけが、これらの設定にアクセスできます。

[Network Configuration]画面（以下の図を参照）では、エンクロージャ管理者がエンクロージャのネットワーク設定を変更できます。これらの設定はエンクロージャに固有であり、Blade PC のネットワーク設定には影響しません。



この画面の一番下には、以下の2つのボタンが表示されます。

- **[Apply]**：この画面に加えた変更を保存します。
- **[Cancel]**：この画面のすべてのフィールドを元の値に戻します。

△ **注意：** Web ベースのユーザ インタフェースへのアクセスを許可するには、Web プロトコルと Secure Shell プロトコルの両方が有効になっている必要があります。

以下の表では、[Network Configuration]画面の各領域に表示される情報について説明します。

表 4-7 [Network Configuration]画面のフィールドの説明：[Information]領域

フィールド	可能な値	説明
[Information]領域		
IP Address		Integrated Administrator の IP アドレス
MAC Address		Integrated Administrator の MAC アドレス

表 4-8 [Network Configuration]画面のフィールドの説明 : [Protocols]領域

フィールド	可能な値	説明
[Protocols]領域		
Web (HTTP/HTTPS)	有効または無効	初期設定は、「有効」です
SNMP	有効または無効	初期設定は、「有効」です
Secure Shell	有効または無効	初期設定は、「有効」です
Telnet	有効または無効	初期設定は、「有効」です
SOAP	有効または無効	初期設定は、「無効」です

表 4-9 [Network Configuration]画面のフィールドの説明 : [Network]領域

フィールド	可能な値	説明
[Network]領域		
DHCP		DHCP から Integrated Administrator の IP アドレスを取得します
Static IP		Integrated Administrator の静的 IP アドレスを設定します
Dynamic DNS		Integrated Administrator が動的 DNS を使用するかどうかを決定します
IP Address	###.###.###.### (###は 0 ~ 255)	Integrated Administrator の静的 IP アドレス ([Static IP]が選択されている場合は必須)
Subnet Mask	###.###.###.### (###は 0 ~ 255)	Integrated Administrator のサブネットマスク ([Static IP]が選択されている場合は必須)
Gateway Address	###.###.###.### (###は 0 ~ 255)	Integrated Administrator のゲートウェイアドレス ([Static IP]が選択されている場合はオプション)
DNS Server 1	###.###.###.### (###は 0 ~ 255)	プライマリ DNS サーバの IP アドレス ([Static IP]が選択されている場合はオプション)
DNS Server 2	###.###.###.### (###は 0 ~ 255)	セカンダリ DNS サーバの IP アドレス ([Static IP]が選択されている場合はオプション)

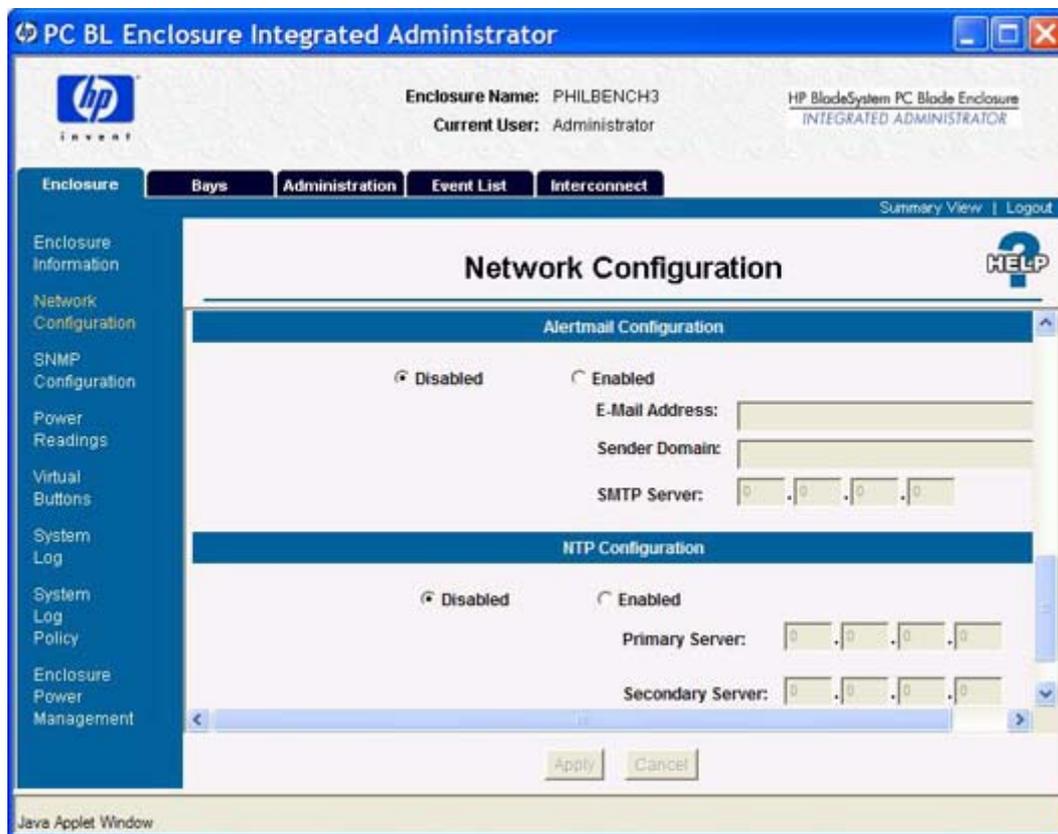


表 4-10 [Network Configuration]画面のフィールドの説明 : [Alertmail Configuration]領域

フィールド	可能な値	説明
[Alertmail Configuration]領域		
AlertMail	有効または無効	初期設定は、「無効」です
E-mail Address	すべての英数字、ハイフン、およびアンダースコアを含む最大 32 文字	送信者の電子メール アドレス
Sender Domain	すべての英数字、ハイフン、およびアンダースコアを含む最大 32 文字	送信者のドメイン
SMTP Server	###.###.###.### (###は 0 ~ 255)	SMTP サーバの IP アドレス

表 4-11 [Network Configuration]画面のフィールドの説明 : [NTP Configuration]領域

フィールド	可能な値	説明
[NTP Configuration]領域		
NTP	有効または無効	初期設定は、「無効」です
Primary Server	###.###.###.### (###は 0 ~ 255)	プライマリ NTP サーバの IP アドレス
Secondary Server	###.###.###.### (###は 0 ~ 255)	セカンダリ NTP サーバの IP アドレス
Poll Interval		

SNMP Configuration

[SNMP Configuration]画面（以下の図を参照）では、エンクロージャ管理者がエンクロージャのSNMP設定を変更できます。これらの設定はエンクロージャに固有であり、Blade PCのネットワーク設定には影響しません。

この画面の一番下には、以下の2つのボタンが表示されます。

- **[Apply]** : この画面に加えた変更を保存します。
- **[Cancel]** : この画面のすべてのフィールドを元の値に戻します。

以下の表では、[SNMP Configuration]画面に表示される情報について説明します。

表 4-12 [SNMP Configuration]画面のフィールドの説明 : [System Information]領域

フィールド	可能な値	説明
[System Information]領域		
SNMP Status	有効または無効	SNMPが有効または無効のどちらになっているかを表示します
System Name		エンクロージャの名前

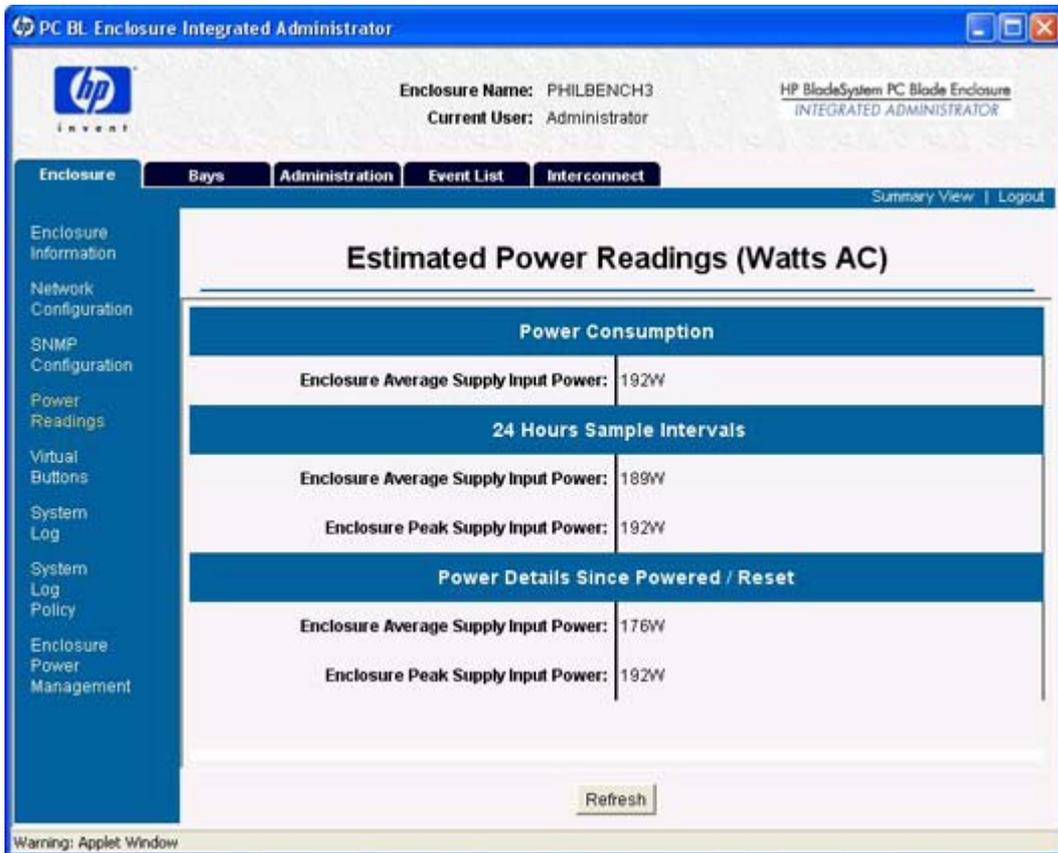
表 4-12 [SNMP Configuration]画面のフィールドの説明 : [System Information]領域 (続き)

System Location	すべての英数字、ハイフン、アンダースコア、@、およびスペースを含む最大 20 文字	エンクロージャの SNMP 位置 初期設定の SNMP の連絡先については、 167 ページの「出荷時の設定」 を参照してください
System Contact	すべての英数字、ハイフン、アンダースコア、およびスペースを含む最大 20 文字	エンクロージャの SNMP の連絡先 初期設定の SNMP の連絡先については、 167 ページの「出荷時の設定」 を参照してください

表 4-13 [SNMP Configuration]画面のフィールドの説明 : [Community Strings and Trap Destinations]領域

フィールド	可能な値	説明
[Community Strings and Trap Destinations]領域		
Read Community	すべての英数字、ハイフン、アンダースコア、およびスペースを含む最大 20 文字	SNMP の読み込みコミュニティ名を表示します このフィールドを空白のままにすると、「public」が割り当てられます 初期設定の読み込みコミュニティ名については、 167 ページの「出荷時の設定」 を参照してください
Write Community	すべての英数字、ハイフン、アンダースコア、およびスペースを含む最大 20 文字	SNMP の書き込みコミュニティ名を設定します このフィールドを空白のままにすると、SNMP SET コマンドは無効になります 初期設定の書き込みコミュニティ名については、 167 ページの「出荷時の設定」 を参照してください
Add		トラップ送信先の一覧に IP アドレスを追加します
Remove		トラップ送信先の一覧から、選択した IP アドレスを削除します

Power Readings



[Power Readings]画面では、エンクロージャの電力消費量の推定値を表示します。この画面には、以下のフィールドが含まれます。

☞ **注記：** [Power Readings]は、エンクロージャに、電力を認識しないブレードが存在する場合にのみ表示されます。これは、HP BladeSystem bc2x00 Blade PC のみの機能です。

実際の画面は、この画面と異なる場合があります。

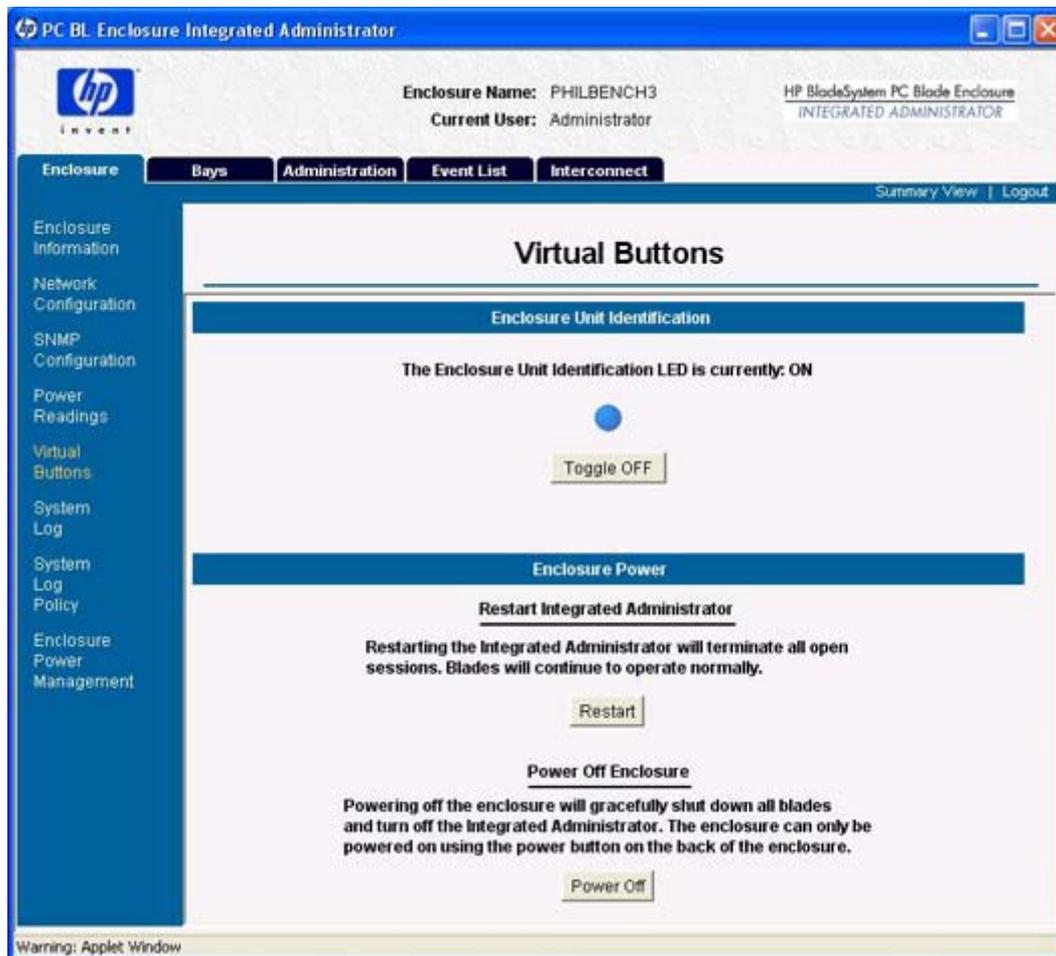
- **[Enclosure Average Supply Input Power]** : 直前の 5 秒間のサンプル間隔での平均電力消費量です。
- **[Enclosure Average Supply Input Power 24-Hour Sample Intervals]** : 直前の 24 時間の稼働時間での電力消費量のローリング平均です。
- **[Enclosure Peak Supply Input Power 24-Hour Sample Intervals]** : 直前の 24 時間の稼働時間での電力消費量のピークです。
- **[Enclosure Average Supply Input Power Time Averaged Since Powered]** : IA の総稼働時間での平均電力消費量です。これは、前回の再起動または IA のリセット以降の値です。
- **[Enclosure Peak Supply Input Power Time Averaged Since Powered]** : IA の総稼働時間での電力消費量のピークです。これは、前回の再起動または IA のリセット以降の値です。

☞ **注記：** すべての統計は、最後の再起動時から、最大を 24 時間として算出されます。

Virtual Buttons

 **注記：** エンクロージャ管理者だけが、これらのコマンドを実行できます。

[Virtual Buttons]画面（以下の図を参照）では、データ センタ内の技術者によるトラブルシューティングを容易にするために、エンクロージャ管理者がエンクロージャの電源状態やユニット確認ランプをリモート サイトから変更できます。



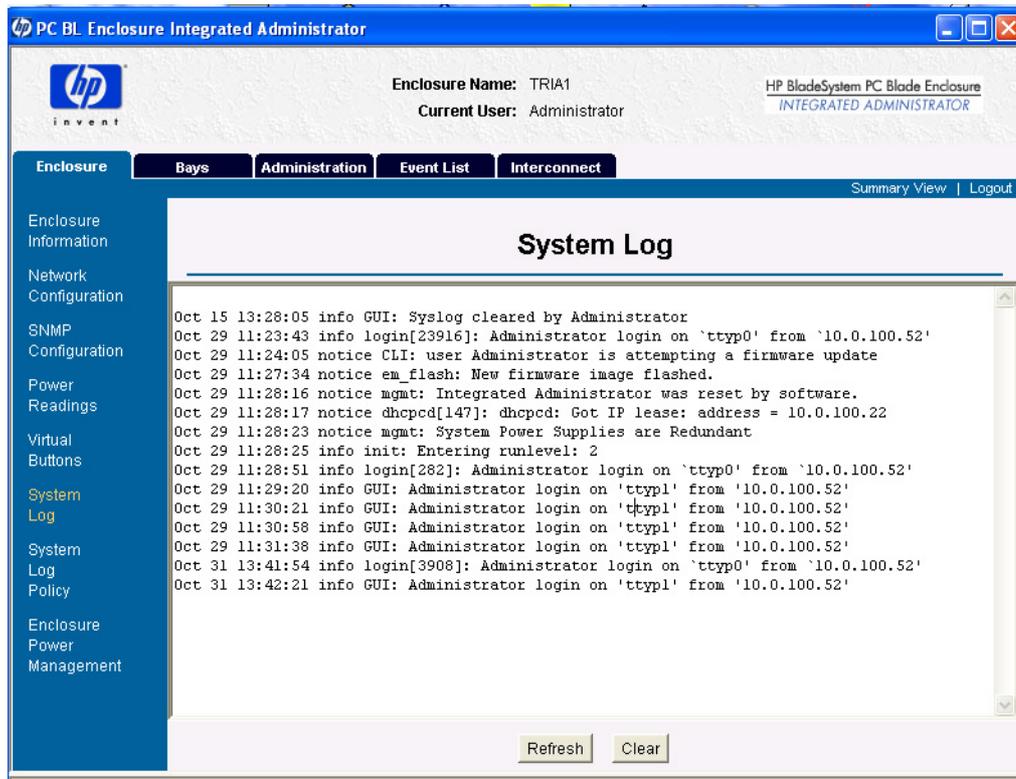
[Toggle On/Toggle Off]ボタンは、エンクロージャのユニット確認ランプの状態をリモートで変更します。以下の図は、[Virtual Buttons]画面の[Enclosure Power]領域に表示される情報を示しています。

以下のボタンを使用して、該当する機能を選択できます。

- **[Restart Integrated Administrator]** : Integrated Administrator を再起動します。Blade PC には影響しません。
 - **[Power Off Enclosure]** : システムの正常なシャットダウンを5分間試みます。それが経過するとただちに、このコマンドによってエンクロージャのすべてのコンポーネントの電源が切られます。
- △ **注意：** オペレーティング システムのシャットダウン手順を実行してから Blade PC またはエンクロージャの電源を切ることをおすすめします。エンクロージャの電源を切ると、システムにローカル アクセスしない限り電源を入れられません。

System Log

[System Log]画面（以下の図を参照）では、エンクロージャ管理者がエンクロージャに関連したイベントと更新の一覧を発生順に表示できます。

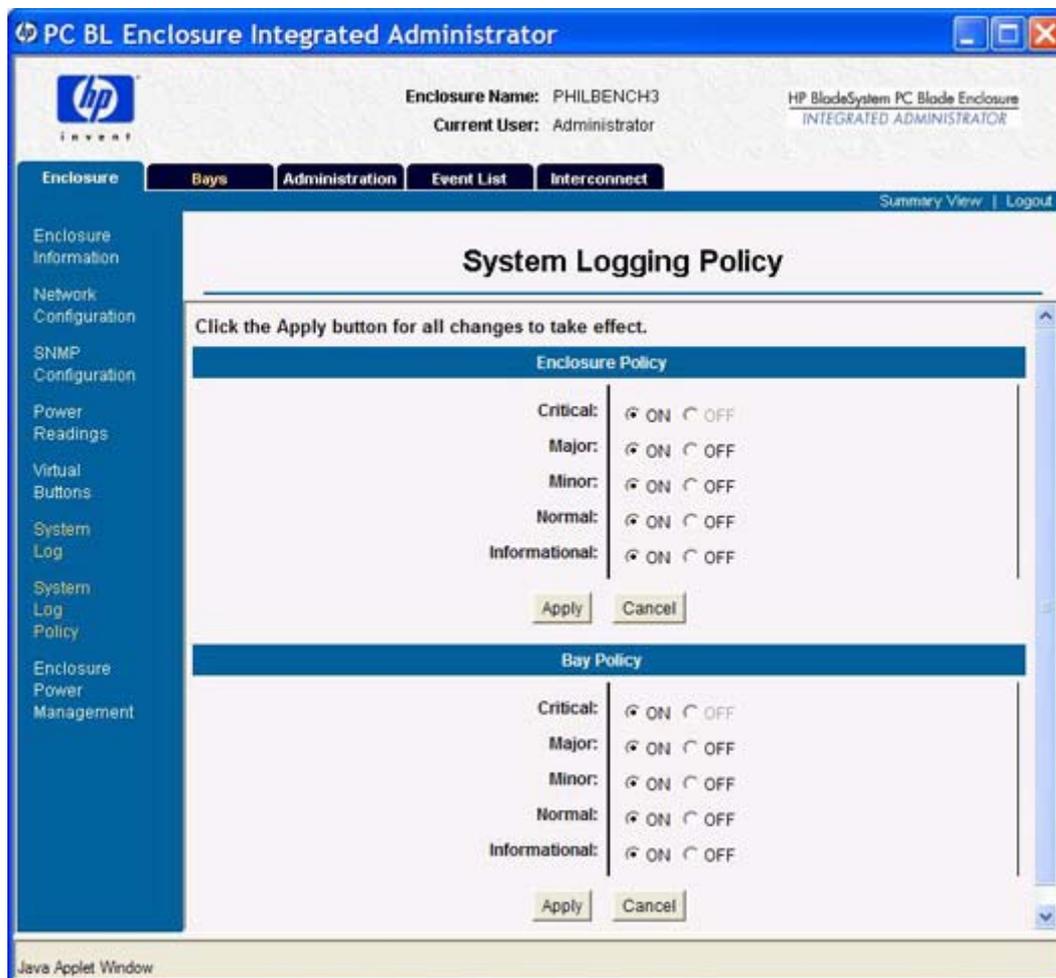


この画面の一番下には、以下の2つのボタンが表示されます。

- [Refresh] : 画面の表示を更新します。
- [Clear] : システム ログを消去します。

System Log Policy

[System Log Policy]画面（以下の図を参照）では、エンクロージャ管理者が、システム ログに記録された任意のイベント メッセージのログを表示および制御できます。



エンクロージャおよびベイのシステム ログ ポリシーに対応した、各イベントの重大度を分類するための2つのラジオ ボタンがあります。

- **[Critical]** : ON または OFF

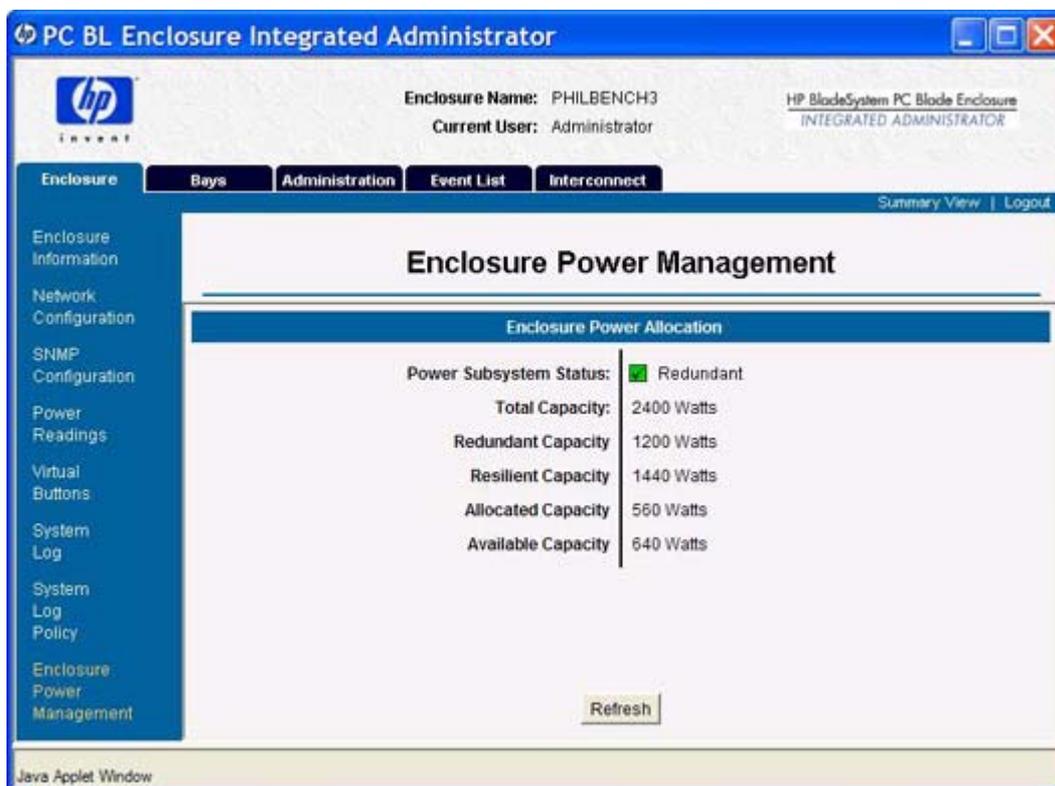
 **注記** : エンクロージャおよびベイの重要な syslog メッセージをマスクすることはできません。

- **[Major]** : ON または OFF
- **[Minor]** : ON または OFF
- **[Normal]** : ON または OFF
- **[Informational]** : ON または OFF

[Informational]の初期設定は、**[OFF]**です。他のすべてのエンクロージャおよびベイのシステム ログ ポリシーは、初期設定では**[ON]**になっています。

具体的なシステム ログ メッセージの詳細については、[144 ページの「エラー メッセージ」](#)で、サポートされているシステム ログ メッセージおよび重大度の分類を参照してください。

[Enclosure Power Management]タブ



このタブには、電源管理に関する電源サブシステムの情報が表示されます。ステータスと容量の値は以下のとおりです。

表 4-14 電源管理の値

表示情報	説明	可能な値
Power Subsystem Status	現在の電源サブシステムの状態	リダンダント、レジリエント、レジリエント（スロットリング）、非リダンダント、および非リダンダント（スロットリング）
Total Capacity	各電源装置の定常状態でのリダンダント容量の合計（ワット）	PC Blade エンクロージャ G2 <ul style="list-style-type: none"> 1つあたり 220 V=2400 W 1つあたり 110V=1800 W 1つあたり 100V=1600 W PC Blade エンクロージャ <ul style="list-style-type: none"> 1200 W
Redundant Capacity	この値は、エンクロージャ内にある、最も出力が低い電源装置の最大定格出力容量です。そのため、この数値は電源装置間で均一にならない可能性があります	PC Blade エンクロージャ G2 <ul style="list-style-type: none"> 1つあたり 220 V=1200 W 1つあたり 110 V=900 W 1つあたり 100 V=800 W

表 4-14 電源管理の値（続き）

表示情報	説明	可能な値
		PC Blade エンクロージャ <ul style="list-style-type: none"> 600 W
Resilient Capacity	この値は、すべての電源装置のリダンダント電源の制限値を超える場合の、電源容量の最大値です。この値は、エンクロージャ内のすべてのデバイスを確実に動作させるためにエンクロージャの電源容量を割り当てる場合に、安全な超過値の範囲での最大値を表します	PC Blade エンクロージャ G2 <ul style="list-style-type: none"> 1つあたり 220 V=1440 W 1つあたり 110V=1080 W 1つあたり 100V=960 W PC Blade エンクロージャ <ul style="list-style-type: none"> 827 W
Allocated Capacity	ブレードおよびエンクロージャの現在の設定に基づいて計算された、割り当て可能な最大電力です。IAはこの数値を使用して、エンクロージャの電源設定を変更する場合に実行可能な動作を決定します	可変値（ワット）
Available Capacity	Redundant Capacity から Allocated Capacity を引いた値	可変値（ワット）

詳しくは、[164 ページの「電源管理およびリダンダント電源装置」](#)を参照してください。

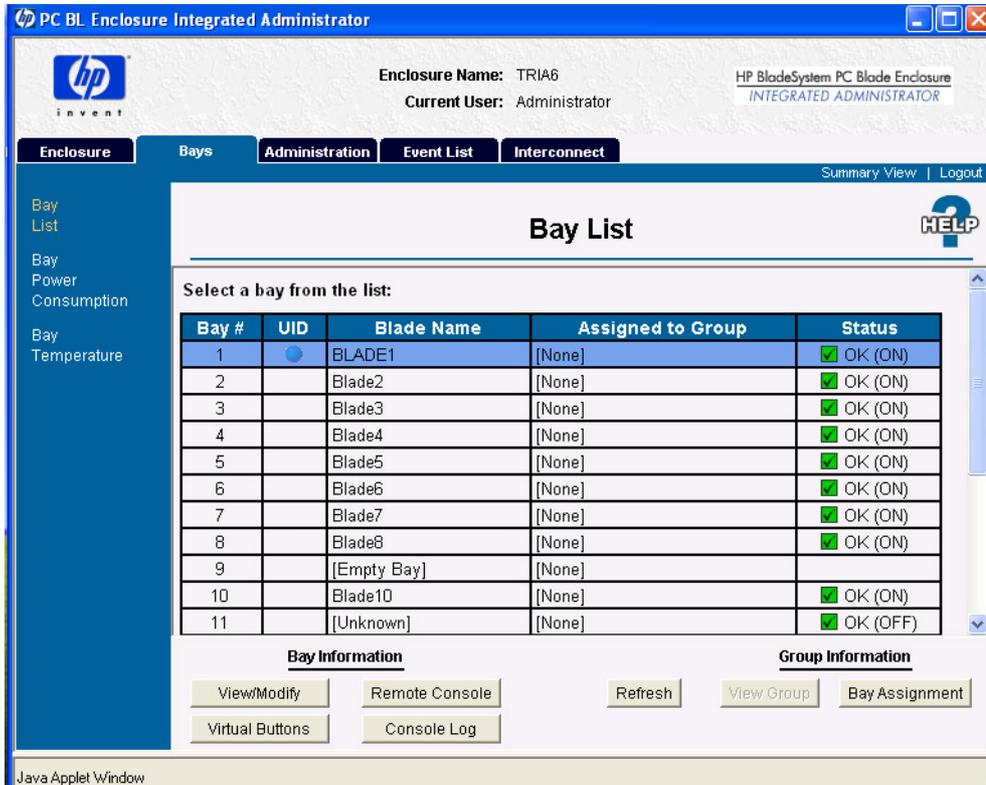
[Bays]タブ

[Bays]タブからは、以下の画面にアクセスできます。

- Bay List
- Bay Information
- Remote Console
- Virtual Buttons
- Console Log
- Bay Power Consumption

Bay List

[Bay List]画面（以下の図を参照）では、エンクロージャ管理者が Blade PC ベイへのグループの割り当てを確認および更新したり、エンクロージャに取り付けられている各 Blade PC のステータスを監視したりできます。



グループ管理者とアクセス権を持つグループメンバは、そのグループに割り当てられた Blade PC ベイを表示できます。

以下の表では、[Bay List]画面に表示される情報について説明します。

表 4-15 [Bay List]画面のフィールドの説明

フィールド	可能な値	説明
Bay #	1 ~ 20	Blade PC の番号
UID		ブレードのユニット確認 (UID) ランプが点灯すると、青い丸が表示されます
Blade PC Name		Blade PC のオペレーティング システムで定義されている、Blade PC ベイ内の Blade PC の名前 注記： Integrated Administrator が、Blade PC 名およびオペレーティング システムの種類を取得できるようにするには、Blade PC のヘルス サービスをインストールする必要があります
Assigned to Group		そのベイを所有するグループの名前
Status	OK、劣化、または障害	Blade PC のステータスおよび電源状態

以下の表では、[Bay List]画面の操作ボタンに関連するアクセス権を一覧表示します。

表 4-16 [Bay List]画面の操作ボタンとアクセス権

フィールド	可能な値	説明
-------	------	----

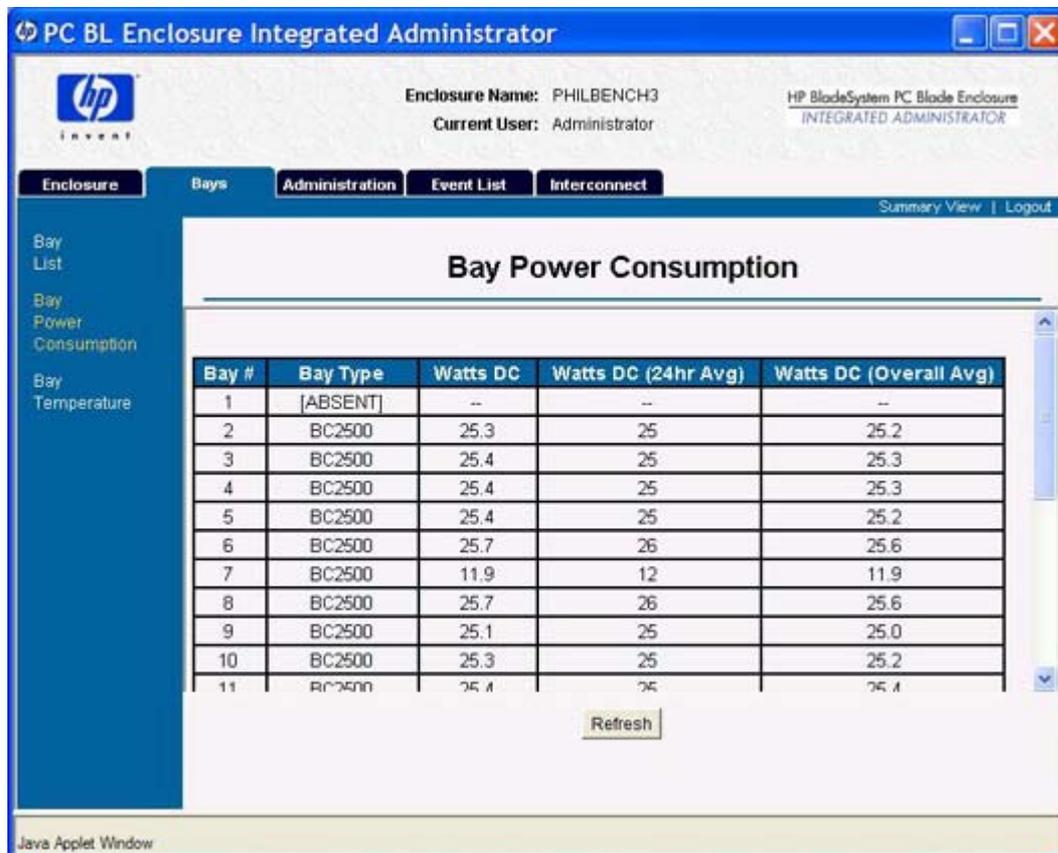
表 4-16 Bay List 画面の操作ボタンとアクセス権 (続き)

View/Modify	[Blade Information]画面を開きます	エンクロージャ管理者、グループ管理者、およびアクセス権を持つグループメンバ
Remote Console	[Remote Console]画面を開きます	エンクロージャ管理者およびアクセス権を持つグループ管理者
Console Log	[Console Log]画面を開きます	エンクロージャ管理者、グループ管理者、およびアクセス権を持つグループメンバ
View Group	[View/Modify Group]画面を開きます	エンクロージャ管理者のみ
Bay Assignment	[Bay Assignment]ダイアログ ボックスを開きます	エンクロージャ管理者のみ

注記： Blade PC を再割り当てする場合は、まず、その Blade PC の割り当てを解除する必要があります

Bay Power Consumption

[Bay Power Consumption]画面 (以下の図を参照) では、エンクロージャの管理者が、エンクロージャ内のブレードが取り付けられているすべてのベイの電力消費量を監視できます。



この表には、以下の情報が示されます。

- **[Bay #]**
- **[Bay Type]** : bc2x00 ブレードだけが電力を認識し、IA に電力量をレポートするため、これを確認するために必要です。
- **[WDC]** : 直前の 1 秒間のサンプリング間隔での、ブレードの平均直流 (DC) 電力消費量 (ワット) です。
- **[WDC (24hr Avg.)]** : エンクロージャ内の直近の 24 時間の稼働時間での、ブレードの平均直流 (DC) 電力消費量 (ワット) です。
- **[WDC (Overall Avg.)]** : エンクロージャ内の直前の 24 時間の稼働時間での、ブレードの平均直流 (DC) 電力消費量 (ワット) です。

 **注記** : 電力消費量のレポートは、bc2x00 シリーズのブレードのみに備えられている機能です。その他のブレードでは、電力消費量に関する列の値はレポートされません。

[Unknown] は、ブレードが初期 POST 送信を完了していないことを示します。

すべての統計は、最後の再起動時から、最大を 24 時間として算出されます。

Bay Temperature

[Bay Temperature]画面では、特定の Blade PC ベイにある Blade PC の周辺温度を管理者が確認できます。また、Blade PC ベイへの表示アクセス権を持つグループ管理者とグループ メンバもこの情報を確認できます。

Bay #	Bay Type	CPU C/F	Graphics C/F	Ambient C/F
1	[ABSENT]	--	--	--
2	BC2500	41.0 / 105.8	49.0 / 120.2	28.0 / 82.4
3	BC2500	40.0 / 104.0	48.5 / 119.3	28.0 / 82.4
4	BC2500	41.0 / 105.8	50.0 / 122.0	29.5 / 85.1
5	BC2500	40.0 / 104.0	51.0 / 123.8	29.5 / 85.1
6	BC2500	41.0 / 105.8	51.5 / 124.7	29.5 / 85.1
7	BC2500	29.0 / 84.2	34.0 / 93.2	25.0 / 77.0
8	BC2500	43.0 / 109.4	54.0 / 129.2	30.5 / 86.9
9	BC2500	43.0 / 109.4	53.0 / 127.4	30.0 / 86.0
10	BC2500	43.5 / 110.3	53.0 / 127.4	30.5 / 86.9
11	BC2500	40.5 / 104.9	52.5 / 126.5	30.5 / 86.9
12	BC2500	43.5 / 110.3	54.0 / 129.2	31.5 / 88.7
13	BC2500	43.5 / 110.3	54.5 / 130.1	31.0 / 87.8
14	BC2500	43.5 / 110.3	55.5 / 131.9	31.5 / 88.7
15	BC2500	46.5 / 115.7	57.0 / 134.6	32.0 / 89.6

表 4-17 [Bay Temperature]画面のフィールドの説明

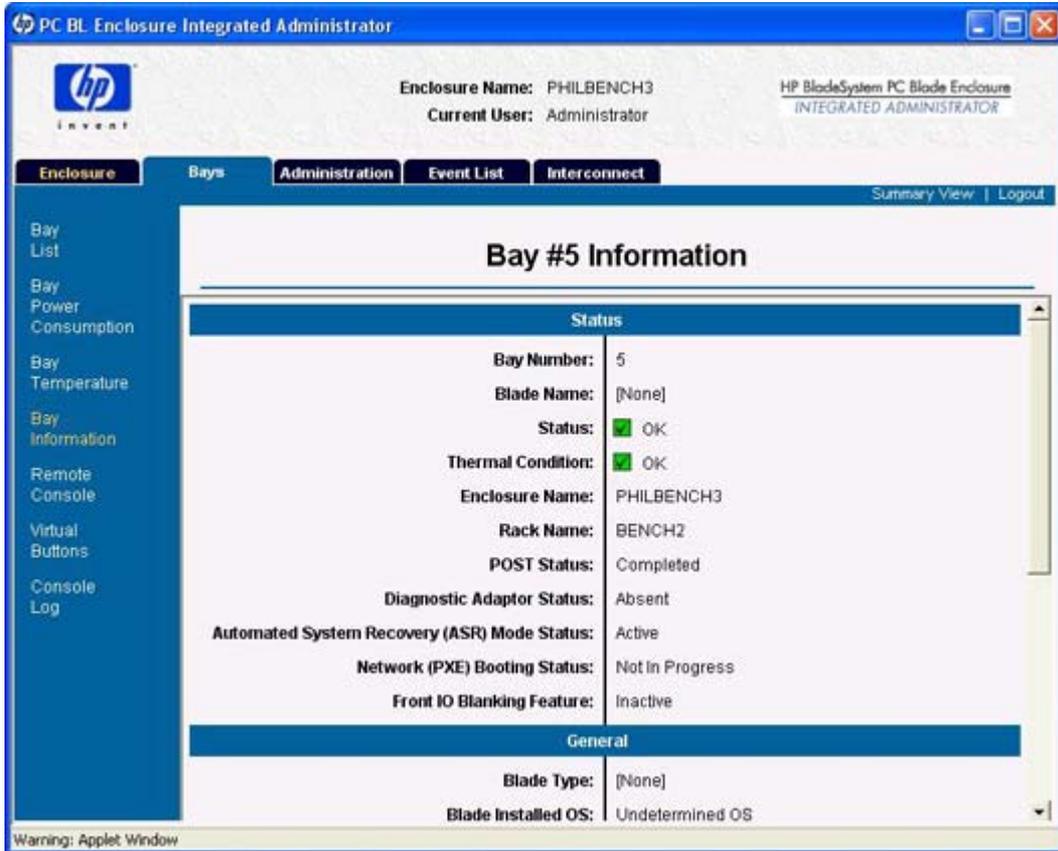
フィールド	可能な値	説明
Bay #		ベイ番号
Bay Type		ベイの種類
CPU C/F		CPU の温度 (□)
Graphics C/F		GPU の温度 (□)
Ambient C/F		ベイの周辺温度 (□)

Bay Information

- ☞ **注記：** Blade PC のヘルス サービスをインストールしてから Blade PC を再起動すると、Integrated Administrator に最新の Blade PC 情報が表示されることを確認してください。Integrated Administrator を完全に更新するには、Blade PC を 2 回再起動する必要があります。

[Bay Information]画面（以下の図を参照）では、エンクローージャ管理者が特定の Blade PC ベイ内の Blade PC のステータスや一般的な情報を確認できます。また、Blade PC ベイへの表示アクセス権を持つグループ管理者とグループ メンバもこの情報を確認できます。

- ☞ **注記：** BIOS 3.x を搭載した bc2x00 ブレードには、追加の情報フィールドがあります。



[Bay Information]画面に、可能な値が最適な数だけ確実に表示されるようにするには、Blade PC にヘルス ドライバをインストールしておく必要があります。

以下の表では、すべてのエンクロージャ管理者と、Blade PC ベイへのアクセス権を持つグループ メンバおよびグループに対して [Bay Information] 画面に表示される情報について説明します。

表 4-18 [Bay Information]画面のフィールドの説明 : [Status]領域

フィールド	可能な値	説明
[Status]領域		
Bay Number		ベイ番号
Blade PC Name		Blade PC のオペレーティング システムで指定されている Blade PC の名前
Status	OK、劣化、または障害	Blade PC のステータス 注記： bc2x00 ブレードで障害が発生した場合または bc2x00 ブレードが劣化した場合、追加の診断メッセージがここで囲まれてポストされます
Thermal Condition	OK、温度上昇、注意、または重大	ブレードの温度状態 注記： 温度状態が重大または注意の場合、bc2x00 ブレードは、障害検出時点の CPU、グラフィックス プロセッサ、および周辺温度センサの温度測定結果を摂氏で示します
Enclosure Name		エンクロージャの名前

表 4-18 [Bay Information]画面のフィールドの説明 : [Status]領域 (続き)

		初期設定のエンクロージャ名については、167 ページの「出荷時の設定」を参照してください
Rack Name		ラックの名前
POST Status	開始、完了、オフ	ブレードの POST (Power-On Self Test) ステータス。BIOS 3 シリーズを搭載した bc2x00 ブレードの場合にのみ表示されます
Diagnostic Adaptor Status	あり、なし、N/A (オフ)	ブレードの診断アダプタが Blade PC の前面 I/O コネクタに取り付けられているかどうかを示します。この状態インジケータは、ブレードの電源がオンの場合にのみ有効です。BIOS 3 シリーズを搭載した bc2x00 ブレードの場合にのみ表示されます
Automated System Recovery (ASR) Mode Status	有効、無効、N/A (オフ)	自動システム復旧 (ASR) モードが有効と無効のどちらになっているかを示します。この状態インジケータは、ブレードの電源がオンの場合にのみ有効です。BIOS 3 シリーズを搭載した bc2x00 ブレードの場合にのみ表示されます
Network (PXE) Booting Status	実行中、停止中、N/A (オフ)	ブレードが現在ネットワークのブート前セキュリティ (PXE) モードになっているかどうかを示します。この状態インジケータは、ブレードの電源がオンの場合にのみ有効です。BIOS 3 シリーズを搭載した bc2x00 ブレードの場合にのみ表示されます
Front IO Blanking Feature Status	有効、無効、N/A (オフ)	前面 I/O が無効になっているブレードをユーザが使用する場合に、そのブレードがセッションのプライバシーを許可するかどうかを示します。この状態インジケータは、ブレードの電源がオンの場合にのみ有効です。BIOS 3 シリーズを搭載した bc2x00 ブレードの場合にのみ表示されます

表 4-19 [Bay Information]画面のフィールドの説明 : [General]領域

フィールド	可能な値	説明
[General]領域		
Blade PC Type		Blade PC の製品名
Blade PC Installed OS		Blade PC にインストールされているオペレーティング システム
Spare Number		Blade PC のスペア番号
Serial Number		Blade PC のシリアル番号
Asset Tag		Blade PC のアセット タグ番号
BIOS Version	mm/dd/yy	Blade PC の ROM バージョン
CPU # Type		Blade PC のプロセッサの種類
CPU # Max Speed		Blade PC のプロセッサに関連した速度

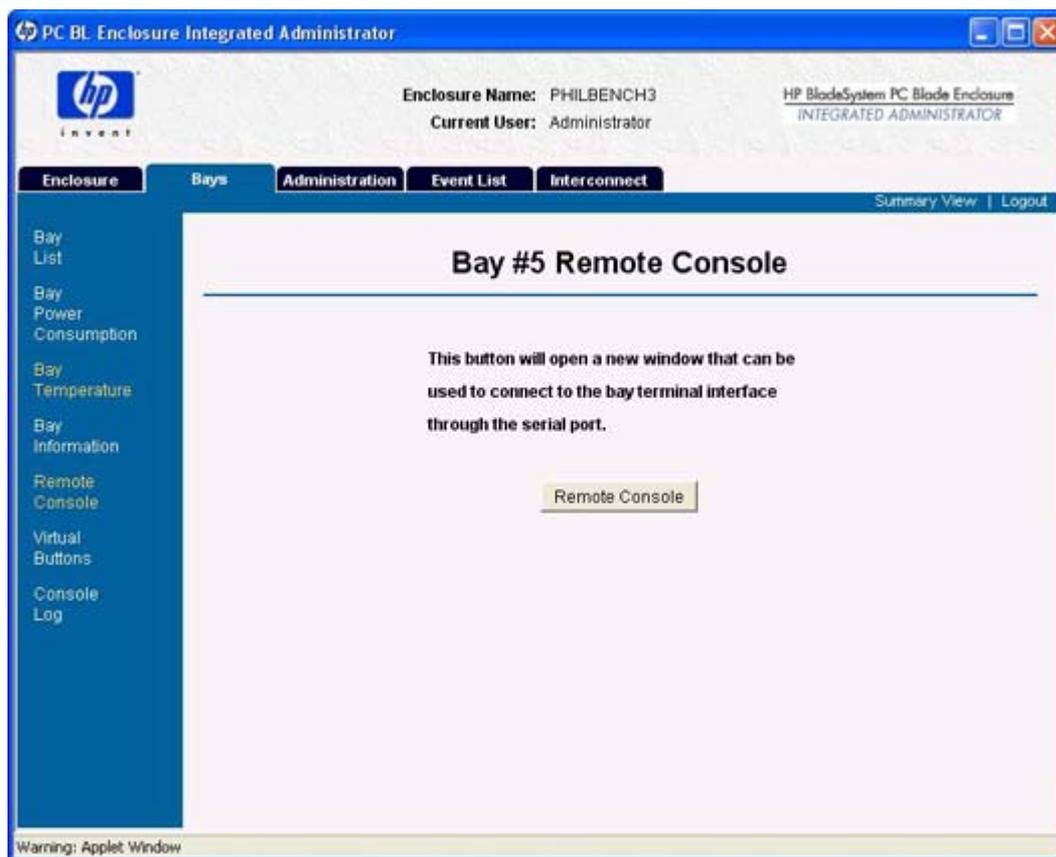
表 4-19 [Bay Information]画面のフィールドの説明 : [General]領域 (続き)

Installed RAM		Blade PC に実装されているメモリ容量
NIC #1 and #2 MAC Addresses	###:###:###:### (##は 00 ~ FF)	NIC 1 インタフェースと NIC 2 インタフェースの MAC アドレス
BMC Revision	00 ~ FF	BMC Revision : bc2x00 ブレードの場合は、BMC (Blade Management Controller) リビジョンがここにポストされます。バージョン 23 以前の BMC バージョンでは、BMC Revision の値はレポートされません。N/A がここに囲まれて表示されます。BMC の将来のバージョンでは、この情報が提供されません
Universal Unique Identifier (UUID)		UUID (Universal Unique Identifier) です。BIOS 3 シリーズを搭載した bc2x00 ブレードの場合にのみ表示されます

Remote Console

エンクロージャ管理者とベイへのアクセス権を持つグループ管理者は、[Remote Console]をクリックして、ベイ内の Blade PC へのテキストベースのリモート コンソール (以下の図を参照) を開くことができます。

注記 : コマンド ウィンドウをクリックして、フォーカスがあることを確認してください。フォーカスがない場合、コマンドを入力できません。



リモート コンソール接続を確立する方法については、[101 ページの「Blade PC へのリモート コンソール セッションの有効化」](#)を参照してください。

Virtual Buttons

エンクロージャ管理者とアクセス権を持つグループ管理者は、[Virtual Buttons]画面（以下の図を参照）を使用して、リモート サイトからのトラブルシューティングを容易にするために、Blade PC の電源状態とユニット確認ランプを変更することができます。



[Virtual Buttons]画面では、グループ管理者とエンクロージャ管理者が以下の機能を使用して Blade PC の再起動、電源切断、または確認を行うことができます。

- [Toggle On/Toggle Off] ボタンは、Blade PC のユニット確認ランプの状態をリモートで変更します。
- 以下のラジオ ボタンを使用して、[Blade PC Power]領域にある該当する機能を選択できます。
 - [Reboot]は、Blade PC を再起動します。
 - [Power Off]は、Blade PC の正常なシャットダウンを 5 分間試みます。それが経過するとただちに、このコマンドによって Blade PC の電源が切られます。これは、標準のデスクトップ PC で、3 秒未満の間電源ボタンを押した場合と同じ動作です。
 - [Power Off Immediately]は、強制的に Blade PC の電源を切ります。これは、標準のデスクトップ PC で、5 秒間電源ボタンを押した場合と同じ動作です。

△ **注意：** サービスとして、ACPI 準拠のオペレーティング システムがないと、Integrated Administrator は Blade PC を正しくシャットダウンできません。この状態が発生すると、データが永久に失われる場合があります。

 **注記：** これらの設定を有効にするには、[Apply]をクリックします。

可能な場合は常に、オペレーティング システムのシャットダウン手順を実行してから Blade PC またはエンクロージャの電源を切ることをおすすめします。エンクロージャの電源を切ると、システムにローカル アクセスしない限り電源を入れられません。

Console Log

 **注記：** グループ メンバ、グループ管理者、およびエンクロージャ管理者だけが、Blade PC のコンソール ログを表示できます。

[Console Log]画面には、指定したベイのコンソール ログが表示されます。ベイのコンソール ログは Integrated Administrator を再起動したときに保存されないため、この情報には Integrated Administrator の最後の電源投入以降に発生した内容だけが含まれます。

コンソール ログに取得されたデータは、コンソールに接続されているユーザがいない間に発生した、Blade PC のシリアル コンソールからのすべての出力です。セキュリティ上の理由から、ユーザ接続セッション中のコンソール出力は記録されません。

[Refresh]ボタンは、現在の Blade PC のコンソール ログの表示を更新します。

[Administration]タブ

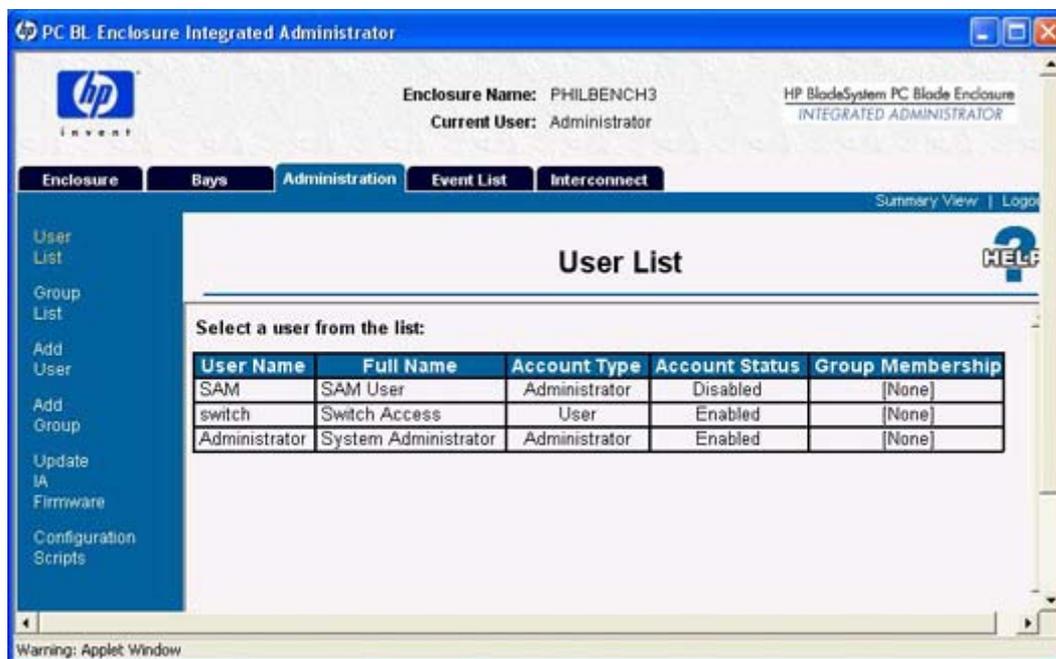
Integrated Administrator に関連したユーザ アクセス権については、[101 ページの「Blade PC へのリモート コンソール セッションの有効化」](#)を参照してください。

[Administration]タブからは、以下の画面にアクセスできます。

- User List
- Group List
- Add User
- Add Group
- View/Modify User
- View/Modify Group

User List

[User List]画面（以下の図を参照）では、該当するグループ管理者またはエンクロージャ管理者が、グループと Blade PC ベイへのユーザ アクセスを確認および更新することができます。



以下の表では、[User List]画面の操作ボタンに関連するアクセス権を一覧表示します。

表 4-20 [User List]画面の操作ボタンとアクセス権

ボタン	機能	アクセス権
-----	----	-------

表 4-20 User List 画面の操作ボタンとアクセス権 (続き)

View/Modify User	[View/Modify User]画面を開きます	エンクロージャ管理者は、任意のユーザの 情報にアクセスし、その情報を変更す ることができます ユーザは、自分のアカウントの情報にア クセスし、その情報を変更することが できます
Remove User	選択したユーザを削除します (アカウン トが本人のものでない場合)	エンクロージャ管理者だけが、このコマ ンドを実行できます

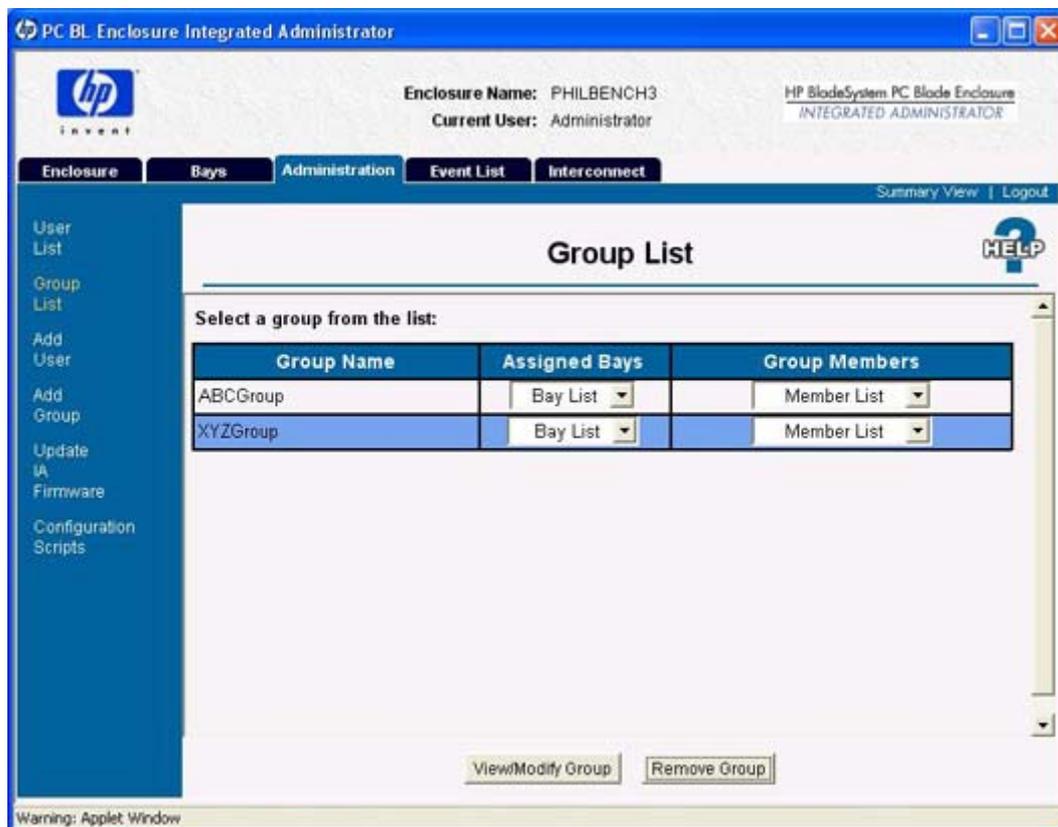
以下の表では、[User List]画面に表示される情報について説明します。

表 4-21 [User List]画面のフィールドの説明

ボタン	機能	アクセス権
User Name		ユーザのログイン名
Full Name		ユーザのフルネーム
Account Type	管理者またはユーザ	ユーザがエンクロージャ管理者であるか どうかを示します
Account Status	有効または無効	ユーザのアカウントが有効であるかどう かを示します
Group Membership		そのユーザがメンバになっているグルー プを示します

Group List

[Group List]画面 (以下の図を参照) では、エンクロージャ管理者が Blade PC ベイへのグループとユーザの割り当てを確認および更新することができます。



この画面には、以下の2つのボタンが表示されます。

- **[View/Modify Group]** : [View/Modify Group]画面を開きます。
- **[Remove Group]** : 選択したグループを削除します。

 **注記** : エンクロージャ管理者は、すべてのグループの情報を表示および変更することができます。グループ管理者とグループメンバは、自分がメンバになっているグループの情報を表示できます。

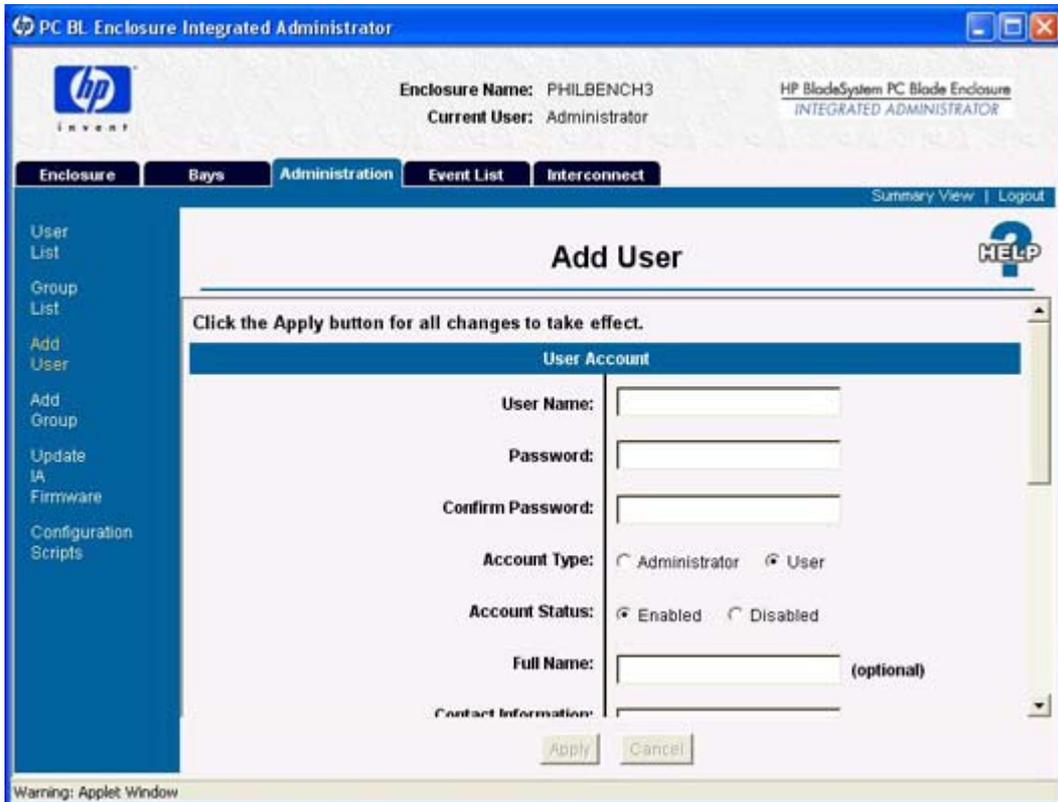
表 4-22 [Group List]画面のフィールドの説明

フィールド	説明
Group Name	グループ名
Assigned Bays	そのグループが所有する Blade PC ベイ
Group Members	そのグループのメンバになっているユーザ

Add User

 **注記** : エンクロージャ管理者だけが、Integrated Administrator のこの領域にアクセスできます。

[Add User]画面（以下の図を参照）では、エンクロージャ管理者がグループや Blade PC ベイの割り当てなどのユーザ プロファイルを作成できます。



この画面には、以下の2つのボタンが表示されます。

- **[Apply]** : この画面に加えた変更を保存します。
- **[Cancel]** : この画面のすべてのフィールドを元の値に戻します。

以下の表では、[Add User]画面のフィールドについて説明します。

表 4-23 [Add User]画面のフィールドの説明

フィールド	可能な値	説明
User Name	英数字、ハイフン、およびアンダースコア文字を含む1～13文字 ユーザ名は、英字で始まる必要があります。予約済みのアカウントに加えて、最大25ユーザを作成できます	ユーザのログイン名 注記 : 「Administrator」、「switch」、「switcha」、「switchb」、「SAM」および「all」は予約済みの名前であり、使用できません。この制限事項については、大文字と小文字は区別されません
Password	すべての印刷可能文字を含む3～8文字	ユーザのパスワード
Confirm Password	すべての印刷可能文字を含む3～8文字	ユーザのパスワード
Account Type	ラジオ ボタン (管理者およびユーザ)	ユーザがエンクロージャ管理者のアクセス権を持つかどうかを指定します
Account Status	ラジオ ボタン (有効および無効)	ユーザのアカウントが有効であるかどうかを指定します
Full Name (オプション)	1～20文字 英数字、ハイフン、アンダースコア、およびスペースだけが使用可能です	ユーザのフル ネーム

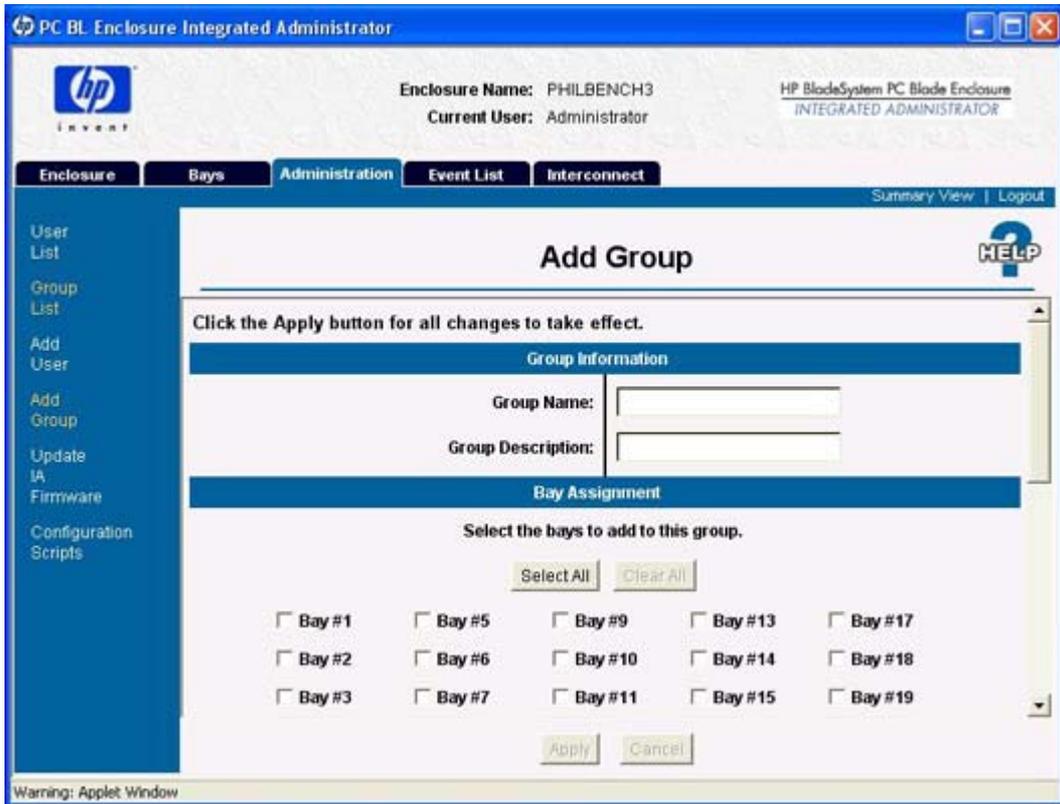
表 4-23 [Add User]画面のフィールドの説明 (続き)

Contact Information (オプション)	1 ~ 20 文字 英数字、ハイフン、アンダースコア、およびスペースだけが使用可能です	オプションのユーザ連絡先情報
Group Names	すべてのグループが一覧表示されます	可能性のあるすべてのグループの一覧
Group Membership	グループの数 (そのユーザがメンバになっているすべてのグループ)	そのユーザがメンバになっているすべてのグループの一覧
Add User [View]>>>		[Group Names] テキスト ボックスで選択したグループに、グループ メンバ用の表示アクセス権を持った状態でユーザを追加します これらのグループは、 [Group Membership] テキスト ボックスに表示されます。ユーザが以前に表示/変更アクセス権を持っていた場合は、そのアクセス権を失います
Add User [View/Modify]>>>		[Group Names] テキスト ボックスで選択したグループに、グループ管理用の表示/変更アクセス権またはグループ メンバ用の表示アクセス権を持った状態でユーザを追加します
<<<		[Group Membership] テキスト ボックスで選択したグループから、ユーザを削除します

Add Group

 **注記:** エンクロージャ管理者だけが、Integrated Administrator のこの領域にアクセスできます。

[Add Group]画面 (以下の図を参照) では、エンクロージャ管理者がユーザや Blade PC ベイの割り当てなどのグループ プロファイルを作成できます。



注記： グレー表示になっているチェック ボックスは、すでに別のグループに割り当てられているため使用できません。

この画面には、以下の2つのボタンが表示されます。

- **[Apply]**：この画面に加えた変更を保存します。
- **[Cancel]**：この画面のすべてのフィールドを元の値に戻します。

表 4-24 [Add Group]画面のフィールドの説明：[Group Information]領域

フィールド	可能な値	説明
[Group Information]領域		
Group Name	英数字、ハイフン、およびアンダースコアを含む1～13文字 グループ名は、英字で始まる必要があります。最大20グループを作成できます	グループの名前
Group Description (オプション)	1～20文字 英数字、ハイフン、およびアンダースコアだけが使用可能です	グループの説明

表 4-25 [Add Group]画面のフィールドの説明：[Bay Assignment]領域

フィールド	可能な値	説明
[Bay Assignment]領域		
Bay 1～Bay 20		グループが所有するベイを指定します

表 4-25 [Add Group]画面のフィールドの説明 : [Bay Assignment]領域 (続き)

		1つのグループだけが特定のベイを所有できます。チェック ボックスが無効になっているベイは、すでに別のグループが所有しています
Select All		すべてのベイのチェック ボックスにチェックを入れます
Clear All		すべてのベイのチェック ボックスのチェックを外します

表 4-26 [Add Group]画面のフィールドの説明 : [Group Membership]領域

フィールド	可能な値	説明
[Group Membership]領域		
User Names	すべてのユーザとエンクロージャ管理者が一覧表示されます	可能性のあるすべてのユーザの一覧
Group Members	ユーザの数 (そのグループのメンバであるすべてのユーザ)	そのグループのメンバであるすべてのユーザの一覧
Add User [View]>>>		[User Names] テキスト ボックスで選択したユーザを、グループ メンバ用の表示アクセス権を持った状態でグループに追加します ユーザが以前に管理者用の表示/変更アクセス権を持っていた場合は、そのアクセス権を失います
Add User [View/Modify]>>>		[User Names] テキスト ボックスで選択したユーザを、グループ管理者用の表示/変更アクセス権を持った状態でグループに追加します
<<<Remove User		[Group Members] テキスト ボックスで選択したユーザをグループから削除します

View/Modify User

[View/Modify User]画面にアクセスするには、[User List]内の任意の行をクリックしてから、[View/Modify User]をクリックします。[View/Modify User]画面では、[Add User]画面と同じ機能および同じアクセス方法が提供されます。この章の「Add User」の項を参照してください。

View/Modify Group

[View/Modify Group]画面にアクセスするには、[Group List]内の任意の行をクリックしてから[View/Modify Group]をクリックします。[View/Modify Group]画面では、[Add Group]画面と同じ機能および同じアクセス方法が提供されます。この章の[50 ページの「Add Group」](#)を参照してください。

IA ファームウェアの更新

[Update IA Firmware]画面には、ファームウェアの情報が表示されます。

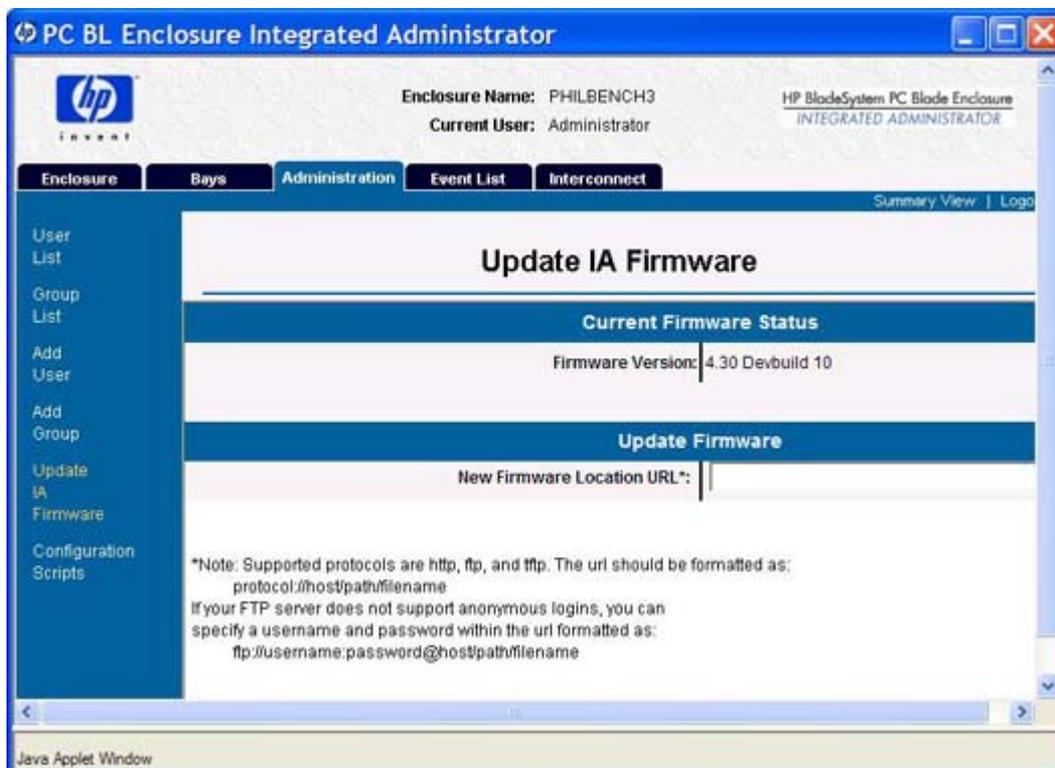


表 4-27 [Update IA Firmware]画面のフィールドの説明

フィールド	可能な値	説明
[Current Firmware Status]領域		
Firmware Version		ファームウェアのバージョン
Update Firmware		
New Firmware Location URL		新しいファームウェアの URL

注記： 特定のファイル拡張子の MIME タイプ (.rom など) が「application/octet-stream」として処理されるようにするには、IIS マネージャの更新が必要な場合があります。

Configuration Scripts

[Configuration Scripts]画面には、設定スクリプトのダウンロードおよびアップロードに使用する URL が表示されます。

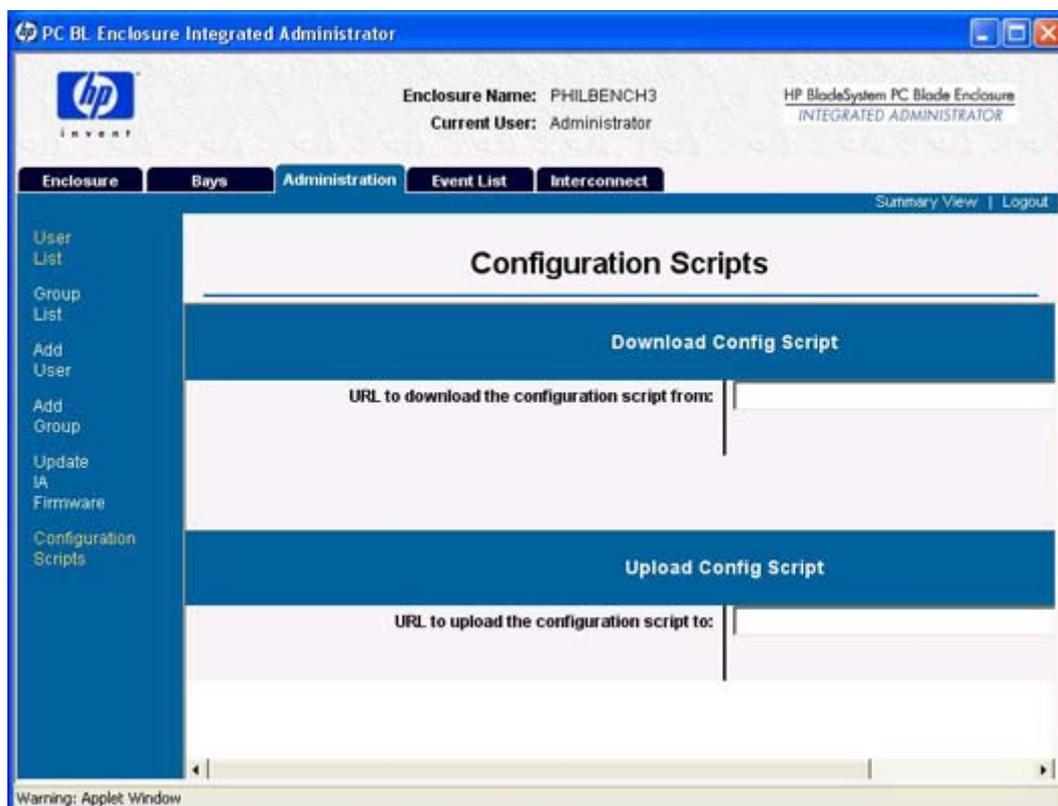


表 4-28 [Configuration Scripts]画面のフィールドの説明

フィールド	可能な値	説明
Download Config Script		
URL to download the configuration script from		設定スクリプトをダウンロードする URL
Upload Config Script		
URL to upload the configuration script to		設定スクリプトをアップロードする URL

[Event List]タブ

[Event List]タブからは、以下の画面にアクセスできます。

- Event List
- Event Log Policy

イベント リストは、以下の点でシステム ログと異なります。

- どのユーザも、イベント リストを表示できます。エンクロージャ管理者だけが、システム ログにアクセスできます。
- イベント リストのメッセージは、注意と重大な障害だけに限定されています。障害と処置の両方に関する情報については、エンクロージャのシステム ログを参照してください。
- [Minor]、[Informational]、および[Normal]の各イベントも、イベント ログ ポリシー設定に基づいてレポートおよび表示されます。[Informational]および[Normal]イベントは、初期設定では無効になっています。
- イベント リストには、ユーザが Integrated Administrator にログインした後に受信したメッセージだけが表示されます。システム ログには、エンクロージャ診断によって生成されたすべてのメッセージが表示されます。最大で 50 個のイベント ログ メッセージが表示されます。この最大数を超えると、古いメッセージから順番に削除されます。

[Event List]画面（以下の図を参照）では、イベントごとに以下の情報が提供されます。

- 重大度
- ソース
- 日付
- 時間
- イベントの詳細（以下の例では、ヒートシンクが正しく取り付けられていないことを示しています）

PC BL Enclosure Integrated Administrator

Enclosure Name: PHILBENCH3
Current User: Administrator

HP BladeSystem PC Blade Enclosure
INTEGRATED ADMINISTRATOR

Enclosure Bays Administration **Event List** Interconnect

Summary View | Logout

Event List
Event Log Policy

CAUTION **Event List** **CAUTION** **HELP**

This list contains events received since this session began based on the settings in Event Log Policy.

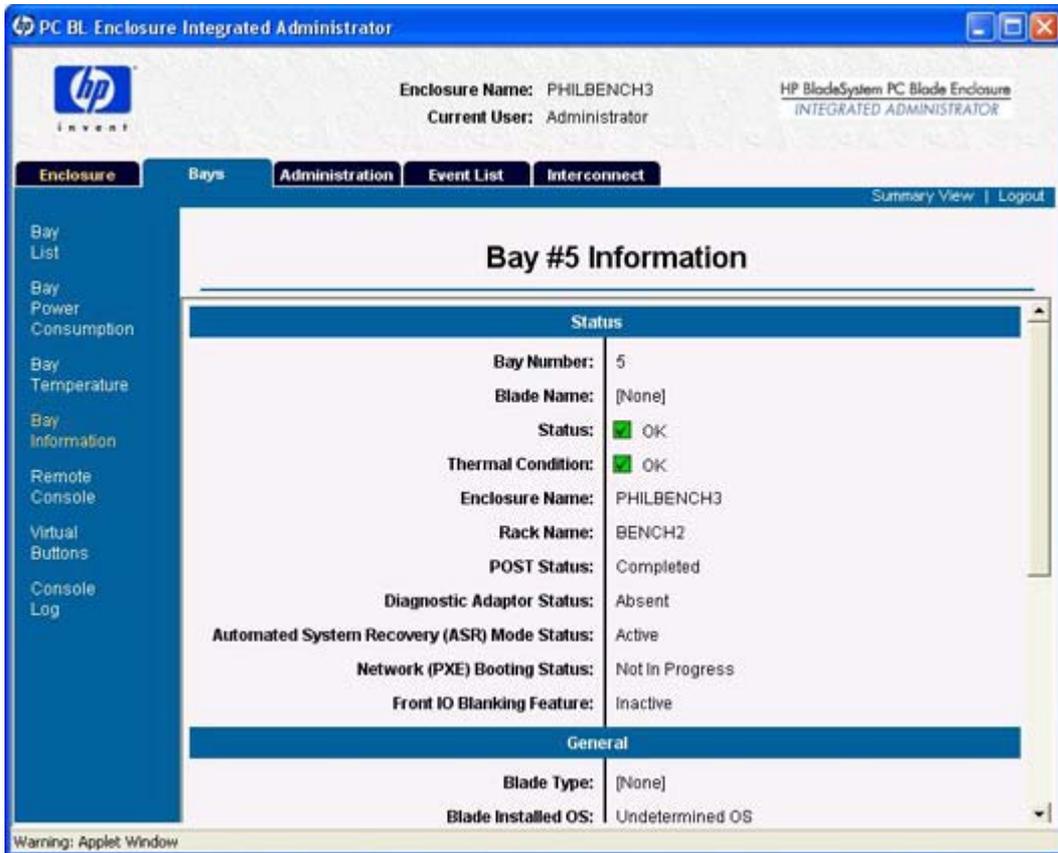
Select an event from the list:

Severity	Source	Date	Time	Event Details
CAUTION	Bay #19	10/16/2008	13:13:04	Bay #19 is in a degraded state.
CAUTION	Bay #19	10/16/2008	13:12:42	Bay #19 is in a degraded state.
CAUTION	Bay #19	10/16/2008	13:12:37	Bay #19 is in a degraded state.
CAUTION	Bay #19	10/16/2008	13:12:37	Bay #19 is in a degraded state.
CAUTION	Bay #19	10/16/2008	13:12:16	Bay #19 is in a degraded state.

View Event Details Clear All Events

Warning: Applet Window

上の例は、ベイの機能が低下した状態であることを示しています。イベントをクリックすると、この障害に関する追加情報を含む、ベイの一覧が表示されます。

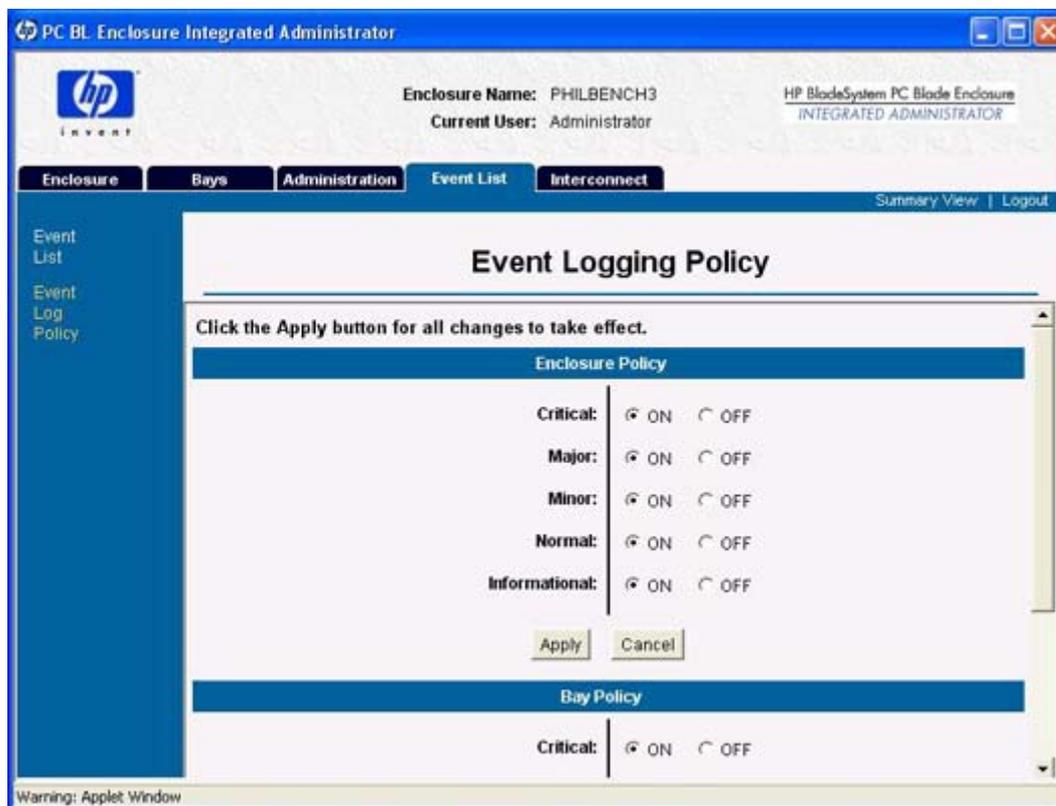


Integrated Administrator は、以下の表に説明されている重大度の 4 つのカテゴリ（Normal、Minor、Caution、および Critical）に従って、エンクロージャのイベントをリアルタイムに通知します。イベント メッセージの完全な一覧を含むイベント リストについては、[161 ページの「イベントのアイコンと詳細」](#)を参照してください。

表 4-29 イベント通知アイコン

アイコン	説明
	Informational : 情報提供目的のメッセージ 情報提供目的のメッセージが正常な動作に影響を与えることはありません
	Normal : エンクロージャの動作で通常発生するイベント [Normal]イベントが発生している場合は、正常な動作が保証されます
	Caution-Minor : エンクロージャの動作、電源の維持、またはエンクロージャのユーザ コミュニティへのサービスを妨げないイベント [Caution-Minor]イベントが発生している場合は、正常な動作が保証されます
	Caution-Major : エンクロージャの動作、電源の維持、またはエンクロージャのユーザ コミュニティへのサービスを妨げないイベント [Caution-Major]イベントが発生すると、正常な動作は保証されなくなります
	Critical : エンクロージャの継続的な動作を妨げるイベント [Critical]イベントが発生すると、エンクロージャが停止する場合があります

Event Log Policy



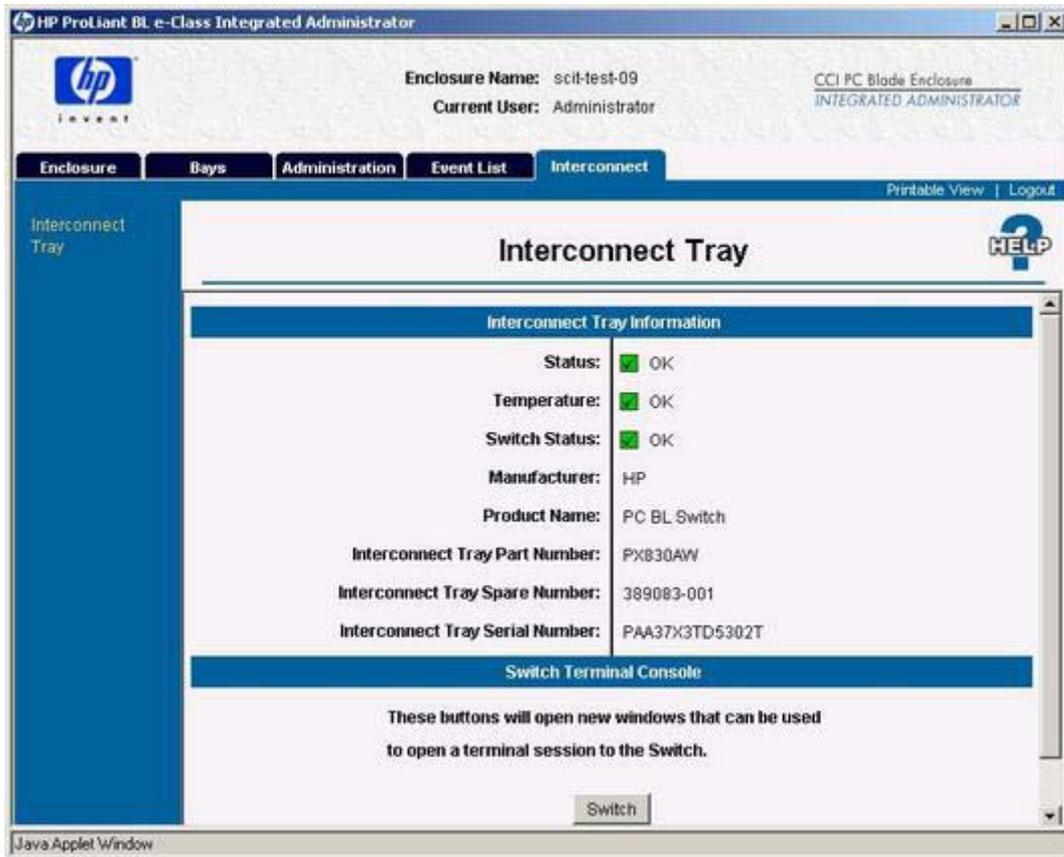
- **[Critical]** : ON または OFF
- **[Caution-Major]** : ON または OFF
- **[Caution-Minor]** : ON または OFF
- **[Normal]** : ON または OFF
- **[Informational]** : ON または OFF

すべてのエンクロージャのイベント ログ ポリシーについて、初期設定では**[ON]**になっています。すべてのベイのイベント ログ ポリシーについて、初期設定では**[ON]**になっています（**[Normal]**および**[Informational]**を除く）。

具体的なイベント ログ メッセージの詳細については、[144 ページの「エラー メッセージ」](#)で、サポートされているイベント ログ メッセージおよび重大度の分類を参照してください。

[Interconnect]タブ

[Interconnect Tray]画面（以下の図を参照）では、誰でもインターコネクト トレイに関する情報を確認できます。インターコネクト スイッチの1つにリモート コンソールが搭載されている場合は、エンクロージャ管理者はこの画面を利用してリモート コンソールに接続できます。



以下の表では、[Interconnect Tray]画面の各領域に表示される情報について説明します。

表 4-30 [Interconnect Tray]画面のフィールドの説明 : [Interconnect Tray Information]領域

フィールド	可能な値	説明
[Interconnect Tray Information]領域		
Status	OK、劣化、または障害	インターコネク トレイのステータス
Temperature	OK、温度上昇、注意、または重大	インターコネク トレイの温度ステータス
Switch A Status	OK、劣化、または障害	スイッチ A のステータス。インターコネク ト スイッチが取り付けられている場合にだけ表示されます
Switch B Status*	OK、劣化、または障害	スイッチ B のステータス。インターコネク ト スイッチが取り付けられている場合にだけ表示されます
Manufacturer		インターコネク トレイの製造元
Product Name		インターコネク トレイの製品名
Interconnect Tray Part Number		インターコネク トレイの製品番号
Interconnect Tray Serial Number		インターコネク トレイのシリアル番号
* Proliant C-GbE e-Class スイッチのみ		

表 4-31 [Interconnect Tray]画面のフィールド：[Switch Terminal Console]領域（インターコネクト スイッチが取り付けられている場合にのみ表示されます）

フィールド	可能な値	説明
[Switch Terminal Console]領域（インターコネクト スイッチが取り付けられている場合にだけ表示されます）		
Switch A ボタン		スイッチ A のリモート コンソール用の新しいウィンドウを開きます
Switch B ボタン*		スイッチ B のリモート コンソール用の新しいウィンドウを開きます
* Proliant C-GbE e-Class スイッチのみ		

5 コマンド ライン インタフェース

この章では、Integrated Administrator のコマンド ライン インタフェース (CLI) を操作するためのリファレンス情報を提供します。コマンド ラインに関連する情報を以下の項目に分けて説明します。

- コマンド ライン インタフェースへのアクセス
- コマンド ライン インタフェースの操作
 - 一般的なコマンド
 - 一般的な管理コマンド
 - ユーザ アカウント コマンド
 - エンクロージャのネットワーク設定コマンド
 - エンクロージャの管理コマンド
 - Blade PC の管理コマンド
- コマンド ライン インタフェース特有の機能

このガイドで使用されているコマンド ラインの規則について詳しくは、[143 ページの「コマンド ラインの規則」](#)を参照してください。

また、容易に参照できるように、このガイドの索引にも Integrated Administrator でサポートされているコマンドの完全な一覧が掲載されています。

コマンド ライン インタフェースへのアクセス

CLI には、管理（10/100 Ethernet）コネクタを介してリモートで、エンクロージャのリア パネルにあるコンソール（シリアル）コネクタを介してローカルに、または VLAN 設定に応じた任意のアップリンクを介してアクセスできます。

管理コネクタを介したリモート アクセス

管理（10/100 Ethernet）コネクタを介して Integrated Administrator のコマンド ライン インタフェースにリモートでアクセスするには、以下の操作を行います。

1. インターコネクト トレイに貼付された設定タグから、初期設定のホスト名を取得します。
 2. Telnet または Secure Shell アプリケーションを開き、アクセスするエンクロージャの IP アドレスまたは DNS 名を入力します。
-
- △ **注意：** Secure Shell の代わりに Telnet を使用すると、そのネットワークでは、パスワードを含むリモート セッションが通常のテキストになります。
-
3. **[Login]** プロンプトに、ユーザ名とパスワードを入力します。

コンソール コネクタを介したローカル アクセス

シリアル コネクタを介して Integrated Administrator にローカルにアクセスするには、以下の操作を行います。

1. nul モデム ケーブルを使用して、ラップトップ コンピュータなどのローカル クライアントデバイスをシリアル コネクタに接続します。
-
- 📖 **注記：** クライアント デバイスは、[11 ページの「ローカル クライアント デバイスの要件」](#)に記載されている要件を満たしている必要があります。
-
2. 端末エミュレータを開き、**Enter** キーを 1 回以上押してログイン プロンプトを表示します。
 3. ユーザ名とパスワードを入力します。

コマンド ライン インタフェースの操作

一般的なコマンド

以下の表では、[Enclosure Information]画面の各領域に表示される情報について説明します。

表 5-1 一般的なコマンド

コマンド	説明	制限事項
CLEAR SCREEN	端末画面を消去します	なし
EXIT	コマンド ライン インタプリタを終了します	なし
HELP {<コマンド>} Tree	<コマンド>にコマンドを指定すると、そのコマンドの使用 法とヘルプ テキストがツリー形式で表示されます。引数を指 定しない場合には、すべての基本コマンドが表示されます	なし
LOGOUT	コマンド ライン インタプリタを終了します	なし
QUIT	コマンド ライン インタプリタを終了します	
SLEEP	セッションを一定の期間一時停止します。スクリプトに遅延 を追加する場合に便利です。<秒>フィールドには、1 ~ 86400 の任意の整数を指定できます。一時停止が開始された 後、時間切れになる前にセッションを再開する方法はありま せん。ただし、そのセッションを終了して別のセッションを 開始することは可能です	なし
? または H	CLI コマンドのヘルプ テキストを表示します	なし

一般的な管理コマンド

以下の表では、[Enclosure Information]画面の各領域に表示される情報について説明します。

表 5-2 一般的な管理コマンド

コマンド	説明	制限事項
CLEAR SESSION SWITCH [A B]	エンクロージャからの端末セッションを終了します これは正しい終了方法ではありません。接続しているユーザ は、まだ保存していない作業をすべて失います	グループ管理者は、アクセス 権を持つ Blade PC ベイに對 してだけ、このコマンドを実 行できます
CLEAR SSHKEY	Secure Shell 認証済みキー ファイルの内容を削除します。 このコマンドを実行すると、パブリック キーベースの認証を 使用してログインすることはできなくなります	エンクロージャ管理者だけ が、このコマンドを実行でき ます
CONNECT SWITCH [A B]	スイッチ A またはスイッチ B へのリモート コンソール接続 を開きます 1つのスイッチで複数のリモート コンソール セッションを 同時にサポートすることはできません	エンクロージャ管理者だけ が、このコマンドを実行でき ます
DOWNLOAD CERTIFICATE <URL>	システムにある現在のセキュリティ証明書を置き換えるため に、CA から提供された PKCS#7 ファイルをダウンロードし ます サポートされているプロトコルは、http、ftp、および tftp で す。URL は、「protocol://host/path/file」の形式にします FTP サーバで匿名接続がサポートされていない場合は、上記 の形式の「host」にあたる部分を	エンクロージャ管理者だけ が、このコマンドを実行でき ます

表 5-2 一般的な管理コマンド (続き)

	「username:password@host」に置き換えることでユーザ名とパスワードを指定できます	
DOWNLOAD SSHKEY	Secure Shell v2 で使用する認証済みのキー ファイルをダウンロードします。このファイルには、任意のエンクロージャ管理者用のパブリック キーを含めることができます。サポートされているプロトコルは、http、ftp、および tftp です。URL は、protocol://host/path/file の形式にします。FTP サーバで匿名接続がサポートされていない場合は、上記の形式の「host」にあたる部分を「username:password@host」に置き換えることでユーザ名とパスワードを指定できます	エンクロージャ管理者だけが、このコマンドを実行できます
GENERATE CERTIFICATE REQUEST	PKCS#10 証明書要求を生成します	エンクロージャ管理者だけが、このコマンドを実行できます
GENERATE CERTIFICATE SELFSIGNED	自己署名証明書を生成します	エンクロージャ管理者だけが、このコマンドを実行できます
PING {<個数>} {<IP アドレス> <サーバ名>}	リモート IP デバイスに ICMP エコー メッセージを送信します <個数>を省略すると、5 つのパケットだけが送信されます。パケットは、1 秒間隔で送信されます	<IP アドレス>は、「###.###.###.###」(###は 0 ~ 255) の形式にする必要があります
SET DISPLAY EVENTS [ON OFF ENCLOSURE BAY]*	イベント通知をオンまたはオフにします。グローバルな ON または OFF の場合のみ、Integrated Administrator は、この設定をすべてのログインにわたって保持します	なし
SET EXPERT {MODE} [ON OFF]	EXPERT MODE をオンまたはオフにします。EXPERT MODE がオンになっている場合、システムはユーザに操作の確認を求めません。元に戻せない操作が多いため、EXPERT MODE で作業する場合は注意してください	なし
SET FACTORY	Integrated Administrator を出荷時の初期設定に戻します Administrator アカウントのパスワードは変更されません。すべての変更が行われた後、Integrated Administrator は再起動されます 注記： このコマンドを実行すると、エンクロージャのメモリからグループ、ユーザ、その他のカスタマイズがすべて削除され、削除された情報を元に戻すことはできません このコマンドは、SET EXPERT コマンドの例外です。SET FACTORY コマンドを EXPERT MODE で実行する場合でも、このコマンドは確認動作を必要とします。確認を不要にするには、SCRIPT MODE をオンにする必要があります SET FACTORY の実行では、初期設定のアセット タグがシリアル番号と同じ値になります	このコマンドは、電源が入っているブレードが1つでもある場合には実行できません。すべてのブレードの電源を切ってから、このコマンドを実行してください
SET SCRIPT MODE [ON OFF]	SCRIPT MODE がオンになっていると、ADD USER <ユーザ名> <パスワード>、SET USER <ユーザ名> <パスワード>、および SET PASSWORD <パスワード> コマンドにはパスワード引数が必要になります。SCRIPT MODE がオフになっているとき、ADD USER、SET USER PASSWORD、および SET PASSWORD コマンドはパスワード引数を必要としません 初期値には、ユーザの介入が必要です	なし
SHOW SESSIONS	各ベイおよびスイッチへの接続を表示します (接続が存在する場合)	ユーザは、このコマンドを実行できません。グループメン

表 5-2 一般的な管理コマンド (続き)

	各ベイおよびスイッチには、1 回に 1 人のユーザしか接続できません。また、現在ログインしている各ユーザ、そのユーザのポート番号、接続時間、およびリモート システム名も表示されます	バとグループ管理者には、自分が所属するグループに割り当てられたベイに関するセッションだけが表示されます。エンクロージャ管理者には、すべてのセッションが表示されます
SHOW SSHFINGERPRINT	Integrated Administrator のホスト SSH パブリック キーのキー フィンガープリントを表示します。このコマンドをシリアル コンソールから使用すると、ネットワーク全体にわたる SSH 接続を初期化する前に、Integrated Administrator の識別情報を検証できます	なし
SHOW SSHKEY	エンクロージャ管理者のキーベースの認証に使用されている既存の Secure Shell 認証済みキー ファイルの内容を表示します	エンクロージャ管理者だけが、このコマンドを実行できます
SHOW ENCLOSURE POWER	すべてのサブコンポーネントを含む、エンクロージャの電力消費量の推定値を表示します。この情報にはエンクロージャの総電力消費量の他に、過去 24 時間および電源投入やりセット以降の電力の最高と時間平均が含まれています	このコマンドは、電力を認識するブレードから報告される測定値およびエンクロージャサブシステム コンポーネントからの推定値に基づいて電力使用量の推定値のみを表示します。この情報は、参考としてのみ使用してください。 注記： この情報は、すべてのブレードが電力を認識する (bc2x00 など) の場合にのみ表示されます。そうでない場合は、エンクロージャが電力消費量を正しく推定できないことを示す注意が表示されます
ENABLE AUTOPOWERON	有効になっている場合は、ブレードが取り付けられたか外部電源サイクルがエンクロージャに適用されたときに、エンクロージャ IA が自動的にブレードの電源を入れます	なし
DISABLE AUTOPOWERON	無効になっている場合は、ブレードの電源を、ローカル アクセスによって入れるか、IA を使用してリモートで入れる必要があります	なし

*イベント表示の重大度ポリシー固有の設定は、セッション固有の設定で、イベントの重大度の種類の特定の分類を細かく制御できるようにするために追加されました

- SET DISPLAY EVENTS ENCLOSURE
 - SET DISPLAY EVENTS ENCLOSURE ALL [ON | OFF]
 - SET DISPLAY EVENTS ENCLOSURE CRITICAL [ON | OFF]
 - SET DISPLAY EVENTS ENCLOSURE INFORMATIONAL [ON | OFF]
 - SET DISPLAY EVENTS ENCLOSURE MAJOR [ON | OFF]
 - SET DISPLAY EVENTS ENCLOSURE MINOR [ON | OFF]
 - SET DISPLAY EVENTS ENCLOSURE NORMAL [ON | OFF]
- SET DISPLAY EVENTS BAY
 - SET DISPLAY EVENTS BAY ALL [ON | OFF]
 - SET DISPLAY EVENTS BAY CRITICAL [ON | OFF]

- SET DISPLAY EVENTS BAY INFORMATIONAL [ON | OFF]
- SET DISPLAY EVENTS BAY MAJOR [ON | OFF]
- SET DISPLAY EVENTS BAY MINOR [ON | OFF]
- SET DISPLAY EVENTS BAY NORMAL [ON | OFF]

イベント分類について詳しくは、[161 ページの「イベントのアイコンと詳細」](#)を参照してください。

ユーザ アカウント コマンド

表 5-3 ユーザ アカウント コマンド

コマンド	説明	制限事項
ADD GROUP <グループ名>	グループ名 初期設定のグループ説明は空白です	エンクロージャ管理者だけが、このコマンドを実行できます。最大 20 グループをシステムに追加できます <グループ名>は、他のすべてのグループ名およびユーザ名と異なる必要があり、大文字と小文字が区別されます。1 ~ 13 文字の長さにする必要があります。英数字、ハイフン、およびアンダースコアを使用できます。また、英字で始まる必要があります 注記： 「Administrator」、「switch」、「switcha」、「switchb」、および「SAM」は予約済みの名前であり、使用できません。この制限事項については、大文字と小文字は区別されません 出荷時の初期設定のアカウントについては、 167 ページの「出荷時の設定」 を参照してください
ADD USER <ユーザ名> <パスワード>	システムにユーザを追加します パスワードを指定しない場合、ユーザはパスワードの入力を求められます。SCRIPT MODE が有効になっている場合、パスワードはオプションではなく必須です	エンクロージャ管理者だけが、このコマンドを実行できます。予約済みのアカウントに加えて、最大 25 ユーザを追加できます <ユーザ名>は、他のすべてのグループ名およびユーザ名と異なる必要があり、大文字と小文字が区別されます。1 ~ 13 文字の長さにする必要があります。英数字、ハイフン、およびアンダースコアを使用できます。また、英字で始まる必要があります <パスワード>は 3 ~ 8 文字の長さにする必要があります。すべての印刷可能文字を使用できます。パスワードが入力され

表 5-3 ユーザ アカウント コマンド (続き)

		ない場合、ユーザはパスワードの入力を求められます
		<p>注記: 「Administrator」、「switch」、「switcha」、「switchb」、および「SAM」は予約済みの名前であり、使用できません。この制限事項については、大文字と小文字は区別されません</p> <p>出荷時の初期設定のユーザ アカウントについては、167 ページの「出荷時の設定」を参照してください</p>
ASSIGN ADMINISTRATOR (RIGHTS) <ユーザ名>	ユーザにエンクロージャ管理者のアクセス権を与えます 後でエンクロージャ管理者のアクセス権が削除されても、グループ メンバシップは削除されません	エンクロージャ管理者だけが、このコマンドを実行できます <ユーザ名>では、大文字と小文字が区別されます
ASSIGN BAY [ALL <ベイ番号> {[, -] <ベイ番号>}] <グループ名>	グループに 1 つまたは複数のベイを割り当てます ベイがすでにグループに割り当てられている場合は、このコマンドを実行する前に、まずその割り当てを解除する必要があります	エンクロージャ管理者だけが、このコマンドを実行できます <グループ名>では、大文字と小文字が区別されます
ASSIGNS USER <ユーザ名> <グループ名> {[VIEW MODIFY]}	グループに、表示アクセス権 (グループ メンバ用) または表示/変更アクセス権 (グループ管理者用) を持った状態でユーザを割り当てます 「View」または「View/Modify」を指定していない場合は、初期設定で「View」が選択されます	エンクロージャ管理者だけが、このコマンドを実行できます <ユーザ名>では、大文字と小文字が区別されます
DISABLE USER <ユーザ名>	ユーザ アカウントを無効にします そのユーザはただちにシステムからログアウトされ、アカウントが有効になるまでログインできません	エンクロージャ管理者だけが、このコマンドを実行できます <ユーザ名>では、大文字と小文字が区別されます。管理者アカウントを無効にすることはできません
ENABLE USER <ユーザ名>	以前に DISABLE USER コマンドで無効にされたユーザ アカウントを有効にします	エンクロージャ管理者だけが、このコマンドを実行できます <ユーザ名>では、大文字と小文字が区別されます

表 5-3 ユーザ アカウント コマンド (続き)

		<p>注記： 「SAM」管理者アカウントは初期設定で無効になっています。「SAM」管理者アカウントは、HP SAM (Session Allocation Manager) をサポートするために提供されています。すべての Integrated Administrator が SamUser123 という同じ初期設定の SAM アカウント パスワードを持つため、有効にする前、または有効にした直後に、SAM アカウントパスワードを変更することを強くおすすめします</p>
REMOVE GROUP [ALL <グループ名>]	<p>グループを削除し、グループ内のすべてのベアの割り当てを自動的に解除します</p>	<p>エンクロージャ管理者だけが、このコマンドを実行できます</p> <p><グループ名>では、大文字と小文字が区別されます</p>
REMOVE USER [ALL <ユーザ名>]	<p>システムからユーザを削除します</p> <p>[ALL]を指定すると、初期設定のシステム アカウントを除くすべてのユーザについて、このコマンドが実行されます</p>	<p>エンクロージャ管理者だけが、このコマンドを実行できます</p> <p><ユーザ名>では、大文字と小文字が区別されます</p> <p>注記： 「Administrator」、 「switch」、「SAM」、 「switcha」、および 「switchb」を削除することはできません</p>
SET GROUP {DESCRIPTION} <グループ名> <説明>	<p>グループの説明を設定します</p>	<p>エンクロージャ管理者だけが、このコマンドを実行できます。<説明>は 1 ~ 20 文字の長さにする必要があり、英数字、ハイフン、およびアンダースコアを使用できます。初期設定のグループ説明は空白です。連絡先情報にスペースを含める場合は、情報全体を引用符で囲んでください</p>
SET PASSWORD <パスワード>	<p>現在 Integrated Administrator にログインしているユーザのパスワードを設定します。コマンド ラインにパスワードを指定しない場合、ユーザはパスワードの入力を求められます</p> <p>注記： パスワードを指定しない場合、このコマンドは SCRIPT MODE では無効です</p>	<p><パスワード>は 3 ~ 8 文字の長さにする必要があり、すべての印刷可能文字を使用できます</p>
SET USER CONTACT <ユーザ名> <連絡先情報>	<p><ユーザ名>が存在しない場合は、コマンドを実行したユーザの連絡先情報を変更されます</p>	<p>エンクロージャ管理者だけが、他のユーザの連絡先情報を変更できます</p> <p><ユーザ名>では、大文字と小文字が区別されます。<連絡先情報>は 1 ~ 20 文字の長さにする必要があり、英数字、ハイフン、アンダースコア、@ (アットマーク)、およびスペースを使用できます。初期設定の連絡先情報は空白で</p>

表 5-3 ユーザ アカウント コマンド (続き)

		す。連絡先情報にスペースを含める場合は、情報全体を引用符で囲んでください
SET USER FULL NAME	ユーザのフル ネームを設定します	エンクロージャ管理者だけが、他のユーザのフル ネームを変更できます
{<ユーザ名>} <フル ネーム>	<ユーザ名>が存在しない場合は、現在ログインしているユーザのフル ネームが変更されます	<ユーザ名>では、大文字と小文字が区別されます。<連絡先情報>は 1 ~ 20 文字の長さにする必要があります。英数字、ハイフン、アンダースコア、およびスペースを使用できます。初期設定のフル ネームは空白です。この情報にスペースを含める場合は、情報全体を引用符で囲んでください
SET USER PASSWORD	ユーザのパスワードを設定します	エンクロージャ管理者だけが、他のユーザのパスワードを変更できます。「Administrator」アカウントだけが、「Administrator」アカウントのパスワードを変更できます
<ユーザ名>	コマンド ラインにパスワードを指定しないと、パスワードの入力を求められます 注記： パスワードを指定しない場合、このコマンドは SCRIPT MODE では無効です	<ユーザ名>では、大文字と小文字が区別されます。<新しいパスワード>は 3 ~ 8 文字の長さにする必要があります。すべての印刷可能文字を使用できます
SHOW GROUP	グループの説明、表示アクセス権を持つメンバーの一覧、表示/変更アクセス権を持つメンバーの一覧、ベイの数、およびそのグループが管理する各ベイの一覧を表示します	グループ メンバとグループ管理者は、自分がメンバになっているグループだけを表示できます。ユーザは、このコマンドを実行できません
[<グループ名> ALL]		<グループ名>では、大文字と小文字が区別されます この情報にスペースを含める場合は、情報全体を引用符で囲んでください
SHOW USER	ユーザのフル ネーム、連絡先、管理者としてのアクセス権の有無、アカウントが有効かどうか、およびそのユーザが表示アクセス権または表示/変更アクセス権を持っているグループを表示します	エンクロージャ管理者だけが、他のユーザの情報を表示できます
[<ユーザ名> ALL]	[ALL]を入力すると、すべてのユーザについてこの情報が表示されます。ユーザ名の前のアスタリスクは現在のユーザを意味します	<ユーザ名>では、大文字と小文字が区別されます。エンクロージャ管理者のアクセス権を持たないユーザは、自分のユーザ情報だけを表示できます
UNASSIGN ADMINISTRATOR (RIGHTS)	ユーザからエンクロージャ管理者のアクセス権を削除します	エンクロージャ管理者だけが、このコマンドを実行できます。「Administrator」アカウントでは、エンクロージャ管理者のアクセス権を削除できません
<ユーザ名>		

表 5-3 ユーザ アカウント コマンド (続き)

		<ユーザ名>では、大文字と小文字が区別されます
UNASSIGN USER	指定したグループからユーザを削除します	エンクロージャ管理者だけが、このコマンドを実行できます
<ユーザ名> <グループ名>		<ユーザ名>と<グループ名>では、大文字と小文字が区別されます

エンクロージャのネットワーク設定コマンド

表 5-4

コマンド	説明	制限事項
ADD SNMP TRAPRECEIVER <IP アドレス>	SNMP トラップを受信するために IP アドレスを追加します v1 トラップだけがサポートされています。トラップは、SNMP の初期設定ポート (162) に送信されます	エンクロージャ管理者だけが、このコマンドを実行できます
DISABLE SECURESH	Integrated Administrator に対する Secure Shell アカウントを無効にします	エンクロージャ管理者だけが、このコマンドを実行できます
DISABLE SNMP	Integrated Administrator に対する SNMP サポートを無効にします 設定されている SNMP トラップ受信者は消去されません。SNMP トラップ受信者を引き続き追加したり削除したりできます。SNMP が無効になっていると、Systems Insight マネージャ エージェントは正常に動作しません	エンクロージャ管理者だけが、このコマンドを実行できます
DISABLE TELNET	Integrated Administrator への Telnet アクセスを無効にします	エンクロージャ管理者だけが、このコマンドを実行できます
DISABLE WEB	Integrated Administrator への HTTP および HTTPS アクセスを無効にします このコマンドによって、Web ベースのユーザ インタフェースへのアクセスができなくなります	エンクロージャ管理者だけが、このコマンドを実行できます
DOWNLOAD CONFIG <URL>	これらのファイルは、スクリプト モードで自動実行されます。このファイルで「Administrator」アカウントのパスワードを変更することはできません。サポートされているプロトコルは、http、ftp、および tftp です。URL は、protocol://host/path/file の形式にします。FTP サーバで匿名接続がサポートされていない場合は、上記の形式の「host」にあたる部分を「username:password@host」に置き換えることでユーザ名とパスワードを指定できます	エンクロージャ管理者だけが、このコマンドを実行できます IP アドレスは、「###.###.###.###」(###は 0 ~ 255) の形式である必要があります
ENABLE SECURESH	Integrated Administrator に対する Secure Shell アカウントを有効にします	エンクロージャ管理者だけが、このコマンドを実行できます
ENABLE SOAP	すべての管理者アカウントにわたって Integrated Administrator に対する SOAP サポートを有効にします	これは組み込みの SAM ユーザ アカウントには影響しません。サポートされる SOAP コマンドについては、 161 ページの「イベントのアイコンと詳細」 を参照してください

(続き)

DISABLE SOAP	すべての管理者アカウントにわたって Integrated Administrator に対する SOAP サポートを無効にします	これは組み込みの SAM ユーザ アカウントには影響しません。サポートされる SOAP コマンドについては、 161 ページの「イベントのアイコンと詳細」 を参照してください
ENABLE SNMP	Integrated Administrator に対する SNMP サポートを有効にします	エンクロージャ管理者だけが、このコマンドを実行できます
ENABLE TELNET	Integrated Administrator への Telnet アクセスを有効にします	エンクロージャ管理者だけが、このコマンドを実行できます
ENABLE WEB	Integrated Administrator への HTTP および HTTPS アクセスを有効にします	エンクロージャ管理者だけが、このコマンドを実行できます
REMOVE SNMP TRAPRECEIVER <IP アドレス>	SNMP トラップを受信するシステムの一覧から IP アドレスを削除します	エンクロージャ管理者だけが、このコマンドを実行できます IP アドレスは、「###.###.###.###」(###は 0 ~ 255) の形式である必要があります
SET DNS <プライマリ アドレス> {<セカンダリ アドレス>}	プライマリおよびセカンダリ DNS サーバ アドレスを設定します これらのサーバは、システムが現在、静的 IP アドレスを使用するように設定されている場合にのみ使用されます	エンクロージャ管理者だけが、このコマンドを実行できます IP アドレスは、「###.###.###.###」(###は 0 ~ 255) の形式である必要があります
SET GATEWAY <IP アドレス>	ネットワークの初期設定のゲートウェイを設定します このゲートウェイは、システムが静的 IP アドレスを使用するように設定されている場合にのみ使用されます	エンクロージャ管理者だけが、このコマンドを実行できます IP アドレスは、「###.###.###.###」(###は 0 ~ 255) の形式である必要があります
SET IPCONFIG [DHCP {DYNAMICDNS} STATIC <IP アドレス> <ネットマスク>]	Integrated Administrator の IP 設定を行います ゲートウェイ アドレスと DNS アドレスは消去されます。オプションの「DYNAMICDNS」引数は、動的 DNS を有効にします	エンクロージャ管理者だけが、このコマンドを実行できます IP アドレスは、「###.###.###.###」(###は 0 ~ 255) の形式である必要があります
SET SNMP COMMUNITY [READ WRITE] <コミュニティ名>	SNMP の読み込みまたは書き込みコミュニティのコミュニティ名を設定します 読み込みおよび書き込みコミュニティの初期名は、それぞれ「public」および空白です。空白の書き込みコミュニティ名を指定すると、空白以外のコミュニティ名を指定するまで SNMP 設定コマンドは無効です	エンクロージャ管理者だけが、他のユーザの連絡先情報を変更できます 書き込み<コミュニティ名>は 1 ~ 20 文字の長さ、読み込み<コミュニティ名>は 1 ~ 20 文字の長さにする必要があります。どちらも英数字、ハイフン、およびアンダースコア

(続き)

		アを使用できます。初期設定の読み込みコミュニティ名は「public」です。初期設定の書き込みコミュニティ名は空白です
SET SNMP CONTACT <連絡先>	システム連絡先の名前を設定します。@（アットマーク）など印刷可能な ASCII 文字を連絡先および位置に使用できます	エンクロージャ管理者だけが、このコマンドを実行できます <連絡先>は 1～20 文字の長さにする必要があり、英数字、ハイフン、アンダースコア、@（アットマーク）、およびスペースを使用できます。この情報にスペースを含める場合は、情報全体を引用符で囲んでください
SET SNMP LOCATION <位置>	エンクロージャの SNMP 位置を設定します 初期設定の位置は空白です	エンクロージャ管理者だけが、このコマンドを実行できます <位置>は 1～20 文字の長さにする必要があり、英数字、ハイフン、アンダースコア、@（アットマーク）、およびスペースを使用できます。この情報にスペースを含める場合は、情報全体を引用符で囲んでください
SHOW NETWORK	エンクロージャ DHCP の状態、動的 DNS の状態、IP アドレス、サブネット マスク、ゲートウェイ アドレス、プライマリおよびセカンダリ DNS アドレス、HTTP および HTTPS サーバのステータス、SNMP のステータス、Secure Shell のステータス、および Telnet のステータスを表示します	なし
SHOW SNMP	SNMP のシステム名、位置、および連絡先、読み込みコミュニティ名、書き込みコミュニティ名、およびトラップ送信先の一覧を表示します	エンクロージャ管理者だけが、このコマンドを実行できます
SET TRAP POLICY	エンクロージャの SNMP エージェントがトラップ ポリシーの設定どおりにトラップを送信するように設定します。詳しくは、MIB (Management Information Base) ファイルの CPQRACK.MIB に記載されているトラップの説明を参照してください	エンクロージャ管理者だけが、このコマンドを実行できます
SHOW TRAP POLICY	エンクロージャが生成する SNMP トラップの一覧を表示します。角かっこの中に「X」が表示されている場合、そのトラップが選択されていることを示します。特定のトラップ機能について詳しくは、MIB (Management Information Base) ファイルの CPQRACK.MIB に記載されているトラップの説明を参照してください	なし

エンクロージャの管理コマンド

表 5-5

コマンド	説明	制限事項
CLEAR SYSLOG ENCLOSURE	エンクロージャのシステム ログを消去します	エンクロージャ管理者だけが、このコマンドを実行でき

(続き)

		ます。この情報は、いったん削除されると復元できません
SET SYSLOG POLICY [ENCLOSURE BAY]*	このコマンドは、重大度の種類ごとにシステム ログ メッセージを有効または無効にします。Integrated Administrator は、この設定をすべてのログインまたはユーザにわたって保持します	なし
POWEROFF ENCLOSURE {FORCE}	エンクロージャの正しいシャットダウンを実行します。最初に各ブレードが正しくシャットダウンされます。「FORCE」引数を指定すると、エンクロージャとすべてのブレードはただちにシャットダウンされます	エンクロージャ管理者だけが、このコマンドを実行できます
RESTART	Integrated Administrator を再起動します。システム内のベイの動作には影響しません	エンクロージャ管理者だけが、このコマンドを実行できます
SET DATE MMDDhhmm {CC}YY {TZ}	以下の定義に従って、エンクロージャの日付を設定します <ul style="list-style-type: none">MM : 月DD : 日hh : 時 (24 時間制)mm : 分CC : 世紀YY : 年TZ : タイム ゾーン (大文字と小文字が区別される) タイム ゾーンを空白のままにすると、現在のタイム ゾーンがそのまま有効になります 注記: タイムゾーンの設定後は、IA の再起動コマンドを実行する必要があります	エンクロージャ管理者だけが、このコマンドを実行できます <ul style="list-style-type: none">MM は、1 ~ 12 の整数ですDD は、1 ~ 31 の整数ですhh は、0 ~ 23 の整数ですmm は、0 ~ 59 の整数です タイム ゾーンの一覧については、 170 ページの「タイムゾーンの設定」 を参照してください。日付と時刻を手動で設定する前に、NTP を無効にする必要があります
SET TIME	エンクロージャの時刻を変更します	エンクロージャ管理者だけが、このコマンドを実行できます タイム ゾーンの一覧については、 170 ページの「タイムゾーンの設定」 を参照してください。日付と時刻を手動で設定する前に、NTP を無効にする必要があります
SET ENCLOSURE ASSET {TAG} <アセット タグ>	エンクロージャのアセット タグを変更します	エンクロージャ管理者だけが、このコマンドを実行できます <アセット タグ>は 1 ~ 31 文字の長さにする必要があります。英数字、ハイフン、およびアンダースコアを使用できます 初期設定のエンクロージャ アセット タグは空白です。空白のアセット タグを設定するには、引用符を使用して空白の値を指定します

(続き)

SET ENCLOSURE NAME <エンクロージャ名>	エンクロージャ名を変更します	エンクロージャ管理者だけが、このコマンドを実行できます <エンクロージャ名>は 1 ~ 32 文字の長さにする必要があり、英数字、ハイフン、およびアンダースコアを使用できます 初期設定のエンクロージャ名は IA-MAC です。この「MAC」は、実際の MAC アドレスに置き換えられます
SET ENCLOSURE UID [ON OFF]	エンクロージャのユニット確認ランプをオンまたはオフにします	エンクロージャ管理者だけが、このコマンドを実行できます
SET RACK NAME <ラック名>	エンクロージャが存在するラックの名前を設定します	エンクロージャ管理者だけが、このコマンドを実行できます <ラック名>は 1 ~ 32 文字の長さにする必要があり、英数字、ハイフン、およびアンダースコアを使用できます 初期設定のラック名は「 UnnamedRack 」です
SET POWER HISTORY INTERVAL [BLADE ENCLOSURE]	各ブレードおよびエンクロージャの両方について、電力消費量レポートのデータを収集する間隔のポリシーを設定します	エンクロージャ管理者だけが、このコマンドを実行できます 可能な設定は、それぞれ 1、5、10、30、および 60 秒で、最大バッファ サイズは 24 時間です
SHOW CONFIG	エンクロージャの設定を再作成するために必要なスクリプトを表示します パスワードは、どのユーザのものも含まれていません	エンクロージャ管理者だけが、このコマンドを実行できます
SHOW DATE	エンクロージャの内部クロックの現在の日付、時間、およびタイムゾーンを表示します	なし
SHOW TIME	エンクロージャの内部クロックの現在時刻およびタイムゾーンを表示します	なし
SHOW DISPLAY	イベント通知がオンまたはオフのどちらになっているかを表示します	なし
SHOW ENCLOSURE FAN [<ファン番号> ALL]	指定したファンのステータス、リダンダント状態、ペアとなるファン、速度、および製品番号を表示します 「ALL」を入力すると、すべてのファンについてこの情報が表示されます 注記： このコマンドを使用して、取り外しができない電源装置ファンである、ファン 5 およびファン 6 の情報を表示することもできます。ファン 5 およびファン 6 は、HP BladeSystem PC Blade エンクロージャ G2 のエンクロージャでのみ利用できます	なし

(続き)

SHOW ENCLOSURE INFO	エンクロージャの名前、種類、製品番号、シリアル番号、およびアセットタグ、Integrated Administrator のソフトウェア (ビルド番号を含む) とハードウェアのバージョン、Integrated Administrator の MAC アドレス、自動電源投入機能の情報、インターコネクト トレイの種類、UUID、製品番号、およびシリアル番号を表示します	なし
SHOW ENCLOSURE POWER SUPPLY [<電源供給装置> ALL]	電源供給装置を指定すると、その電源供給装置について、エンクロージャのバージョン、電源供給装置のステータス、AC 入力ステータス、容量、入力電圧範囲#1 (V)、入力電圧範囲#2 (V、必要な場合)、入力周波数範囲 (Hz)、製品番号、シリアル番号、電源供給装置のスペア部品番号、およびハードウェア リビジョンが表示されます。「ALL」を指定すると、すべての電源供給装置についてこの情報が表示されます また、BladeSystem PC Blade エンクロージャ G2 のエンクロージャの場合にのみ、[Currently In Input Range] テキスト フィールドが表示されます	なし
SHOW ENCLOSURE STATUS	エンクロージャ ステータスの見出しに、エンクロージャのヘルス、Integrated Administrator のヘルス、およびユニット確認ランプを表示します 電源ステータスの見出しに、電源のステータスと容量を表示します 電源サブシステムの見出しに、ステータス、リダンダント状態、総容量、レジリエント容量、リダンダント容量、割り当て済みの電源容量、および利用可能な電源容量を表示します	なし
SHOW ENCLOSURE TEMP	エンクロージャのすべての温度センサについて、場所、ステータス (OK、温度上昇、機能低下、または障害)、温度 (°C)、およびしきい値を表示します HP BladeSystem PC Blade エンクロージャ G2 の場合は、電源供給装置の内部センサおよびインレット センサの温度も表示します	なし
SHOW ENCLOSURE TEMP LIST	センサを表形式で一覧表示します	なし
SHOW RACK NAME <ラック名>	エンクロージャが存在するラックの名前を表示します 初期設定のラック名は、「 UnnamedRack 」です	なし
SHOW POWER SUMMARY		なし
SHOW POWER HISTORY BAY	設定間隔およびサンプル数に基づく平均電力消費量の、直近 24 時間のデータ ポイントを表示します 注記： これらのサンプルは、電源を入れ直すかリセットを行うと破棄されます	なし
SHOW POWER HISTORY ENCLOSURE	設定間隔およびサンプル数に基づく平均電力消費量の、直近 24 時間のデータ ポイントを表示します 注記： これらのサンプルは、電源を入れ直すかリセットを行うと破棄されます	なし
SHOW POWER HISTORY INTERVAL [BLADE ENCLOSURE]	ブレードまたはエンクロージャの電力消費履歴の間隔を表示します	なし
SHOW SYSLOG ENCLOSURE	エンクロージャのシステム ログを、1 画面あたり 22 行で表示します	エンクロージャ管理者だけが、このコマンドを実行できます

(続き)

[CRIT WARN NOTICE INFO]	エンクロージャのシステム ログを表示します。表示をフィルタリングするには、オプションでパラメータを指定します	
	<ul style="list-style-type: none">● SYSLOG Type から IML への変換は、以下のとおりです<ul style="list-style-type: none">◦ CRIT : Critical◦ WARN : Major◦ WARN : Minor◦ NOTICE : Normal◦ INFO : Informational	
	<p>Q キーを押すと、コマンドが終了します。さらに表示情報が続く場合は、他の任意のキーを押すと次の画面が表示されず</p>	
	<p>C キーを押すと、システム ログがページの区切りなく連続して表示されます</p>	
SHOW TRAY INFO	インターコネクト トレイの製造元、製品名、製品番号、シリアル番号、およびスペア番号を表示します	なし
UPDATE IMAGE <URL>	ネットワーク経由でブレードから新しいイメージをダウンロードし、そのイメージを使用してエンクロージャのファームウェアを更新します	エンクロージャ管理者だけが、このコマンドを実行できます <URL>は以下のどれかです <ul style="list-style-type: none">● http://host/path● tftp://host/path● ftp://username:password● @host/path● ftp://host/path。ここで、「host」は完全修飾ドメイン名または IP アドレスであり、「path」はダウンロードするフラッシュ イメージのパス名です
UPLOAD CONFIG <URL>	現在の実行時設定を指定した FTP または TFTP サーバにアップロードします	エンクロージャ管理者だけが、このコマンドを実行できます

システム ログの重大度ポリシーの固有設定は、グローバルで、管理者アカウントによってのみ設定されます。この設定は、システム ログ メッセージの重大度の種類の特定の分類を細かく制御できるようにするために追加されました

- SET SYSLOG POLICY ENCLOSURE
 - SET SYSLOG POLICY ENCLOSURE ALL [ON | OFF]
 - SET SYSLOG POLICY ENCLOSURE INFORMATIONAL [ON | OFF]
 - SET SYSLOG POLICY ENCLOSURE MAJOR [ON | OFF]
-

- SET SYSLOG POLICY ENCLOSURE MINOR [ON | OFF]
 - SET SYSLOG POLICY ENCLOSURE NORMAL [ON | OFF]
 - SET SYSLOG POLICY BAY
 - SET SYSLOG POLICY BAY ALL [ON | OFF]
 - SET SYSLOG POLICY BAY INFORMATIONAL [ON | OFF]
- 注記：** 初期設定は、OFF です。
- SET SYSLOG POLICY BAY MAJOR [ON | OFF]
 - SET SYSLOG POLICY BAY MINOR [ON | OFF]
 - SET SYSLOG POLICY BAY NORMAL [ON | OFF]

Blade PC ベイの管理コマンド

表 5-6

コマンド	説明	制限事項
CLEAR BAY BOOT [FIRST ONCE ALWAYS] [ALL <ベイ番号> {[, -] <ベイ番号>}]	次の再起動時にブレードに渡される IPL の設定を消去します。「FIRST」引数は、以降のすべての再起動に対して IPL をリセットします。「ONCE」引数は、次の再起動だけに対して IPL をリセットします。「Always」引数は、すべての再起動に対して IPL をリセットします。このコマンドは、存在するブレードに対してだけ有効です	エンクローージャ管理者とグループ管理者だけが、このコマンドを実行できます
	このコマンドを実行するには、特定の HP Blade PC の BIOS ROM 用ファームウェアのアップデートが必要になる場合があります	
CLEAR SESSION BAY <ベイ番号>	エンクローージャから端末セッションを終了します これは正しい終了方法ではありません。接続しているユーザは、まだ保存していない作業をすべて失います	エンクローージャ管理者は、Blade PC ベイとインターコネク ト スイッチに対してこのコマンドを実行できます
CONNECT BAY <ベイ番号>	Blade PC へのリモート コンソール セッションを、その Blade PC のベイ番号を使用して開きます 1 つの Blade PC が同時にサポートできるリモート コンソール セッションは、1 つだけです。	エンクローージャ管理者とグループ管理者だけが、このコマンドを実行できます
GENERATE NMI <ベイ番号>	指定したブレードで NMI を生成します NMI の結果は、オペレーティング システム固有です	エンクローージャ管理者とグループ管理者だけが、このコマンドを実行できます
		注記： ブレード固有のオペレーティング システムは、NMI の「クラッシュ ダンプ」機能をサポートする必要があります。そうでない場合、ブレード上で予測不能な結果が発生する可能性があります。詳しくは、OS に付属の説明書を参照するか、ベンダに問い合わせてください

(続き)

<p>POWEROFF BAY</p> <p><ベイ番号> {[, -] <ベイ番号>} {FORCE}</p>	<p>指定したベイ内の Blade PC の正しいシャットダウンを実行します</p> <p>FORCE 引数を指定すると、Blade PC はただちにシャットダウンされます。これによって、Blade PC のデータが失われるか、または Blade PC が不安定になる可能性があります。指定したベイに Blade PC が存在しない場合は、ベイが空であることがユーザに通知されます</p>	<p>エンクロージャ管理者とグループ管理者だけが、このコマンドを実行できます</p>
<p>POWERON BAY</p> <p><ベイ番号> {[, -] <ベイ番号>} {PXE HDD RBSU}</p>	<p>指定した Blade PC の電源を入れます</p> <p>指定したベイに Blade PC が存在しない場合は、ベイが空であることがユーザに通知されます</p> <p>オプションの起動引数を使用するには、特定の HP Blade PC の BIOS ROM 用ファームウェアのアップデートが必要になる場合があります</p> <p>オプションの起動引数を追加すると、強制的に Blade PC は通常の起動順序を破棄し、指定した方法を使用して起動するようになります</p>	<p>エンクロージャ管理者とグループ管理者だけが、このコマンドを実行できます</p>
<p>REBOOT BAY <ベイ番号> {[, -] <ベイ番号>} {FORCE} {PXE HDD RBSU}</p>	<p>正しいシャットダウンを実行する要求を Blade PC に送信します</p> <p>次に、Blade PC の電源が入ります。指定したベイに Blade PC が存在しない場合は、ベイが空であることがユーザに通知されます</p> <p>オプションの起動引数を使用するには、特定の HP Blade PC の BIOS ROM 用ファームウェアのアップデートが必要になる場合があります</p> <p>オプションの起動引数を追加すると、強制的に Blade PC は通常の起動順序を破棄し、指定した方法を使用して起動するようになります</p>	<p>エンクロージャ管理者とグループ管理者だけが、このコマンドを実行できます</p>
<p>SET BAY BOOT FIRST [HDD PXE] <ベイ番号> {[, -] <ベイ番号>}</p>	<p>以降の再起動ごとに IPL を設定します。この設定は、存在するブレードに対してだけ有効であり、ブレードが取り外されると消去されます</p> <p>このコマンドを実行するには、特定の HP Blade PC の BIOS ROM 用ファームウェアのアップデートが必要になる場合があります</p>	<p>エンクロージャ管理者だけが、このコマンドを実行できます</p>
<p>SET BAY BOOT ONCE [HDD PXE RBSU] <ベイ番号> {[, -] <ベイ番号>}</p>	<p>指定したベイの、次の起動時に使用する起動デバイスを設定します。この設定は、存在するブレードに対してだけ有効であり、ブレードが取り外されると消去されます</p> <p>このコマンドを実行するには、特定の HP Blade PC の BIOS ROM 用ファームウェアのアップデートが必要になる場合があります</p>	<p>エンクロージャ管理者とグループ管理者だけが、このコマンドを実行できます</p>
<p>SET BAY UID <ベイ番号> {[, -] <ベイ番号>} [ON OFF]</p>	<p>Blade PC のユニット確認ランプをオンまたはオフにします</p>	<p>エンクロージャ管理者とグループ管理者だけが、このコマンドを実行できます</p>
<p>SHOW BAY INFO [ALL <ベイ番号> {[, -] <ベイ番号>}]</p>	<p>割り当て先グループ、種類、名前、インストールされているオペレーティングシステム、製品番号、シリアル番号、アセットタグ、BIOSバージョン、すべてのCPUの種類とその最大速度、メモリ、NIC #1 MAC、およびNIC #2 MACのフィールドを表示します。bc2x00ブレードの場合は、BMCリビジョンも表示されます。BMCバージョン22またはそれ以前のバージョンではこの情報が提供されないため、バージョンは22hまたはそれ以前と想定され、そのように示されます</p>	<p>グループメンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p>

(続き)

	<p>す。将来のバージョンではこの機能がサポートされる予定です。以前のバージョンは (N/A) と示されます</p> <p>BIOS 3.x シリーズを搭載したブレードの場合は、UUID (Universal Unique Identifier) も表示されます</p> <p>ベイに Blade PC が存在しない場合は、割り当て先グループと Blade PC の種類が表示されます</p>	
SHOW BAY INFO LIST	<p>ブレードの BMC (Blade Management Controller) リビジョン、BIOS リビジョン、および保留中の起動順序を表形式で表示します</p>	<p>グループ メンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p>
SHOW BAY LIST [ALL <グループ名>]	<p>グループ名を指定すると、特定のグループ内の各ベイについて、割り当て先グループ、リモートコンソールユーザ、および Blade PC 名が表示されます。「ALL」を指定すると、すべてのベイについてこの情報が表示されます</p>	<p>グループ メンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p>
SHOW BAY STATUS [ALL <ベイ番号> {[, -] <ベイ番号>}]	<p>Blade PC の電源 (オンまたはオフ)、割り当て先グループ、リモート コンソール ユーザ、ヘルス、温度 (OK、温度上昇、機能低下、または障害)、およびユニット確認ランプ (オンまたはオフ) を表示します</p> <p>BIOS 3.x シリーズを搭載した bc2x00 ブレードの場合は、診断アダプタ、システム BIOS の POST ステータス、ネットワーク (PXE) 起動ステータス、前面 I/O ブランク機能ステータス、および自動システム復旧 (ASR) モード ステータスも表示します</p>	<p>グループ メンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p>
SHOW BAY STATUS LIST	<p>ベイの温度情報およびステータスを表形式で表示します</p>	<p>グループ メンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p>
SHOW BAY POWER [ALL <ベイ番号> {[, -] <ベイ番号>}]	<p>測定された DC 電源の電力消費量、AC 電源の推定電力消費量、電力の過去 24 時間の平均およびブレードの取り付け以降の時間平均を表示します</p>	<p>グループ メンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p> <p>注記： AC の推定電力消費量は、ブレードの測定された DC 電力消費量をエンクロージャの推定電力供給効率で割った値です。以前のバージョンは (N/A) と示されます</p>
SHOW BAY POWER LIST [ALL <ベイ番号> {[, -] <ベイ番号>}]	<p>AC 電源の推定電力消費量を除く、上記のすべてのブレード電力消費量の指標を見やすい表形式で表示します</p>	<p>グループ メンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p> <p>注記： 電力測定値を表示できるのは、bc2x00 ブレードのみです。電力を認識しないブレードはすべて、(N/A) と報告します</p>
SHOW BAY TEMP [ALL <ベイ番号> {[, -] <ベイ番号>}]	<p>CPU、グラフィックス プロセッサ、および周辺温度センサの実際の温度を表示します</p>	<p>グループ メンバとグループ管理者は、自分のグループ内のベイに関する情報だけを表示できます</p>
SHOW BAY TEMP LIST	<p>ベイの温度情報およびステータスを表形式で表示します</p>	<p>グループ メンバとグループ管理者は、自分のグループ内の</p>

(続き)

		ベイに関する情報だけを表示 できます
SHOW SYSLOG BAY <ベイ番号>	指定したブレードのシステム ログを、1 画面あたり 22 行で 表示します Q キーを押すと、コマンドが終了します。さらに表示情報が 続く場合は、他の任意のキーを押すと次の画面が表示されま す。Blade PC のシステム ログは再起動したときに保存され ないため、この情報には Integrated Administrator の最後の電 源投入以降に発生した内容だけが含まれます C キーを押すと、システム ログがページの区切りなく連続し て表示されます	グループ メンバとグループ管 理者は、自分のグループ内の ベイに関する情報のみを表示 できます
UNASSIGN BAY [ALL <ベ イ番号> {[, -] <ベイ番号 >}]	割り当てられたグループからベイを削除します	エンクロージャ管理者だけ が、このコマンドを実行でき ます

コマンド ライン イベント メッセージ

表 5-7 コマンド ライン イベント メッセージ

メッセージ	考えられる原因
ユーザのイベント メッセージ	
User Permission Change	以下のどちらかの操作が行われました <ul style="list-style-type: none">ユーザが追加、削除、または変更されたユーザのグループ メンバシップが変更された 少なくとも 1 人のユーザについて、グループの Blade PC ベ イのメンバシップが変更されました
エンクロージャのイベント メッセージ	
Enclosure Shutdown	エンクロージャをシャットダウンしています
Enclosure Status Change	Integrated Administrator が、1 つまたは複数のハードウェ ア コンポーネントまたは Blade PC 読み取り値の状態の変 化によるステータスの変化を検出しました
Fan Inserted	ファンが取り付けられました
Fan Removed	ファンが取り外されました
Fan Status Change	ファンのステータスが変化しました
Power Supply Inserted	電源供給装置が取り付けられました
Power Supply Overload	電源システムが過負荷状態になっています。各電源供給装置 のステータスをチェックして、原因を特定してください
Power Supply Redundancy Change	電源供給装置がリダンダントになったか、またはリダンダン トでなくなりました 電源サブシステムが、リダンダント、レジリエント、または 非リダンダントのどれかのステータスに変わりました
Power Supply Removed	電源供給装置が取り外されました
Power Supply Status Change	電源供給装置のステータスが変化しました

表 5-7 コマンド ライン イベント メッセージ (続き)

Restart Event	Integrated Administrator を再起動します
Thermal Status Change	温度センサの状態が変化しました 注記: bc2x00 ブレードの場合、ベイ センサによって報告される温度関連のイベントには、最も温度が高いサブコンポーネント センサが報告した値に対するベイ温度が含まれます
ベイのイベント メッセージ	
Bay Event	Blade PC ベイがグループに割り当てられたか、またはグループの割り当てを解除されました
Blade Inserted	Blade PC がエンクロージャに取り付けられました
Blade Removed	Blade PC がエンクロージャから取り外されました
Blade Status Change	ヘルス サービス、つまり BMC (Blade Management Controller) は、1 つまたは複数のハードウェア コンポーネントの状態の変化またはブレードで自動システム復旧 (ASR) が有効になっている場合のソフトウェア OS ロックアップによるステータスの変化を検出しました bc2x00 ブレードの場合、診断文字列にはイベント メッセージが含まれています。診断文字列とその説明については、 144 ページの「エラー メッセージ」 を参照してください <ul style="list-style-type: none"> • Blade in bay # has powered off. • Blade in bay # has powered on. • Blade in bay # has started flash mode. 注記: BMC をサポートするブレードだけが、このメッセージを表示します。さらに、フラッシュ モードが完了すると、BAY REMOVED、BAY INSERTED イベント メッセージが表示されます。これは正常なフラッシュ プロセスの一部であり、無視してかまいません
Blade BMC in bay # has exited flash mode and will auto-powercycle in 10 seconds.	ベイ#の Blade BMC がフラッシュ モードを終了しました。10 秒後に電源が自動的に入れ直されます。
Blade BMC in bay # will now auto powercycle OFF and then back ON.	ベイ#の Blade BMC の電源が自動的にオフになり、その後オンになります。
Blade in bay # POST completed.	ベイ#のブレードが POST を完了しました。
Blade in bay # unexpected shutdown occurred.	ベイ#のブレードで予期しないシャットダウンが発生しました。
Blade in bay # entered PXE boot mode.	ベイ#のブレードが PXE 起動モードを開始しました。
Blade in bay # exited PXE boot mode.	ベイ#のブレードが PXE 起動モードを終了しました。
Blade in bay # warm reset occurred.	ベイ#のブレードで温度上昇によるリセットが発生しました。
Blade in bay # Diagnostic Adaptor status changed to [Present Absent].	ベイ#のブレードの診断アダプタが、[あり なし]の状態に変わりました。
Blade in bay # Front IO Blanking Feature status changed to [Active Inactive].	ベイ#のブレードの前面 I/O ブランク機能が、[非アクティブ アクティブ]の状態に変わりました。

表 5-7 コマンドライン イベント メッセージ (続き)

Blade in bay # system BIOS flashing completed.	ベイ#のブレードでシステム BIOS のフラッシュが完了しました。
Blade in bay # system BIOS flashing started.	ベイ#のブレードでシステム BIOS のフラッシュが開始されました。

コマンド ライン インタフェース特有の機能

以下の表では、Web ベースのインタフェースを使用しているときには利用できない、コマンド ライン インタフェース (CLI) 特有の機能について説明します。

表 5-8 コマンド ライン インタフェース特有の機能：一般的なコマンドおよび一般的な管理コマンド

機能	説明	CLI 特有の機能
一般的なコマンド		
Sleep <秒>	セッションを一定の期間一時停止します。スクリプトに遅延を追加する場合に便利です。<秒>フィールドには、1～86400 の任意の整数を指定できます。一時停止が開始された後、時間切れになる前にセッションを再開する方法はありません。ただし、そのセッションを終了して別のセッションを開始することは可能です	なし
一般的な管理コマンド		
CLEAR SESSION SWITCH [A B]	エンクロージャから端末セッションを終了します これは正しい終了方法ではありません。接続しているユーザは、まだ保存していない作業をすべて失います	すべて
CLEAR SSHKEY	Secure Shell 認証済みキー ファイルの内容を削除します。このコマンドを実行すると、パブリック キーベースの認証を使用してログインすることはできなくなります	エンクロージャ管理者だけが、このコマンドを実行できます
DOWNLOAD CERTIFICATE <URL>	システムにある現在のセキュリティ証明書を置き換えるために、CA から提供された PKCS#7 ファイルをダウンロードします サポートされているプロトコルは、http、ftp、および tftp です。URL は、 protocol://host/path/file の形式にします。FTP サーバで匿名接続がサポートされていない場合は、上記の形式の「host」にあたる部分を「username:password@host」に置き換えることでユーザ名とパスワードを指定できます	すべて
DOWNLOAD SSHKEY	Secure Shell v2 で使用する認証済みのキー ファイルをダウンロードします。このファイルには、任意のエンクロージャ管理者用のパブリック キーを含めることができます。サポートされているプロトコルは、http、ftp、および tftp です。URL は、 protocol://host/path/file の形式にします。FTP サーバで匿名接続がサポートされていない場合は、上記の形式の「host」にあたる部分を「username:password@host」に置き換えることでユーザ名とパスワードを指定できます	エンクロージャ管理者だけが、このコマンドを実行できます
GENERATE CERTIFICATE REQUEST	PKCS#10 証明書要求を生成します	すべて
GENERATE CERTIFICATE SELFSIGNED	自己署名証明書を生成します	すべて
PING {<回数>} [<IP アドレス> <サーバ名>]	リモート IP デバイスに ICMP エコー メッセージを送信します <回数>を省略すると、5つのパケットだけが送信されます。パケットは、1秒間隔で送信されます	すべて
SET DISPLAY EVENTS [ON OFF]	イベント通知をオンまたはオフにします	すべて
SET EXPERT {MODE} [ON OFF]	EXPERT MODE をオンまたはオフにします。EXPERT MODE がオンになっている場合、システムはユーザに操作の	なし

表 5-8 コマンド ライン インタフェース特有の機能：一般的なコマンドおよび一般的な管理コマンド（続き）

	確認を求めません。元に戻せない操作が多いため、EXPERT MODE で作業する場合は注意してください	
SET FACTORY	<p>Integrated Administrator を出荷時の設定に戻します</p> <p>「Administrator」アカウントのパスワードは変更されません。すべての変更が行われた後、Integrated Administrator は再起動されます</p> <p>注記： このコマンドを実行すると、エンクロージャのメモリからグループ、ユーザ、その他のカスタマイズがすべて削除され、削除された情報を元に戻すことはできません</p> <p>このコマンドは、SET EXPERT コマンドの例外です。SET FACTORY コマンドを EXPERT MODE で実行する場合でも、このコマンドは確認動作を必要とします。確認を不要にするには、SCRIPT MODE をオンにする必要があります</p> <p>SET FACTORY の実行では、初期設定のアセット タグがシリアル番号と同じ値になります</p>	すべて
SET SCRIPT MODE [ON OFF]	<p>SCRIPT MODE がオンになっていると、すべての入力プロンプトとその確認が停止します</p> <p>SCRIPT MODE がオンになっていると、ADD USER、SET USER PASSWORD、または SET PASSWORD コマンドにはパスワード引数が必要になります。パスワード引数を指定しないと、空のパスワードが割り当てられます</p> <p>エンクロージャ管理者は、ユーザがシステムにログインできるようにパスワードを変更する必要があります。通常は、ユーザの入力が必要なパラメータについては、初期値が使用されます</p>	すべて
SHOW EXPERT {MODE}:	現在のユーザに対する現在の EXPERT MODE 設定を表示します	なし
SHOW SESSIONS	<p>各ベイおよびスイッチへの接続を表示します（接続が存在する場合）</p> <p>各ベイおよびスイッチには、1 回に 1 人のユーザしか接続できません。また、現在ログインしているユーザ、そのユーザのポート番号、接続時間、およびリモート システム名も表示されます</p>	すべて
SHOW SSHFINGERPRINT	Integrated Administrator のホスト SSH パブリック キーのキー フィンガープリントを表示します。このコマンドをシリアル コンソールから使用すると、ネットワーク全体にわたる SSH 接続を初期化する前に、Integrated Administrator の識別情報を検証できます	なし
SHOW SSHKEY	エンクロージャ管理者のキーベースの認証に使用されている既存の Secure Shell 認証済みキー ファイルの内容を表示します	エンクロージャ管理者だけが、このコマンドを実行できます
DOWNLOAD CONFIG <URL>	<p>以前に保存された設定ファイルを特定の IP ホストからダウンロードします</p> <p>このファイルは、SCRIPT MODE で自動実行されます。このファイルで「Administrator」アカウントのパスワードを変更することはできません。サポートされているプロトコルは、http、ftp、および tftp です。URL は、protocol://host/path/file の形式にします。FTP サーバで匿名接続がサポートされていない場合は、上記の形式の「host」にあたる部分を「username:password@host」に置き換えることでユーザ名とパスワードを指定できます</p>	なし

表 5-9 コマンド ライン インタフェース特有の機能：エンクロージャの管理コマンド

機能	説明	CLI 特有の機能
エンクロージャの管理コマンド		
SHOW CONFIG	エンクロージャの設定を再作成するために必要なスクリプトを表示します パスワードはどのユーザのものも含まれていません	すべて
SHOW ENCLOSURE FAN [<ファン番号> ALL]	指定したファンのステータス、リダundant状態、ペアとなるファン、速度、および製品番号を表示します	コマンドラインでは、ペアとなるファンが追加されます
SHOW ENCLOSURE POWERSUPPLY [<電源番号> ALL]	電源を指定すると、その電源について、電源のステータス、AC 入力のステータス、容量、入力電圧範囲#1 (V)、入力電圧範囲#2 (V)、入力周波数範囲 (Hz)、製品番号、シリアル番号、およびハードウェア リビジョンが表示されます。「ALL」を指定すると、すべての電源についてこの情報が表示されます	コマンドラインでは、入力電圧範囲、入力周波数範囲、シリアル番号、およびハードウェア リビジョンが追加されます
SHOW ENCLOSURE STATUS	エンクロージャ ステータスの見出しに、エンクロージャのヘルス、Integrated Administrator のヘルス、およびユニット確認ランプを表示します 電源ステータスの見出しに、電源のステータスと容量を表示します	コマンドラインでは、Integrated Administrator のヘルスが追加されます
UPDATE IMAGE <URL>	ネットワーク経由でサーバから新しいイメージをダウンロードし、そのイメージを使用してエンクロージャのファームウェアをアップデートします	なし
UPLOAD CONFIG <URL>	現在の実行時設定を、指定した FTP または TFTP サーバにアップロードします	なし
CLEAR SESSION BAY <ベイ番号>	エンクロージャから端末セッションを終了します	すべて
CLEAR BAY BOOT [FIRST ONCE] [ALL <ベイ番号> {[, -] <ベイ番号>}>]]	次の再起動時に Blade PC に渡される IPL の設定を消去します。「FIRST」引数は、以降のすべての再起動に対して IPL をリセットします。「ONCE」引数は、次の再起動だけに対して IPL をリセットします。このコマンドは、存在する Blade PC に対してだけ有効です このコマンドを実行するには、特定の HP Blade PC の BIOS ROM 用にファームウェア アップグレードが必要になる場合があります	エンクロージャ管理者とグループ管理者だけが、このコマンドを実行できます
GENERATE NMI <ベイ番号>		
POWERON BAY <ベイ番号> {[, -] <ベイ番号>} {[PXE HDD RBSU]}	指定した Blade PC の電源を入れます 指定したベイに Blade PC が存在しない場合は、ベイが空であることがユーザに通知されます オプションの起動引数を使用するには、特定の HP Blade PC の BIOS ROM 用にファームウェア アップグレードが必要になる場合があります オプションの起動引数を追加すると、強制的に Blade PC は通常の起動順序を破棄し、指定した方法を使用して起動するようになります	オプションの起動引数が使用可能
REBOOT BAY <ベイ番号> {[, -] <ベイ番号>}	正しいシャットダウンを実行する要求を Blade PC に送信します	オプションの起動引数が使用可能

表 5-9 コマンドライン インタフェース特有の機能：エンクロージャの管理コマンド（続き）

{FORCE} {[PXE HDD RBSU]}	次に、Blade PC の電源が入ります。指定したベイに Blade PC が存在しない場合は、ベイが空であることがユーザーに通知されます	
	オプションの起動引数を使用するには、特定の HP Blade PC の BIOS ROM 用にファームウェア アップグレードが必要になる場合があります	
	オプションの起動引数を追加すると、強制的に Blade PC は通常の起動順序を破棄し、指定した方法を使用して起動するようになります	
SET BAY BOOT FIRST [HDD PXE] <ベイ番号> {[, -] <ベイ番号>}	以降の再起動ごとに IPL を設定します。この設定は、存在する Blade PC に対してだけ有効であり、Blade PC が取り外されると消去されます	エンクロージャ管理者だけが、このコマンドを実行できます
	このコマンドを実行するには、BIOS のファームウェア アップグレードが必要になる場合があります	
SET BAY BOOT ONCE [HDD PXE RBSU] <ベイ番号> {[, -] <ベイ番号>}	指定したベイの、次の起動時に使用する起動デバイスを設定します。この設定は、存在する Blade PC に対してだけ有効であり、Blade PC が取り外されると消去されます	エンクロージャ管理者だけが、このコマンドを実行できます
	このコマンドを実行するには、特定の HP Blade PC の BIOS ROM 用にファームウェア アップグレードが必要になる場合があります	
SHOW BAY LIST [ALL <グループ名>]	グループ名を指定すると、特定のグループ内の各ベイについて、割り当て先グループ、リモートコンソールユーザ、および Blade PC 名が表示されます。「ALL」を指定すると、すべてのベイについてこの情報が表示されます	コマンドラインでは、リモートコンソールユーザが表示されます
SHOW SYSLOG BAY <ベイ番号>	指定した Blade PC のシステム ログを、1 画面あたり 22 行で表示します	すべて
	Q キーを押すと、コマンドが終了します。さらに表示情報が続く場合は、他の任意のキーを押すと次の画面が表示されます。Blade PC のシステム ログは再起動したときに保存されないため、この情報には Integrated Administrator の最後の電源投入以降に発生した内容だけが含まれます	
	C キーを押すと、システム ログがページの区切りなく連続して表示されます	
ADD IPMANAGER <IP アドレス>	Integrated Administrator への接続を許可されたクライアントの一覧に、IP アドレスを追加します	エンクロージャ管理者だけが、このコマンドを実行できます
DISABLE ALERTMAIL	電子メールによる Integrated Administrator のアラート送信を無効にします	エンクロージャ管理者だけが、このコマンドを実行できます
DISABLE IPSECURITY	すべてのクライアントに Integrated Administrator への接続を許可します	エンクロージャ管理者だけが、このコマンドを実行できます
DISABLE NTP	Integrated Administrator に対する日付と時刻の自動更新を無効にします	一部のネットワークの有効/無効パラメータのみが対象です
ENABLE ALERTMAIL	電子メールによる Integrated Administrator のアラート送信を有効にします	エンクロージャ管理者だけが、このコマンドを実行できます
ENABLE IPSECURITY	クライアントの Integrated Administrator への接続を制限しません	エンクロージャ管理者だけが、このコマンドを実行できます

表 5-9 コマンド ライン インタフェース特有の機能 : エンクロージャの管理コマンド (続き)

ENABLE NTP	Integrated Administrator に対する日付と時刻の自動更新を有効にします	エンクロージャ管理者だけが、このコマンドを実行できます
REMOVE IPMANAGER <IP アドレス>	Integrated Administrator への接続を許可されたクライアントの一覧から、IP アドレスを削除します	エンクロージャ管理者だけが、このコマンドを実行できます
SET ALERTMAIL [MAILBOX SENDERDOMAIN SMTPSERVER]	アラート受信者の電子メール アドレス、ドメイン名、およびメール サーバ アドレスを設定します	なし
SET NTP [PRIMARY SECONDARY POLL]	プライマリおよびセカンダリ NTP サーバの IP アドレスを設定します。また、更新の頻度も設定します	なし
SHOW NETWORK	エンクロージャの DHCP の状態、動的 DNS の状態、IP アドレス、サブネット マスク、ゲートウェイ アドレス、プライマリおよびセカンダリ DNS アドレス、MAC アドレス、HTTP および HTTPS サーバのステータス、SNMP のステータス、Secure Shell のステータス、Telnet のステータス、NTP のステータス、NTP プライマリおよびセカンダリ サーバのアドレス、NTP ポーリング間隔、NTP 最終更新時間、IP セキュリティ設定、AlertMail のステータス、AlertMail のメールボックス、SMTP サーバ アドレス、および送信者ドメインを表示します	エンクロージャ管理者だけが、このコマンドを実行できます
SET ENCLOSURE SERIAL {NUMBER} <シリアル番号>	エンクロージャ情報によって報告されたシリアル番号の変更を許可します	エンクロージャ管理者だけが、このコマンドを実行できます
SHOW BAY TEMP [ALL <ベイ番号> {[, -] <ベイ番号>}]	CPU、グラフィックス プロセッサ、および周辺温度センサの実際の温度を表示します	なし

6 システムの設定

この章では、まず Integrated Administrator によって認識されるユーザ アクセス権のレベルについて説明し、次に Integrated Administrator で提供されている管理機能を設定するための詳細な手順を示します。

- エンクロージャ設定のカスタマイズ
 - 管理者パスワードの変更
 - エンクロージャ名とラック名の変更
 - アセット タグ番号の変更
 - 日付と時刻の変更
 - ブレード自動電源投入機能の有効/無効の設定
- ユーザ アカウントの設定
 - グループの追加
 - ユーザの追加
- Blade PC へのリモート コンソール セッションの有効化
- AlertMail の設定
 - メールボックス アドレスの追加
 - SMTP サーバ アドレスの追加
 - 送信者ドメインの追加
 - AlertMail の有効化
 - AlertMail の無効化
- IP セキュリティの設定
 - IP アドレスの追加
 - IP セキュリティの有効化
 - IP セキュリティの無効化

- 自動時間設定（NTP）の設定
 - プライマリ NTP サーバの追加
 - セカンダリ NTP サーバの追加
 - ポーリング間隔の設定
 - NTP の有効化
 - NTP の無効化
 - トラップ ポリシーの設定
- SNMP サポートの設定
 - コミュニティ名の入力
 - システムの位置の変更
 - システム連絡先情報の変更
 - トラップ送信先の追加
 - トラップ送信先の削除
 - SOAP の設定
 - SOAP インタフェースの有効化
 - SAM アカウントの有効化

このガイドで使用されているコマンド ラインの規則については、[143 ページの「コマンド ラインの規則」](#)を参照してください。

特に記載がない限り、これらの手順は、Web ベースのユーザ インタフェースと CLI の両方でサポートされています。

 **注記：** これらのタスクのほとんどは、実行が一部のユーザに制限されています。各タスクを実行できるユーザについては詳しくは、この章の[89 ページの「ユーザ アクセス権」](#)、およびそれらのタスクを説明している項を参照してください。

ユーザ アクセス権

ユーザ アクセス権に関する Integrated Administrator のグループ中心の方式は、ユーザ グループや Blade PC ベイのグループのメンテナンスを容易にします。この方式は、以下の原理に従っています。

- 1 つの Blade PC ベイは、排他的に 1 つのグループにだけ割り当てられます。
- 1 つのグループに、多数の Blade PC ベイを割り当てることができます。
- 1 人のユーザが任意の数のグループ内で、さまざまなアクセス権レベルを持つことができます。
- ユーザまたはグループによる Blade PC へのアクセスは、その Blade PC が搭載されている Blade PC ベイに割り当てられたアクセス権に依存します。

以下の表では、HP PC Blade Enclosure Integrated Administrator から使用できる各種のアクセス権レベルの違いについて説明します。

表 6-1 HP PC Blade Enclosure Integrated Administrator のアクセス権レベル

タイトル	アカウントの種類	アクセス権	説明
エンクロージャ管理者	管理者	エンクロージャ内のすべてのグループに対する表示/変更	<p>エンクロージャ管理者は、Blade PC ベイのアクセス権のメンテナンス、エンクロージャの管理、Blade PC ベイの管理、およびグループの作成とメンテナンスが可能です</p> <p>「Administrator」という名前の特殊なエンクロージャ管理者アカウントについては、削除、無効化、およびエンクロージャ管理者のアクセス権の剥奪ができません。他のどのエンクロージャ管理者も、このアカウントのパスワードを変更できません</p> <p>エンクロージャ管理者は、自分のアカウントを無効にしたり、削除したりすることはできません</p>
グループ管理者	ユーザ	表示/変更	<p>グループ管理者は、自分が管理者になっているグループの Blade PC ベイ データを管理できます</p> <p>グループ管理者は、自分がメンバになっているグループの Blade PC ベイ データを表示できます</p> <p>グループ管理者は、自分のプロフィール（アクセス権を除く）の変更と、エンクロージャデータの表示ができます</p>
グループ メンバ	ユーザ	表示	<p>グループ メンバは、自分がメンバになっているグループの Blade PC ベイ データを表示できます</p> <p>グループ メンバは、自分のプロフィール（アクセス権を除く）の変更と、エンクロージャデータの表示ができます</p>
グループ メンバ	ユーザ		グループ メンバ

エンクロージャ設定のカスタマイズ

 **注記：** エンクロージャ管理者だけが、これらのコマンドを実行できます。

Web ベースのユーザ インタフェースを使用して初期設定の管理者パスワードを変更するには、以下の操作を行います。

1. [Administration] タブをクリックします。
2. 左パネルにある [User List] をクリックします。
3. ユーザー一覧で、[Administrator] ユーザ名をクリックします。
4. [View/Modify User] をクリックします。[View/Modify User] 画面が表示されます。
5. [Change Password] をクリックします。

6. **[Password]**フィールドと**[Confirm password]**フィールドに、新しい管理者パスワードを入力します。
7. **[OK]**をクリックします。

CLI を使用して初期設定の管理者パスワードを変更するには、以下のように入力します。

```
SET USER PASSWORD Administrator <新しいパスワード>
```

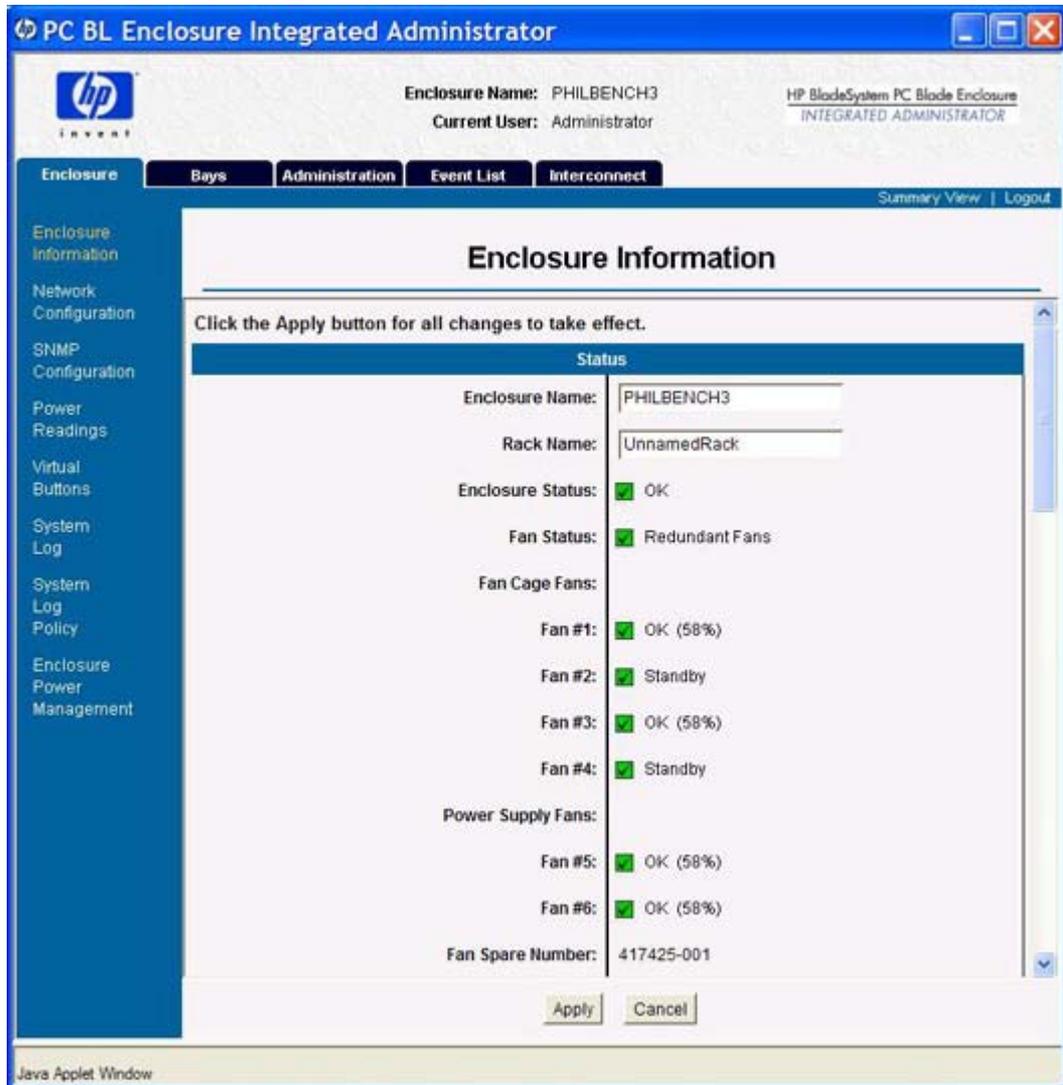
 **注記：** ユーザ名 (Administrator) では、大文字と小文字が区別されます。<新しいパスワード>は 3 ~ 8 文字の長さにする必要があり、すべての印刷可能文字を使用できます。

エンクロージャ名およびラック名の変更

Web ベースのユーザ インタフェースを使用してエンクロージャ名またはラック名を変更するには、以下の操作を行います。

1. **[Enclosure]** タブをクリックします。
2. 左パネルにある**[Enclosure Information]**をクリックします。
3. **[Status]** 領域の**[Enclosure Name]**フィールドをクリックします。
4. エンクロージャ名を入力します。
5. **[Status]** 領域の**[Rack Name]**フィールドをクリックします。

6. ラック名を入力します。



7. [Apply]をクリックします。

CLI を使用してエンクロージャ名またはラック名を変更するには、次のコマンドを続けて入力します。SET ENCLOSURE NAME <エンクロージャ名>

- 注記：** <エンクロージャ名>は 1 ~ 32 文字の長さにする必要があり、すべての英数字、ハイフン、およびアンダースコアを使用できます。

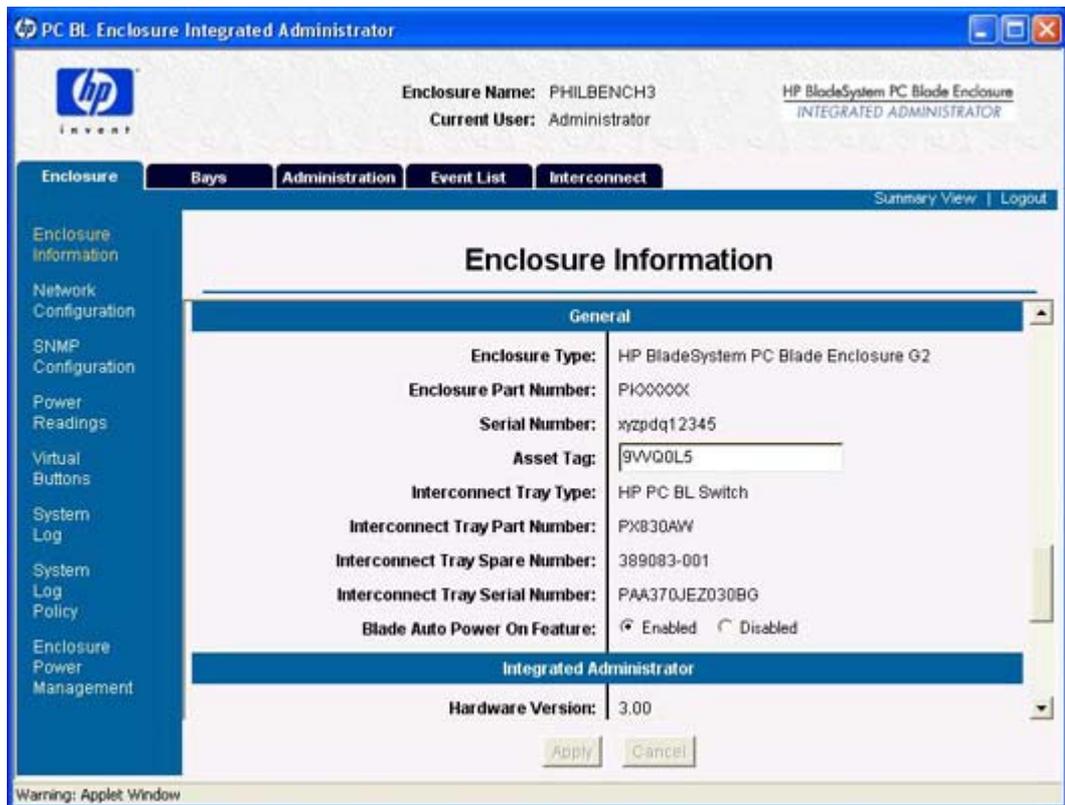
初期設定のエンクロージャ名は、IA-XXXXXXXXXXXXX です。この XXXXXXXXXXXXXXXX は、実際の MAC アドレスに置き換えられます。SET RACK NAME <ラック名>

- 注記：** <ラック名>は最大 32 文字の長さにする必要があり、すべての英数字、ハイフン、およびアンダースコアを使用できます。初期設定のラック名は「UnnamedRack」です。

アセット タグ番号の変更

Web ベースのユーザ インタフェースを使用してアセット タグを変更するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある [Enclosure Information] をクリックします。
3. [General] 領域まで下にスクロールします。
4. [Asset Tag] フィールドをクリックします。
5. アセット タグ番号を入力します。



6. [Apply] をクリックします。

CLI を使用してアセット タグ番号を変更するには、以下のように入力します。

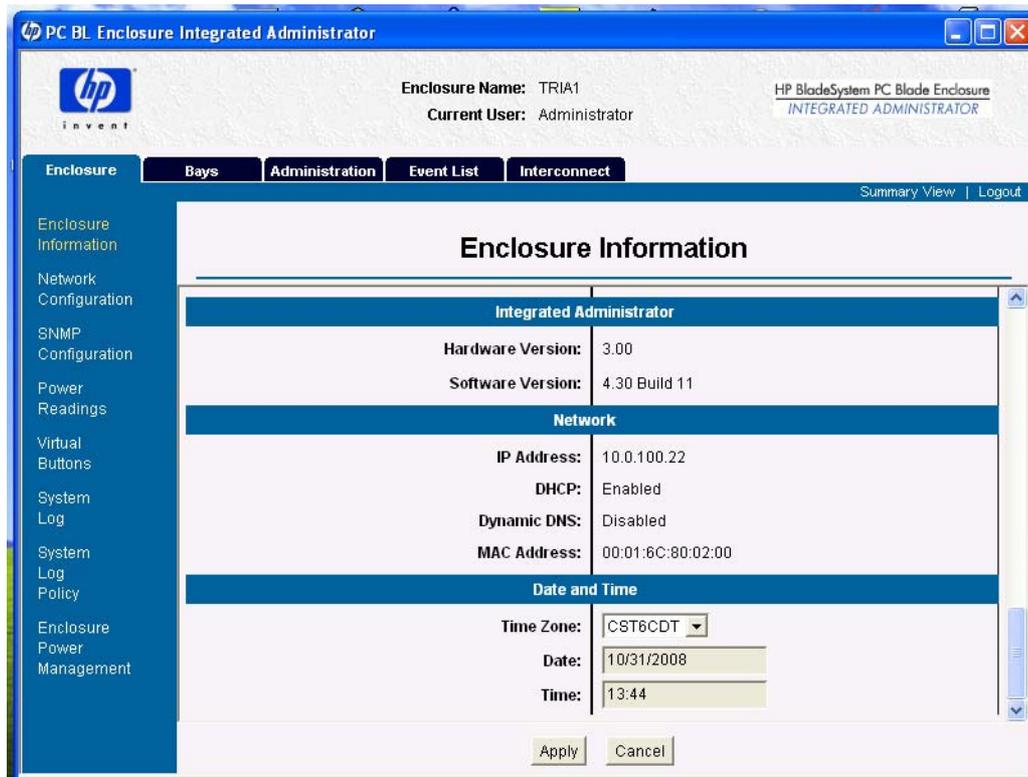
```
SET ENCLOSURE ASSET {TAG} <アセット タグ>
```

注記： <アセット タグ>は 1～31 文字の長さにする必要があり、英数字、ハイフン、およびアンダースコアを使用できます。初期設定のエンクロージャ アセット タグは空白です。

日付と時刻の変更

Web ベースのユーザ インタフェースを使用して日付と時刻の設定を変更するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある [Enclosure Information] をクリックします。
3. [Date and Time] 領域まで下にスクロールします。
4. プルダウン リストから、該当するタイム ゾーンを選択します。
5. [Date] フィールドまたは [Time] フィールドをクリックします。
6. 日付または時刻を入力します。



7. [Apply] をクリックします。

CLI を使用して日付と時刻の設定を変更するには、以下のように入力します。

```
SET DATE MMDDhhmm{{CC}YY} {TZ}
```

ここで、各パラメータの意味は以下のとおりです。

- MM : 月
- DD : 日
- hh : 時 (24 時間制、0 ~ 23 の整数)
- mm : 分

- CC : 世紀
- YY : 年
- TZ : タイム ゾーン

📖 **注記 :** タイム ゾーンを空白のままにすると、現在のタイム ゾーンがそのまま有効になります。サポートされているタイム ゾーンの一覧については、[170 ページの「タイム ゾーンの設定」](#)を参照してください。

ユーザ アカウントの設定

📖 **注記 :** エンクロージャ管理者だけが、このタスクを実行できます。

Integrated Administrator では、Blade PC ベイやユーザをグループにまとめることによってそれらを管理できます。

この方式を使用すると、たとえば、エンクロージャ管理者は Blade PC のグループにユーザ アクセス権を一括して再割り当てでき、1 回に 1 ユーザずつアクセス権を変更する必要がなくなります。

エンクロージャ管理者は、以下のタスクを通して Blade PC ベイにユーザ アクセス権を割り当てます。

- エンクロージャ内の特定の Blade PC ベイへのアクセス権を持つグループの追加
- 特定のグループ内での特定のアクセス権を持つユーザの追加

グループの追加

📖 **注記 :** グループ アカウントとユーザ アカウントの限定された初期名 (Administrator、switch、switcha、switchb、および SAM) では、大文字と小文字が区別されません。初期設定以外のグループ名とユーザ名では、大文字と小文字が区別されます。

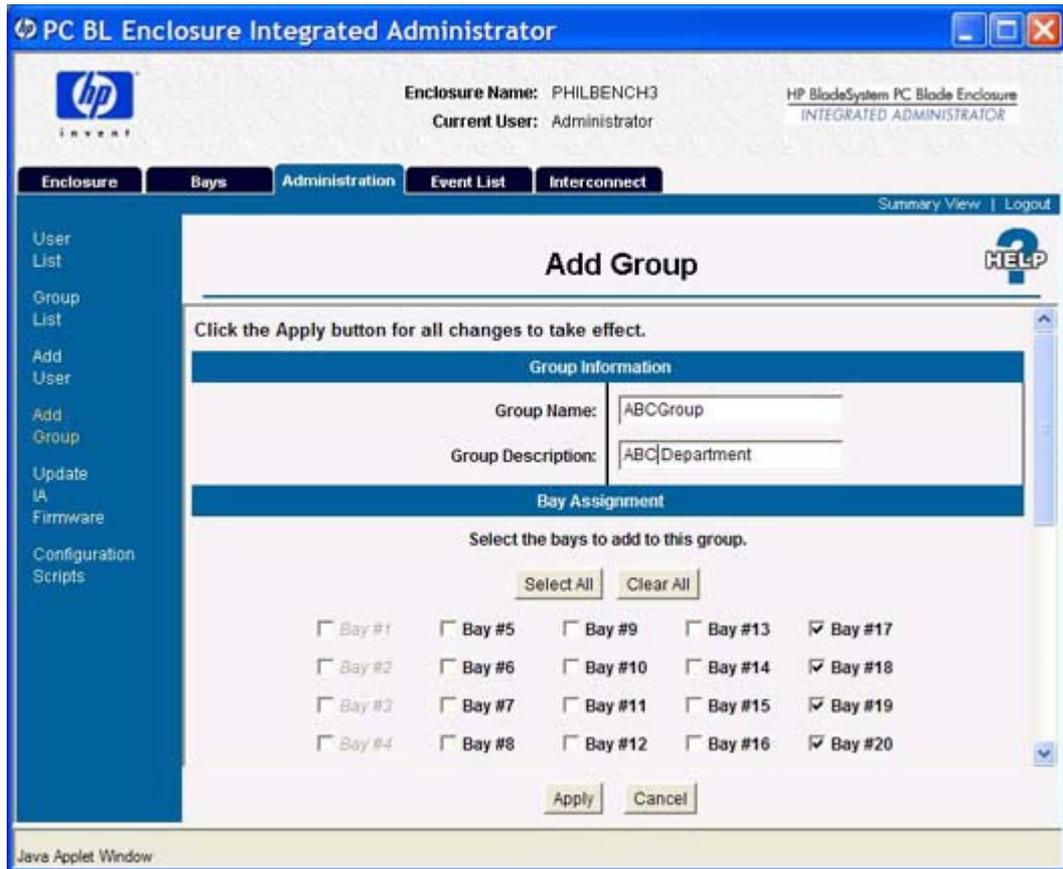
この機能のための Web ベースのユーザ インタフェース画面について詳しくは、[47 ページの「Group List」](#)を参照してください。CLI の使用方法については、[66 ページの「ユーザ アカウント コマンド」](#)を参照してください。

Web ベースのユーザ インタフェースを使用してグループを作成するには、以下の操作を行います。

1. **[Administration]** タブをクリックします。
2. 左パネルにある **[Add Group]** をクリックします。
3. 各フィールドに、グループ名と説明を入力します。

4. そのグループ用のベイを、該当するチェック ボックスにチェックを入れて選択します。

 **注記：** グレー表示になっている Blade PC ベイはすでに別のグループに属しているため、その Blade PC ベイにはアクセスできません。



PC BL Enclosure Integrated Administrator

Enclosure Name: PHILBENCH3
Current User: Administrator

HP BladeSystem PC Blade Enclosure
INTEGRATED ADMINISTRATOR

Enclosure Bays Administration Event List Interconnect

Summary View | Logout

Add Group

Click the Apply button for all changes to take effect.

Group Information

Group Name: ABCGroup
Group Description: ABCDepartment

Bay Assignment

Select the bays to add to this group.

Select All Clear All

<input type="checkbox"/> Bay #1	<input type="checkbox"/> Bay #5	<input type="checkbox"/> Bay #9	<input type="checkbox"/> Bay #13	<input checked="" type="checkbox"/> Bay #17
<input type="checkbox"/> Bay #2	<input type="checkbox"/> Bay #6	<input type="checkbox"/> Bay #10	<input type="checkbox"/> Bay #14	<input checked="" type="checkbox"/> Bay #18
<input type="checkbox"/> Bay #3	<input type="checkbox"/> Bay #7	<input type="checkbox"/> Bay #11	<input type="checkbox"/> Bay #15	<input checked="" type="checkbox"/> Bay #19
<input type="checkbox"/> Bay #4	<input type="checkbox"/> Bay #8	<input type="checkbox"/> Bay #12	<input type="checkbox"/> Bay #16	<input checked="" type="checkbox"/> Bay #20

Apply Cancel

Java Applet Window

5. このグループに既存のユーザを追加するには、以下の操作を行います。
 - a. [User Names]領域でユーザを選択します。



- b. [Add User [View]]または[Add User [View/Modify]]をクリックします。アクセス権レベルについて詳しくは、この章の89 ページの「ユーザ アクセス権」を参照してください。
6. [Apply]をクリックします。

CLI を使用してグループを作成するには、以下のコマンドを続けて入力します。

```
ADD GROUP <グループ名>
```

注記： <グループ名>は、他のすべてのグループ名およびユーザ名と異なる必要があり、大文字と小文字が区別されます。1～13文字の長さにする必要があり、すべての英数字、ハイフン、およびアンダースコアを使用できます。

```
SET GROUP {DESCRIPTION} <グループ名><説明>
```

注記： <説明>は1～20文字の長さにする必要があり、すべての英数字、ハイフン、アンダースコア、およびスペースを使用できます。

```
ASSIGN BAY [ALL | <ベイ番号> {[ , | - ]<ベイ番号>}] <グループ名>
```

```
ASSIGN USER <ユーザ名> <グループ名> {[VIEW | MODIFY]}
```

注記： <ユーザ名>と<グループ名>では、大文字と小文字が区別されます。「Administrator」アカウントをグループに追加することはできません。初期設定は、[View]です。

ユーザの追加

- ☞ **注記：** グループ アカウントとユーザ アカウントの限定された初期名では、大文字と小文字が区別されません。初期設定以外のグループ名とユーザ名では、大文字と小文字が区別されます。

アクセス権レベルについては、この章の89 ページの「ユーザ アクセス権」を参照してください。

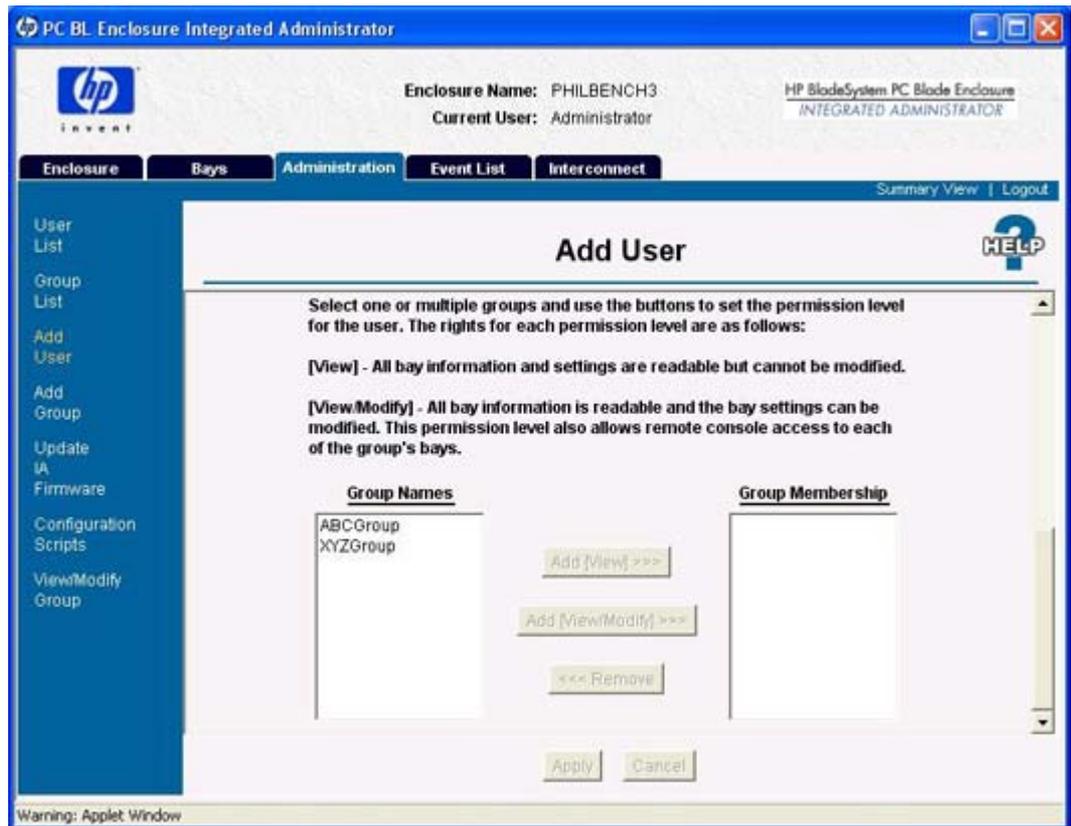
Web ベースのユーザ インタフェースを使用してユーザを作成するには、以下の操作を行います。

1. [Administration] タブをクリックします。
2. 左パネルにある [Add User] をクリックします。
3. 該当するフィールドに、ユーザ情報を入力します。[Account Type] については、この章の89 ページの「ユーザ アクセス権」を参照してください。

The screenshot displays the 'Add User' form within the HP BladeSystem PC Blade Enclosure Integrated Administrator. The interface includes a navigation menu on the left with options like 'User List', 'Group List', and 'Add User'. The main content area is titled 'Add User' and contains a 'User Account' form with the following fields: 'User Name' (filled with 'RCrusoe'), 'Password' (masked with '****'), 'Confirm Password' (masked with '****'), 'Account Type' (radio buttons for 'Administrator' and 'User', with 'User' selected), 'Account Status' (radio buttons for 'Enabled' and 'Disabled', with 'Enabled' selected), 'Full Name' (optional), and 'Contact Information' (optional). Below the form are 'Apply' and 'Cancel' buttons. The top of the window shows the enclosure name 'PHILBENCH3' and the current user 'Administrator'.

- ☞ **注記：** [Account Type] の設定によって、そのアカウント所有者が管理アクセス権を持つかどうかが決まります。オプションの [Full Name] フィールドと [Contact Information] フィールドには、アカウント所有者の名前および緊急時にすぐに連絡が取れる手段を記載します。

4. そのユーザを既存のグループに割り当てるには、以下の操作を行います。
 - a. [Group Names]領域のグループを選択します。



- b. [Add User [View]]または[Add User [View/Modify]]をクリックします。アクセス権レベルについて詳しくは、この章の89 ページの「ユーザ アクセス権」を参照してください。



5. [Apply]をクリックします。

CLI を使用してユーザを追加するには、以下のコマンドを続けて入力します。

```
ADD USER <ユーザ名> {<パスワード>}
```

- ☞ **注記：** <ユーザ名>は、他のすべてのユーザ名およびグループ名と異なる必要があり、大文字と小文字が区別されます。1～13文字の長さにする必要があり、すべての英数字、ハイフン、およびアンダースコアを使用できます。<パスワード>は3～8文字の長さにする必要があり、すべての印刷可能文字を使用できます。

```
ASSIGN ADMINISTRATOR {RIGHTS} <ユーザ名>
```

```
SET USER FULLNAME {<ユーザ名>} <フル ネーム>
```

- ☞ **注記：** <フル ネーム>は1～20文字の長さにする必要があり、すべての英数字、ハイフン、アンダースコア、およびスペースを使用できます。

```
SET USER CONTACT {<ユーザ名>} <連絡先情報>
```

- ☞ **注記：** <連絡先情報>は1～20文字の長さにする必要があり、すべての英数字、ハイフン、アンダースコア、およびスペースを使用できます。

```
ASSIGN USER <ユーザ名> <グループ名> {[VIEW | MODIFY]}
```

Blade PC へのリモート コンソール セッションの有効化

Integrated Administrator のリモート コンソール機能を使用すると、ユーザは Blade PC のコンソール（シリアル）コネクタに接続して、[ROM ベース セットアップ ユーティリティ]（RBSU）にアクセスできます。Blade PC に接続するだけで、その Blade PC の RBSU にアクセスできます。

AlertMail の設定

AlertMail を使用すると、ユーザは SNMP トラップを使用せずに、電子メールによってシステム イベントを受信できます。AlertMail は SNMP とは完全に独立しており、この両方を同時に有効にすることができます。AlertMail は、標準の SMTP コマンドを使用して、SMTP 対応のメール サーバと通信します。

Web ベースのユーザ インタフェースを使用して AlertMail を設定するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある [Network Administration] をクリックします。
3. [Alertmail Configuration] 領域まで下にスクロールします。
4. [Enabled] ボタンをクリックします。
5. [E-Mail Address] フィールドに電子メール アドレスを入力します。
6. [Sender Domain] フィールドに送信者のドメインを入力します。
7. [SMTP Server] フィールドに SMTP サーバのアドレスを入力します。
8. [Apply] をクリックします。

表 6-2 AlertMail の CLI コマンド

機能	コマンド
コマンド ライン インタフェースを使用して、電子メール アドレスを追加する	SET ALERTMAIL MAILBOX <電子メール アドレス>
SMTP サーバ アドレスを追加する	SET ALERTMAIL SMTPSERVER <IP アドレス>
送信者ドメインを設定する	SET ALERTMAIL SENDERDOMAIN <ドメイン名>
Alertmail を有効にする	ENABLE ALERTMAIL
Alertmail を無効にする	DISABLE ALERTMAIL

*セキュリティ上の理由から、送信者のドメインが正しく設定されていると、一部の SMTP サーバはメールの転送だけを行います。ネットワーク ドメインに対応させるために、このパラメータの設定が必要な場合があります。

電子メール アラート

AlertMail が有効になっている場合、以下のイベントに関して、電子メールでアラートが送信されません。

- エンクロージャの起動メッセージ
- Integrated Administrator の再起動メッセージ
- ファンのステータスの変化
- ファンの取り付け
- ファンの取り外し
- エンクロージャの温度ステータスの変化
- 電源供給装置のステータスの変化
- 電源供給装置の取り付け
- 電源供給装置の取り外し
- 電源サブシステムのリダンダント状態の変化
- Blade PC の取り付け
- Blade PC の取り外し
- Blade PC のステータスの変化
- Blade PC の温度の変化
- Blade PC の障害
- Blade PC の診断文字列（bc2x00 のみ）（ブレードの具体的な診断文字列の一覧については、[144 ページの「エラー メッセージ」](#)を参照）

 **注記：** エンクロージャにスイッチが取り付けられている場合は、システムが起動してから AlertMail を送信するまでに、最大 60 秒かかる場合があります。この間に生成されたイベントは、スイッチがオンラインになった時点で送信されます。

すべての電子メールには、次のヘッダがあります。

Subject:HP AlertMail-SEQ:<重大度>件名

Date: 標準形式での日時

From:Enclosure エンクロージャ名<エンクロージャ名@ドメイン>

To: 受信者のメールボックス

ここで、重大度は以下のどれかです（高いものから順に示しています）。

- # CRITICAL
- # WARNING
- # NOTICE
- # INFO

電子メールの例 :

----サンプルの開始----

Subject: HP AlertMail-010: (CRITICAL) Power Supply #1: Failed

Date: Wed, 23 Apr 2003 15:02:22 +0200

From:Enclosure IA-00508BEBA571 <IA-00508BEBA571@hp.com>

To: user@userdomain

X-OS: HP Integrated Administrator

X-Priority: 1

Content-Type: text/plain; charset=us-ascii

EVENT (26 May 07:09): Power Supply #1 Status has changed to: Failed

Enclosure, IA-00508BEBA571, has detected that a power supply in bay 1 has changed from status OK to Failed.

The power supply should be replaced with the appropriate spare part. You can ensure that the center wall assembly is operating correctly by swapping the two power supplies. Make sure that there are no bent pins on the power supply connectors before reinserting and that each power supply is fully seated.

An amber LED on the power supply indicates either an over-voltage, over-temperature, or loss of AC power event has occurred. A blinking LED on the power supply indicates a current limit condition.

Enclosure Status: Degraded

Enclosure Management URL:<https://16.181.75.213/>

- PLEASE DO NOT REPLY TO THIS EMAIL ?

----サンプルの終了----

IP セキュリティの設定

 **注記 :** これは、IPSec ではありません。

IP セキュリティを使用すると、管理者は提供されているサービス（SSH、HTTP、HTTPS、TELNET、SNMP）への接続を許可された唯一の IP アドレスである、一連の IP アドレスを定義できます。つまり、管理者は、特定のシステム一式のみを Integrated Administrator にアクセス可能な状態にできます。最大 5 つの IP アドレスを入力できます。

表 6-3 IP セキュリティのコマンド

機能	コマンド
IP アドレスを追加する	ADD IPMANAGER <IP アドレス>
IP アドレスを削除する	REMOVE IPMANAGER <IP アドレス>
IP セキュリティを有効にする	ENABLE IPSECURITY
IP セキュリティを無効にする	DISABLE IPSECURITY

自動ネットワーク タイム プロトコル (NTP) の設定

自動時間設定によって、Integrated Administrator はシステムの日付と時刻を、NTP をサポートする NTP 対応デバイスと同期させることができます。

Web ベースのユーザ インタフェースを使用して NTP を設定するには、以下の操作を行います。

1. **[Enclosure]** タブをクリックします。
2. 左パネルにある **[Network Administration]** をクリックします。
3. **[NTP Configuration]** 領域まで下にスクロールします。
4. **[Enabled]** ボタンをクリックします。
5. **[Primary Server]** フィールドおよび **[Secondary Server]** フィールドにサーバのアドレスを入力します。
6. **[Poll Interval]** フィールドにポーリング間隔を入力します。
7. **[Apply]** をクリックします。

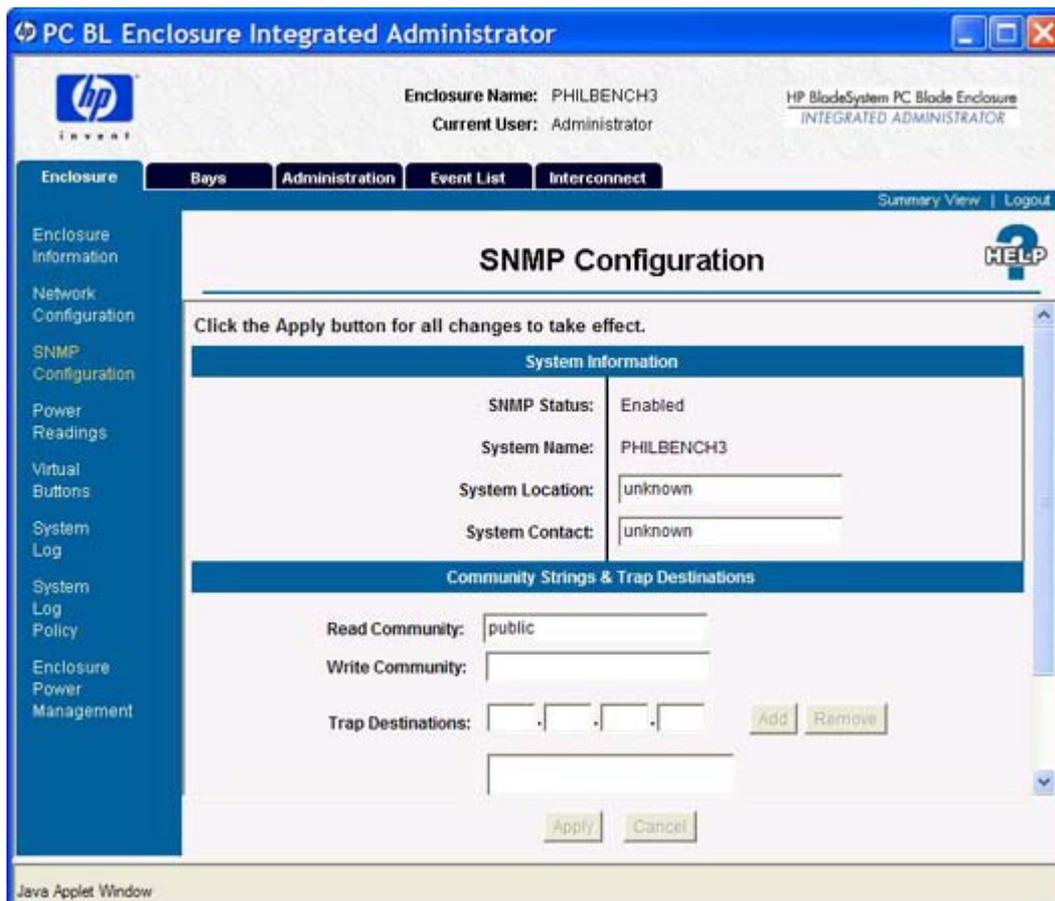
表 6-4 自動時間設定の CLI コマンド

機能	コマンド
NTP ポーリング間隔を設定する*	SET NTP POLL <秒>
プライマリ NTP サーバを設定する	SET NTP PRIMARY <IP アドレス>
セカンダリ NTP サーバを設定する	SET NTP SECONDARY <IP アドレス>
セカンダリ NTP サーバを無効にする	SET NTP SECONDARY NONE
NTP を有効にする	ENABLE NTP
NTP を無効にする	DISABLE NTP

*NTP ポーリング間隔を設定していない場合は、720 秒を初期値とします。最短時間は 60 秒、最長時間は 9999 秒です。

SNMP サポートの設定

 **注記：** エンクロージャ管理者だけが、これらのタスクを実行できます。



コミュニティ名の入力

Web ベースのユーザ インタフェースを使用して読み込みコミュニティ名または書き込みコミュニティ名を入力するには、以下の操作を行います。

1. **[Enclosure]** タブをクリックします。
2. 左パネルにある **[SNMP Configuration]** をクリックします。
3. **[Read Community]** フィールドまたは **[Write Community]** フィールドをクリックします。
4. コミュニティ名を入力します。

 **注記：** **[Read Community]** フィールドに空白の名前を入力すると、読み込みコミュニティ名が「public」に設定されます。**[Write Community]** フィールドに空白の名前を入力すると、SNMP の set コマンドが無効になります。

5. **[Apply]** をクリックします。

CLI を使用して読み込みコミュニティ名または書き込みコミュニティ名を入力するには、以下のように入力します。

SET SNMP COMMUNITY [READ | WRITE] <コミュニティ名>

書き込み<コミュニティ名>は1～20文字の長さ、読み込み<コミュニティ名>は1～20文字の長さにする必要があります。どちらのコミュニティ名も、すべての英数字、アンダースコア、およびハイフンを使用できます。

初期設定の読み込みコミュニティ名は「public」、初期設定の書き込みコミュニティ名は空白です。

システムの位置の変更

 **注記：** Web ベースのユーザ インタフェースの[Network Configuration]領域で、SNMP プロトコルを無効にすることができます。

Web ベースのユーザ インタフェースを使用してシステムの位置の情報を変更するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある[SNMP Configuration]をクリックします。
3. [System Location] フィールドにカーソルを置いて、適切な情報を入力します。
4. [Apply] をクリックします。

CLI を使用してシステムの位置の情報を変更するには、以下のように入力します。

SET SNMP LOCATION <位置>

<位置>フィールドは1～20文字の長さにする必要があります。すべての英数字、アンダースコア、ハイフン、および引用符で囲んだスペースを使用できます。

システム連絡先情報の変更

Web ベースのユーザ インタフェースを使用してシステム連絡先情報を変更するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある[SNMP Configuration]をクリックします。
3. [System Contact] フィールドにカーソルを置いて、適切な情報を入力します。
4. [Apply] をクリックします。

CLI を使用してシステム連絡先情報を変更するには、以下のように入力します。

SET SNMP CONTACT <連絡先>

<連絡先>フィールドは1～20文字の長さにする必要があります。すべての英数字、アンダースコア、ハイフン、および引用符で囲んだスペースを使用できます。

トラップ送信先の追加

Web ベースのユーザ インタフェースを使用してトラップ送信先を追加するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある[SNMP Configuration]をクリックします。

3. **[SNMP]**領域の該当するフィールドに、IP アドレスを入力します。
4. **[Add]**をクリックします。
5. **[Apply]**をクリックします。

CLI を使用してトラップ送信先を追加するには、以下のように入力します。

```
ADD SNMP TRAPRECEIVER <IP アドレス>
```

<IP アドレス>は、「###.###.###.###」（###は 0 ~ 255）の形式である必要があります。

Integrated Administrator は v1 トラップだけをサポートしており、初期設定ではトラップを SNMP ポート 162 に送信します。SNMP トラップを受信するために、最大 8 つの IP アドレスを追加できます。

トラップ送信先の削除

Web ベースのユーザ インタフェースを使用してトラップ送信先の一覧を削除するには、以下の操作を行います。

1. **[Enclosure]**タブをクリックします。
2. 左パネルにある**[SNMP Configuration]**をクリックします。
3. **[SNMP]**領域の該当するフィールドに、一覧の名前を入力します。
4. **[Remove]**をクリックします。
5. **[Apply]**をクリックします。

CLI を使用してトラップ送信先の一覧を追加または削除するには、以下のように入力します。

```
REMOVE SNMP TRAPRECEIVER <IP アドレス>
```

<IP アドレス>は、「###.###.###.###」（###は 0 ~ 255）の形式である必要があります。

トラップ ポリシーの変更

CLI を使用してトラップ ポリシーを変更するには、以下のように入力します。

エンクロージャの場合：

```
SET TRAP POLICY ENCLOSURE [ALL | CRITICAL | MAJOR | MINOR | INFORMATIONAL]  
[ON | OFF]
```

ベイの場合：

```
SET TRAP POLICY BAY [ALL | CRITICAL | MAJOR | MINOR | INFORMATIONAL] [ON | OFF]
```

特定のトラップ番号の場合：

```
SET TRAP POLICY TRAP [TRAP # {optional range}]
```

トラップおよび詳細については、[177 ページの「サポートされる SNMP トラップ」](#)を参照してください。

7 SOAP サポート タスクの設定

SOAP インタフェースの有効化

Web ベースのユーザ インタフェースを介して SOAP インタフェースを有効にするには、以下の操作を行います。

1. **[Enclosure]** タブをクリックします。
2. 左パネルにある **[Network Configuration]** をクリックします。
3. **[SOAP]** ボタンをクリックして、**[Enable]** にします。
4. **[Apply]** をクリックします。

CLI ベースのユーザ インタフェースを介して SOAP インタフェースを有効にするには、以下を入力します。

```
ENABLE SOAP
```

SOAP インタフェースの無効化

Web ベースのユーザ インタフェースを介して SOAP インタフェースを無効にするには、以下の操作を行います。

1. **[Enclosure]** タブをクリックします。
2. 左パネルにある **[Network Configuration]** をクリックします。
3. **[SOAP]** ボタンをクリックして、**[Disable]** にします。
4. **[Apply]** をクリックします。

CLI ベースのユーザ インタフェースを介して SOAP インタフェースを無効にするには、以下を入力します。

```
DISABLE SOAP
```

サポートされている SOAP インタフェース コマンド

以下の表は、サポートされている SOAP インタフェース コマンドとその簡単な説明の要約を示しています。

コマンド	説明
userLogin	SOAP インタフェース Web サービスを使用するために、IA との SOAP セッションを確立します
userLogout	userLogout は、IA との SOAP セッションを終了します
modifyPassword	SOAP インタフェースを介して、ユーザ アカウント パスワードを変更します
getEnclosurePowerCollectionInfo	エンクロージャの電源レギュレータおよび電力消費量のレポート機能に関する情報を取得します
setEnclosurePowerCollectionInfo	エンクロージャの電源レギュレータおよび電力消費量のレポート機能に関する情報を設定します。1分、5分、10分、1時間、または24時間のサンプル レートを設定できます
getEnclosurePowerRecords	エンクロージャの、収集された電力消費量の履歴データ ポイントを返します
getBladePowerCollectionInfo	任意のベイの電源レギュレータおよび電力消費量のレポート機能に関する情報を取得します
setBladePowerCollectionInfo	任意のベイの電源レギュレータおよび電力消費量のレポート機能に関する情報を設定します。1分、5分、10分、1時間、または24時間のサンプル レートを設定できます
getBladePowerRecords	任意のベイの、収集された電力消費量の履歴データ ポイントを返します
getEnclosureInfo	一部の IA 固有の情報を除き、CLI の Get Enclosure Info コマンドと同様に機能します
getIAInfo	IA 固有の情報を取得します
getEnclosureStatus	CLI の Get Enclosure Status コマンドと同様に機能します
setBladePowerState	CLI の power[on/off] {ベイ番号}コマンドと同様に機能します
getBladePowerState	ブレードの電源状態を取得します
getBladeStatus	CLI の Get Blade Status {ベイ番号}コマンドと同様に機能します
getBladeStatusArray	CLI の Get Blade Status All コマンドと同様に機能します
getBladeInfo	CLI の Get Blade Info {ベイ番号}コマンドと同様に機能します
getEnclosurePowerData	収集された最新の電源データ ポイントのスナップショットを提供します
SetBladeOneTimeBoot	次回の POST 時にブレードの起動順序を変更します。CLI コマンドの SET BAY BOOT ONCE と同様に機能します
SetBladeIPLBootPriority	次回の POST 時にブレードの起動順序を変更します。CLI コマンドの SET BAY BOOT ALWAYS と同様に機能します
flashIAROM	SOAP インタフェース経由で IA をフラッシュできますが、管理者アカウントでのみ使用できます
getBladeBootInfo	IA で設定された、ブレードの保留中の起動順序設定を返します
setBladeUID	ブレードの UID ランプを変更します
setEnclosureUID	エンクロージャの UID ランプを変更します

これらのコマンドの XML スキーマおよび説明については、WDSL ファイルを参照してください。このファイルは、Integrated Administrator で URL を https://IA_IP_address/iasoap.wsdl (「IA_IP_address」は Integrated Administrator の IP アドレス) と入力して、直接ダウンロードできます。

8 一般的な管理タスクの実行

この章では、Integrated Administrator の以下の管理機能について説明します。

- Blade PC ベイの管理
 - Blade PC へのリモート コンソール セッションの開始
 - Blade PC の[ROM ベース セットアップ ユーティリティ]へのアクセス
 - Blade PC の動作の確認
 - Blade PC の電源切断
- △ **注意：** ブレードが ACPI 対応の OS を使用していないと、Integrated Administrator は Blade PC を正しくシャットダウンできません。
- ユニット確認ランプによる Blade PC の確認
- エンクロージャの管理
 - エンクロージャの動作の確認
 - ユニット確認ランプによるエンクロージャの確認
 - エンクロージャ概要の生成
 - 問題コンポーネントの特定
- ユーザの管理
 - Blade PC ベイへのユーザのアクセス権の変更
 - ユーザ アカウントの無効化と削除

Blade PC ベイの管理

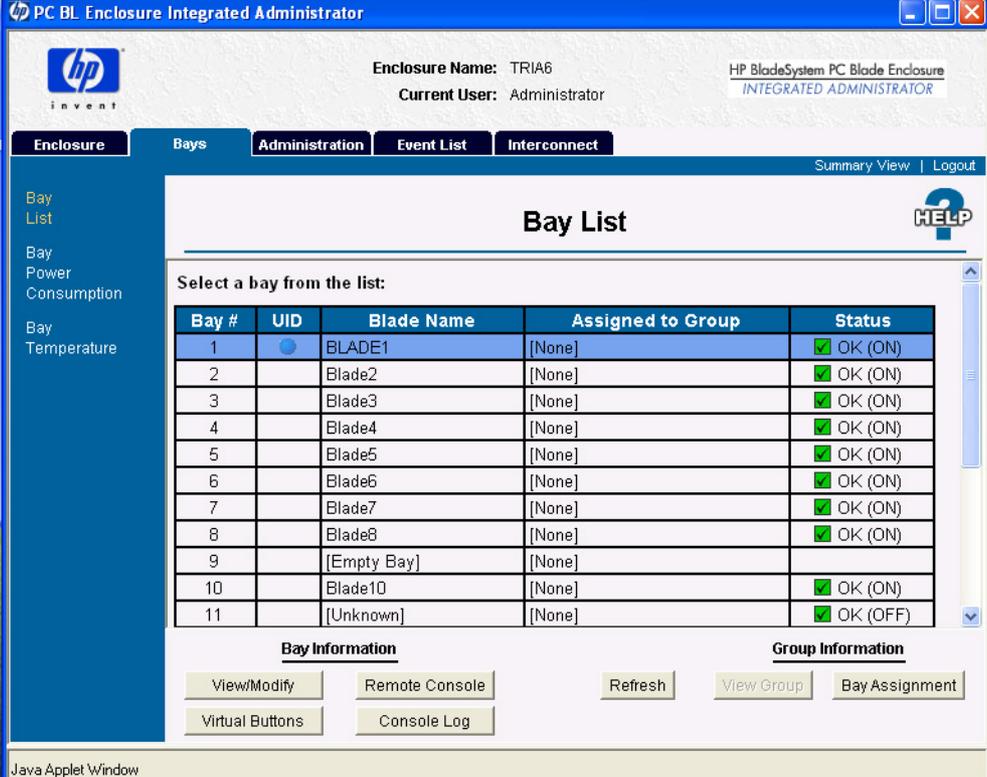
Blade PC へのリモート コンソール セッションの開始

 **注記：** ベイにアクセス可能なエンクロージャ管理者およびグループ管理者は、[Remote Console] ボタンをクリックして、ベイ内の Blade PC へのテキストベースのリモート コンソールを開始できます。

Web ベースのユーザ インタフェースを使用してリモート コンソールにアクセスするには、以下の操作を行います。

1. [Bays] タブをクリックします。
2. 左パネルにある [Bay List] をクリックします。
3. Blade PC の一覧から Blade PC を選択します。

 **注記：** [Blade Name] という名前の付いた列に、Blade PC 名の一覧が表示されます。Blade PC を強調表示すると、[Bay Information] ボタンがアクティブになります。



The screenshot shows the HP BladeSystem PC Blade Enclosure Integrated Administrator interface. The main content area displays the "Bay List" table. The table has columns for Bay #, UID, Blade Name, Assigned to Group, and Status. Bay 1 is selected, and its status is "OK (ON)". Below the table, there are buttons for "View/Modify", "Remote Console", "Refresh", "View Group", "Bay Assignment", "Virtual Buttons", and "Console Log".

Bay #	UID	Blade Name	Assigned to Group	Status
1		BLADE1	[None]	OK (ON)
2		Blade2	[None]	OK (ON)
3		Blade3	[None]	OK (ON)
4		Blade4	[None]	OK (ON)
5		Blade5	[None]	OK (ON)
6		Blade6	[None]	OK (ON)
7		Blade7	[None]	OK (ON)
8		Blade8	[None]	OK (ON)
9		[Empty Bay]	[None]	
10		Blade10	[None]	OK (ON)
11		[Unknown]	[None]	OK (OFF)

4. [Remote Console] をクリックします。[Remote Console] 画面が表示されます。
5. [Remote Console] をクリックすると、Blade PC の端末インタフェースに接続するための新しいウィンドウが開きます。

CLI を使用してリモート コンソールにアクセスするには、以下のように入力します。

CONNECT BAY <ベイ番号>

 **注記：** 1 つの Blade PC が同時にサポートできるリモート コンソール セッションは、1 つだけです。

Blade PC の [ROM ベース セットアップ ユーティリティ] へのアクセス

 **注記：** エンクロージャ管理者とベイへのアクセス権を持つグループ管理者は、[Remote Console] ボタンを選択して、ベイ内の Blade PC へのテキストベースのリモート コンソールを開くことができます。

Web ベースのインターフェースを使用して Blade PC の[ROM ベース セットアップ ユーティリティ] (RBSU) にアクセスするには、以下の操作を行います。

1. **[Bays]** タブをクリックします。
2. 左パネルにある **[Bay List]** をクリックします。
3. ベイの一覧からベイを選択します。
4. 画面の一番下にある **[Remote Console]** をクリックします。
5. **[Remote Console]** 画面から、**[Remote Console]** をクリックします。
6. Blade PC が Windows 2000 オペレーティング システムを実行している場合は、以下の操作を行います。
 - a. Web ベースのユーザ インタフェースに戻り、左パネルにある **[Virtual Buttons]** をクリックします。

△ **注意：** Blade PC のヘルス ドライバがないと、Integrated Administrator は Blade PC を再起動できません。
 - b. Blade PC の電源が切れている場合は、画面の一番下にある **[Power On]** を選択します。それ以外の場合は、画面の一番下にある **[Reboot]** を選択します。
 - c. **[Apply]** をクリックし、リモート コンソール セッションに戻ります。
7. RBSU を起動する **F10** キーを押すように求められたら、以下の操作を行います。
 - a. **Esc** キーを押します。
 - b. **0** キーを押します。
8. RBSU を終了するには、以下の操作を行います。
 - a. **Esc** キーを押します。
 - b. **F10** キーを押すように求められたら、**Esc** キーを押し、**0** キーを押して確認します。
9. リモート コンソール セッションを閉じるには、以下の操作を行います。
 - a. **Ctrl + Shift + _** キーを押します。
 - b. **D** キーを押します。

コマンド ライン インタフェースを使用して Blade PC の RBSU にアクセスするには、以下の操作を行います。

- △ **注意：** Blade PC のヘルス ドライバがないと、Integrated Administrator は Blade PC を再起動できません。

1. Blade PC が Windows 2000 オペレーション システムを実行している場合は、以下のコマンドを続けて入力して Blade PC を再起動します。

REBOOT BAY <ベイ番号>

Yes

2. ベイ番号を確認し、以下のように入力して Blade PC に接続します。

CONNECT BAY <ベイ番号>

3. Blade PC の RBSU を起動する F10 キーを押すように求められたら、以下の操作を行います。
 - a. Esc キーを押します。
 - b. 0 キーを押します。
4. [ROM ベース セットアップ ユーティリティ] (RBSU) を終了するには、以下の操作を行います。
 - a. Esc キーを押します。
 - b. F10 キーを押すように求められたら、Esc キーを押し、0 キーを押して確認します。
5. リモート コンソール セッションを閉じるには、以下の操作を行います。
 - a. Ctrl + Shift + _ キーを押します。
 - b. D キーを押します。

Blade PC の動作の確認

 **注記：** 特定の Blade PC ベイへのこのタスクの実行は、その Blade PC へのアクセス権を持つエンクロージャ管理者、グループ管理者、およびグループ メンバだけが行えます。

Web ベースのインタフェースを使用して Blade PC のコンソール ログにアクセスするには、以下の操作を行います。

1. [Bays] タブをクリックします。
2. 左パネルにある [Bay List] をクリックします。
3. [Bay List] からベイを選択します。
4. [Bay Information] の下にある [Console Log] をクリックします。

CLI を使用して Blade PC のシステム ログを表示するには、以下のように入力します。

```
SHOW SYSLOG BAY <ベイ番号>
```

 **注記：** Q キーを押すと、コマンドが終了します。さらに表示情報が続く場合は、他の任意のキーを押すと次の画面が表示されます。Blade PC のシステム ログは再起動したときに保存されないため、この情報には Integrated Administrator の最後の電源投入以降に発生した内容だけが含まれます。

Blade PC の電源の切断

 **注意：** Blade PC のヘルス ドライバまたは ACPI 準拠のオペレーティング システムがないと、Integrated Administrator は Blade PC を正しくシャットダウンできません。この状態が発生すると、重要なデータが永久に失われる場合があります。

Blade PC を再起動または電源切断すると、Blade PC からすべての電源が切断され、開いているすべてのセッションが終了します。

 **注記：** 特定の Blade PC ベイへのこのタスクの実行は、その Blade PC へのアクセス権を持つエンクロージャ管理者、およびグループ管理者だけが行えます。

Web ベースのインターフェースを使用して Blade PC を再起動するかまたは電源を切断するには、以下の操作を行います。

1. **[Bays]** タブをクリックします。
2. 左パネルにある **[Bay List]** をクリックします。
3. 電源状態を変更する Blade PC をクリックします。
4. 画面の一番下にある **[Virtual Buttons]** をクリックします。
5. **[Reboot]**、**[Power Off]**、または **[Power Off Immediately]** をクリックします。



6. **[Apply]** をクリックします。

Blade PC の電源が切れると、**[Power Off]** ボタンの文字が **[Power On]** になります。

CLI を使用して Blade PC を再起動するには、以下のように入力します。

```
REBOOT BAY <ベイ番号> {[ , | - ] <ベイ番号>} {FORCE} {[PXE | HDD | RBSU]}
```

注記： このコマンドは、正しいシャットダウンを実行してから Blade PC を再起動する要求を、特定のベイ内の Blade PC に送信します。

CLI を使用して、(ただちに、または後で) Blade PC の電源を切るには、以下のように入力します。

```
POWEROFF BAY <ベイ番号> {[ , | - ] <ベイ番号>} {FORCE}
```

注記： FORCE 引数を指定すると Blade PC の電源がただちに切断されるため、データが失われるか、または不安定になる場合があります。

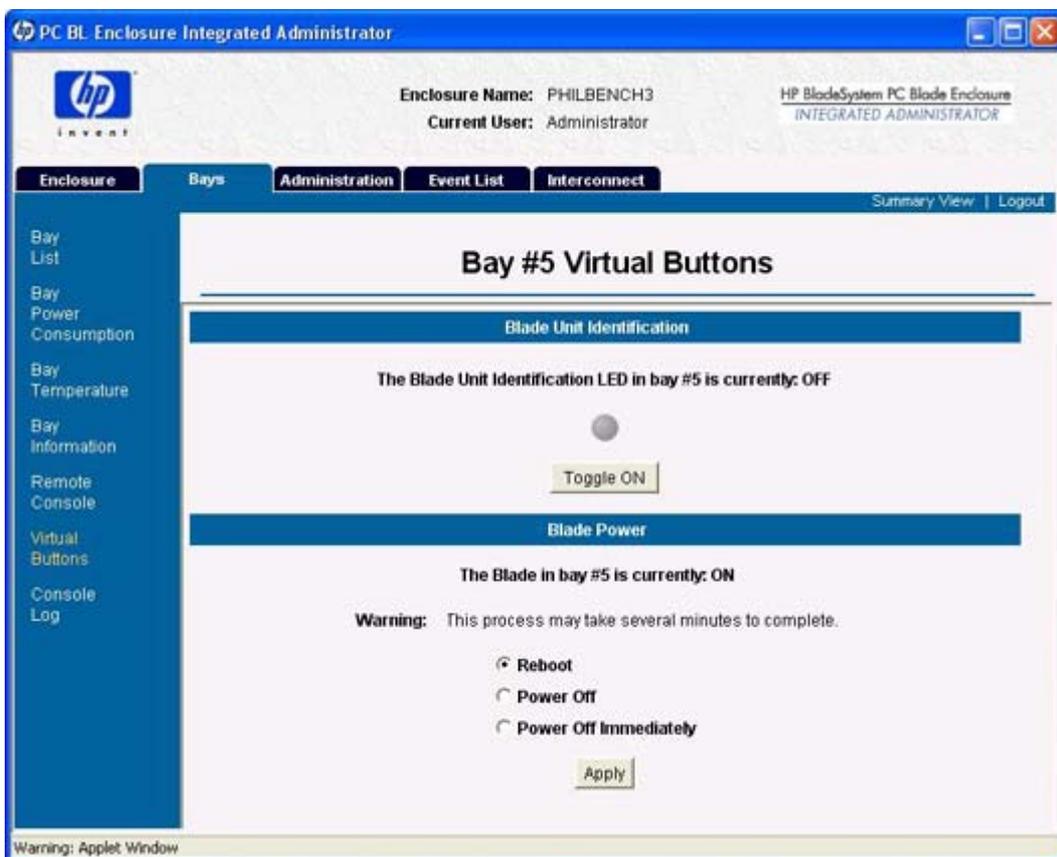
ユニット確認ランプによる Blade PC の確認

 **注記：** 特定の Blade PC ベイへのこのタスクの実行は、その Blade PC へのアクセス権を持つエンクロージャ管理者、およびグループ管理者だけが行えます。

Blade PC のユニット確認ランプ用の仮想ボタンは、Blade PC のフロント パネルにあるユニット確認ランプの状態をオフからオン、またはオンからオフに物理的に変更します。ユニット確認ランプは明るい青色に点灯し、技術者がデータ センタ内の特定の Blade PC を迅速に識別できるように設計されています。

Web ベースのユーザ インタフェースを使用して Blade PC のユニット確認ランプの状態を変更するには、以下の操作を行います。

1. [Bays] タブをクリックします。
2. 左パネルにある [Bay List] をクリックします。
3. ユニット確認ランプの状態を変更する Blade PC をクリックします。
4. 画面の一番下にある [Virtual Buttons] をクリックします。
5. Blade PC のユニット確認ランプの現在の状態に応じて、[Toggle On] または [Toggle Off] をクリックします。



CLI を使用して Blade PC のユニット確認ランプの状態を変更するには、以下のように入力します。

```
SET BAY UID <ベイ番号> {[ , | - ] <ベイ番号>} [ON | OFF]
```

エンクロージャの管理

エンクロージャの動作の確認

Integrated Administrator のシステム ログには、ユーザのログイン、エンクロージャのシャットダウン、システム障害などのシステムの動作が発生順に記録されます。また、以下に示すような HP PC Blade エンクロージャで発生する警告やエラーも表示されます。

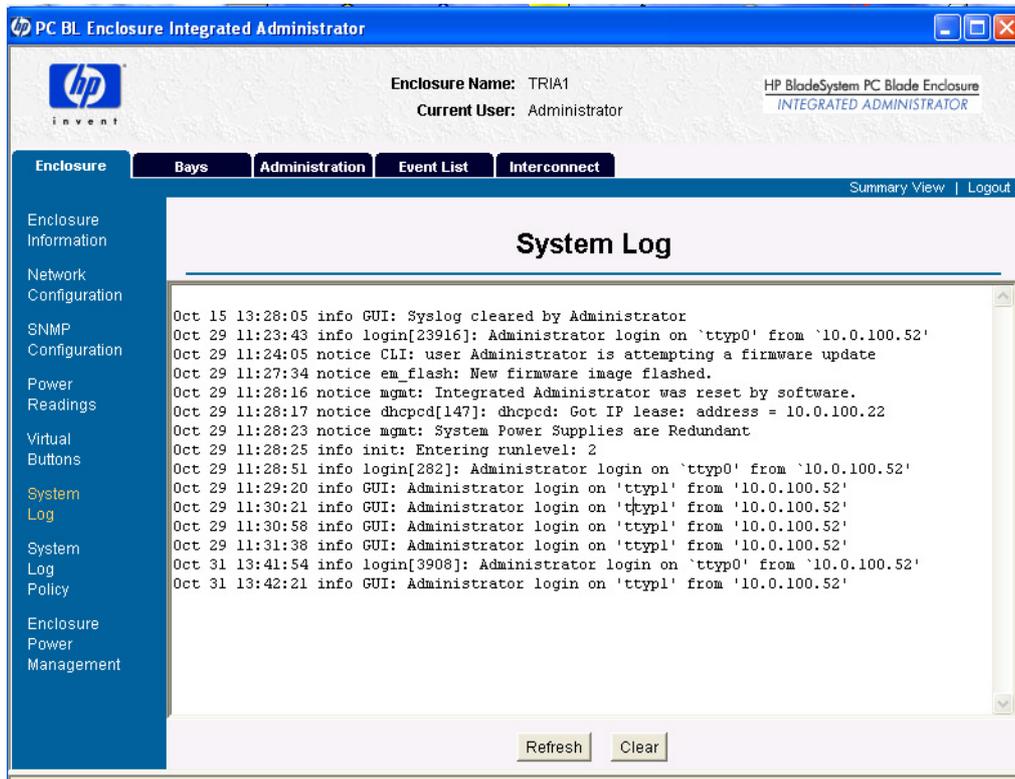
- ユーザ アカウントの変更
- グループの変更
- ベイ割り当ての変更
- 有効および無効なログイン試行
- システム障害
- システムのステータスの変化
- Blade PC の取り付けおよび取り外し
- DHCP、動的 DNS、および WINS メッセージ
- Integrated Administrator のファームウェアの更新
- ベイのヘルス ステータスの変化
- ベイの電源状態の変化

エンクロージャ管理者は、システム ログにアクセスすることによって、エンクロージャ内のイベントを表示できます。さらに、管理者は、システム ログ ポリシーを使用してシステム ログに記録されるイベントの重大度にフィルタを適用することができます。これは、診断目的で特定のベイとエンクロージャのイベント クラスを追跡して比較する際に役に立ちます。イベント リストと異なり、他のユーザはシステム ログにアクセスできません。イベント リストとシステム ログの違いについて詳しくは、この章の [121 ページの「問題コンポーネントの特定」](#) を参照してください。

Web ベースのユーザ インタフェースを使用してシステム ログを表示するには、以下の操作を行います。

1. **[Enclosure]** タブをクリックします。

2. 左パネルにある[System Log]をクリックします。



3. システム ログを更新するには、[Refresh]をクリックします。
4. システム ログを消去するには、[Clear Log]をクリックします。Integrated Administrator から、操作の確認をを求めるメッセージが表示されます。

CLI を使用してエンクロージャのシステム ログを表示するには、以下のように入力します。

```
SHOW SYSLOG ENCLOSURE
```

エンクロージャ管理者だけが、このコマンドを実行できます。

CLI を使用してエンクロージャのシステム ログ ポリシーを表示するには、以下のように入力します。

```
SHOW SYSLOG POLICIES
```

エンクロージャ管理者だけが、このコマンドを実行できます

CLI を使用してエンクロージャのシステム ログ ポリシーを設定するには、以下のように入力します。

```
SET SYSLOG POLICY ENCLOSURE {ALL, MAJOR, MINOR, NORMAL, INFORMATIONAL} [ ON | OFF ] (エンクロージャのシステム ログ メッセージの種類を有効または無効にする場合)
```

```
SET SYSLOG POLICY BAY {ALL, MAJOR, MINOR, NORMAL, INFORMATIONAL} [ ON | OFF ] (ベイのシステム ログ メッセージの種類を有効または無効にする場合)
```

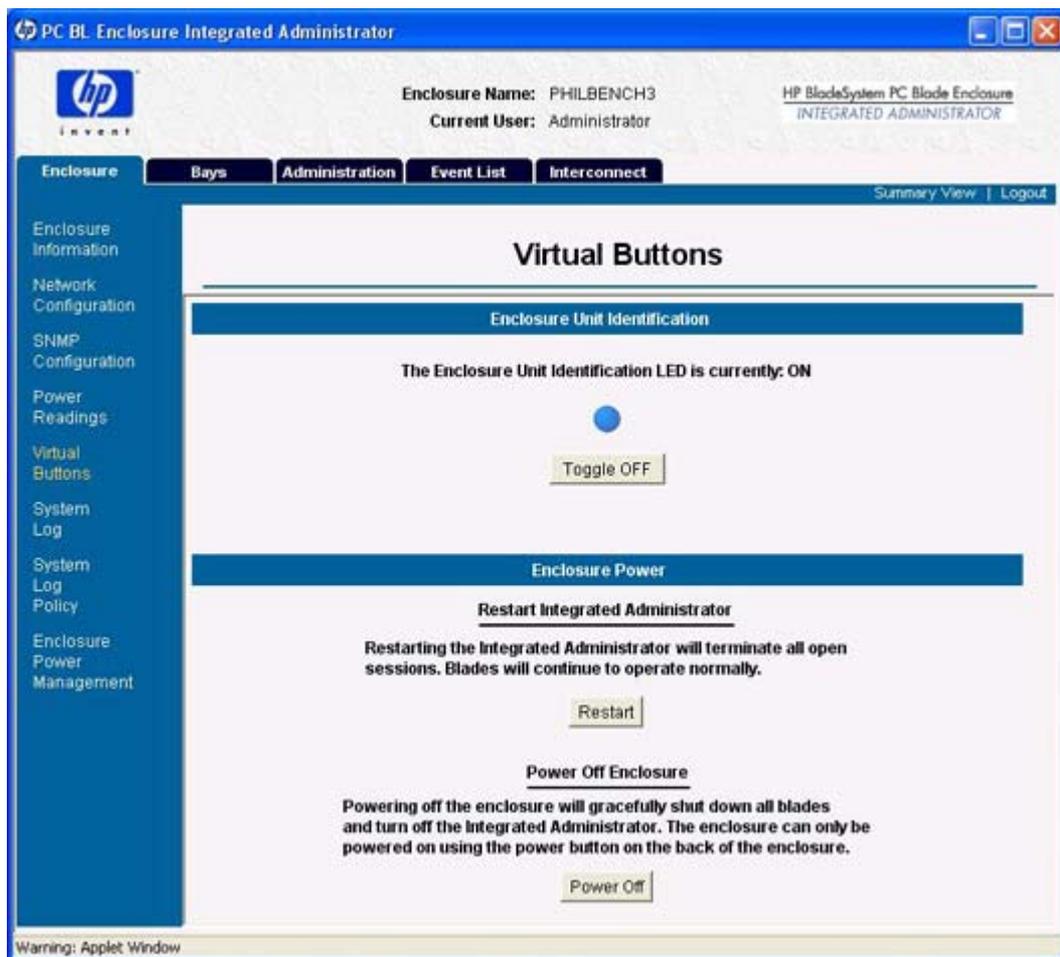
エンクロージャ管理者だけが、このコマンドを実行できます。マスク可能なシステム ログ メッセージとその重大度分類の一覧については、[144 ページの「エラー メッセージ」](#)を参照してください。

ユニット確認ランプによるエンクロージャの確認

エンクロージャのユニット確認ランプ用の仮想ボタンは、エンクロージャのリア パネルにあるユニット確認ランプの状態をオフからオン、またはオンからオフに物理的に変更します。ユニット確認ランプは明るい青色に点灯し、技術者がデータ センタ内の特定のエンクロージャを迅速に識別できるように設計されています。

Web ベースのユーザ インタフェースを使用してエンクロージャのユニット確認ランプの状態を変更するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある [Virtual Buttons] をクリックします。
3. エンクロージャのユニット確認ランプの現在の状態に応じて、[Toggle On] または [Toggle Off] をクリックします。



CLI を使用してエンクロージャのユニット確認ランプの状態を変更するには、以下のように入力します。

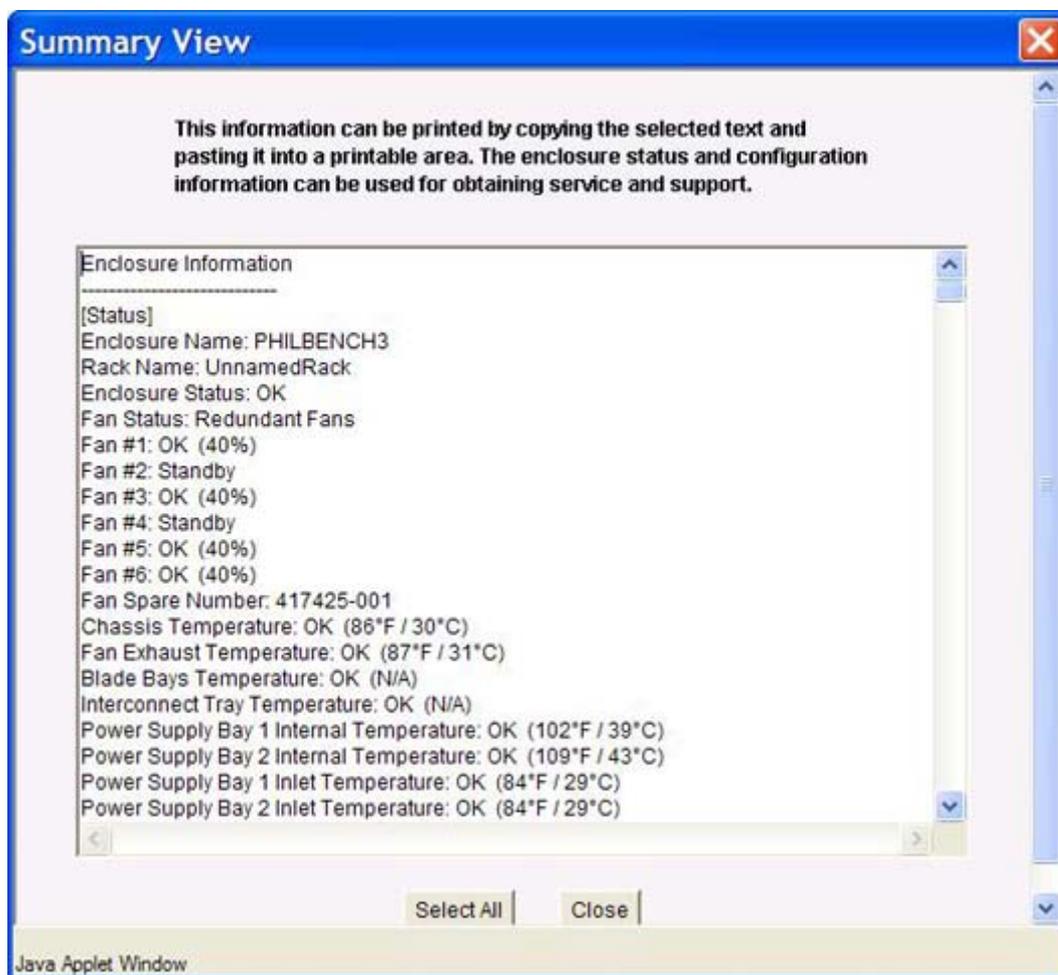
```
SET ENCLOSURE UID [ON | OFF]
```

エンクロージャ管理者だけが、このコマンドを実行できます。

エンクロージャ概要の生成

エンクロージャのすべてのデータの印刷可能な概要情報を生成できます。このデータには、エンクロージャの名前と種類、エンクロージャの製品番号、シリアル番号およびアセット タグ番号、Integrated Administrator のソフトウェアとハードウェアのバージョン、Integrated Administrator の MAC アドレス、インターコネクト トレイの種類、製品番号およびシリアル番号が含まれます。

Web ベースのユーザ インタフェースを使用してエンクロージャのすべてのデータの印刷可能な概要情報を生成するには、トップ パネルにある[Summary View]をクリックします。Web ベースのユーザ インタフェースで新しいウィンドウが開きます。このウィンドウ内の情報は、コピーして印刷可能なファイルに貼り付けることができます。



CLI を使用してエンクロージャ情報を取得するには、必要に応じて以下のコマンドを入力します。

```
SHOW ENCLOSURE FAN [<ファン番号> | ALL]
```

このコマンドは、エンクロージャ内の 1 つまたはすべてのファンについて、ステータス、リダンダント状態、ペアとなるファン、速度、および製品番号を表示します。

```
SHOW ENCLOSURE INFO
```

このコマンドは、エンクロージャの名前と種類、Integrated Administrator のソフトウェアとハードウェアのバージョン、エンクロージャの製品番号、シリアル番号およびアセット タグ番号、Integrated Administrator の MAC アドレス、インターコネクト トレイの種類、製品番号およびシリアル番号を表示します。

SHOW ENCLOSURE POWERSUPPLY [<電源供給装置番号> | ALL]

このコマンドは、エンクロージャ内の1つまたはすべての電源供給装置について、ステータス、AC 入力ステータス、容量、入力電圧範囲#1 (V)、入力電圧範囲#2 (V)、入力周波数範囲 (Hz)、製品番号、シリアル番号、およびハードウェア リビジョンを表示します。

SHOW ENCLOSURE STATUS

このコマンドは、[Enclosure Status]の見出しに、エンクロージャのヘルス、Integrated Administrator のヘルス、およびユニット確認ランプのステータスを表示し、[Power Status]の見出しに、エンクロージャの電源供給装置のステータスと容量を表示します。

SHOW ENCLOSURE TEMP

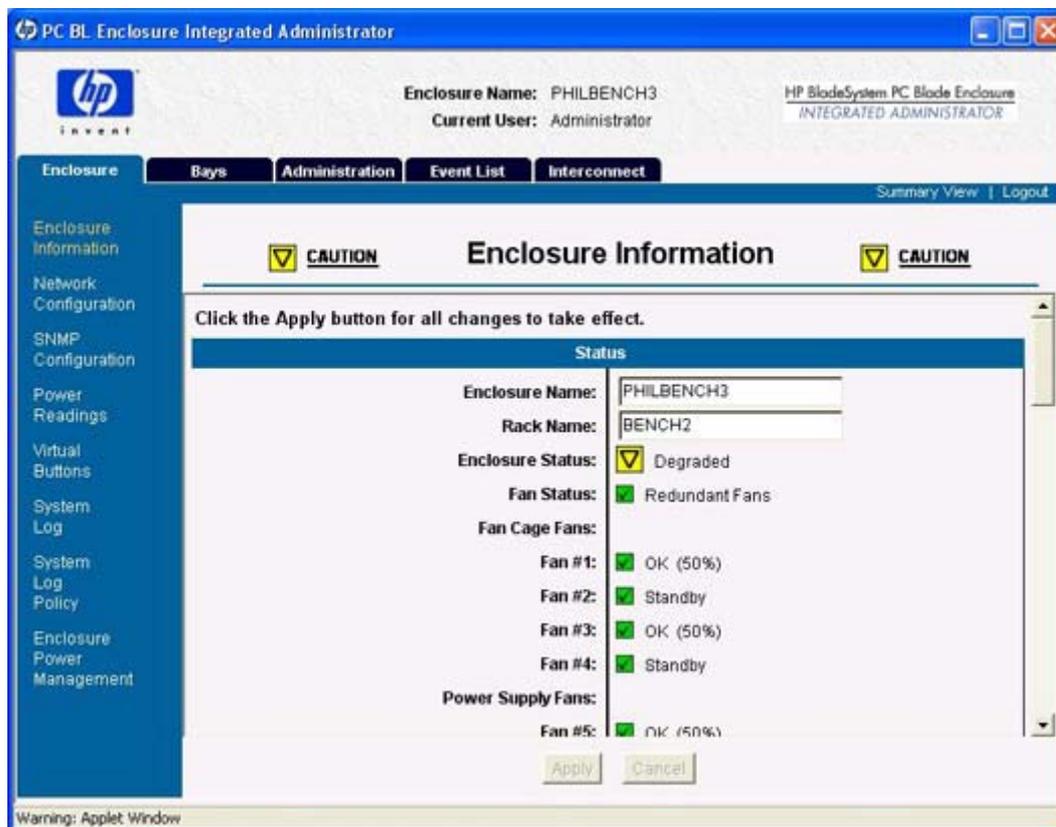
このコマンドは、エンクロージャのすべての温度センサについて、場所、ステータス (OK、温度上昇、機能低下、または障害)、および温度 (□) を表示します。

問題コンポーネントの特定

Integrated Administrator は、エンクロージャ内の以下のような問題の状況や障害コンポーネントに関するアラートを、ユーザに通知します。

- ファン
- 電源供給装置
- Blade PC
- 過熱状態

エンクロージャが機能低下した状態に陥ると、Integrated Administrator の Web ベースのユーザ インタフェースは、デッキ パネルの一番上にアイコンを表示してユーザに警告します。



エンクロージャ内の機能低下コンポーネントとそれらの各製品番号は、以下の方法で特定できます。

- エンクロージャのシステム ログを開きます。
- イベント リストを開きます。イベント リストは、以下の点でシステム ログと異なります。
 - どのユーザも、イベント リストを表示できます。エンクロージャ管理者だけが、システム ログにアクセスできます。
 - イベント リストのメッセージは、注意と重大な障害だけに限定されています。処置に関する情報については、エンクロージャのシステム ログを参照してください。
 - イベント リストには、ユーザが Integrated Administrator にログインした後に受信したメッセージだけが表示されます。システム ログには、エンクロージャ診断によって生成されたすべてのメッセージが表示されます。
- デッキ パネルの一番上にある[Caution]アイコンまたは[Critical]アイコンをクリックします。

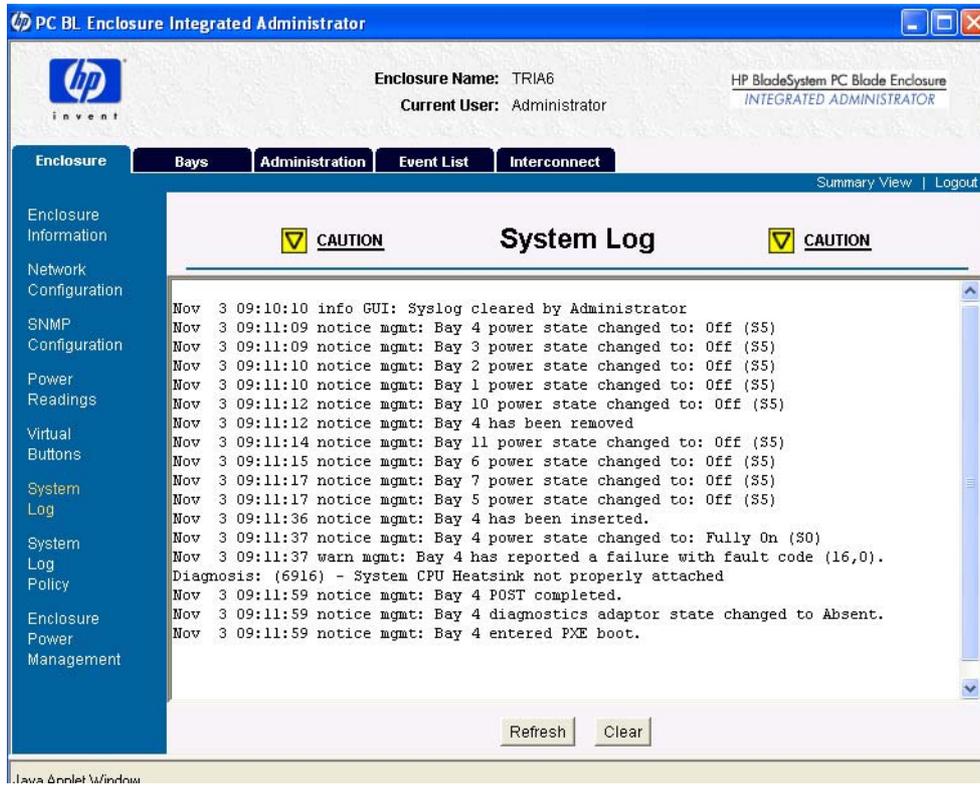
この操作によって、イベント リストが開きます。イベント リスト内の項目を強調表示し、[View Event Details]をクリックすると、機能低下コンポーネントに関する詳細な情報を提供する Integrated Administrator 内の領域にアクセスできます。

注記： [Caution]アイコンまたは[Critical]アイコンをクリックするとすぐに、機能低下の状態が解消されたかどうかにかかわらず、そのアイコンは消えます。

Web ベースのユーザ インタフェースからシステム ログを使用して機能低下コンポーネントを特定するには、以下の操作を行います。

1. [Enclosure]タブをクリックします。

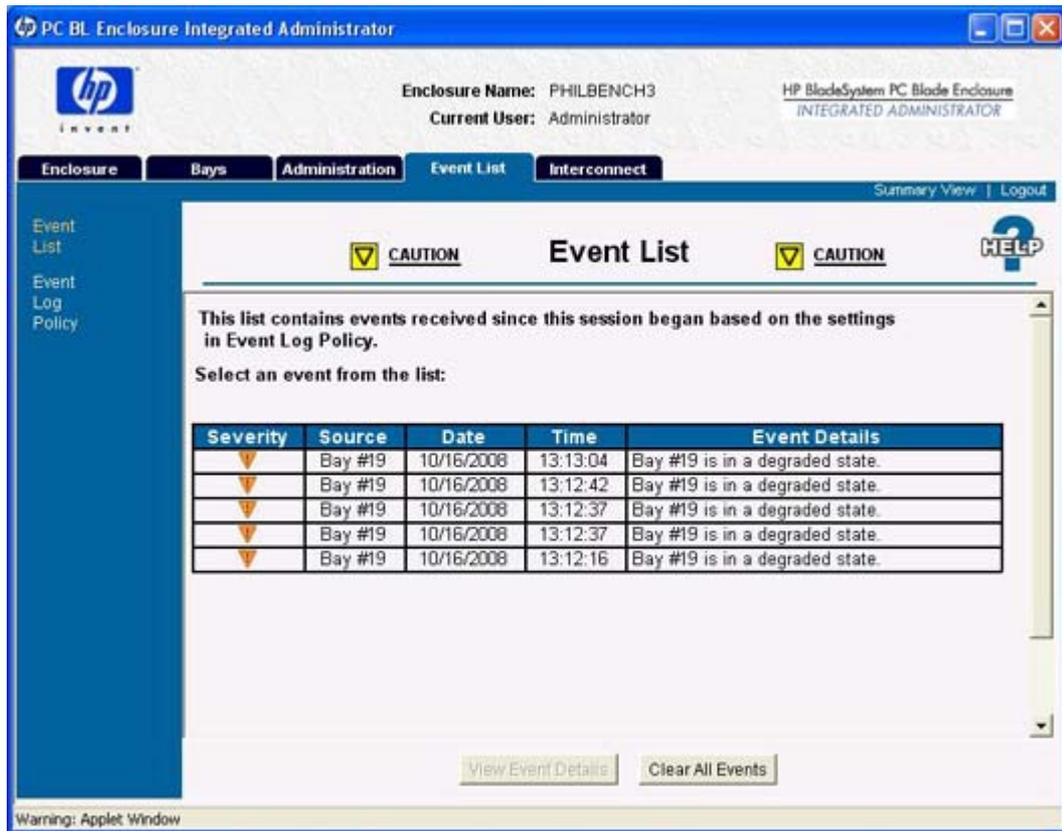
2. 左パネルにある[System Log]をクリックします。



3. 機能低下コンポーネントのスペア番号が表示された、Integrated Administrator内の該当する領域に移動します。

Web ベースのユーザ インタフェースからイベント リストを使用して機能低下コンポーネントを特定するには、以下の操作を行います。

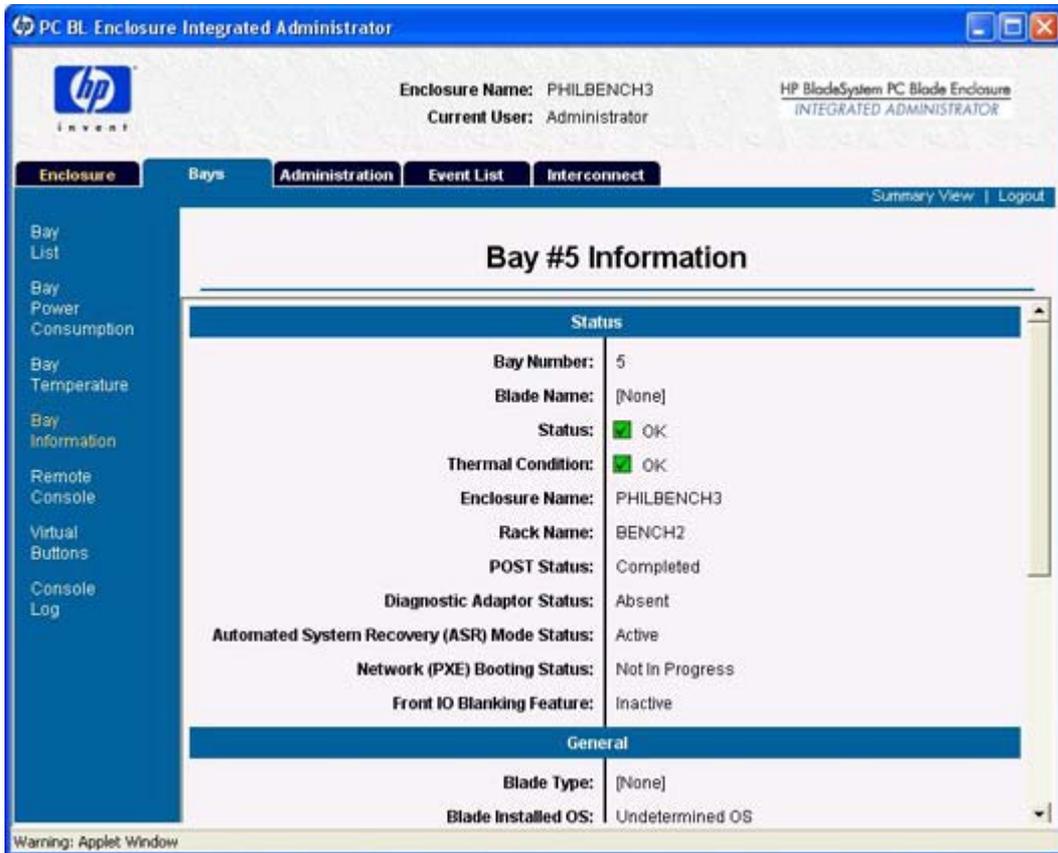
1. [Event List] タブをクリックします。



2. イベント リストで、機能が低下している項目をクリックします。
3. 画面の一番下にある[View Event Details]をクリックします。この操作によって、機能低下コンポーネントに関する情報を表示する Integrated Administrator 内のページが開きます。

Web ベースのユーザ インタフェースから、デッキ パネルの一番上に表示されている[Caution]アイコンまたは[Critical]アイコンを使用して機能低下コンポーネントを特定するには、アイコンをクリックします。この操作によって、イベント リストが開きます。

イベント リスト内の項目を強調表示し、[View Event Details]をクリックすると、機能低下コンポーネントに関する詳細な情報を提供する Integrated Administrator 内の領域にアクセスできます。



CLI を使用して機能低下コンポーネントを特定するには、以下の操作を行います。

1. 次のように入力します。 SET DISPLAY EVENTS [BAY | ENCLOSURE | ON | OFF] to ON.
2. 次のように入力します。 SET DISPLAY EVENTS ENCLOSURE ALL ON.
3. 次のように入力します。 SET DISPLAY EVENTS BAY ALL ON.
4. 該当するコマンドを入力します。

SHOW ENCLOSURE FAN [<ファン番号> | ALL]

このコマンドは、エンクロージャ内の 1 つまたはすべてのファンについて、ステータス、リダンダント状態、ペアとなるファン、速度、および製品番号を表示します。

SHOW ENCLOSURE INFO

このコマンドは、エンクロージャの名前、種類、製品番号、シリアル番号、およびアセット タグ番号、Integrated Administrator のソフトウェアとハードウェアのバージョン、Integrated Administrator の MAC アドレス、インターコネクト トレイの種類、製品番号およびシリアル番号を表示します。

SHOW ENCLOSURE POWERSUPPLY [<電源供給装置番号> | ALL]

このコマンドは、エンクロージャ内の片方または両方の電源供給装置について、ステータス、AC 入力のステータス、容量、入力電圧範囲#1 (V)、入力電圧範囲#2 (V)、入力周波数範囲 (Hz)、製品番号、シリアル番号、およびハードウェア リビジョンを表示します。

SHOW ENCLOSURE STATUS

このコマンドは、[Enclosure Status]の見出しに、エンクロージャのヘルス、Integrated Administrator のヘルス、およびユニット確認ランプのステータスを表示し、[Power Status]の見出しに、エンクロージャの電源供給装置のステータスと容量を表示します。

SHOW ENCLOSURE TEMP

このコマンドは、エンクロージャのすべての温度センサについて、場所、ステータス（OK、温度上昇、機能低下、または障害）、および温度（□）を表示します。

ユーザの管理

 **注記：** エンクロージャ管理者だけが、これらのタスクを実行できます。

グループ アカウントとユーザ アカウントの限定された初期名（Administrator、switch、switcha、switchb、および SAM）では、大文字と小文字が区別されません。初期設定以外のグループ名とユーザ名では、大文字と小文字が区別されます。

Blade PC ベイへのユーザのアクセス権の変更

Blade PC ベイへのユーザのアクセス権を変更するには、そのユーザが属するグループのアクセス権を変更します。具体的には、以下の方法のどちらかを選択します。

- Blade PC ベイへのアクセス権を更新したユーザ用に、新しいグループを作成する
- そのユーザがメンバになっているグループの、Blade PC ベイへのアクセス権を変更する

アクセス権を更新した新しいグループの作成

そのユーザに割り当てる、Blade PC アクセス プロファイルを更新した新しいグループを作成するには、[95 ページの「グループの追加」](#)を参照してください。

Blade PC ベイへのグループ アクセス権の変更

Web ベースのユーザ インタフェースを使用して Blade PC ベイへのグループ アクセス権を変更するには、以下の操作を行います。

1. [Administration] タブをクリックします。

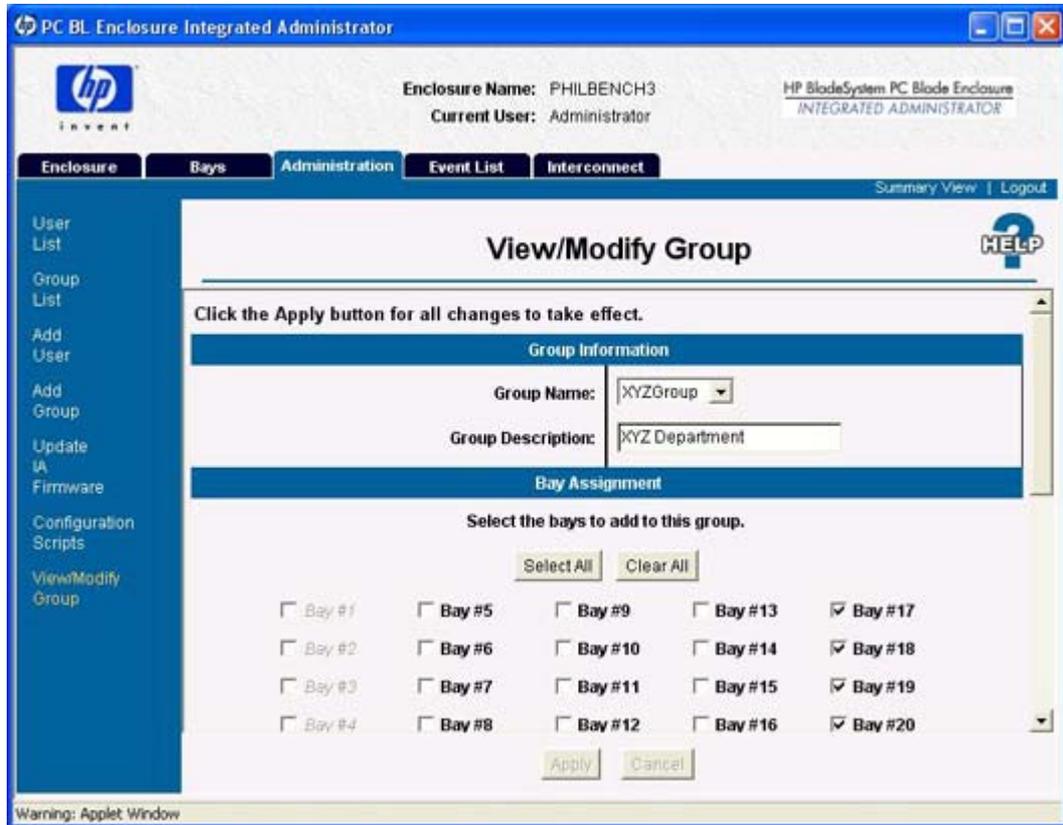
2. 左パネルにある [Group List] をクリックします。

The screenshot shows the HP BladeSystem PC Blade Enclosure Integrated Administrator web interface. The title bar reads "PC BL Enclosure Integrated Administrator". The HP logo is in the top left. The top right shows "Enclosure Name: PHILBENCH3" and "Current User: Administrator". Below the HP logo is the text "HP BladeSystem PC Blade Enclosure INTEGRATED ADMINISTRATOR". The main navigation bar includes "Enclosure", "Bays", "Administration", "Event List", and "Interconnect". The "Administration" tab is selected. On the left is a vertical menu with options: "User List", "Group List", "Add User", "Add Group", "Update IA", "Firmware", and "Configuration Scripts". The "Group List" option is highlighted. The main content area is titled "Group List" and contains a "Select a group from the list:" section. Below this is a table with three columns: "Group Name", "Assigned Bays", and "Group Members". The table lists two groups: "ABCGroup" and "XYZGroup". The "XYZGroup" row is highlighted. Below the table are two buttons: "View/Modify Group" and "Remove Group". A "Warning: Applet Window" message is visible at the bottom left of the interface.

Group Name	Assigned Bays	Group Members
ABCGroup	Bay List	Member List
XYZGroup	Bay List	Member List

3. アクセス権を変更するグループをクリックします。

4. [View/Modify Group]をクリックします。



5. そのグループに許可しようとしている更新されたアクセス権が反映された、使用可能な Blade PC ベイの該当するチェック ボックスにチェックを入れます。
6. [Apply]をクリックします。

CLI を使用して既存のグループの Blade PC ベイへのアクセス権を変更するには、以下のコマンドの中から選択します。

注記： エンクロージャ管理者だけが、これらのコマンドを実行できます。

- グループに割り当てる Blade PC の数を増やすには、以下のように入力します。

```
ASSIGN BAY [ALL | <ベイ番号> {[ , | - ]<ベイ番号>}] <グループ名>
```

Blade PC ベイが現在グループに割り当てられている場合、このコマンドはそのベイを現在のグループから新しいグループに再割り当てします。

- 任意のグループの Blade PC ベイへのグループ アクセス権を削除するには、以下のように入力します。

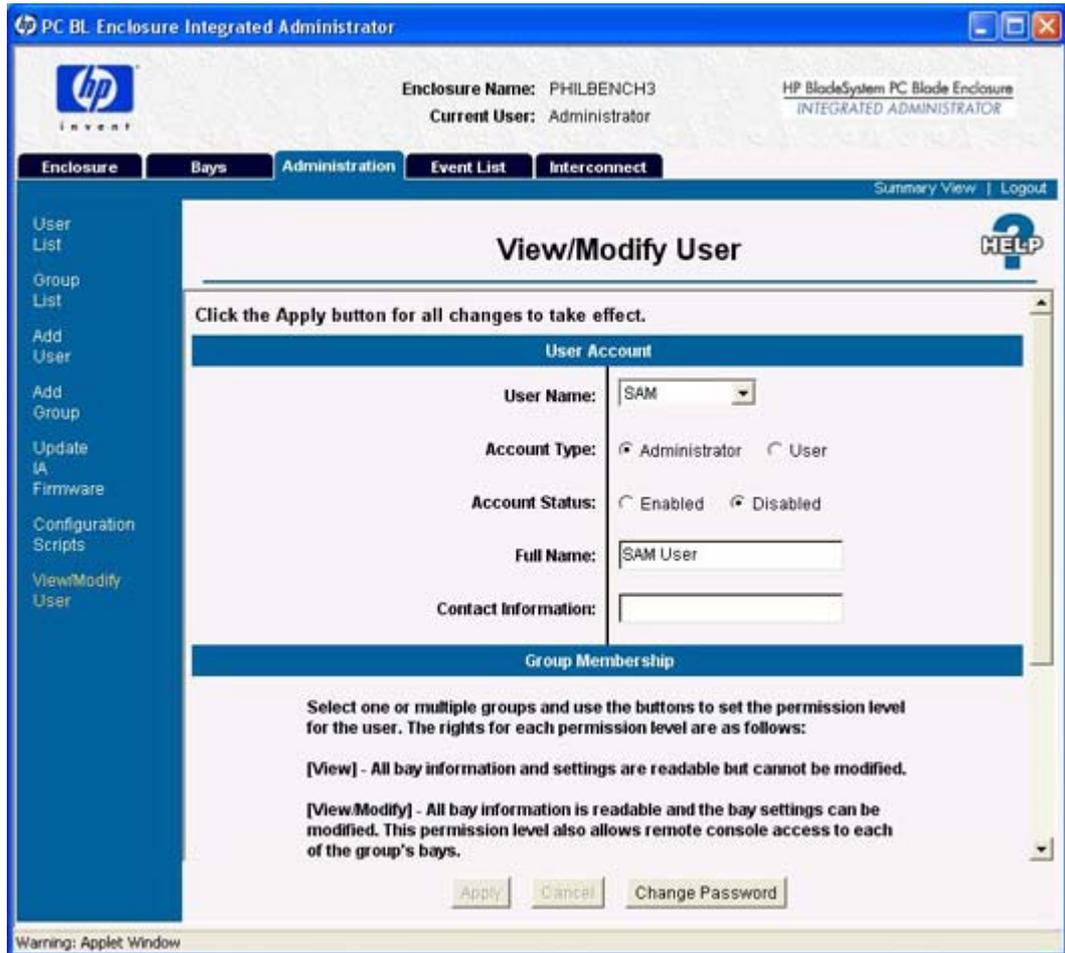
```
UNASSIGN BAY [ALL | <ベイ番号> {[ , | - ] <ベイ番号>}]
```

ユーザ アカウントの無効化と削除

注記： エンクロージャ管理者だけが、このコマンドを実行できます。グループ アカウントは削除できませんが、無効にすることはできません。

Web ベースのユーザ インタフェースを使用してユーザ アカウントを無効にするには、以下の操作を行います。

1. **[Administration]** タブをクリックします。
2. 左パネルにある **[User List]** をクリックします。
3. ユーザー一覧から、アカウントを無効にするユーザを選択します。
4. **[View/Modify User]** をクリックします。



5. アカウント ステータスを **[Disabled]** に設定します。
6. **[Apply]** をクリックします。

CLI を使用してユーザ アカウントを無効にするには、以下のように入力します。

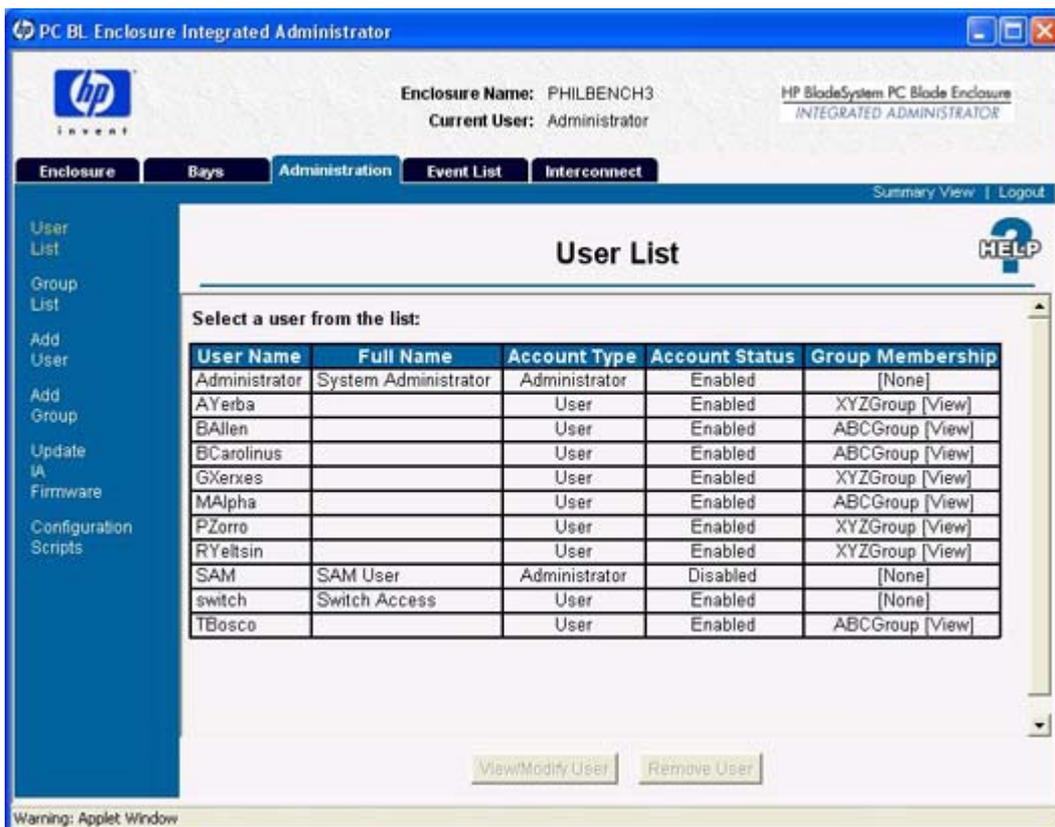
```
DISABLE USER <ユーザ名>
```

このコマンドを実行すると、そのユーザはただちにシステムからログアウトされ、アカウントが有効になるまでログインできません。

ユーザ アカウントの削除

Web ベースのユーザ インタフェースを使用してユーザ アカウントを削除するには、以下の操作を行います。

1. [Administration] タブをクリックします。
2. 左パネルにある [User List] をクリックします。
3. ユーザー一覧から、削除するユーザ アカウントを選択します。



4. [Remove User] をクリックします。

CLI を使用してユーザ アカウントを削除するには、以下のように入力します。

```
REMOVE USER [ALL | <ユーザ名>]
```

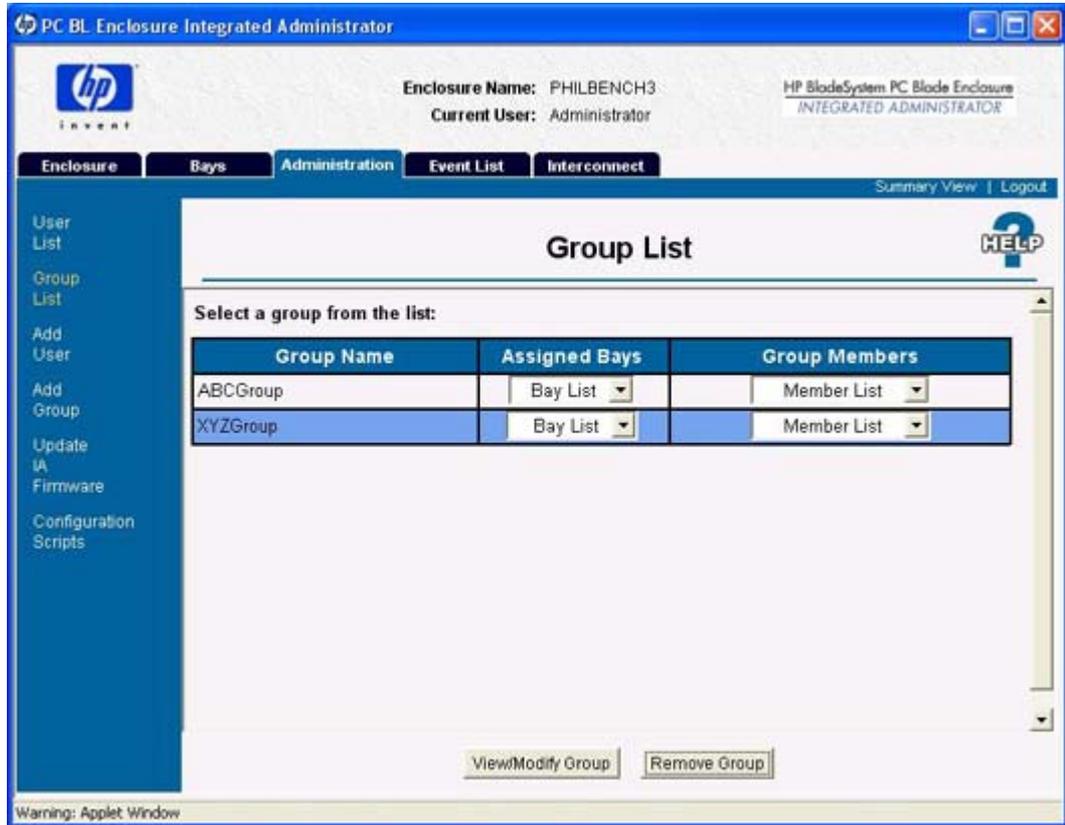
[ALL] を指定すると、このコマンドによって「Administrator」アカウントを除くすべてのユーザ アカウントが削除されます。「Administrator」アカウントを削除することはできません。

グループ アカウントの削除

Web ベースのユーザ インタフェースを使用してグループ アカウントを削除するには、以下の操作を行います。

1. [Administration] タブをクリックします。
2. 左パネルにある [Group List] をクリックします。

3. グループ一覧からグループを選択します。



4. [Remove Group]をクリックします。

CLI を使用してグループ アカウントを削除するには、以下のように入力します。

```
REMOVE GROUP [ALL | <グループ名>]
```

[ALL]を指定すると、このコマンドによってすべてのグループ アカウントが削除されます。

9 高度な機能の実行

この章では、Integrated Administrator を使用して実行できる、以下の高度なタスクについて説明します。特に記載がないかぎり、これらの手順は、Web ベースのユーザ インタフェースと CLI の両方でサポートされています。

- Integrated Administrator の設定の複製
- セキュリティ証明書管理
 - セキュリティ証明書の作成
 - セキュリティ証明書のダウンロード
- キーベースの SSH 認証
- Blade PC の起動順序の設定
- エンクロージャの電源切断
- Integrated Administrator へのネットワーク プロトコルの無効化
- Integrated Administrator のファームウェアのアップグレード
- 消失した管理者パスワードの復元
- Flash Disaster Recovery の起動

 **注記：** エンクロージャ管理者だけが、この章のタスクを実行できます。

Integrated Administrator の設定の複製

 **注記：** このタスクは、Integrated Administrator の Web ベースのユーザ インタフェースではサポートされていません。

同じ設定で複数のエンクロージャを設定するには、1 台のエンクロージャを設定し（すべてのユーザ アカウントの追加、すべてのグループの追加、ベイの割り当てなどを行い）、次のその設定を他のエンクロージャに複製します。

CLI を使用して Integrated Administrator の設定を複製するには、以下の操作を行います。

1. 最初のエンクロージャに、管理者としてログインします。
2. 「UPLOAD CONFIG <URL>」のように入力します。このコマンドは、現在の実行時設定を、指定した TFTP または FTP サーバにアップロードします。FTP サーバで匿名アップロードが許可されていない場合は、以下の構文を使用して FTP のユーザ名とパスワードを指定します。

```
ftp://username:password@ftpserver/filename
```

3. アップロードされた設定ファイルをテキスト エディタで編集して、設定（ユーザ名、パスワード、ネットワーク設定など）を他のエンクロージャ用にカスタマイズします。

 **注記：** 手順 4 は、他のエンクロージャがあらかじめ設定されている場合にだけ適用されます。

セキュリティ上の理由から、パスワードは設定ファイルに複製されません。

4. 他のエンクロージャに出荷時の設定を復元して、以前の設定をすべて消去します。
 - a. 設定を複製する先のエンクロージャに、管理者としてログインします。
 - b. 「SET FACTORY」のように入力します。このコマンドは、Integrated Administrator を出荷時の設定に戻し、SSH フィンガープリントなどの資格情報を消去します。ただし、「Administrator」アカウントのパスワードは変更されません。すべての変更が行われた後、Integrated Administrator は再起動されます。重要：Administrator アカウントだけが、このコマンドを実行できます。
 5. 他の各エンクロージャに設定をダウンロードします。
 - a. 設定を複製する先のエンクロージャに、管理者としてログインします。
 - b. 「DOWNLOAD CONFIG <URL>」のように入力します。Integrated Administrator は設定ファイルのエラーをチェックしませんが、そのファイルをスクリプト モードで自動実行します。このファイルで「Administrator」アカウントのパスワードを変更することはできません。サポートされているプロトコルは、http、ftp、および tftp です。URL は、protocol://host/path/file の形式にします。FTP サーバで匿名接続がサポートされていない場合は、上記の形式の「host」にあたる部分を username:password@host に置き換えることでユーザ名とパスワードを指定します。
-  **注記：** 手順 C は、設定ファイルにユーザ アカウントのパスワードを設定していない場合にだけ適用されます。
- c. 各ユーザ アカウントのパスワードを設定します。コマンドについては、[66 ページの「ユーザ アカウント コマンド」](#)を参照してください。

セキュリティ証明書の管理

 **注記：** これらのタスクは、Integrated Administrator の Web ベースのユーザ インタフェースではサポートされていません。

証明書要求の作成

CLI を使用してセキュリティ証明書を作成するには、以下のように入力します。GENERATE CERTIFICATE REQUEST

このコマンドは、PKCS#10 証明書要求を生成します。この証明書要求を証明書機関 (CA) に送信すると、以下で使用する PKCS#7 証明書ファイルを取得できます。

CLI を使用して自己署名セキュリティ証明書を作成するには、次のように入力します。GENERATE CERTIFICATE SELFSIGNED

このコマンドは、自己署名 PKCS#7 証明書を生成して、既存の SSL 証明書を置き換えます。この証明書は、エンクロージャの現在の名前を使用して署名されており、10 年間有効です。証明機関 (CA) を持たないユーザは、この証明書を代わりに使用できます。

セキュリティ証明書のダウンロード

CLI を使用してセキュリティ証明書をダウンロードするには、以下のように入力します。

DOWNLOAD CERTIFICATE <URL>

このコマンドは、システムにある現在のセキュリティ証明書を置き換えるために、CA から提供された PKCS#7 ファイルをダウンロードします。

サポートされているプロトコルは、http、ftp、および tftp です。URL は、次の形式にします。protocol://host/path/file

FTP サーバで匿名接続がサポートされていない場合は、上記の形式の「host」にあたる部分を次のように置き換えることで、ユーザ名とパスワードを指定できます。username:password@host

キーベースの SSH 認証

ユーザは、Integrated Administrator にパスワードなしでログインするために、独自のパブリック SSH キーをインストールできます。エンクロージャ管理者だけが、キーベースの認証を使用できます。CLI には、認証済み SSH キーのインストールと管理のために、4 つのコマンドが用意されています。

▲ 現在インストールされている認証済み SSH キーを表示するには、次のように入力します。SHOW SSHKEY

このコマンドは、Integrated Administrator に現在インストールされている、エンクロージャ管理者アカウントを使用してログインが許可されているキーをすべて表示します。

▲ Integrated Administrator のホスト キーのフィンガープリントを表示するには、次のように入力します。SHOW SSHFINGERPRINT

このコマンドは、Integrated Administrator のホスト キーのフィンガープリントを表示します。ユーザは、Integrated Administrators に接続するときに、このフィンガープリントを SSH クライアントで表示されているフィンガープリントと比較して、Integrated Administrator への接続の信

信頼性を保証できます。保証された信頼性が必要なユーザは、Integrated Administrator のシリアル コンソールを使用して SSH フィンガープリントを最初に取得します。

- ▲ 現在インストールされている認証済み SSH キーをすべて消去するには、次のように入力します。CLEAR SSHKEY

このコマンドは、ログインを許可された、Integrated Administrator に現在インストールされている認証済みのキーをすべて消去します。このコマンドを発行した後は、すべてのユーザが、ログインのために有効なパスワードの入力が必要になります。

- ▲ 1つまたは複数の SSH キーをダウンロードしてインストールするには、次のように入力します。DOWNLOAD SSHKEY <URL>

このコマンドは、Integrated Administrator へのログインを許可された 1つまたは複数の SSH キーを含むファイルをダウンロードし、インストールします。この新しいファイルによって、既存のキーはすべて置き換えられます。

サポートされているプロトコルは、http、ftp、および tftp です。URL は、次の形式にします。
protocol://host/path/file

FTP サーバで匿名ログインがサポートされていない場合は、上記の形式の「host」にあたる部分を次のように置き換えることで、ユーザ名とパスワードを指定できます。username:password@host

Integrated Administrator は、1つのダウンロード ファイル内の複数の SSH キーをサポートします。SSH キーの最大ファイル サイズは、16 KB です。

キーベースの SSH ログインは、スクリプティングとともに使用する場合にも利点があります。適切な認証済みキーがインストールされていれば、各コマンドの間でパスワードを入力する必要なしに任意の Integrated Administrator にリモート コマンドを送信できます。OpenSSH パッケージを使用すると、ユーザは次の構文を使用してコマンドを送信できます。ssh user@host command

コマンドをグループ化して、一連の操作を実行させることができます。エンクロージャとすべての Blade PC のヘルス ステータスを 1つのコマンドで表示するには、以下のように入力します。

```
ssh user@host "SHOW ENCLOSURE STATUS; SHOW STATUS BAY ALL"
```

Integrated Administrator に認証済みのキー ファイルをインストールすることにより、ユーザは、Integrated Administrator に送信される各コマンドの間でパスワードを入力する必要なしに、これらのコマンドを結合できます。

Blade PC の起動順序の設定

エンクロージャ管理者とグループ管理者は、Integrated Administrator の CLI を使用して、Blade PC の起動順序 (IPL (Initial Program Load) と呼ばれる) を変更できます。この変更は、永久に設定することも、次回の再起動だけについて設定することもできます。CLI には、この方法で Blade PC を制御するためのいくつかのコマンドが用意されています。

Blade PC の起動順序を設定するには、以下のように入力します。

```
SET BAY BOOT FIRST [HDD | PXE] [ALL | <ベイ番号> {[,-] <ベイ番号>}]
```

このコマンドによって、次の再起動の間、特定の起動デバイスを最初に使用するよう指定した Blade PC の起動順序が設定されます。この設定には、Blade PC の[ROM ベース セットアップ ユーティリティ] (RBSU) で標準の起動順序 (IPL) の設定を変更したのと同じ効果があります。

次の起動に関してだけ Blade PC の起動順序を設定するには、以下のように入力します。

SET BAY BOOT [ONCE | ALWAYS] [HDD | PXE | RBSU] [ALL | <ベイ番号> {[,-] <ベイ番号>}]

このコマンドによって、指定した Blade PC は次の起動時だけ強制的に、指定したメディアから起動されます。[ROM ベース セットアップ ユーティリティ] (RBSU) を指定すると、Blade PC の起動時に RBSU が起動され、この RBSU はリモート コンソール機能を使用して表示できます。HDD を指定すると、Blade PC は強制的にハードディスク ドライブから起動され、PXE を指定すると、強制的に内蔵 NIC から起動されます。

まだ有効になっていない Blade PC の起動順序の設定をリセットするには、以下のように入力します。

CLEAR BAY BOOT [FIRST | ONCE | ALWAYS] [ALL | <ベイ番号> {[,-] <ベイ番号>}]

このコマンドによって、SET BAY BOOT コマンドで設定した Blade PC の起動順序の変更が消去されます。このコマンドは保留中の変更にしか影響しないため、SET BAY BOOT コマンドの実行後に Blade PC を再起動した場合は、このコマンドの効果はありません。

POWERON BAY コマンドと REBOOT BAY コマンドは、その起動に関してだけ Blade PC の起動順序を設定する引数ができるように拡張されました。これらの設定は、SET BAY BOOT ONCE コマンドと同じです。

特定の Blade PC について、保留中の起動順序の変更があるかどうかを調べるには、SHOW BAY INFO コマンドを使用します。保留中の起動順序の変更がある場合は、1 回だけの変更または永久的な変更のどちらも「Pending Boot Order:」のステータス行に表示されます。

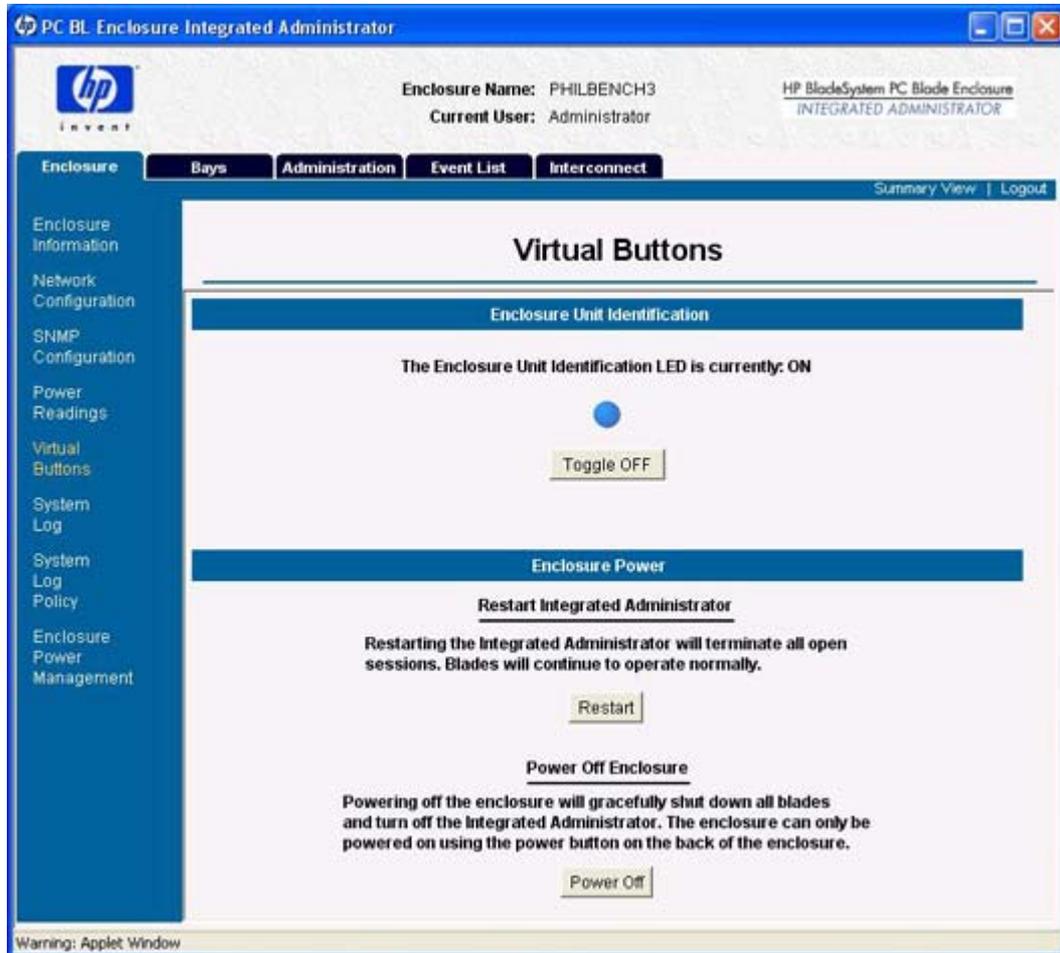
エンクロージャの電源切断

- △ **注意：** エンクロージャの電源を切ると、Blade PC からすべての電源が切断され、開いているすべてのセッションが終了します。エンクロージャの電源を切った後は、エンクロージャに物理的にアクセスしないと電源を入れることができません。

Web ベースのインタフェースを使用してエンクロージャの電源を切るには、以下の操作を行います。

1. [Enclosure] タブをクリックします。
2. 左パネルにある [Virtual Buttons] をクリックします。

3. [Power Off] をクリックします。



4. [Apply] をクリックします。

CLI を使用してエンクロージャの電源を切るには、次のように入力します。POWEROFF ENCLOSURE

このコマンドは、最初に各 Blade PC の電源、次にエンクロージャの電源を切ることによって、エンクロージャの正しいシャットダウンの実行を試みます。5 分が経過してもまだ電源が切れていない場合、このコマンドはシステムのすべてのコンポーネントの電源をただちに切ります。

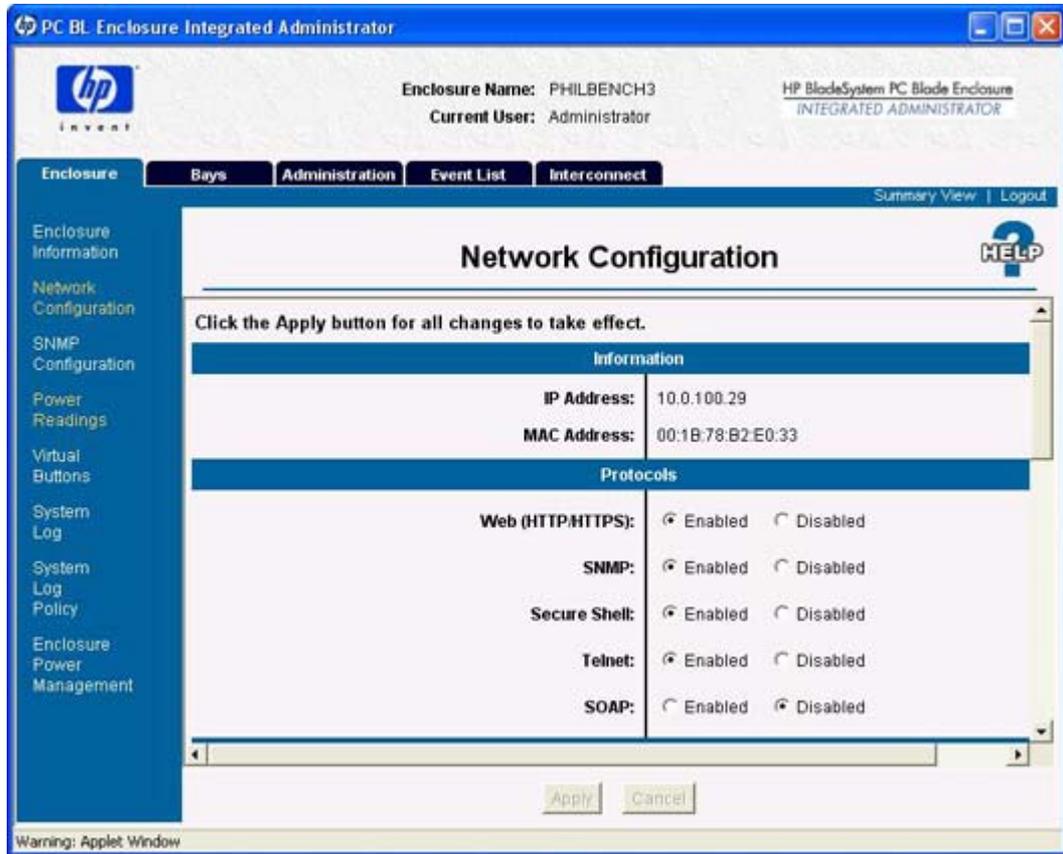
- △ **注意：** Blade PC のヘルス ドライバまたは ACPI 準拠のオペレーティング システムがないと、Integrated Administrator は Blade PC を正しくシャットダウンできません。この状態が発生すると、重要なデータが永久に失われる場合があります。

ネットワーク タイム プロトコルの無効化

Web ベースのユーザ インタフェースを使用して、エンクロージャでサポートされている通信プロトコルを変更するには、以下の操作を行います。

1. [Enclosure] タブをクリックします。

2. 左パネルにある[Network Configuration]をクリックします。



3. [Protocols]領域で、該当するラジオ ボタンを選択します。
4. [Apply]をクリックします。

CLI を使用して、エンクロージャでサポートされている通信プロトコルを変更するには、以下のコマンドの中から選択します。

- HTTP/HTTPS 通信を無効にするには、次のように入力します。DISABLE WEB
HTTP/HTTPS 通信を無効にすると、ユーザは Web ベースのユーザ インタフェースにアクセスできなくなります。
- 時間の自動更新を無効にするには、次のように入力します。DISABLE NTP
- SNMP 通信を無効にするには、次のように入力します。DISABLE SNMP
- Secure Shell 通信を無効にするには、次のように入力します。DISABLE SECURESH
Secure Shell を無効にすると、ユーザは Web ベースのユーザ インタフェースにアクセスできなくなります。
- Telnet 通信を無効にするには、次のように入力します。DISABLE TELNET
- SOAP インタフェースを無効にするには、次のように入力します。DISABLE SOAP

Integrated Administrator のファームウェアのアップグレード

Integrated Administrator に関連するファームウェアは、エンクロージャのリア パネルにある管理 (10/100 Ethernet) コネクタを介して、CLI を使用してリモートでアップグレードできます。

```
UPDATE IMAGE <URL>
```

<URL>は、以下のどれかです。

- http://host/path
- tftp://host/path
- ftp://username:password@host/path
- ftp://host/path

ここで、「host」は完全修飾ドメイン名または IP アドレスであり、「path」はダウンロードするフラッシュ イメージのパス名です。詳しくは、ファームウェアのアップグレードに関連した説明書を参照してください。

 **注記：** [Administration] タブのアップデート イメージのページにある GUI から Integrated Administrator ファームウェアをアップグレードすることもできます。

アップデート機能の設定

http を使用しているときにアップデート機能が動作するようにするには、以下の設定を行う必要があります。

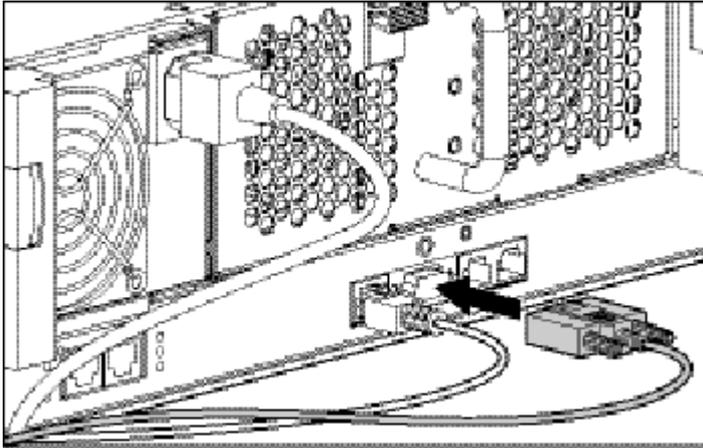
- Windows ベースの Web サーバの場合は、.rom ファイルの拡張子を処理するように IIS マネージャが設定されていることを確認します。
- Web サーバで、MIME タイプを正しく設定する必要があります。MIME タイプを設定するには、以下の操作を行います。
 1. サイトの[プロパティ]→[HTTP ヘッダー]タブ→[MIME の種類]の順に選択します。
[MIME の種類]ウィンドウが開き、登録済みの MIME タイプ（ファイル拡張子）が表示されます。
 2. [新規]をクリックします。
 3. [拡張子]で、.rom と入力します。
 4. [MIME の種類]で、application/octet-stream と入力します。

消失した管理者パスワードの復元

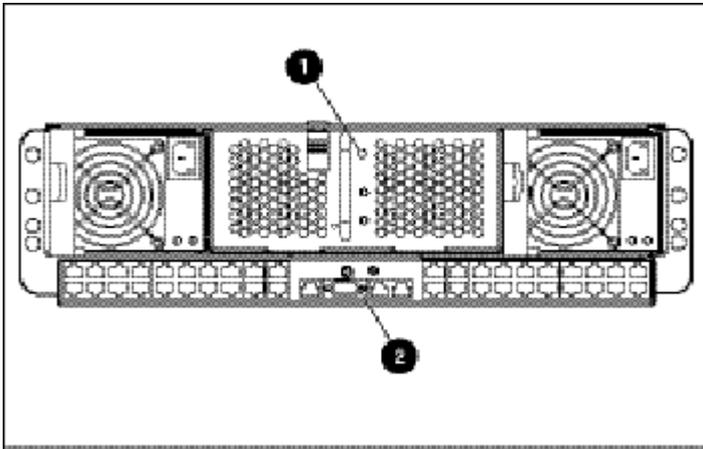
消失した管理者パスワードを復元するには、以下の操作を行います。

1. ローカル クライアント デバイスが Integrated Administrator へのローカル アクセス用に正しく設定されていることを確認してください。第 3 章の [11 ページの「ローカル クライアント デバイスの要件」](#) を参照してください。

2. エンクロージャに付属のヌル モデム シリアル ケーブルを使用して、ローカル クライアント デバイスを Integrated Administrator のコンソール (シリアル) コネクタに接続します。



3. 端末エミュレーション アプリケーションを開きます。
4. Blade PC のリア パネルにあるエンクロージャのユニット確認ボタン (1) を押しながら、同時に Integrated Administrator のリセット ボタン (2) を押して、エンクロージャを Lost Password/Flash Disaster Recovery モードにします。



5. シリアル コンソールのプロンプトが表示されたら、L キーを押します。

このコマンドは、システムを Lost Password モードで起動します。これによって、管理者パスワードが出荷時の設定にリセットされ、コンソール上に表示されます。

Flash Disaster Recovery の起動

Flash Recovery モードには、以下のものがが必要です。

- DHCP サーバ
- TFTP サーバ
- DHCP サーバおよび TFTP サーバの両方がアクセス可能なネットワーク接続

- Integrated Administrator のシリアル コンソールへの接続
- TFTP サーバ上の Integrated Administrator の ROM イメージ ファイル

 **注記：** Integrated Administrator の ROM イメージのファイル名は、任意の有効な ASCII ファイル名です。Integrated Administrator の ROM イメージは、オペレーティング システムの「イメージ更新」機能をサポートする任意の有効なイメージです。

破損したイメージが検出されると、Integrated Administrator は自動的に Flash Recovery モードに入ります。Flash Recovery モードは、手動でも開始できます。

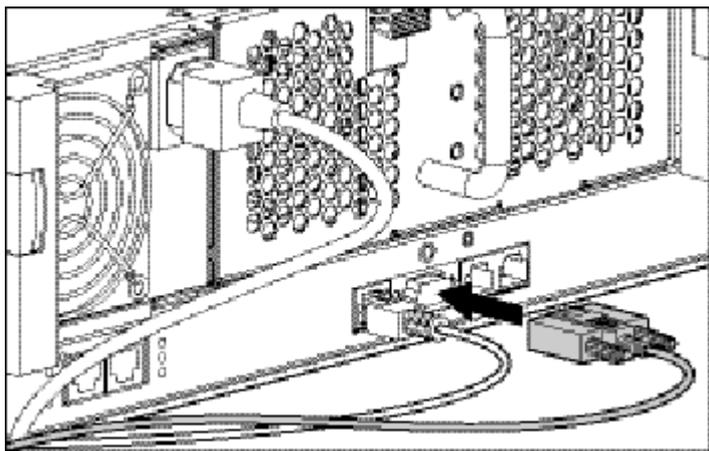
 **注記：** DHCP アドレスの取得には、タイムアウトは存在しません。

標準の「イメージ更新」フラッシュ手順中の電源障害や致命的な障害などの、何らかの予期しない問題によってオペレーティング システム イメージが破損しているために Integrated Administrator が正常に起動できない場合にだけ、Flash Recovery 処理を開始してください。

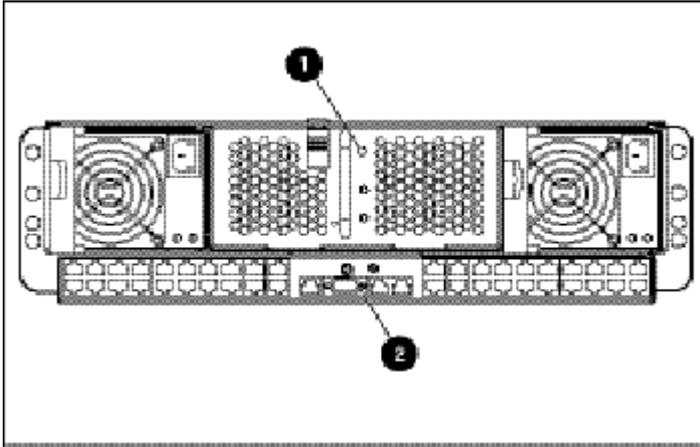
Flash Recovery モードでは、Integrated Administrator のオペレーティング システム イメージを正常にフラッシュするために、あらゆることが試みられます。イメージを正常に更新しないで Flash Recovery モードから抜けるには、Integrated Administrator をリセットするしかありません。

Integrated Administrator を手動で Flash Recovery モードにするには、以下の操作を行います。

1. エンクロージャに付属のヌル モデム シリアル ケーブルを使用して、ローカル クライアント デバイスを Integrated Administrator のコンソール (シリアル) コネクタに接続します。[11 ページの「ローカル クライアント デバイスの要件」](#)を参照してください。



2. Blade PC のリア パネルにあるエンクロージャのユニット確認ボタン (1) を押しながら、同時に Integrated Administrator のリセット ボタン (2) を押して、エンクロージャを Lost Password/Flash Disaster Recovery モードにします。



3. シリアル コンソールのプロンプトが表示されたら、F キーを押します。

注記： このコマンドでは、大文字と小文字が区別されません。

L キーを押すと、Lost Password Recovery モードが開始します。他の任意のキーを押すと、Lost Password/Flash Disaster Recovery モードが終了し、システムが再起動します。

このコマンドは、システムを Flash Disaster Recovery モードで起動し、メッセージを出力し、エンクロージャをリセットします。

Integrated Administrator は、Flash Disaster Recovery モードに入ると、DHCP アドレスの取得を試みます。DHCP アドレスの取得に成功すると、Integrated Administrator は、ユーザに以下の入力を求めます。

- TFTP サーバの IP アドレス
- TFTP サーバ上の ROM のファイル名

Integrated Administrator は次に、ROM をダウンロードして確認し、フラッシュ メモリを更新します。

注記： DHCP アドレスの取得には、タイムアウトは存在しません。

注記： ROM が正常にダウンロードされなかった場合や、ROM の確認に失敗した場合は、Flash Disaster Recovery モードが再開して、DHCP アドレスの取得が再試行されます。

Integrated Administrator を再起動します。

A コマンド ラインの規則

以下の表は、コマンド ライン インタフェース (CLI) で使用される規則を一覧表示しています。

表 A-1 CLI の規則

記号	説明
<小文字>	入力する文字列を表します
大文字	記載どおりに入力する文字列を表します
[]	選択が必須の場合の選択肢を表します
{ }	選択がオプションの場合の選択肢を表します
	入力オプションを区切ります
“”	スペースを含む引数を囲むときに使用します

たとえば、以下のコマンドでは、Integrated Administrator が動作するネットワーク環境を「DHCP」または「Static」として入力する必要があります。

```
SET IPCONFIG [DHCP {DYNAMICDNS} | STATIC <IP アドレス> <ネットマスク>
```

DHCP 環境の場合は、このコマンドで「Dynamic DNS」を指定するかどうかはオプションですが、静的環境の場合は、このコマンドで IP アドレスとネットマスクを指定する必要があります。

B エラー メッセージ

この付録では、以下のカテゴリに分けてメッセージを説明します。

- 警告メッセージ
- エラー メッセージ

警告メッセージ

この項では、Integrated Administrator の主要コンポーネントごとに、包括的な警告メッセージの一覧を示します。これらの警告メッセージは、設定が変更されたことを通知するため、または要求された操作を続行してよいかどうかの確認を求めするために表示されます。

エンクロージャの警告メッセージ

表 B-1 エンクロージャの警告メッセージ

警告メッセージ	原因
Are you sure you want to disable the Web protocol? Disabling this protocol will prevent access to the Web-based user interface until a terminal session re-enables the Web protocol.	Web (HTTP / HTTPS) プロトコルを無効にしようとした
Are you sure you want to disable the Secure Shell protocol? Disabling this protocol will prevent access to the Web-based user interface and Secure Shell terminal interface until a terminal session re-enables the Secure Shell protocol.	Secure Shell プロトコルを無効にしようとした
The SNMP protocol is currently disabled. The new settings will not take effect until this protocol is enabled on the Network Configuration screen.	SNMP プロトコルを無効にして SNMP の値を変更しようとした
The Read Community field is empty. The Read Community will be set to "public". The SNMP protocol may be disabled on the Network Configuration screen.	読み込みコミュニティ名を空白に設定しようとした
Are you sure that you want to power off the enclosure?	エンクロージャの電源を切ろうとした
Are you sure that you want to restart the Integrated Administrator? This process will take several minutes.	Integrated Administrator を再起動しようとした
Are you sure that you want to clear the system log?	システム ログを消去しようとした
Enabling IP Security may disconnect this session. Are you sure you still want to perform this action?	IP セキュリティを有効にしようとした

Blade PC の警告メッセージ

表 B-2 Blade PC の警告メッセージ

警告メッセージ	原因
This blade has been removed from the enclosure.	ブレードがエンクロージャから取り外された
This blade has been powered off. All open sessions will be closed.	現在のブレードの電源が切れた
Are you sure that you want to power off the blade immediately? This process may result in the loss of any unsaved data on the blade.	ただちにブレードの電源を切ろうとした

管理警告メッセージ

表 B-3 管理警告メッセージ

警告メッセージ	原因
Are you sure you want to permanently remove <user name>?All data for this account will be removed from the system.	ユーザを削除しようとした
Are you sure you want to permanently remove <group name>?All bays in this group will be unassigned and the data for this group will be permanently removed from the system.	グループを削除しようとした

エラー メッセージ

エンクロージャのエラー メッセージ

表 B-4 エンクロージャのエラー メッセージ

エラー メッセージ	原因	有効な入力
The maximum number (8) of trap destinations has been reached.	9 番目のトラップ送信先を追加しようとした	なし
The trap destination of ####.####.####.#### is already on the list. Enter a new value.	重複するトラップ送信先を追加しようとした	なし
An error occurred while clearing the system log. Please try again.	システム ログを消去しようとした	なし

Blade PC ベイのエラー メッセージ

表 B-5 Blade PC ベイのエラー メッセージ

エラー メッセージ	原因	有効な入力
You no longer have permissions to view this bay.	ユーザ アクセス権の変更	なし

管理エラー メッセージ

表 B-6 管理エラー メッセージ

エラー メッセージ	原因	有効な入力
The user name field is empty. Please enter a user name.	ユーザ名を空白にしてユーザを作成しようとした	英数字、ハイフン、およびアンダースコア文字を含む 1 ~ 13 文字。ユーザ名は、英字で始まる必要があります
This user name already exists. Please select a different user name.	一意のユーザ名でないユーザを作成しようとした	英数字、ハイフン、およびアンダースコア文字を含む 1 ~ 13 文字。ユーザ名は、英字で始まる必要があります
The Password fields are empty. Please enter a value in each password field.	パスワードを空白にしてユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The Password field is empty. Please enter a password.	Password フィールドを空白にしてユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The Confirm Password field is empty. Please enter a password.	Confirm Password フィールドを空白にしてユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The password must be at least 3 characters in length. Please enter a new password.	3 文字未満のパスワードでユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The passwords do not match. Please try again.	Password フィールドと Confirm Password フィールドの文字列が一致しない	すべての印刷可能文字を含む 3 ~ 8 文字
The maximum number (25) of users exists on the system.	26 番目のユーザを作成しようとした	なし

表 B-6 管理エラー メッセージ (続き)

The group name is blank. Please enter a valid name.	グループ名を空白にしてグループを作成しようとした	なし
The maximum number (20) of groups exists on the system.	21 番目のグループを作成しようとした	なし
The Password fields are empty. Please enter a value in each password field.	パスワードを空白にしてユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The Password field is empty. Please enter a password.	Password フィールドを空白にしてユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The Confirm Password field is empty. Please enter a password.	Confirm Password フィールドを空白にしてユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The password must be at least 3 characters in length. Please enter a new password.	3 文字未満のパスワードでユーザを作成しようとした	すべての印刷可能文字を含む 3 ~ 8 文字
The passwords do not match. Please try again.	Password フィールドと Confirm Password フィールドの文字列が一致しない	すべての印刷可能文字を含む 3 ~ 8 文字
NTP Poll-Interval has to be between 60 and 9999 seconds.	60 ~ 9999 秒の範囲にない NTP ポーリング間隔を設定しようとした	60 ~ 9999
Invalid NTP address supplied. IP address should be in ###.###.###.### format where ### is between 0 and 255.	間違った形式で IP アドレスを入力しようとした	###.###.###.### (###は 0 ~ 255)
###.###.###.### is not a valid NTP server.	NTP サーバのアドレスを設定しようとしたが、入力されたアドレスが NTP サーバではない	なし
Please set at least the Primary NTP server before enabling NTP.	プライマリ NTP サーバ セットを有効にする前に、NTP サーバを有効にしようとした	なし
<IP address> is already set as secondary NTP server.	<IP アドレス>がすでにセカンダリ NTP サーバとして設定されているのに、プライマリ NTP サーバを <IP アドレス>に設定しようとした	なし
<IP address> is already set as primary NTP server.	<IP アドレス>がすでにプライマリ NTP サーバとして設定されているのに、セカンダリ NTP サーバを <IP アドレス>に設定しようとした	なし
Primary NTP server is already cleared.	すでに消去されているか、設定されていないプライマリ NTP サーバを消去しようとした	なし
The secondary NTP server is already cleared.	すでに消去されているか、設定されていないセカンダリ NTP サーバを消去しようとした	なし
Please set the primary NTP server first.	まだプライマリ NTP サーバが設定されていないのに、セカンダリ NTP サーバを設定しようとした	なし
Invalid IP address supplied. IP address should be in ###.###.###.### or ###.###.###/### format where ### is between 0 and 255 and ## is between 0 and 32.	間違った形式で IP アドレスを設定しようとした	###.###.###.### (###は 0 ~ 255、##は 0 ~ 32)

表 B-6 管理エラー メッセージ (続き)

Invalid e-mail address supplied. Address should be in user@domain.tld format.	間違った形式で電子メール アドレスを入力しようとした	「user@domain.tld」の形式で、最大 64 文字の電子メール アドレス
E-mail address is too long. Length must be less than 65 characters.	64 文字を越える電子メール アドレスを入力しようとした	「user@domain.tld」の形式で、最大 64 文字の電子メール アドレス

C Blade PC の診断メッセージ

IA は、ブレードから性能低下または重大なヘルス イベントと関連付けられた診断文字列を生成します。以下の表は、ブレードヘルスの変化状況の検出時に生成される可能性がある診断文字列を一覧表示しています。一部のブレードモデルはこの機能はサポートしていません。モデルの種類については、サポートされるモデル列を参照してください。

ブレードのヘルス状態	メジャーコード	マイナーコード	診断メッセージ	サポートされるモデル
Critical / Degraded	0	0	Unknown. Please check blade for possible cause.	すべてのモデル
Degraded / Critical	-1	-1	Unknown. Please check blade for possible cause.	すべてのモデル
Degraded	1	0	(1800) - Temperature Alert*	すべてのモデル
Critical	2	65	(101) - Option ROM Checksum Error	bc2000/bc2500
Critical	2	66	(102) - System Board Failure	bc2000/bc2500
Critical	2	67	(103) - System Board Failure 2	bc2000/bc2500
Critical	2	201	(201) - Memory Error	bc2000/bc2500
Critical	2	1782	(1782) - Disk Controller Failure	bc2000/bc2500
Degraded	3	162	(162) - System Options Not Set	bc2000/bc2500
Degraded	3	163	(163) - Time & Date Not Set	bc2000/bc2500
Critical	3	163	(164) - Memory Size Error	bc2000/bc2500
Degraded	3	301	(301) - Keyboard Controller Error	bc2000/bc2500
Degraded	3	302	(302) - Keyboard Controller Error	bc2000/bc2500
Degraded	3	303	(303) - Keyboard Controller Error	bc2000/bc2500
Degraded	3	304	(304) - Keyboard or System Unit Error	bc2000/bc2500
Degraded	3	1720	(1720) - SMART Hard Drive Detects Imminent Failure	bc2000/bc2500
Degraded	3	1780	(1780) - Disk 0 Failure	bc2000/bc2500
Degraded	3	1790	(1790) - Disk 0 Error	bc2000/bc2500
Degraded	3	1792	(1792) - No fixed disk present	bc2000/bc2500
Degraded	3	1998	(1998) - Master Boot Record Backup Has Been Lost	bc2000/bc2500

ブレードのヘルス状態	メジャーコード	マイナコード	診断メッセージ	サポートされるモデル
Degraded	3	9999	(9999) - Invalid Electronic Serial Number	bc2000/bc2500
Degraded	3	6928	(6928) - POST under Recovery BIOS image	bc2000/bc2500
Degraded	3	6929	(6929) - Blade performance is reduced due to insufficient enclosure power and/or cooling.	bc2500/bc2800
Critical	6	0	(6906) - Embedded Network Controller B Hardware Failure Detected	bc2000/bc2500
Critical	7	0	(6907) - System Embedded Network Controller A Hardware Failure Detected	bc2000/bc2500
Critical	8	0	(6908) - System Board Failure Detected	bc2000/bc2500
Critical	9	0	(6909) - System Graphics Subsystem Failure Detected	bc2000/bc2500
Critical	10	0	(201) - System Memory Subsystem Failure Detected	bc2000/bc2500
Critical	11	0	(6911) - System Board CPU Failure Detected	すべてのモデル
Critical	12	0	(6912) - System On-Board Regulator Failure Detected	bc2000/bc2500
Critical	13	0	(6913) - System Main Voltage Failure	すべてのモデル
Critical	14	0	(6914) - System Has Indicated a Thermal Critical Fault Condition*	すべてのモデル
Critical	15	0	(6915) - System CPU Not Present on Current Attempt to Boot	bc2000/bc2500
Degraded	16	0	(6916) - System CPU Heatsink Attachment Fault	bc2000/bc2500
Degraded	17	0	(6917) - System rebooted due to an Automated System Recovery (ASR) timer expiration	bc2000/bc2500
Critical	18	0	(6918)- System Real Time Clock Oscillator not running within tolerance	bc2000/bc2500
Critical	19	0	(6919) - Temperature and Power Monitoring Hardware failure	bc2000/bc2500
Degraded	20	0	(6920) - Processor Running in Forced Performance Throttling Mode	bc2000/bc2500
Degraded	21	0	(6921) - System BMC Operating Using Backup Image	bc2000/bc2500
Degraded	22	0	(6922) - System temperature detected to be below 0 degrees Celsius	bc2000/bc2500
Critical	23	0	(6923) - System CPU Temperature Monitoring Hardware failure	bc2000/bc2500
Critical	24	0	(6924) - Graphics Temperature Monitoring Hardware failure	bc2000/bc2500
Critical	25	0	(6925) - Blade / Enclosure Communication Error	bc2000/bc2500

ブレードのヘルス状態	メジャーコード	マイナコード	診断メッセージ	サポートされるモデル
Degraded	27	0	(6927) - System Operating Using Recovery BIOS Image	bc2000/bc2500

*ブレードで Critical (重大) イベントまたは Warning (警告) イベントが発生すると、エンクロージャのファンの回転数が上昇し、イベントがクリアされるまで 100% の状態で回転し続けます。これらのイベントが発生するとブレードがシャットダウンされるため、電源を入れ直してイベントをクリアする必要があります

注記： このメッセージは、ブレード システムの BIOS POST メッセージと同じです。これらの多くは、ブレード POST の実行中または終了時にブレード システム BIOS によってのみ検出され、発生時にブレード ビデオ サブシステムに表示されなかったり、リモート コンソール経由で IA に送信されなかったりする場合があります。

D マスク可能なエンクロージャのシステム ログ メッセージ

IA では、重大度の分類に基づいて、システム ログ メッセージがシステム ログ メッセージにポストされないようにマスクすることができます。前に述べたセクションのシステム ログ ポリシーに関する CLI および GUI コマンドの詳細を参照してください。Critical (重大) なエンクロージャ メッセージは、システム ログへのログ記録を防止するべきではない大きな障害状況を表しているため、マスクできません。以下の表は、SET SYSLOG POLICY コマンドを使用して制御可能なメッセージを一覧表示しています。

クラス	サブクラス	システム ログ メッセージ	Critical (重大)	Major (メジャー)	Minor (マイナー)	Normal (標準)	Info (情報)	NOTES (注意事項)
エンクロージャ	-	-	-	-	-	-	-	-
	基本機能	Automatic Operating System Shutdown Initiated by a Soft Power Down	-	-	-	-	●	-
	パワー サプライ	System Power Supply:General Failure (Power Supply #)	●	-	-	-	-	-
	-	System Power Supply Removed (Power Supply #)	-	-	-	●	-	-
	-	System Power Supply Inserted (Power Supply #)	-	-	-	●	-	-
	-	System Power Supply:AC Power Restored (Power Supply #)	-	-	●	-	-	-
	-	System Power Supplies are Redundant	-	-	●	-	-	-
	-	System Power Supply:Repaired (Power Supply #)	-	-	●	-	-	-
	-	System Power Supplies Operating In Non-Redundant Mode	-	-	-	-	●	-
	-	System Power Supplies Operating In Resiliency Mode	-	-	-	-	●	-

-		System Power Supplies Operating In Redundant Mode	-	-	-	-	●	-
温度		Blade Bay # Temperature has returned to normal.	-	-	●	-	-	-
-		Network Tray Temperature has returned to normal	-	-	●	-	-	-
-		Fan Exhaust Temperature has returned to normal.	-	-	●	-	-	-
-		Chassis Temperature has returned to normal.	-	-	●	-	-	-
-		System Overheating (Zone 0, Location [location], Temperature [value] deg. C)	-	●	-	-	-	bc2x00 の場合のみ、[bay]の位置に過熱状態のコンポーネントの温度が表示されます
ファン		System Fans:Repaired (Fan #)	-	-	●	-	-	-
-		System Fan Removed (Fan #, Location #)	-	-	-	●	-	-
-		System Fan Inserted (Fan #, Location #)	-	-	-	●	-	-
-		System Fans are Redundant.	-	-	●	-	-	-
-		System Fans Not Redundant (Location #)	-	●	-	-	-	-
ネット ワーク レイ		Interconnect Switch A has returned to normal.	-	-	●	-	-	-
-		Interconnect Switch A status is degraded	-	●	-	-	-	-
-		Interconnect Switch B has returned to normal.	-	-	●	-	-	-
-		Interconnect Switch B status is degraded.	-	●	-	-	-	-
-		Interconnect Switch Degraded: Low Performance	-	●	-	-	-	-
-		Interconnect Switch Degraded: Temp Degrade	-	●	-	-	-	-
-		Interconnect Switch has returned to normal.	-	-	●	-	-	-
ベイ	基本機能	-	-	-	-	-	-	-
-		Bay # has been inserted	-	-	-	●	-	-
-		Bay # has been removed	-	-	-	●	-	-

-	Bay # power state changed to: {ON (S0) OFF (S5)}	-	-	-	-	●	-
-	Bay # BMC Flash Process Started	-	-	-	-	●	bc2x00 のみ
ヘルス	Bay # has reported a failure with fault code (#, #).Diagnosis: {Diagnostic Fault String}	●	●	-	-	-	メッセージは、重大と性能低下の両方のヘルス状況に対して表示されません
-	Blade Bay # Status Normal	-	-	●	-	-	-
Blade PC	Bay %d warm reset occurred	-	-	-	-	●	-
-	Bay Blade # Front IO Blanking Feature status changed to active	-	-	-	-	●	-
-	Bay Blade # Front IO Blanking Feature status changed to inactive	-	-	-	-	●	-
-	Bay Blade # POST completed	-	-	-	-	●	-
-	Bay Blade # diagnostics adaptor state changed to present	-	-	-	-	●	-
-	Bay Blade # diagnostics adaptor state changed to absent	-	-	-	-	●	-
-	Bay Blade # unexpected shutdown occurred	-	-	-	-	●	-
-	Bay Blade # BIOS Flash Process Started	-	-	-	-	●	-
-	Bay Blade # BIOS Flash Process Completed	-	-	-	-	●	-
-	Bay Blade # entered PXE boot	-	-	-	-	●	-
-	Bay Blade # exited PXE boot mode	-	-	-	-	●	-
-	Bay Blade # powered off due to power management policy violation	-	-	-	-	●	-
-	Bay Blade # BMC flash process completed and will auto-powercycle in 10 seconds	-	-	-	-	●	-
-	Bay Blade # will auto-powercycle now	-	-	-	-	●	-

E マスク可能なエンクロージャのイベントメッセージ

IA では、重大度の分類に基づいて、イベントメッセージがアクティブセッション中に CLI によって表示されないようにマスクすることができます。前に述べたセクションのイベント ログ ポリシーに関する CLI および GUI コマンドの詳細を参照してください。ポリシー設定はセッションでのみ有効です。ペイの Info (情報) イベントは初期設定で無効になっており、有効にする必要があります。以下の表は、SET EVENT POLICY コマンドを使用して制御可能なメッセージを一覧表示しています。

クラス	サブクラス	イベント文字列	Critical (重大)	Major (メ ジャー)	Minor (マイ ナー)	Normal (標準)	Info (情報)	NOTES (注意事 項)
エンクロージャ	-	-	-	-	-	-	-	-
	基本機能	Enclosure Status has changed to: Failed	●	-	-	-	-	-
	-	Enclosure Status has changed to: Degraded	-	●	-	-	-	-
	-	Enclosure Status has changed to:OK	-	-	●	-	-	-
	パワー サプライ	Power Supply # Status has changed to: Failed	●	-	-	-	-	# =ペイ番号
	-	Power Supply # Status has changed to: Degraded	-	●	-	-	-	# =ペイ番号
	-	Power Supply # Status has changed to:OK	-	-	●	-	-	# =ペイ番号
	-	Power Supply # was inserted.	-	-	-	●	-	# =ペイ番号
	-	Power Supply # was removed.	-	-	-	●	-	# =ペイ番号
	-	Power Supply # has an AC line problem	●	-	-	-	-	# =ペイ番号
	-	System Power Supplies Operating In Non-Redundant Mode	-	-	-	-	●	-
	-	System Power Supplies Operating In Resiliency Mode	-	-	-	-	●	-

-		System Power Supplies Operating In Redundant Mode	-	-	-	-	●	-
温度		Enclosure Temperature {value}F / {value}C: Degraded	-	●	-	-	-	-
-		Enclosure Temperature {value}F / {value}C: Warm	-	-	●	-	-	-
-		Enclosure Temperature {value}F / {value}C:OK	-	-	●	-	-	-
ファン		Fan # Status has changed to: Failed - {value} (paired with Fan #)	●	-	-	-	-	値=組み合わせられたファン ステータス
-		Fan # Status has changed to: Degraded - {value} (paired with Fan #)	-	●	-	-	-	値=組み合わせられたファン ステータス
-		Fan # Status has changed to: OK - {value} (paired with Fan #)	-	-	-	-	●	値=組み合わせられたファン ステータス
-		Fan # was inserted	-	-	-	-	●	# =ベイ番号
-		Fan # was removed.	-	-	-	-	●	# =ベイ番号
ネット ワーク レイ		Interconnect Tray Status has changed to Failed	●	-	-	-	-	-
-		Interconnect Tray Status has changed to Degraded	-	●	-	-	-	-
-		Interconnect Tray Status has changed to OK	-	-	●	-	-	-
-		Interconnect Tray has reset	-	-	-	-	●	-
-		-	-	-	-	-	-	-
ベイ	障害	Blade in bay # status has changed to: Critical	●	-	-	-	-	# =ベイ番号
-		Blade in bay # status has changed to: Degraded	-	●	-	-	-	# =ベイ番号
-		Blade in bay # status has changed to:OK	-	-	●	-	-	# =ベイ番号
-		Reason: {Fault Diagnostic String}	-	-	-	-	-	対応するステータス イベントがマスクされる場合のみマスクされます
-		Blade in bay # has experienced CPU Failure	●	-	-	-	-	bc1x00 のみ。bc2x00 の場合、この状況は理由文字列で説明されます

-	Blade in bay # has experienced VRD Failure	●	-	-	-	-	bc1x00のみ。 bc2x00の場合、 この状況は理由文字列で説明されます
基本機能	Blade in bay # was inserted.	-	-	-	●	-	# =ベイ番号
-	Blade in bay # was removed	-	-	-	●	-	# =ベイ番号
-	Blade in bay # has powered on	-	-	-	-	●	# =ベイ番号
-	Blade in bay # has powered off.	-	-	-	-	●	# =ベイ番号
-	Blade in bay # has started BMC flash mode.	-	-	-	-	●	# =ベイ番号
温度	Blade in bay # thermal state has changed to: Critical	●	-	-	-	-	# =ベイ番号
-	Blade in bay # thermal state has changed to: Caution	-	●	-	-	-	# =ベイ番号
-	Blade in bay # thermal state has changed to: Warm	-	-	●	-	-	# =ベイ番号
-	Blade in bay # thermal state has changed to:OK	-	-	●	-	-	# =ベイ番号
-	Bay # Temperature (CPU {value} deg. C, Graphics {value} deg. C, Ambient {value} deg. C)	●	●	●	-	-	bc2x00のみ。ベイ温度イベントの発生後に生成されます。温度ステータスがマスクされる場合のみマスクされます
Blade PC	Blade in bay # system BIOS flashing started	-	-	-	-	●	-
-	Blade in bay # system BIOS flashing completed	-	-	-	-	●	-
-	Blade in bay # Front IO Blanking Feature status changed to %s	-	-	-	-	●	-
-	Blade in bay # Diagnostic Adaptor status changed to %s	-	-	-	-	●	-
-	Blade in bay # warm reset occurred	-	-	-	-	●	-
-	Blade in bay # entered PXE boot mode	-	-	-	-	●	-
-	Blade in bay # exited PXE boot mode	-	-	-	-	●	-

-	Blade in bay # unexpected shutdown occurred	-	-	-	-	●	-
-	Blade in bay # POST completed	-	-	-	-	●	-
-	Blade BMC in bay # has exited flash mode and will auto-powercycle in 10 seconds	-	-	-	-	●	-
-	Blade BMC in bay # will now auto powercycle OFF and then back ON	-	-	-	-	●	-

F トラブルシューティング

この付録では、HP PC Blade エンクロージャに搭載されている Integrated Administrator のトラブルシューティングについて説明します。Integrated Administrator を使用して、エンクロージャ、Blade PC、またはユーザ情報を表示または管理するときに発生する可能性のある性能に関する問題を解決するために、この付録を利用してください。

HP PC Blade エンクロージャのランプ、スイッチ、およびトラブルシューティングに関する情報については、『HP PC Blade エンクロージャ セットアップおよびインストール ガイド』を参照してください。

表 F-1 Integrated Administrator のトラブルシューティング

問題	実行できる処置
Web ブラウザに、Integrated Administrator アプレットが正しく表示されない	クライアント ブラウザの表示色が 16 ビット以上であることを確認してください
使用している Web ブラウザが Integrated Administrator でサポートされていない	サポートされている Web ブラウザを使用するようにしてください。サポートされている Web ブラウザに関する最新の情報については、以下の Web サイト（英語サイト）にある注意事項を参照してください http://www.hp.com/go/ccii/
一般的なブラウザの問題が発生している	Integrated Administrator に関連する最新のヒントについては、以下の Web サイト（英語サイト）にある注意事項を参照してください http://www.hp.com/go/ccii/
Integrated Administrator にアクセスすると、Web ブラウザが不安定になる	JVM (Java Virtual Machine) は、Build 3802 以上でなければなりません。 [Netscape]ユーザは、この JVM を含む[Netscape 6.2]以上を使用することをおすすめします。また、[Internet Explorer]ユーザは、Sun Microsystems 社から最新の JVM をダウンロードできます このアップデートは、Windows 95 および Windows 98 ユーザには必須であり、Windows 2000 ユーザの場合は Service Pack 2 に含まれています。Windows XP または Windows Vista®の場合は、Sun Microsystems 社の Web サイトにアクセスして最新の JVM サポートもダウンロードしてください
Integrated Administrator に、最新のブレード情報が表示されない	Blade PC の設定情報は、Blade PC の電源投入時セルフ テスト (POST) 中に Integrated Administrator と交換されます
Blade PC 情報が不明	Blade PC を起動した後に Integrated Administrator を再起動した場合は、Blade PC を再起動するまで Integrated Administrator に Blade PC の設定情報は表示されません また、Blade PC BIOS は、Blade PC の情報の一部をヘルス サービスから取得するため、ヘルス サービスまたは OS をインストールした後、Integrated Administrator が新しい情報を参照できるようにするには Blade PC の電源を入れなおす必要が生じる場合があります

表 F-1 Integrated Administrator のトラブルシューティング (続き)

GUI からログアウトされた。その理由と対処方法は何か	アクセス権が変更されている可能性があります。その場合は、もう一度ログインして、新しいアクセス権を使用してください。問題が解決しない場合は、エンクロージャ管理者に連絡してください
「upload config」を実行すると、不要情報が画面に表示され、次にコマンドが正常終了したというメッセージが表示される	このコマンドでエラーが発生したわけではありません。すべて想定された動作です
エラーが発生したのか	
ファンの速度が一定周期で上昇し、その後通常の速度に戻る	ファンは、24 時間ごとに 60 秒間セルフテストを実行します
ユーザ名とパスワードは有効であるのに、Integrated Administrator にログインできない	Integrated Administrator は、最大 48 の同時実行セッションをサポートしていません。セッション数がこのしきい値に達していないことを確認してください。また、アカウントが無効になっていないことをエンクロージャ管理者に確認してください
イベント リストに、イベントの修復が表示されない	Integrated Administrator は修復およびすべての Normal/Informational イベントをレポートしますが、それらを表示するには、ユーザはイベント ポリシーを選択する必要があります また、ユーザは、エンクロージャのシステム ログを表示することもできます

G イベントのアイコンと詳細

Integrated Administrator は、「Caution（注意）」および「Critical（重大）」という2つのカテゴリに従って、エンクロージャのイベントをリアルタイムに通知します。イベントが発生すると、Integrated Administrator は、クリックすると詳細が表示されるアイコンを生成してユーザに通知します。

表 G-1 イベント通知アイコン

アイコン	説明
	Informational（情報）：情報提供目的のメッセージ 情報提供目的のメッセージが正常な動作に影響を与えることはありません
	Normal（標準）：エンクロージャの動作で通常発生するイベント Normal イベントが発生している場合は、正常な動作が保証されます
	Caution-Minor（注意-マイナー）：エンクロージャの動作、電源の維持、またはエンクロージャのユーザ コミュニティへのサービスを妨げないイベント Caution-Minor イベントが発生している場合は、正常な動作が保証されます
	Caution（注意）：エンクロージャの動作、電源の維持、またはエンクロージャのユーザ コミュニティへのサービスを妨げないイベント Caution イベントが発生すると、正常な動作は保証されなくなります
	Warning（警告）： 問題が発生する可能性のある状態です
	Critical（重大）：エンクロージャの継続的な動作を妨げるイベント 重大イベントが発生すると、エンクロージャが停止する場合があります

以下の表に、すべてのイベント メッセージを Integrated Administrator によって表示される形式で示します。

表 G-2 イベントの詳細

重大度	ソース	日付	時間	イベントの詳細
	エンクロージャ	<日付>	<時間>	エンクロージャで障害が発生しました
	エンクロージャ	<日付>	<時間>	ファン#で障害が発生しました
	エンクロージャ	<日付>	<時間>	電源供給装置#で障害が発生しました
	エンクロージャ	<日付>	<時間>	エンクロージャの温度が、重大しきい値を超えました

表 G-2 イベントの詳細 (続き)

	ベイ#のブレード	<日付>	<時間>	ブレード#で障害が発生しました
	ベイ#のブレード	<日付>	<時間>	ブレード#の温度が、重大しきい値を超えました
	エンクロージャ	<日付>	<時刻>	電源装置#が「OK」の状態になりました
	エンクロージャ	<日付>	<時刻>	ファン#が「OK - リダンダント変更」の状態になりました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの温度が「温度上昇」の状態になりました
	エンクロージャ	<日付>	<時間>	エンクロージャは、機能が低下した状態です
	エンクロージャ	<日付>	<時間>	ファン#は、機能が低下した状態です
	エンクロージャ	<日付>	<時間>	電源供給装置のリダンダント状態が不明です
	エンクロージャ	<日付>	<時間>	電源供給装置がリダンダント状態ではなくなりました
	エンクロージャ	<日付>	<時間>	電源供給装置#は、機能が低下した状態です
	エンクロージャ	<日付>	<時間>	エンクロージャの温度が、注意しきい値を超えました
	ベイ#のブレード	<日付>	<時間>	ブレード#は、機能が低下した状態です
	ベイ#のブレード	<日付>	<時間>	ブレード#の温度が、注意しきい値を超えました
	エンクロージャ	<日付>	<時刻>	電源サブシステムの容量がリダンダント状態になりました
	エンクロージャ	<日付>	<時刻>	電源サブシステムの容量がレジリエント状態になりました
	エンクロージャ	<日付>	<時刻>	電源サブシステムの容量がレジリエント状態になりました
	エンクロージャ	<日付>	<時刻>	ホットプラグ対応電源装置が取り付けられました
	エンクロージャ	<日付>	<時刻>	ホットプラグ対応電源装置が取り外されました
	エンクロージャ	<日付>	<時刻>	ホットプラグ対応ファンが取り付けられました
	エンクロージャ	<日付>	<時刻>	ホットプラグ対応ファンが取り外されました
	ベイ#のブレード	<日付>	<時刻>	ホットプラグ対応ブレードが取り付けられました
	ベイ#のブレード	<日付>	<時刻>	ホットプラグ対応ブレードが取り外されました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの電源が投入されました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの電源が切断されました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの BMC (Blade Management Controller) がフラッシュ モードを開始しました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードが POST を完了しました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの電源が投入されました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの電源が切断されました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードで予期しないシャットダウンが発生しました
	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードでシステム BIOS のフラッシュが開始されました

表 G-2 イベントの詳細 (続き)

①	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードでシステム BIOS のフラッシュが完了しました
①	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの前面 I/O ブランク機能が、「不明」「N/A」「非アクティブ」「アクティブ」のどれかの状態に変わりました
①	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードの診断アダプタが、「不明」「N/A」「なし」「あり」のどれかの状態に変わりました
①	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードで温度上昇によるリセットが発生しました
①	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードが PXE 起動モードに入りました
①	ベイ#のブレード	<日付>	<時刻>	ベイ#のブレードが PXE 起動モードを終了しました
①	ベイ#のブレード	<日付>	<時刻>	ベイ#の BMC (Blade Management Controller) がフラッシュ モードを終了しました。10 秒後に電源が自動的に入れ直されます
①	ベイ#のブレード	<日付>	<時刻>	ベイ#の BMC (Blade Management Controller) の電源が自動的にオフにされ、その後オンにされます

H 電源管理およびリダンダント電源装置

Integrated Administrator は、バージョン 4.30 から、HP PC Blade エンクロージャおよび HP PC Blade エンクロージャ G2 の両方で電源装置のリダンダントをサポートします。HP PC Blade エンクロージャ G2 のエンクロージャで 2 つの電源装置が 1 つの 200 V 以上の電源コンセントに接続されていれば、電源装置が停止した場合にも、PC Blade エンクロージャ G2 のエンクロージャ内にあるすべてのブレードは、その数や種類にかかわらず動作を継続し、パフォーマンスも低下しません。リダンダント電源装置の使用が必要な場合のベスト プラクティスがこの方法であり、推奨される導入方式だと考えられます。

HP PC Blade エンクロージャ G2 のエンクロージャで 200 V 未満の電力しか利用できない場合、または HP PC Blade エンクロージャ G2 にアップグレードされていない HP PC Blade エンクロージャが使用されている場合には、利用できる外部電源の出力、ブレードの総数、および存在するブレードの種類を組み合わせてによって、電源装置の冗長性の度合いが異なります。

 **注記：** IA FW バージョン 4.3 がインストールされた PC Blade エンクロージャで、2 つの電源装置が 1 つの電源に接続され、bc2000 ブレードまたは bc2200 のみを取り付けられている場合には、電源装置の冗長性が常に確保されます。PC Blade エンクロージャ G2 の場合には、AC 電圧が 100 V 程度であっても同様です。

この項の後半では、200 V 未満の電源コンセントに接続された PC Blade エンクロージャ G2 のエンクロージャ、または PC Blade エンクロージャ G2 にアップグレードされていないエンクロージャで、IA 4.3 の電源装置による冗長性のサポートを適用する方法について説明しています。どちらの場合も、エンクロージャに取り付けるブレードは、bc2500、bc2800、またはその両方です。

IA 4.3 では、5 つの電源サブシステム状態が導入されています。エンクロージャの電源サブシステム状態（またはステータス）は、ブレード数、ブレードの種類組み合わせ、および利用できる AC 電圧によって決まります。ブレード数または AC 電圧によって、エンクロージャのサブシステムの状態およびその結果のステータスが異なります。5 つの状態は以下のとおりです。

- **リダンダント：** 電源装置の停止によってパフォーマンスが低下しているブレードはありません。ブレードの総数は、リダンダント電源容量の範囲内です。
- **レジリエント：** 電源装置の停止のため、すべてのブレードのパフォーマンスを低下させます。ブレードの総数は、リダンダント電源容量の範囲を超えていますが、レジリエント電源容量の範囲内にあります。
- **レジリエント（スロットリング）：** 電源装置の停止によってエンクロージャまたはブレードがシャットダウンするのを防ぐため、すべてのブレードのパフォーマンスを事前に低下させます。ブレードの総数が、レジリエント電源容量の範囲を超えています。
- **非リダンダント：** 電源装置の停止が発生したため、エンクロージャで電源装置がリダンダント状態ではなくなっています。ただし、AC 電圧が 200 V 以上あるか、ブレードの総数がリダンダント

ト容量の範囲内にある場合は、すべてのブレードが引き続き動作し、パフォーマンスも低下しません。

- 非リダンダント（スロットリング）電源装置の停止が発生しました。1つの電源装置に対して割り当てられた電源容量に合わせて、すべてのブレードのパフォーマンスを低下させています。ブレードの総数が、リダンダント電源容量の範囲を超えています。

ブレードの総数がエンクロージャのリダンダント電源容量で許可されている最大ブレード数以下である限り、エンクロージャの電源はリダンダント状態とみなされ、電源装置が停止した場合でもすべてのブレードを最大の電力で実行できます。エンクロージャのリダンダント電源割り当て容量に適合する最大ブレード数を判断するには、電力計算ツールを使用する必要があります。詳しくは、<http://h30099.www3.hp.com/configurator/calc/Power%20Calculator%20Catalog.xls>（英語サイト）の「Power Calculator Links」を参照してください。

以下の表では、電源状態ごとに、AC 電圧およびブレード数の変化によってブレードおよびエンクロージャのステータスがどのような結果になるかを示しています。

ブレード数	電源の数	電源サブシステムのステータス	ブレードのステータス	エンクロージャのステータス
<最大リダンダント	2	リダンダント	<ul style="list-style-type: none"> ● 最大電力 ● 緑色ランプ 	<ul style="list-style-type: none"> ● ヘルス ステータス OK ● 緑色ランプ
	1	非リダンダント	<ul style="list-style-type: none"> ● 最大電力 ● 緑色ランプ 	<ul style="list-style-type: none"> ● ヘルス=低下 ● オレンジ色のランプ ● システム ログ、イベント、および SNMP トラップがヘルスの低下を示す
>最大リダンダント <=最大レジリエント	2	レジリエント	<ul style="list-style-type: none"> ● 最大電力 ● 緑色ランプ 	<ul style="list-style-type: none"> ● ヘルス=低下 ● オレンジ色のランプ ● システム ログ、イベント、および SNMP トラップがヘルスの低下を示す
	1	非リダンダント（スロットリング）	<ul style="list-style-type: none"> ● パフォーマンス低下 ● ヘルス低下 ● オレンジ色のランプ 	<ul style="list-style-type: none"> ● ヘルス=低下 ● オレンジ色のランプ ● システム ログ、イベント、および SNMP トラップがヘルスの低下を示す
>最大レジリエント	2	レジリエント（スロットリング）	<ul style="list-style-type: none"> ● パフォーマンス低下 ● ヘルス低下 ● オレンジ色のランプ 	<ul style="list-style-type: none"> ● ヘルス=低下 ● オレンジ色のランプ ● システム ログ、イベント、および SNMP トラップがヘルスの低下を示す
	1	非リダンダント（スロットリング）	<ul style="list-style-type: none"> ● パフォーマンス低下 ● ヘルス低下 ● オレンジ色のランプ 	<ul style="list-style-type: none"> ● ヘルス=低下 ● オレンジ色のランプ ● システム ログ、イベント、および SNMP トラップがヘルスの低下を示す

 **注記：** HP BladeSystem bc2800 Blade PC には、HP BladeSystem PC Blade エンクロージャ G2 で追加された電源および冷却機能によるサポートが必要です。したがって、bc2800 を前の世代の HP PC Blade エンクロージャに取り付けると、ブレードの実行パフォーマンスの低下につながります。Blade PC を最高のパフォーマンスで実行するには、HP PC Blade エンクロージャ G2 を購入するか、別売のアップグレード キットを使用して既存のエンクロージャを PC Blade エンクロージャ G2 にアップグレードする必要があります。

I 出荷時の設定

この付録では、HP PC Blade Enclosure Integrated Administrator の以下のコンポーネントについて、出荷時の設定を説明します。

- エンクロージャ
- ユーザ
- グループ
- ネットワーク
- プロトコル

エンクロージャ

以下の表に、Blade PC エンクロージャに関連するフィールドの、Integrated Administrator での初期値を示します。

 **注記：** SET FACTORY コマンドを実行すると、[Trap Policy]設定および[Syslog Policy]設定も出荷時設定に戻ります。

表 1-1 エンクロージャの初期値

フィールド	初期値
Name	IA-XXXXXXXXXXXX XXXXXXXXXXXX は、Integrated Administrator の MAC アドレスです
Rack Name	UnnamedRack
Asset Tag	アセット タグ=シリアル番号
Time Zone	CST6CDT
Autopoweron	Enabled
Trap Policy	すべて Enabled
Syslog Policy	すべて Enabled

ユーザ

より新しい HP BladeSystem PC ブレード スイッチを使用している場合、Integrated Administrator での初期設定のユーザは以下の通りです。

- Administrator
- switch
- SAM (HP PC Session Allocation Manager)

HP BladeSystem PC Blade Switch、製品番号 243283-B21 または DW367A を使用している場合、Integrated Administrator での初期設定のユーザは以下の通りです。

- Administrator
- switcha
- switchb
- SAM (HP PC Session Allocation Manager)

 **注記：**「switcha」アカウントと「switchb」アカウントは、オプションで取り付けるインターコネク ト スイッチ コンソールにアクセスする場合に使用します。

グループ

Integrated Administrator に、初期設定のグループはありません。

ネットワーク

Integrated Administrator の出荷時には、以下の初期値が割り当てられています。

表 1-2 エンクロージャの初期値

フィールド	初期値
DHCP	Enabled
Dynamic DNS	Enabled

プロトコル

以下の表に、ネットワーク インタフェース プロトコルに関連するフィールドの、Integrated Administrator での初期値を示します。

表 1-3 プロトコルの初期値

フィールド	初期値
HTTP	On
SSH	On
TELNET	On
SOAP	OFF

表 1-3 プロトコルの初期値 (続き)

SNMP	On
SNMP location	(空白)
SNMP contact	(空白)
READ community	Public
WRITE community	(空白)
NTP	Disabled
IP Security	Disabled
AlertMail	Disabled

J タイム ゾーンの設定

HP PC Blade Enclosure Integrated Administrator でサポートされているすべてのタイム ゾーンをこの付録に記載します。これらのタイム ゾーンは、以下のカテゴリに分類されています。

- ユニバーサル
- アフリカ
- アジア
- ヨーロッパ
- オセアニア
- 極地
- 南北アメリカ

Universal

以下の表に、Integrated Administrator でサポートされているユニバーサル タイム ゾーンの設定値を示します。

△ **注意：** Integrated Administrator に GMT タイム ゾーンを認識させるには、「Etc:」の文字列を前に付ける必要があります。

表 J-1 ユニバーサル タイム ゾーンの数値

CET	Etc:GMT+5	Etc:GMT-4	HST
CST6CDT	Etc:GMT+6	Etc:GMT-5	MET
EET	Etc:GMT+7	Etc:GMT-6	MST
EST	Etc:GMT+8	Etc:GMT-7	MST7MDT
EST6EDT+1	Etc:GMT+9	Etc:GMT-8	Navajo
Etc:GMT	Etc:GMT+10	Etc:GMT-9	PST8PDT
Etc:GMT0	Etc:GMT+11	Etc:GMT-10	UCT
Etc:GMT+0	Etc:GMT+12	Etc:GMT-11	Universal
Etc:GMT+1	Etc:GMT-0	Etc:GMT-12	UTC
Etc:GMT+2	Etc:GMT-1	Etc:GMT-13	WET

表 J-1 ユニバーサル タイム ゾーン の値 (続き)

Etc:GMT+3	Etc:GMT-2	Etc:GMT-14	W-SU
Etc:GMT+4	Etc:GMT-3	Greenwich	Zulu

アフリカ

以下の表に、Integrated Administrator でサポートされているアフリカのタイム ゾーンの設定値を示します。

表 J-2 アフリカのタイム ゾーン値

Africa:Abidjan	Africa:Ceuta	Africa:Lagos	Africa:Niamey
Africa:Accra	Africa:Conakry	Africa:Libreville	Africa:Nouakchott
Africa:Addis Ababa	Africa:Dakar	Africa:Lome	Africa:Ouagadougou
Africa:Algiers	Africa:Dar_es_Salaam	Africa:Luanda	Africa:Porto-Novo
Africa:Asmera	Africa:Djibouti	Africa:Lubumbashi	Africa:Sao_Tome
Africa:Bamako	Africa:Douala	Africa:Lusaka	Africa:Timbuktu
Africa:Bangui	Africa:El_Aaiun	Africa:Malabo	Africa:Tripoli
Africa:Banjul	Africa:Freetown	Africa:Maputo	Africa:Tunis
Africa:Bissau	Africa:Gaborone	Africa:Maseru	Africa:Windhoek
Africa:Blantyre	Africa:Harare	Africa:Mbabane	Egypt
Africa:Brazzaville	Africa:Johannesburg	Africa:Mogadishu	Libya
Africa:Brazzaville	Africa:Kampala	Africa:Monrovia	-
Africa:Cairo	Africa:Kigali	Africa:Nairobi	-
Africa:Casablanca	Africa:Kinshasa	Africa:Ndjamena	

アジア

以下の表に、Integrated Administrator でサポートされているアジアのタイム ゾーンの設定値を示します。

表 J-3 アジアのタイム ゾーン値

Asia:Aden	Asia:Dushanbe	Asia:Nicosia	Asia:Tokyo
Asia:Almaty	Asia:Gaza	Asia:Novosibirsk	Asia:Ujung_Pandang
Asia:Amman	Asia:Harbin	Asia:Omsk	Asia:Ulaanbaatar
Asia:Anadyr	Asia:Hong_Kong	Asia:Phnom_Penh	Asia:Ulan_Bator
Asia:Aqtau	Asia:Hovd	Asia:Pyongyang	Asia:Urumqi
Asia:AqtobeAqtobe	Asia:Irkutsk	Asia:Qatar	Asia:Vientiane
Asia:Ashgabat	Asia:Istanbul	Asia:Rangoon	Asia:Vladivostok
Asia:Ashkhabad	Asia:Jakarta	Asia:Riyadh	Asia:Yakutsk

表 J-3 アジアのタイム ゾーン値 (続き)

Asia:Baghdad	Asia:Jayapura	Asia:Riyadh87	Asia:Yekaterinburg
Asia:Bahrain	Asia:Jerusalem	Asia:Riyadh88	Asia:Yerevan
Asia:Baku	Asia:Kabul	Asia:Riyadh89	Hongkong
Asia:Bangkok	Asia:Kamchatka	Asia:Saigon	Iran
Asia:Beirut	Asia:Karachi	Asia:Samarkand	Israel
Asia:Bishkek	Asia:Kashgar	Asia:Seoul	Japan
Asia:Brunei	Asia:Katmandu	Asia:Shanghai	Mideast:Riyadh87
Asia:Calcutta	Asia:Krasnoyarsk	Asia:Singapore	Mideast:Riyadh88
Asia:Chungking	Asia:Kuala_Lumpur	Asia:Taipei	Mideast:Riyadh89
Asia:Colombo	Asia:Kuching	Asia:Tashkent	PRC
Asia:Dacca	Asia:Kuwait	Asia:Tbilisi	ROC
Asia:Damascus	Asia:Macao	Asia:Tehran	ROK
Asia:Dhaka	Asia:Magadan	Asia:Tel_Aviv	Singapore
Asia:Dili	Asia:Manila	Asia:Thimbu	Turkey
Asia:Dubai	Asia:Muscat	Asia:Thimphu	

ヨーロッパ

以下の表に、Integrated Administrator でサポートされているヨーロッパのタイム ゾーンの設定値を示します。

表 J-4 ヨーロッパのタイム ゾーン値

Eire	Europe:Lisbon	Europe:Skopje
Europe:Amsterdam	Europe:Ljubljana	Europe:Sofia
Europe:Andorra	Europe:London	Europe:Stockholm
Europe:Athens	Europe:Luxembourg	Europe:Tallinn
Europe:Belfast	Europe:Madrid	Europe:Tirane
Europe:Belgrade	Europe:Malta	Europe:Tiraspol
Europe:Berlin	Europe:Minsk	Europe:Uzhgorod
Europe:Bratislava	Europe:Monaco	Europe:Vaduz
Europe:Brussels	Europe:Moscow	Europe:Vatican
Europe:Bucharest	Europe:Nicosia	Europe:Vienna
Europe:Budapest	Europe:Oslo	Europe:Vilnius
Europe:Chisinau	Europe:Paris	Europe:Warsaw
Europe:Copenhagen	Europe:Prague	Europe:Zagreb
Europe:Dublin	Europe:Riga	Europe:Zaporozhye
Europe:Gibraltar	Europe:Rome	Europe:Zurich

表 J-4 ヨーロッパのタイムゾーン値 (続き)

Europe:Helsinki	Europe:Samara	GB
Europe:Istanbul	Europe:San_Marino	GB-Eire
Europe:Kaliningrad	Europe:Sarejevo	Poland
Europe:Kiev	Europe:Simferopol	Portugal

オセアニア

以下の表に、Integrated Administrator でサポートされているオセアニアのタイムゾーンの設定値を示します。

表 J-5 オセアニアのタイムゾーン値

Atlantic:Azores	Australia:North	Kwajalein
Atlantic:Bermuda	Australia:NSW	NZ
Atlantic:Canary	Australia:Perth	NZ-CHAT
Atlantic:Cape_Verde	Australia:Queensland	Pacific:Apia
Atlantic:Faeroe	Australia:South	Pacific:Auckland
Atlantic:Jan_Mayen	Australia:Sydney	Pacific:Chatham
Atlantic:Madeira	Australia:Tasmania	Pacific:Easter
Atlantic:Reykjavik	Australia:Victoria	Pacific:Efate
Atlantic:South_Georgia	Australia:West	Pacific:Enderbury
Atlantic:St_Helena	Australia:Yancowinna	Pacific:Fakaofu
Atlantic:Stanley	Iceland	Pacific:Fiji
Australia:ACT	Indian:Antananarivo	Pacific:Funafuti
Australia:Adelaide	Indian:Chagos	Pacific:Galapagos
Australia:Brisbane	Indian:Christmas	Pacific:Gambier
Australia:Broken_Hill	Indian:Cocos	Pacific:Guadalcanal
Australia:Canberra	Indian:Comoro	Pacific:Guam
Australia:Darwin	Indian:Kerguelen	Pacific:Honolulu
Australia:Hobart	Indian:Mahe	Pacific:Johnston
Australia:LHI	Indian:Maldives	Pacific:Kiritimati
Australia:Lindeman	Indian:Mauritius	Pacific:Kosrae
Australia:Lord_Howe	Indian:Mayotte	Pacific:Kwajalein
Australia:Melbourne	Indian:Reunion	Pacific:Majuro
Pacific:Marquesas	Pacific:Pitcairn	Pacific:Tongatapu
Pacific:Midway	Pacific:Ponape	Pacific:Truk
Pacific:Nauru	Pacific:Port_Moresby	Pacific:Wake
Pacific:Niue	Pacific:Rarotonga	Pacific:Wallis

表 J-5 オセアニアのタイム ゾーン値 (続き)

Pacific:Norfolk	Pacific:Saipan	Pacific:Yap
Pacific:Noumea	Pacific:Samoa	US:Hawaii
Pacific:Pago_Pago	Pacific:Tahiti	US:Samoa
Pacific:Palau	Pacific:Tarawa	-

極地

以下の表に、Integrated Administrator でサポートされている極地のタイム ゾーンの設定値を示します。

表 J-6 極地のタイム ゾーン値

Antarctica:Casey	Antarctica:McMurdo	Antarctica:Vostok
Antarctica:Davis	Antarctica:Palmer	Antarctica:Longyearbyen
Antarctica:DumontDUrville	Antarctica:South_Pole	Antarctica:
Antarctica:Mawson	Antarctica:Syowa	

南北アメリカ

以下の表に、Integrated Administrator でサポートされている南北アメリカのタイム ゾーンの設定値を示します。

表 J-7 南北アメリカのタイム ゾーン値

America:Adak	America:Chihuahua	America:Guatemala
America:Anchorage	America:Cordoba	America:Guayaquil
America:Anguilla	America:Costa_Rica	America:Guyana
America:Antigua	America:Cuiaba	America:Halifax
America:Araguaina	America:Curacao	America:Havana
America:Aruba	America:Dawson	America:Hermosillo
America:Asuncion	America:Dawson_Creek	America:Indiana:Indianapolis
America:Atka	America:Denver	America:Indiana:Knox
America:Barbados	America:Detroit	America:Indiana:Marengo
America:Belem	America:Dominica	America:Indiana:Vevay
America:Belize	America:Edmonton	America:Indianapolis
America:Boa_Vista	America:Eirunepe	America:Inuvik
America:Bogota	America:El_Salvador	America:Iqaluit
America:Boise	America:Ensenada	America:Jamaica
America:Buenos_Aires	America:Fort_Wayne	America:Jujuy
America:Cambridge_Bay	America:Fortaleza	America:Juneau

表 J-7 南北アメリカのタイムゾーン値 (続き)

America:Cancun	America:Glace_Bay	America:Kentucky:Louisville
America:Caracas	America:Godthab	America:Kentucky:Monticello
America:Catamarca	America:Goose_Bay	America:Knox_IN
America:Cayenne	America:Grand_Turk	America:La_Paz
America:Chicago	America:Guadeloupe	America:Los_Angeles
America:Louisville	America:Rainy_River	Brazil:DeNoronha
America:Maceio	America:Rankin_Inlet	Brazil:East
America:Managua	America:Recife	Canada:Central
America:Manaus	America:Regina	Canada:Eastern
America:Martinique	America:Rio_Branco	Canada:East-Saskatchewan
America:Mazatlan	America:Rosario	Canada:Mountain
America:Mendoza	America:Santiago	Canada:Newfoundland
America:Menominee	America:Santo_Domingo	Canada:Pacific
America:Merida	America:Sao_Paulo	Canada:Saskatchewan
America:Mexico_City	America:Scoresbysund	Canada:Yukon
America:Miquelon	America:Shiprock	Chile:Continental
America:Monterrey	America:St_Johns	Chile:EasterIsland
America:Montevideo	America:St_Kitts	Cuba
America:Montreal	America:St_Lucia	Jamaica
America:Montserrat	America:St_Thomas	Mexico:BajaNorte
America:Nassau	America:St_Vincent	Mexico:BajaSur
America:New_York	America:Swift_Current	Mexico:General
America:Nipigon	America:Tegucigalpa	US:Alaska
America:Nome	America:Thule	US:Aleutian
America:Noronha	America:Thunder_Bay	US:Arizona
America:Panama	America:Tijuana	US:Central
America:Pangnirtung	America:Tortola	US:Eastern
America:Paramaribo	America:Vancouver	US:East-Indiana
America:Phoenix	America:Virgin	US:Indiana-Starke
America:Port_of_Spain	America:Whitehorse	US:Michigan
America:Prince	America:Winnipeg	US:Mountain
America:Porto_Acre	America:Yakutat	US:Pacific
America:Porto_Velho	America:Yellowknife	-
America:Puerto_Rico	Brazil:Acre	-

K オープン ソースの利用

Integrated Administrator は内蔵 Linux をベースにしており、多数のオープン ソース コンポーネントを含んでいます。HP はオープン ソース ライセンスに準拠し、使用されているすべてのオープン ソース コンポーネントのソース コードを以下の URL のサイト（英語サイト）で公開しています。

<http://opensource.hp.com/>

Integrated Administrator プロジェクトを見つけるには、すべてのプロジェクトの一覧を参照してください。

L サポートされる SNMP トラップ

以下の表は、サポートされる SNMP トラップを示しています。

 **注記：** トラップについて詳しくは、HP SNMP MIB ファイル CPQRACK.MIB バージョン 1.10 を参照してください。

表 L-1 サポートされる CRQRACK MIB トラップ

#	トラップ名	説明	重大度	状態
22001	cpqRackNameChanged	ラック名変更	INFORMATIONAL	OPERATIONAL
22002	cpqRackEnclosureNameChanged	エンクロージャ名変更	INFORMATIONAL	OPERATIONAL
22003	cpqRackEnclosureRemoved	エンクロージャの取り外し	INFORMATIONAL	OPERATIONAL
22004	cpqRackEnclosureInserted	エンクロージャの取り付け	INFORMATIONAL	OPERATIONAL
22005	cpqRackEnclosureTempFailed	エンクロージャ温度、異常	CRITICAL	NONOPERATIONAL
22006	cpqRackEnclosureTempDegraded	エンクロージャ温度、性能低下	MAJOR	DEGRADED
22007	cpqRackEnclosureTempOk	エンクロージャ温度、正常	INFORMATIONAL	OPERATIONAL
22008	cpqRackEnclosureFanFailed	エンクロージャ ファン、故障	CRITICAL	NONOPERATIONAL
22009	cpqRackEnclosureFanDegraded	エンクロージャ ファン、性能低下	MAJOR	DEGRADED
22010	cpqRackEnclosureFanOk	エンクロージャ ファン、正常	INFORMATIONAL	OPERATIONAL
22011	cpqRackEnclosureFanRemoved	エンクロージャ ファンの取り外し	MINOR	DEGRADED
22012	cpqRackEnclosureFanInserted	エンクロージャ ファンの取り付け	INFORMATIONAL	OPERATIONAL
22013	cpqRackPowerSupplyFailed	ラック電源、故障	CRITICAL	NONOPERATIONAL
22014	cpqRackPowerSupplyDegraded	ラック電源、性能低下	MAJOR	DEGRADED
22015	cpqRackPowerSupplyOk	ラック電源、正常	INFORMATIONAL	OPERATIONAL
22016	cpqRackPowerSupplyRemoved	ラック電源の取り外し	MINOR	DEGRADED

表 L-1 サポートされる CRQRACK MIB トラップ (続き)

#	トラップ名	説明	重大度	状態
22017	cpqRackPowerSupplyInserted	ラック電源の取り付け	INFORMATIONAL	OPERATIONAL
22018	cpqRackPowerSubsystemNotRedundant	ラック電源サブシステム、非冗長	MAJOR	DEGRADED
22019	cpqRackPowerSubsystemLineVoltageProblem	ラック電源入力電圧の問題	MAJOR	DEGRADED
22020	cpqRackPowerSubsystemOverloadCondition	ラック電源サブシステム、過負荷状況	MAJOR	DEGRADED
22028	cpqRackServerBladeRemoved	Blade PC の取り外し	INFORMATIONAL	OPERATIONAL
22029	cpqRackServerBladeInserted	Blade PC の取り付け	INFORMATIONAL	OPERATIONAL
22037	cpqRackEnclosureManagerDegraded	IA ヘルス ステータス、性能低下	MAJOR	DEGRADED
22038	cpqRackEnclosureManagerOK	IA ヘルス ステータス、修復	INFORMATIONAL	OPERATIONAL
22052	cpqRackServerBladeStatusRepaired	Blade PC ヘルス ステータス、修復	INFORMATIONAL	OPERATIONAL
22053	cpqRackServerBladeStatusDegraded	Blade PC ヘルス ステータス、性能低下	MAJOR	OPERATIONAL
22054	cpqRackServerBladeStatusCritical	Blade PC ヘルス ステータス、重大	CRITICAL	OPERATIONAL
22056	cpqRackServerBladeUnexpectedShutdown	ブレードの予期しないシャットダウン	INFORMATIONAL	OPERATIONAL
22057	cpqRackServerBladeManagementControllerFWUpdating	BMC ファームウェアのアップデート	INFORMATIONAL	OPERATIONAL
22058	cpqRackServerBladeSystemBIOSFWUpdating	ブレードのシステム BIOS ファームウェアのアップデート	INFORMATIONAL	OPERATIONAL
22059	cpqRackServerBladeManagementControllerFirmwareUpdateComplete	サーバの BMC ファームウェアのアップデート完了	INFORMATIONAL	OPERATIONAL
22060	cpqRackServerBladeSystemBIOSFWUpdateComplete	ブレードのシステム BIOS ファームウェアのアップデート完了	INFORMATIONAL	OPERATIONAL
22061	cpqRackServerBladeRGSSessionActive	ブレードの RGS セッションがアクティブに変更	INFORMATIONAL	OPERATIONAL
22062	cpqRackServerBladeRGSSessionInactive	ブレードの RGS セッションが非アクティブに変更	INFORMATIONAL	OPERATIONAL
22063	cpqRackServerBladeDiagnosticAdaptorInserted	ブレード診断アダプタを取り付け	INFORMATIONAL	OPERATIONAL
22064	cpqRackServerBladeDiagnosticAdaptorRemoved	ブレード診断アダプタを取り外し	INFORMATIONAL	OPERATIONAL
22065	cpqRackServerBladeEnteredPXEBootMode	ブレードが PXE 起動モードを開始	INFORMATIONAL	OPERATIONAL

表 L-1 サポートされる CRQRACK MIB トラップ (続き)

#	トラップ名	説明	重大度	状態
22066	cpqRackServerBladeExitedPXEBootMode	ブレードが PXE 起動モードを終了	INFORMATIONAL	OPERATIONAL
22067	cpqRackServerBladeWarmReset	ブレードが温度上昇によりリセット	INFORMATIONAL	OPERATIONAL
22068	cpqRackServerBladeBIOSPOSTCompleted	ブレードのシステム BIOS の POST が完了	INFORMATIONAL	OPERATIONAL
22069	cpqRackServerBladePoweredOn	ブレードに電源投入	INFORMATIONAL	OPERATIONAL
22070	cpqRackServerBladePoweredOff	ブレードの電源切断	INFORMATIONAL	OPERATIONAL

索引

記号/数字

802.1Q 8

A

[Administration]タブ 46
AlertMail 5, 101, 169
Asset Tag 23

B

[Bays]タブ 36
Blade PC
RBSU 112
エラー メッセージ 146
確認 116
起動順序 135
警告メッセージ 145
電源の切断 114
動作 114
ベイの管理コマンド 77
ベイ 111
ユーザのアクセス権 126

C

CLI
Blade PC ベイの管理コマンド 77
アクセス 62
一般的な管理コマンド 63
一般的なコマンド 63
イベント メッセージ 80
エンクロージャの管理コマンド 72
エンクロージャのネットワーク設定コマンド 70
規則 143
コマンド ライン インタフェース 61
操作 63
特有の機能 83

ユーザ アカウント コマンド 66
リモート アクセス 62
ローカルアクセス 62

D

DHCP 6

E

[Enclosure]タブ 20
ESR (Enclosure Self Recovery) 8
[Event List]タブ 55

F

Fan Status 22
Flash Disaster Recovery 140

H

HP Blade エンクロージャ管理システムおよびユーティリティ 8
HP SAM との統合 7
HP Systems Insight Manager 5, 7, 8
[HP Systems Insight Manager]の Web サイト 7
HP の Web サイト 2, 3
HTTP 168

I

IA (Integrated Administrator)
各部 11
機能 4, 10
参考資料 2
注意事項についての Web サイト 159
ハイパーリンク 7
プロセッサのグループ化 7
IA ファームウェア 52
IA ファームウェアの更新 52

IEEE 802.1Q VLAN 8
Interconnect Tray Type 23
[Interconnect]タブ 58
Internet Explorer 159
IP Security 169
IP アドレス
初期 11
ローカル コンソール 13
IP セキュリティ 103

J

Java Virtual Machine 159

L

LAN 接続 4

N

Netscape 159
NTP 6, 104, 169

P

Power Subsystem Status 23
ProLiant Essentials Rapid Deployment Pack 8
[ProLiant Essentials Rapid Deployment パック]の Web サイト 8

R

Rapid Deployment Pack 8
RBSU 8, 112
Read Community 30, 169
RMON 8
ROM ベース セットアップ ユーティリティ 8, 112

S

SAM、統合 7
Secure Sockets Layer 5

- SNMP
 - アラート 5
 - サポート 105
 - 設定 29
 - トラップ 177
- SOAP
 - インタフェース 6
 - インタフェース、無効化 108
 - インタフェース、有効化 108
 - サポートされているインタフェース コマンド 109
 - サポート タスクの設定 108
- SSH 168
- SSH 認証 134
- SSL 5
- [Systems Insight Manager]の Web サイト 7

- T**
- TELNET 168
- Total Capacity 23

- V**
- Virtual Buttons
 - [Bays]タブ 44
 - [Enclosure]タブ 32

- W**
- Web サイト
 - HP 2, 3
 - HP Systems Insight Manager 7
 - Integrated Administrator についての注意事項 159
 - ProLiant Essentials Rapid Deployment パック 8
 - オープン ソース 176
 - サポートおよびトラブルシューティング 2
- Web ブラウザ 17
- Web ベースのユーザ インタフェース
 - アクセス 17
 - 移動 18
 - 設定 14
- Write Community 30, 169

- あ**
- アイコン 161

- アクセス
 - ROM ベース セットアップ ユーティリティ 112
 - Web ベースのユーザ インタフェース 17
 - リモート 62
- アクセス権、ユーザ 89
- アジアのタイム ゾーン 171
- アセット タグ番号 93
- アフリカのタイム ゾーン 171
- アラート
 - SNMP 5
 - 電子メール 5, 102
- 暗号化 5
- 安全に関する情報 1

- い**
- 位置、システムの変更 106
- 一般的な管理コマンド 63
- 一般的なコマンド 63
- 移動 18
- イベント
 - CLI メッセージ 80
 - アイコン 161
 - 詳細 161
 - 通知 7
 - マスク可能なエンクロージャのメッセージ 155
 - ログ ポリシー 58
- インタフェース
 - SOAP 6
 - SOAP、無効化 108
 - SOAP、有効化 108
 - サポートされている SOAP コマンド 109

- え**
- エミュレーション 12
- エラー メッセージ
 - Blade PC ベイ 146
 - エンクロージャ 146
 - 管理 146
- エンクロージャ
 - Integrated Administrator 4
 - アラート 5
 - エラー メッセージ 146
 - 概要 120
 - 確認 119
 - 管理コマンド 72
 - 管理 117
- 警告メッセージ 144
- システム ソフトウェアの機能 4
- 情報 21
- 設定、カスタマイズ 90
- 設定 167
- 通知 5
- 電源の切断 136
- 動作の確認 117
- 名前 91
- ネットワーク設定コマンド 70
- マスク可能なイベント メッセージ 155
- マスク可能なログ メッセージ 152
- 問題、通知 5
- エンクロージャ設定のカスタマイズ 90

- お**
- オープン ソース Web サイト 176
- オープン ソース 176
- オセアニアのタイム ゾーン 173

- か**
- 概要、エンクロージャ概要の生成 120
- 概要 10
- 確認
 - Blade PC 116
 - Blade PC の動作 114
 - エンクロージャ 119
 - 設定ツールと情報 10
 - 問題コンポーネント 121
- 各部、リア パネル 11
- 管理タスク 111
- 管理
 - Blade PC ベイ 111
 - エラー メッセージ 146
 - エンクロージャ 117
 - 警告メッセージ 145
 - コネクタ 62
 - システムおよびユーティリティ 8
 - プロセッサ 7
 - ユーザ 126

- き**
- キーベースの SSH 認証 134
- 規則、CLI 143

起動、Flash Disaster

Recovery 140

機能

Integrated Administrator 4

エンクロージャ システム ソフトウェア 4

高度 132

極地のタイム ゾーン 174

く

グループ化、IA (Integrated Administrator) プロセッサ 7

グループ

アカウントの削除 130

作成 126

設定 168

追加 50, 95

表示/変更 52

変更 126

リスト 47

け

警告メッセージ

Blade PC 145

エンクロージャ 144

管理 145

こ

工場設定 167

更新、ファームウェア 139

高度な機能 132

コネクタ 11

コマンド、CLI

Blade PC ベイの管理 77

一般的な管理 63

一般的 63

エンクロージャの管理 72

エンクロージャのネットワーク設定 70

ユーザ アカウント 66

コマンド

サポートされている SOAP インタフェース 109

コマンド ライン イベント メッセージ 80

コマンド ライン インタフェース (CLI) 61, 143

コミュニティ名 105

コミュニティ名の入力 105

コンソール

コネクタ 62

リモート セッションの開始 111

リモート セッションの有効化 101

ローカル 13

ログ 45

さ

削除

グループ アカウント 130

ユーザ アカウント 128, 130

作成

グループ 126

証明書要求 134

サポートおよびトラブルシューティング 2

サポートおよびトラブルシューティングの Web サイト 2

サポート 2

サポートされるユーザ 5

サポートされるユーザの数 5

参考資料、IA (Integrated Administrator) 2

し

時刻 94

システム

位置 106

設定 88

連絡先情報 106

ログ ポリシー 33

ログ 33

出荷時

設定 167

詳細、イベント 161

証明書、セキュリティ 134

証明書要求 134

初期 IP アドレス 11

初期設定

Integrated Administrator の値 12

資料、IA (Integrated Administrator) 関連 2

診断メッセージ 149

す

推奨されるタスク 16

ストップ ビット 12

せ

セキュリティ証明書のダウンロード 134

セキュリティ

IP の設定 103

証明書 134

ダウンロード 134

セッション、リモート コンソール セッションの開始 111

接続、LAN 4

設定スクリプト 53

設定、タイム ゾーン 170

設定の複製 133

設定

AlertMail 101

Blade PC の起動順序 135

IP セキュリティ 103

NTP 104

SNMP 29

SNMP サポート 105

Web ベースのユーザ インタフェース 14

工場 167

システム 88

出荷時 167

ネットワーク 26

複製 133

ユーザ アカウント 95

そ

送信先 106, 107

装置の記号 1

ソフトウェア

エンクロージャ システムの機能 4

ツール 8

た

タイム ゾーン

アジア 171

アフリカ 171

オセアニア 173

極地 174

南北アメリカ 174

ユニバーサル 170

ヨーロッパ 172

タイム ゾーンの設定 170

タブ

Administration 46

Bays 36

- Enclosure 20
 - Event List 55
 - Interconnect 58
- つ**
- 追加のタスク 16
 - 追加
 - グループ 50, 95
 - トラップ送信先 106
 - ユーザ 48, 98
 - 通信速度 12
 - 通知、イベント 7
 - 通知 5
- て**
- デッキ パネル 19
 - デバイスの要件 11
 - 電源装置、リダンダント 164
 - 電源の管理 164
 - 電源の切断
 - Blade PC 114
 - エンクロージャ 136
 - 電子メール アラート 102
 - 電力消費量
 - [Bays]タブ 38
 - [Enclosure]タブ 31
 - レポート 6
- と**
- 動作、Blade PC 114
 - トップ パネル 18
 - トラップ、SNMP 177
 - トラップ送信先 106, 107
 - トラップ送信先の削除 107
 - トラブルシューティング 2, 159
- な**
- 名前、エンクロージャおよびラック 91
 - 南北アメリカのタイムゾーン 174
- に**
- 認証 134
- ね**
- ネットワーク タイム プロトコル 6, 104
 - ネットワーク
 - 自動構成 6
- 設定 26, 168
 - プロトコル 137
- は**
- ハイパーリンク 7
 - パスワード、復元 139
 - パリティ 12
- ひ**
- 左パネル 19
 - 日付と時刻 94
 - ビット数 12
 - 表示
 - グループ 52
 - ユーザ 52
- ふ**
- ファームウェア、更新 52, 139
 - 復元、パスワード 139
 - ブラウザ、Web 17
 - フロー制御 12
 - プロトコルの設定 168
 - プロトコル 137
- へ**
- ベイ
 - 温度 39
 - 情報 40
 - リスト 36
 - ヘッドレス操作 8
 - 変更
 - Blade PC ベイへのユーザのアクセス権 126
 - アセット タグ番号 93
 - エンクロージャ名およびラック名 91
 - グループ 52, 126
 - システムの位置 106
 - システム連絡先情報 106
 - 日付と時刻 94
 - ユーザ 52
- ほ**
- ポリシー
 - イベント ログ 58
 - システム ログ 33
- ま**
- マスク可能
 - エンクロージャのイベント メッセージ 155
 - ログ メッセージ 152
- む**
- 無効化
 - ネットワーク プロトコル 137
 - ユーザ アカウント 128
- め**
- メッセージ
 - Blade PC の診断 149
 - CLI 80
 - エンクロージャ システム 152
 - エンクロージャのイベント 155
 - マスク可能なイベント 155
 - マスク可能なログ 152
- も**
- 問題コンポーネント 121
- ゆ**
- 有効化、リモート コンソール セッション 101
 - ユーザ
 - CLI コマンド 66
 - アカウント アクセス権 89
 - アカウント管理 5
 - アカウント セキュリティ 5
 - アカウントの削除 130
 - アカウントの設定 95, 168
 - アカウントの表示/変更 52
 - アカウントの無効化と削除 128
 - 管理 126
 - サポート対象 5
 - 追加 48, 98
 - リスト 46
 - ユーティリティ
 - HP Session Allocation Manager 7
 - HP Systems Insight Manager 7, 8
 - ROM ベース セットアップ ユーティリティ 8
 - ユニット確認ランプ 116, 119
 - ユニバーサル タイム 170

よ

要件、ローカル デバイス 11
ヨーロッパのタイム ゾーン 172

ら

ラック名 91
ランプ 116, 119

り

リア パネルの各部 11
リダンダント電源装置 164
リモート
 アクセス 5, 62
 コンソール 43
 コンソール セッションの開
 始 111
 コントロール 5
 セッション 101

れ

レポート、電力消費量 6

ろ

ローカル コンソール 13
ログ
 [Bays]タブ 45
 システム 33
 マスク可能なメッセージ 152