



統合管理モジュール II  
ユーザーズ・ガイド







統合管理モジュール II  
ユーザーズ・ガイド

本装置は、高調波電流規格 JIS C 61000-3-2 に適合しています。

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： Integrated Management Module II  
User's Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第3版第1刷 2013.6

© Copyright IBM Corporation 2013.

# 目次

|             |     |
|-------------|-----|
| 表 . . . . . | vii |
|-------------|-----|

## 第 1 章 概要 . . . . . 1

|  |   |
|--|---|
| IMM2 の基本レベル、標準レベル、および拡張レベルの機能 . . . . .              | 2 |
| IMM2 基本レベル機能 . . . . .                               | 3 |
| IMM2 標準レベル機能 . . . . .                               | 3 |
| IMM2 拡張レベル機能 . . . . .                               | 3 |
| IMM2 機能の改善点 . . . . .                                | 3 |
| IMM2 のアップグレード . . . . .                              | 4 |
| IMM2 と BladeCenter アドバンスド・マネージメント・モジュールの使用 . . . . . | 4 |
| Web ブラウザーとオペレーティング・システムの要件 . . . . .                 | 4 |
| 本書で使用される注記 . . . . .                                 | 6 |

## 第 2 章 IMM2 Web インターフェースの開始および使用 . . . . . 7

|  |    |
|--|----|
| IMM2 Web インターフェースへのアクセス . . . . .  | 7  |
| IBM System x サーバー・ファームウェアの Setup ユーティリティを使用した IMM2 ネットワーク接続のセットアップ . . . . . | 8  |
| IMM2 へのログイン . . . . .  | 10 |
| IMM2 のアクションの説明 . . . . .   | 11 |

## 第 3 章 IMM2 Web ユーザー・インターフェースの概要 . . . . . 15

|                                   |    |
|-----------------------------------|----|
| Web セッションの設定 . . . . .            | 15 |
| ページの自動最新表示 . . . . .              | 15 |
| 侵入警告メッセージ . . . . .               | 17 |
| ログアウト . . . . .                   | 18 |
| 「System Status」タブ . . . . .       | 19 |
| 「Events」タブ . . . . .              | 25 |
| イベント・ログ . . . . .                 | 26 |
| イベント受信者 . . . . .                 | 29 |
| 「Service and Support」タブ . . . . . | 31 |
| サービス・データのダウンロード . . . . .         | 31 |
| 「Server Management」タブ . . . . .   | 32 |
| サーバー・ファームウェア . . . . .            | 33 |
| Remote Control . . . . .          | 38 |
| サーバーのプロパティ . . . . .              | 43 |
| サーバー電源アクション . . . . .             | 47 |
| ディスク . . . . .                    | 47 |
| メモリー . . . . .                    | 48 |
| Processors . . . . .              | 49 |
| サーバー・タイムアウト . . . . .             | 50 |
| PXE ネットワーク・ブート . . . . .          | 50 |
| 最新の OS の障害画面 . . . . .            | 50 |
| 「IMM Management」タブ . . . . .      | 51 |

## 第 4 章 IMM2 の構成 . . . . . 53

|                                   |    |
|-----------------------------------|----|
| サーバー・タイムアウトの設定 . . . . .          | 56 |
| IMM2 の日付と時刻の設定 . . . . .          | 58 |
| シリアル・ポート設定の構成 . . . . .           | 60 |
| ユーザー・アカウントの構成 . . . . .           | 61 |
| ユーザー・アカウント . . . . .              | 61 |
| グループ・プロファイル . . . . .             | 64 |
| グローバル・ログイン設定の構成 . . . . .         | 65 |
| 一般設定 . . . . .                    | 65 |
| アカウントのセキュリティー・ポリシーの設定 . . . . .   | 67 |
| ネットワーク・プロトコルの構成 . . . . .         | 70 |
| イーサネット設定の構成 . . . . .             | 70 |
| SNMP アラート設定の構成 . . . . .          | 72 |
| DNS の構成 . . . . .                 | 74 |
| DDNS の構成 . . . . .                | 74 |
| SMTP の構成 . . . . .                | 75 |
| LDAP の構成 . . . . .                | 76 |
| Telnet の構成 . . . . .              | 81 |
| USB の構成 . . . . .                 | 82 |
| ポート割り当ての構成 . . . . .              | 83 |
| セキュリティー設定の構成 . . . . .            | 84 |
| HTTPS プロトコルの構成 . . . . .          | 85 |
| CIM over HTTPS プロトコルの構成 . . . . . | 86 |
| LDAP クライアント・プロトコルの構成 . . . . .    | 87 |
| セキュア・シェル・サーバーの構成 . . . . .        | 89 |
| SSL の概要 . . . . .                 | 90 |
| SSL 証明書の処理 . . . . .              | 90 |
| SSL 証明書管理 . . . . .               | 91 |
| IMM の構成の復元と変更 . . . . .           | 92 |
| IMM2 の再始動 . . . . .               | 92 |
| IMM2 の出荷時のデフォルト値へのリセット . . . . .  | 93 |
| アクティベーション管理キー . . . . .           | 94 |

## 第 5 章 サーバー状況のモニター . . . . . 95

|                         |    |
|-------------------------|----|
| システム状況の表示 . . . . .     | 95 |
| システム情報の表示 . . . . .     | 97 |
| サーバー・ヘルスの表示 . . . . .   | 98 |
| ハードウェア・ヘルスの表示 . . . . . | 99 |

## 第 6 章 IMM2 タスクの実行 . . . . . 103

|   |     |
|---|-----|
| サーバーの電源状況の制御 . . . . .                              | 104 |
| リモート・プレゼンス機能および Remote Control 機能 . . . . .         | 105 |
| IMM2 ファームウェアおよび Java または ActiveX アプレットの更新 . . . . . | 106 |
| リモート・プレゼンス機能の使用可能化 . . . . .                        | 107 |
| Remote Control のスクリーン・キャプチャー . . . . .              | 107 |
| Remote Control の Video Viewer モード . . . . .         | 108 |
| Remote Control のビデオ・カラー・モード . . . . .               | 108 |
| Remote Control のキーボード・サポート . . . . .                | 109 |
| Remote Control のマウス・サポート . . . . .                  | 111 |

|                       |     |
|-----------------------|-----|
| リモート電源制御              | 113 |
| パフォーマンス統計の表示          | 113 |
| リモート・デスクトップ・プロトコルの始動  | 113 |
| Knock-knock 機能の説明     | 113 |
| リモート・ディスク             | 117 |
| PXE ネットワーク・ブートのセットアップ | 119 |
| サーバー・ファームウェアの更新       | 120 |
| システム・イベントの管理          | 126 |
| イベント・ログの管理            | 126 |
| システム・イベントの通知          | 128 |
| サービスおよびサポート情報の収集      | 132 |
| 最新の OS 障害画面データのキャプチャー | 134 |
| サーバー電源の管理             | 135 |
| 電源機構と全体のシステム電源の制御     | 136 |
| 現在取り付けられている電源機構の表示    | 138 |
| 電源機構の容量の表示            | 138 |
| 電力使用量の履歴の表示           | 139 |

## 第 7 章 Features on Demand . . . . 141

|                     |     |
|---------------------|-----|
| アクティベーション・キーのインストール | 141 |
| アクティベーション・キーの削除     | 144 |
| アクティベーション・キーのエクスポート | 145 |

## 第 8 章 コマンド・ライン・インターフ

### ェース . . . . . 147

|                                    |     |
|------------------------------------|-----|
| IPMI を使用した IMM2 の管理                | 147 |
| IPMItool の使用                       | 147 |
| コマンド・ライン・インターフェースへのアクセス            | 147 |
| コマンド・ライン・セッションへのログイン               | 148 |
| Serial-to-Telnet または SSH リダイレクトの構成 | 148 |
| コマンド構文                             | 149 |
| 機能および制限                            | 149 |
| アルファベット順のコマンド・リスト                  | 150 |
| ユーティリティー・コマンド                      | 152 |
| exit コマンド                          | 152 |
| help コマンド                          | 152 |
| history コマンド                       | 152 |
| モニター・コマンド                          | 153 |
| clearlog コマンド                      | 153 |
| fans コマンド                          | 153 |
| ffdc コマンド                          | 153 |
| led コマンド                           | 154 |
| readlog コマンド                       | 156 |
| show コマンド                          | 157 |
| syshealth コマンド                     | 158 |
| temps コマンド                         | 158 |
| volts コマンド                         | 159 |
| vpd コマンド                           | 159 |
| サーバーの電源および再始動制御コマンド                | 160 |
| power コマンド                         | 160 |
| pxeboot コマンド                       | 160 |
| reset コマンド                         | 161 |
| シリアル・リダイレクト・コマンド                   | 161 |
| console コマンド                       | 161 |
| 構成コマンド                             | 161 |
| accseccfg コマンド                     | 162 |

|                      |     |
|----------------------|-----|
| alertcfg コマンド        | 164 |
| asu コマンド             | 165 |
| backup コマンド          | 168 |
| dhcpcfg コマンド         | 169 |
| dns コマンド             | 170 |
| ethusb コマンド          | 172 |
| gprofile コマンド        | 173 |
| ifconfig コマンド        | 173 |
| keycfg コマンド          | 175 |
| ldap コマンド            | 177 |
| ntp コマンド             | 178 |
| passwordcfg コマンド     | 179 |
| ports コマンド           | 180 |
| portcfg コマンド         | 181 |
| restore コマンド         | 182 |
| restoredefaults コマンド | 183 |
| set コマンド             | 183 |
| smtp コマンド            | 184 |
| snmp コマンド            | 184 |
| snmpalerts コマンド      | 187 |
| srcfg コマンド           | 189 |
| sshcfg コマンド          | 189 |
| ssl コマンド             | 190 |
| sslcfg コマンド          | 191 |
| telnetcfg コマンド       | 195 |
| thermal コマンド         | 195 |
| timeouts コマンド        | 195 |
| usbeth コマンド          | 196 |
| users コマンド           | 196 |
| IMM2 制御コマンド          | 201 |
| alertentries コマンド    | 202 |
| batch コマンド           | 205 |
| clearcfg コマンド        | 206 |
| clock コマンド           | 206 |
| identify コマンド        | 207 |
| info コマンド            | 207 |
| resetsp コマンド         | 208 |
| spreset コマンド         | 208 |

## 付録 A. ヘルプおよび技術サポートの入手 . . . . . 209

|                       |     |
|-----------------------|-----|
| 依頼する前に                | 209 |
| 資料の使用                 | 210 |
| ヘルプおよび情報を WWW から入手する  | 210 |
| IBM への DSA データの送信方法   | 210 |
| 個別設定したサポート Web ページの作成 | 211 |
| ソフトウェアのサービスとサポート      | 211 |
| ハードウェアのサービスとサポート      | 211 |

## 付録 B. 特記事項 . . . . . 213

|                                    |     |
|------------------------------------|-----|
| 商標                                 | 213 |
| 重要事項                               | 214 |
| サーバーの廃棄・譲渡時のハード・ディスク上のデータ消去に関するご注意 | 215 |
| 粒子汚染                               | 216 |
| 通信規制の注記                            | 216 |

|   |     |
|---|-----|
| 電波障害自主規制特記事項 . . . . .                                | 217 |
| Federal Communications Commission (FCC)               |     |
| statement . . . . .                                   | 217 |
| Industry Canada Class A emission compliance           |     |
| statement . . . . .                                   | 217 |
| Avis de conformité à la réglementation d'Industrie    |     |
| Canada. . . . .                                       | 217 |
| Australia and New Zealand Class A statement . . . . . | 217 |
| European Union EMC Directive conformance              |     |
| statement . . . . .                                   | 217 |
| Germany Class A statement . . . . .                   | 218 |

|   |            |
|---|------------|
| VCCI クラス A 情報技術装置 . . . . .                       | 219        |
| Korea Communications Commission (KCC)             |            |
| statement . . . . .                               | 219        |
| Russia Electromagnetic Interference (EMI) Class A |            |
| statement . . . . .                               | 220        |
| People's Republic of China Class A electronic     |            |
| emission statement . . . . .                      | 220        |
| Taiwan Class A compliance statement. . . . .      | 220        |
| <b>索引 . . . . .</b>                               | <b>221</b> |



---

## 表

|                              |    |                            |     |
|------------------------------|----|----------------------------|-----|
| 1. IMM2 アクション . . . . .      | 11 | 6. 電源アクションと説明 . . . . .    | 105 |
| 2. サーバーの電源状態と作動状態 . . . . .  | 22 | 7. ASU コマンド . . . . .      | 165 |
| 3. セキュリティー設定ポリシーの値 . . . . . | 67 | 8. トランザクション・コマンド . . . . . | 168 |
| 4. 許可ビット . . . . .           | 79 | 9. 微粒子およびガスの制限 . . . . .   | 216 |
| 5. システム状態の説明 . . . . .       | 96 |                            |     |



---

## 第 1 章 概要

統合管理モジュール II サービス・プロセッサ (IMM2) は、統合管理モジュール (IMM) サービス・プロセッサの第 2 世代であり、サービス・プロセッサ機能、Super I/O、ビデオ・コントローラー、およびリモート・プレゼンス機能をサーバー・システム・ボード上の単一のチップに統合しています。IMM の場合と同様に、IMM2 はベースボード管理コントローラー (BMC) とリモート管理アダプター II の機能を結合し、次のようないくつかの改良点を提供します。

- システム管理のための、専用あるいは共有のイーサネット接続の選択。
- Intelligent Platform Management Interface (IPMI) およびサービス・プロセッサ・インターフェースの両方で 1 つの IP アドレスを使用。この機能は、IBM® BladeCenter ブレード・サーバーには適用されません。
- 組み込み Dynamic System Analysis (DSA)。
- Advanced Settings ユーティリティ (ASU) を使用したリモート構成。この機能は、IBM BladeCenter ブレード・サーバーには適用されません。
- インバンドあるいはアウト・オブ・バンドのいずれかで IMM2 にアクセスするためのアプリケーションおよびツールの機能。IBM BladeCenter ブレード・サーバーでは、インバンド IMM2 接続のみがサポートされます。
- 拡張リモート・プレゼンス機能。この機能は、IBM BladeCenter ブレード・サーバーには適用されません。

### 注:

- 専用のシステム管理ネットワーク・ポートは、IBM BladeCenter ブレード・サーバーおよび一部の System x サーバーでは使用できません。このようなサーバーでは、共有の設定のみが使用可能です。
- IBM BladeCenter ブレード・サーバーの場合、IBM BladeCenter アドバンスド・マネージメント・モジュールは、システム管理機能およびキーボード、ビデオ、マウス (KVM) 多重方式のための 1 次マネージメント・モジュールです。

IBM System x® サーバー・ファームウェアは、IBM の Unified Extensible Firmware Interface (UEFI) 実装環境です。これは、IBM System x サーバーおよび IBM BladeCenter ブレード・サーバーの基本入出力システム (BIOS) に置き換わるものです。BIOS は、ディスク・ドライブ、ハード・ディスク、およびキーボードとの対話など、基本的なハードウェア操作を制御する標準のファームウェア・コードでした。IBM System x サーバー・ファームウェアは、UEFI 2.3 準拠、iSCSI 互換性、Active Energy Manager テクノロジー、および拡張された信頼性とサービス機能など、BIOS にはないいくつかの機能を提供します。Setup ユーティリティは、サーバー情報、サーバー・セットアップ、カスタマイズ互換性の提供、およびブート・デバイス順序の設定を行うことができます。

### 注:

- IBM System x サーバー・ファームウェアは、本書ではサーバー・ファームウェアあるいは UEFI と呼ばれることもあります。

- IBM System x サーバー・ファームウェアは、非 UEFI オペレーティング・システムと完全に互換性があります。
- IBM System x サーバー・ファームウェアの使用について詳しくは、ご使用の IBM サーバーに付属の資料を参照してください。

本書では、IBM サーバーでの IMM2 の機能の使用方法について説明しています。IMM2 は、IBM System x サーバー・ファームウェアと連動し、System x、BladeCenter、および IBM Flex System のシステム管理機能を提供します。

ファームウェア更新を確認するには、以下のステップを実行してください。

注: IBM サポート・ポータルに初めてアクセスする際、ご使用のストレージ・サブシステムの製品カテゴリ、製品ファミリー、および型式番号を選択する必要があります。次回、IBM サポート・ポータルにアクセスすると、最初に選択した製品が Web サイトによってプリロードされ、ご使用の製品用のリンクのみが表示されます。製品リストを変更するか、製品リストに追加するには、「**Manage my product lists (My プロダクト・リストの管理)**」リンクをクリックします。

IBM Web サイトは、定期的に変更されます。ファームウェアおよび資料の検索手順は、本書の記載とは若干異なる場合があります。

1. <http://www.ibm.com/support/entry/portal> にアクセスします。
2. 「**Choose your products (製品の選択)**」の下で、「**Browse for a product (製品リストから選択)**」を選択し、「**Hardware**」を展開します。
3. サーバーのタイプに応じて、「**Systems**」 > 「**System x**」または「**Systems**」 > 「**BladeCenter**」をクリックし、ご使用のサーバー (複数も可) のチェック・ボックスにチェック・マークを付けます。
4. 「**Choose your task**」で、「**Downloads**」をクリックします。
5. 「**See your results**」で、「**View your page**」をクリックします。
6. 「**Flashes & alerts**」ボックスで、該当するダウンロードのリンクをクリックし、「**More results**」をクリックして追加のリンクを確認します。

---

## IMM2 の基本レベル、標準レベル、および拡張レベルの機能

IMM2 では、基本、標準、および拡張の各レベルの IMM2 機能が提供されます。ご使用の IBM サーバーに取り付けられている IMM2 のレベルについて詳しくは、ご使用のサーバーの資料を参照してください。以下の機能は、すべてのレベルで提供されます。

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

さらに、標準レベルおよび拡張レベルでは、標準の Web ブラウザーを使用した Web ベースの管理がサポートされます。

注: 一部の機能が、IBM BladeCenter ブレード・サーバーに適用されない場合があります。

以下は、IMM2 基本レベル機能のリストです。

## IMM2 基本レベル機能

以下は、IMM2 基本レベル機能のリストです。

- IPMI 2.0 インターフェース
- 温度のモニター
- ファンの制御
- LED 管理
- サーバーの電源/リセットの制御
- センサー・モニター
- IPMI PET アラート (Platform Event Trap Alerting)
- IPMI Serial over LAN

## IMM2 標準レベル機能

以下は、IMM2 標準レベル機能のリストです。

- すべての IMM2 基本レベル機能
- 標準の Web ブラウザーを使用した Web ベースの管理
- SNMPv1 および SNMPv3 インターフェース
- Telnet および SSH CLI
- サーバーの電源/リセット制御のスケジューリング
- 人間が読み取れるイベント・ログおよび監査ログ
- システム・ヘルス標識
- オペレーティング・システム・ローダーおよびオペレーティング・システム・ウォッチドッグ
- LDAP 認証および許可
- SNMP トラップ、E メール、Syslog、および CIM 通知のアラート
- NTP クロックの同期
- Telnet/SSH を使用したシリアル・コンソールのリダイレクト

## IMM2 拡張レベル機能

以下は、IMM2 拡張レベル機能のリストです。

- IMM2 の基本レベルおよび標準レベルのすべての機能
- リモート・プレゼンス Java および ActivX クライアント:
  - リモートのキーボード、ビデオ、マウスのサポート
  - リモート・メディア
  - カード上のリモート・ディスク
- オペレーティング・システムがハングした場合の、障害画面キャプチャー

## IMM2 機能の改善点

以下は、IMM から改善された IMM2 機能のリストです。

- セキュリティー (信頼できるサービス・プロセッサ):
  - セキュア・ブート

- 署名付き更新
- IMM2 Core Root for Trust Measurement
- Trusted Platform Module
- IBM System x 全体で一貫性のある新しい Web GUI の設計
- リモート・プレゼンスのビデオ解像度およびカラー階調の向上
- ActiveX リモート・プレゼンス・クライアント
- Ethernet-over-USB インターフェースを USB 2.0 にアップグレード
- Syslog アラート
- 構成変更後の IMM2 リセットは不要

## IMM2 のアップグレード

ご使用の IBM サーバーに基本レベルまたは標準レベルの IMM2 ファームウェア機能が付属している場合は、ご使用のサーバーの IMM2 機能をアップグレードすることもできます。使用可能なアップグレード・レベルおよびオーダーの方法について詳しくは、141 ページの『第 7 章 Features on Demand』を参照してください。

---

## IMM2 と BladeCenter アドバンスド・マネージメント・モジュールの使用

BladeCenter アドバンスド・マネージメント・モジュールは、IBM BladeCenter 製品での標準のシステム管理インターフェースです。現在、一部の IBM BladeCenter ブレード・サーバーには IMM2 が組み込まれていますが、アドバンスド・マネージメント・モジュールは、IBM ブレード・サーバーを含む IBM BladeCenter 製品のシステム管理機能および KVM 多重方式のためのマネージメント・モジュールとして残っています。

IBM BladeCenter ブレード・サーバーには IMM2 への外部ネットワーク・アクセスはなく、アドバンスド・マネージメント・モジュールは、IBM BladeCenter ブレード・サーバーのリモート管理に使用する必要があります。IMM2 は、過去の IBM ブレード・サーバー製品で使用可能な BMC および並行キーボード、ビデオ、マウス (cKVM) オプション・カードの機能に置き換わります。

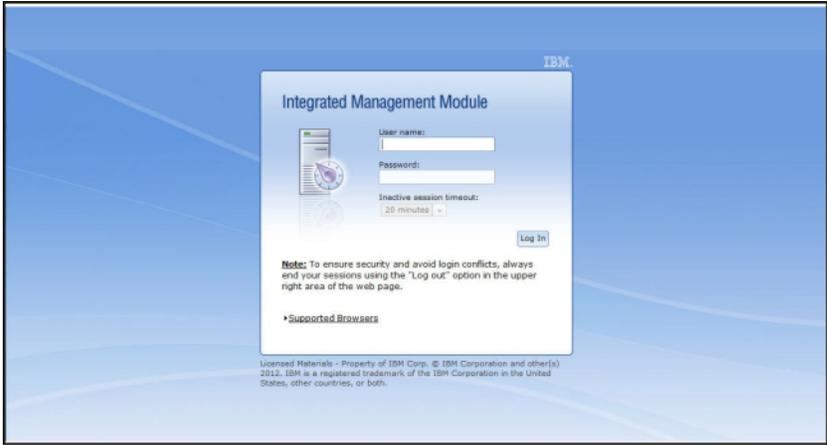
---

## Web ブラウザーとオペレーティング・システムの要件

IMM2 Web インターフェースには、Java™ プラグイン 1.5 以降 (リモート・プレゼンス機能用) と、次のいずれかの Web ブラウザーが必要です。

- Microsoft Internet Explorer バージョン 7 または 8
- Mozilla Firefox バージョン 3.5 以降

これより新しいバージョンの Microsoft Internet Explorer を使用している場合は、Internet Explorer の互換表示を使用して IMM2 Web ページを表示することをお勧めします。前にリストしたブラウザーは、IMM2 ファームウェアで現在サポートされているものと一致します。IMM2 ファームウェアは定期的に拡張され、他のブラウザーのサポートが組み込まれる可能性があります。現在システム上で稼働している IMM2 ファームウェアのバージョンでサポートされているブラウザーのリストについては、IMM2 ログイン・ページの「Supported Browsers」リストを参照してください。次の図は、IMM2 ログイン画面を示しています。



以下のサーバー・オペレーティング・システムには、リモート・プレゼンス機能に必要な USB サポートが搭載されています。

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux バージョン 4.0 および 5.0
- SUSE Linux バージョン 10.0
- Novell NetWare 6.5

ご使用のインターネット・ブラウザのキャッシュには、後でロードが高速になるように、訪問した Web ページに関する情報が保管されます。IMM2 ファームウェアのフラッシュ更新後、ご使用のブラウザが情報を IMM2 から取得する代わりに、キャッシュからの情報を引き続き使用する可能性があります。IMM2 ファームウェアの更新後は、IMM2 から提供される Web ページが正しく表示されるように、ブラウザ・キャッシュを消去することをお勧めします。

---

## 本書で使用される注記

本書では、以下の注意書きが使用されています。

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

---

## 第 2 章 IMM2 Web インターフェースの開始および使用

**重要:** このセクションは、IBM BladeCenter および IBM ブレード・サーバーには適用されません。一部の IBM BladeCenter 製品および IBM ブレード・サーバーでは IMM2 が標準ですが、IBM BladeCenter アドバンスド・マネージメント・モジュールは、IBM ブレード・サーバーを含む IBM BladeCenter 製品のシステム管理機能および KVM 多重方式のための 1 次管理モジュールです。ブレード・サーバー上で IMM2 設定を構成するユーザーは、ブレード・サーバー上で Advanced Settings ユーティリティ (ASU) を使用してこれらのアクションを実行する必要があります。

IMM2 は、サービス・プロセッサ機能、ビデオ・コントローラー、およびリモート・プレゼンス機能 (オプションの仮想メディア・キーが取り付けられている場合) を単一のチップに統合しています。IMM2 Web インターフェースを使用してリモートで IMM2 にアクセスするには、最初にログインする必要があります。この章では、ログインの手順を説明し、IMM2 Web インターフェースから実行できるアクションについても説明します。

---

### IMM2 Web インターフェースへのアクセス

IMM2 は、固定 IP アドレスおよび動的ホスト構成プロトコル (DHCP) による IPv4 アドレス指定をサポートします。IMM2 に割り当てられるデフォルトの固定 IPv4 アドレスは、192.168.70.125 です。IMM2 は、まず DHCP からのアドレスの取得を試行し、取得できない場合は固定 IPv4 アドレスを使用します。

IMM2 は IPv6 もサポートしますが、IMM2 には、デフォルトで決められた固定 IPv6 IP アドレスがありません。IPv6 環境で IMM2 へ最初にアクセスする場合は、IPv4 IP アドレスまたは IPv6 リンク・ローカル・アドレスのいずれかを使用することもできます。IMM2 は固有のリンク・ローカル IPv6 アドレスを生成し、このアドレスは IMM2 Web インターフェースの「Network Interfaces」ページに表示されます。このリンク・ローカル IPv6 アドレスのフォーマットは、以下の例と同様です。

```
fe80::21a:64ff:fee6:4d5
```

IMM2 にアクセスする際は、以下の IPv6 の状態がデフォルトで設定されます。

- IPv6 アドレスの自動構成は、使用可能です。
- IPv6 固定 IP アドレスの構成は、使用不可です。
- DHCPv6 は、使用可能です。
- ステートレス自動構成は、使用可能です。

IMM2 では、専用のシステム管理ネットワーク接続を使用するか、(該当する場合は) サーバーと共有のシステム管理ネットワーク接続を使用するかを選択することができます。ラック・マウント型のサーバーおよびタワー型のサーバーの場合、デフォルトの接続は専用のシステム管理ネットワーク・コネクタを使用します。

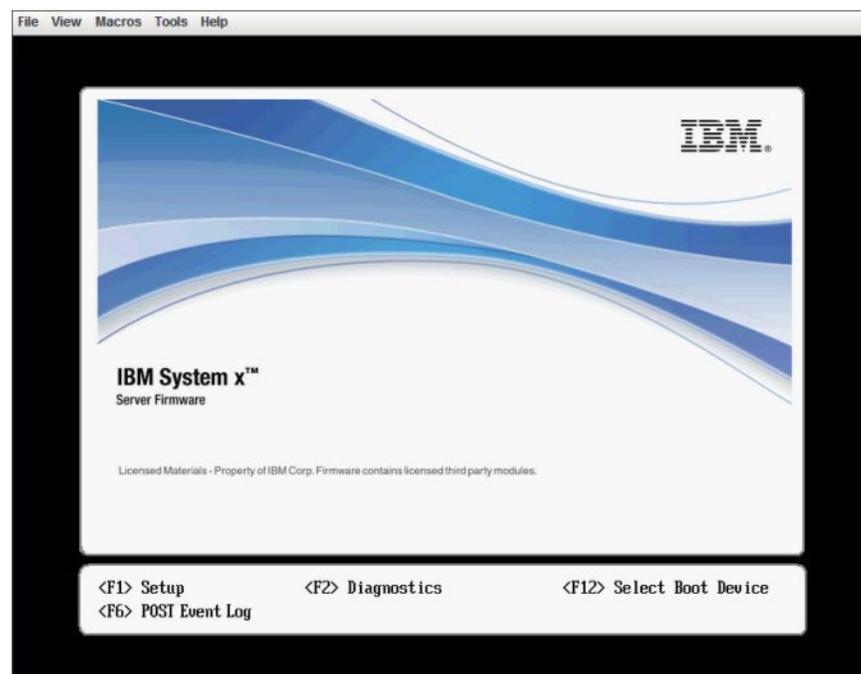
注: 専用のシステム管理ネットワーク・ポートは、ご使用のサーバーで使用できない場合があります。ご使用のハードウェアに専用のネットワーク・ポートがない場合、IMM2 の設定で使用可能なのは、共有の 設定のみです。

## IBM System x サーバー・ファームウェアの Setup ユーティリティを使用した IMM2 ネットワーク接続のセットアップ

サーバーを始動した後、Setup ユーティリティを使用して IMM2 ネットワーク接続を選択することができます。IMM2 ハードウェアを搭載したサーバーは、DHCP サーバーに接続するか、あるいはサーバー・ネットワークが IMM2 固定 IP アドレスを使用するように構成されている必要があります。Setup ユーティリティを使用して IMM2 ネットワーク接続をセットアップするには、以下のステップを実行します。

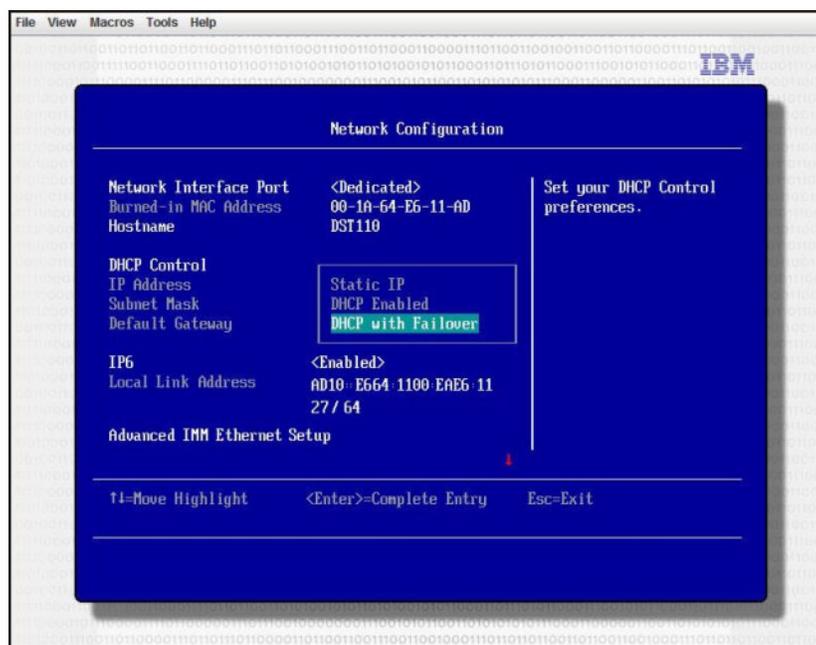
1. サーバーの電源を入れます。IBM System x サーバー・ファームウェアの初期画面が表示されます。

注: サーバーが AC 電源に接続されてから約 90 秒後に、電源制御ボタンがアクティブになります。



2. プロンプト「<F1> Setup」が表示されたら、F1 キーを押します。始動パスワードと管理者パスワードの両方を設定している場合、Setup ユーティリティの完全メニューにアクセスするには、管理者パスワードを入力する必要があります。
3. Setup ユーティリティのメインメニューから「**System Settings**」を選択します。
4. 次の画面で「**Integrated Management Module**」を選択します。
5. 次の画面で「**Network Configuration**」を選択します。
6. 「**DHCP Control**」を強調表示します。「**DHCP Control**」フィールドに、次の 3 つの IMM2 ネットワーク接続の選択項目があります。

- Static IP
- DHCP Enabled
- DHCP with Failover (default)



7. ネットワーク接続の選択項目から 1 つを選択します。
8. 固定 IP アドレスの使用を選択した場合、IP アドレス、サブネット・マスク、およびデフォルト・ゲートウェイを指定する必要があります。
9. また、Setup ユーティリティを使用して、専用のネットワーク接続 (ご使用のサーバーに専用ネットワーク・ポートがある場合)、または共有 IMM2 ネットワーク接続のどちらを使用するかを選択することができます。

**注:**

- 専用のシステム管理ネットワーク・ポートは、ご使用のサーバーで使用できない場合があります。ご使用のハードウェアに専用のネットワーク・ポートがない場合、IMM2 の設定で使用可能なのは、共有の設定のみです。  
「Network Configuration」画面の「Network Interface Port」フィールドで、「Dedicated」(該当する場合) または「Shared」を選択します。
- IMM2 で使用するサーバー上のイーサネット・コネクタの位置を見つけるには、ご使用のサーバーに付属の資料を参照してください。

10. スクロールダウンし、「Save Network Settings」を選択します。
11. Setup ユーティリティを終了します。

**注:**

- サーバー・ファームウェアが再度機能するには、変更が有効になるまで約 1 分間待つ必要があります。
- IMM2 Web インターフェースまたはコマンド・ライン・インターフェース (CLI) から、IMM2 ネットワーク接続を構成することもできます。IMM2 Web インター

フェースでは、ネットワーク接続は「**Network Protocol Properties**」ページ (「**IMM Management**」メニューから「**Network**」を選択) で構成されます。IMM2 CLI では、ご使用のインストール済み環境の構成に応じたいくつかのコマンドを使用して、ネットワーク接続が構成されます。

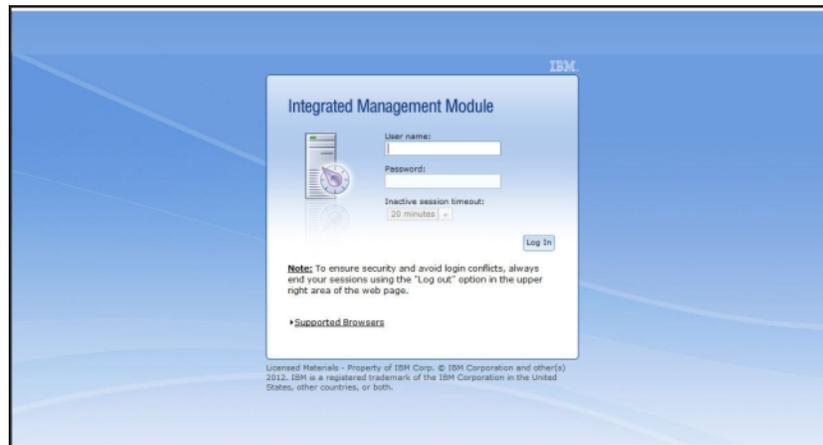
## IMM2 へのログイン

**重要:** IMM2 は、最初はユーザー名 USERID とパスワード PASSWORD (英字の O でなくゼロ) を使用して設定されます。このデフォルトのユーザー設定では、Supervisor アクセス権があります。拡張セキュリティーを使用するには、初期構成時にこのユーザー名とパスワードを変更してください。

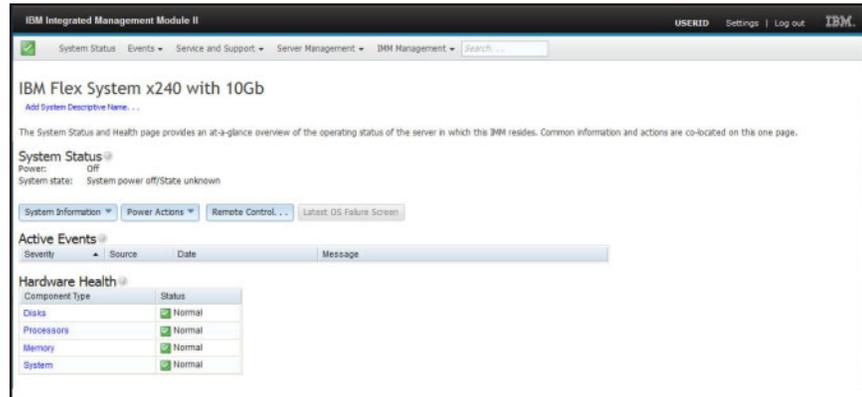
IMM2 Web インターフェースで IMM2 にアクセスするには、以下の手順に従ってください。

1. Web ブラウザーを開きます。アドレスまたは URL フィールドで、接続したい IMM2 の IP アドレスまたはホスト名を入力します。
2. IMM2 ログイン・ウィンドウでユーザー名とパスワードを入力します。IMM2 を初めて使用する場合は、ユーザー名およびパスワードをシステム管理者から入手できます。すべてのログイン試行は、イベント・ログに書き込まれます。システム管理者がどのようにユーザー ID を構成したかに応じて、新規パスワードを入力する必要がある場合があります。

次の図にログイン・ウィンドウを示します。



3. 「Log In」をクリックしてセッションを開始します。次の図に示すように、ブラウザは、「System Status」ページを開きます。このページでは、サーバーの状況とサーバー・ヘルスの要約を簡単に確認することができます。



IMM2 Web インターフェース上部にあるタブから実行できるアクションの説明については、『IMM2 のアクションの説明』を参照してください。

## IMM2 のアクションの説明

IMM2 ウィンドウの上部までナビゲートして、IMM2 を使用したアクティビティーを実行します。タイトル・バーには、ログインしているユーザー名が示されます。タイトル・バーを使用すると、「Settings」で状況画面のリフレッシュ頻度およびカスタム侵入警告メッセージを構成したり、「Log out」で IMM2 Web インターフェースからログアウトしたりすることができます。タイトル・バーの下のタブを使用して、表 1 にリストされているさまざまな IMM2 機能にアクセスすることができます。



表 1. IMM2 アクション

| タブ            | 選択               | 説明  |
|---------------|------------------|---|
| System Status |                  | 「System Status」ページでは、システム状況、アクティブ・システム・イベント、およびハードウェア・ヘルス情報を表示することができます。このページには、「Server Management」タブの「System Information」、「Server Power Actions」、および「Remote Control」機能へのクイック・リンクが表示されます。また、最後のオペレーティング・システム障害の画面キャプチャーのイメージを表示することもできます。詳しくは、19 ページの『「System Status」タブ』および 95 ページの『システム状況の表示』を参照してください。                              |
| Events        | Event Log        | 「Event Log」ページには、現在 IMM2 イベント・ログに保管されているエントリが表示されます。このログには、報告されたシステム・イベントのテキスト記述 (すべてのリモート・アクセス試行および構成変更に関する情報を含む) が含まれます。ログ内のすべてのイベントには、IMM2 の日時の設定を使用したタイム・スタンプが付いています。一部のイベントは、アラートも生成します (そのように構成されている場合)。イベント・ログ内のイベントをソートしたりフィルタリングして、その結果をテキスト・ファイルにエクスポートすることができます。詳しくは、25 ページの『「Events」タブ』および 126 ページの『イベント・ログの管理』を参照してください。 |
|               | Event Recipients | 「Event Recipients」ページでは、システム・イベントの通知先を管理することができます。このページを使用して、各受信者を構成したり、すべてのイベント受信者に適用される設定を管理することができます。また、テスト・イベントを生成して、通知機能の操作を確認することもできます。詳しくは、29 ページの『イベント受信者』および 128 ページの『システム・イベントの通知』を参照してください。  |

表 1. IMM2 アクション (続き)

| タブ                  | 選択                    | 説明  |
|---------------------|-----------------------|---|
| Service and Support | Download Service Data | 「Download Service Data」ページでは、IBM サポートがユーザーを支援するために使用できる情報の圧縮ファイルを作成します。詳しくは、31 ページの『サービス・データのダウンロード』および 132 ページの『サービスおよびサポート情報の収集』を参照してください。  |
| Server Management   | Server Firmware       | 「Server Firmware」ページには、ファームウェア・レベルが表示され、ユーザーが IMM2 ファームウェア、サーバー・ファームウェア、および DSA ファームウェアを更新することができます。詳しくは、33 ページの『サーバー・ファームウェア』および 120 ページの『サーバー・ファームウェアの更新』を参照してください。   |
|                     | Remote Control        | 「Remote Control」ページでは、オペレーティング・システム・レベルでサーバーを制御することができます。このページを使用して、リモート・ディスク機能およびリモート・コンソール機能の両方にアクセスすることができます。ご使用のコンピューターからサーバー・コンソールを表示および操作したり、コンピューターのディスク・ドライブ (CD-ROM ドライブやディスクケット・ドライブなど) の 1 つをサーバーにマウントすることができます。ディスクをマウントした場合は、そのディスクを使用してサーバーを再始動し、サーバー上のファームウェアを更新できます。マウントされたディスクは、サーバーに接続された USB ディスク・ドライブのように表示されます。詳しくは、38 ページの『Remote Control』および 105 ページの『リモート・プレゼンス機能および Remote Control 機能』を参照してください。   |
|                     | Server Properties     | <p>「Server Properties」ページでは、次のように、ご使用のサーバーの各種プロパティ、状況条件、および設定にアクセスすることができます。「Server Properties」ページから使用可能なオプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>「General Settings」タブには、操作およびサポート担当者がシステムを識別するための情報が表示されます。</li> <li>「LEDs」タブには、すべてのシステム LED の状況が表示されます。このタブでは、ロケーション LED の状態を変更することもできます。</li> <li>「Hardware Information」タブには、サーバーの重要プロダクト・データ (VPD) が表示されます。IMM2 は、サーバー情報、サーバー・コンポーネント情報、およびネットワーク・ハードウェア情報を収集します。</li> <li>「Environmentals」タブには、サーバーとそのコンポーネントの電圧および温度の情報が表示されます。</li> <li>「Hardware Activity」タブには、システムに追加された、またはシステムから取り外された FRU (現場交換可能ユニット) コンポーネントの履歴が表示されます。</li> </ul> <p>詳しくは、43 ページの『サーバーのプロパティ』を参照してください。</p> |
|                     | Server Power Actions  | 「Server Power Actions」ページでは、ご使用のサーバーを通じての完全なリモート電源制御 (電源オン、電源オフ、および再始動アクション) を提供します。詳しくは、47 ページの『サーバー電源アクション』および 104 ページの『サーバーの電源状況の制御』を参照してください。   |
|                     | Disks                 | 「Hard Disks」ページには、サーバー内のハード・ディスクの状況が表示されます。ドライブ名をクリックすると、そのハード・ディスクに関するアクティブ・イベントが表示されます。詳しくは、47 ページの『ディスク』を参照してください。   |
|                     | Memory                | 「Memory」ページには、システムで使用可能なメモリー・モジュールと、その状況、タイプ、および容量が表示されます。モジュール名をクリックすると、そのメモリー・モジュールに関するイベントおよびハードウェアの追加情報が表示されます。デュアル・インライン・メモリー・モジュール (DIMM) の取り外しまたは交換を行った場合、正しいメモリー情報を表示するには、取り外しまたは交換の後で少なくとも 1 度はサーバーの電源をオンにする必要があります。詳しくは、48 ページの『メモリー』を参照してください。   |

表 1. IMM2 アクション (続き)

| タブ                          | 選択                       | 説明   |
|-----------------------------|--------------------------|--|
| Server Management<br>(続き)   | Processors               | 「CPUs」ページには、システム内のマイクロプロセッサと、その状況およびクロック・スピードが表示されます。マイクロプロセッサ名をクリックすると、そのマイクロプロセッサに関するイベントおよび追加のハードウェア情報が表示されます。詳しくは、49 ページの『Processors』を参照してください。  |
|                             | Server Timeouts          | 「Server Timeouts」ページでは、サーバー・ハングの発生を検出してリカバリーするためのサーバー始動タイムアウトを管理することができます。詳しくは、50 ページの『サーバー・タイムアウト』および 56 ページの『サーバー・タイムアウトの設定』を参照してください。   |
|                             | PXE Network Boot         | 「PXE Network Boot」ページでは、次の再始動で Preboot Execution Environment (PXE)/動的ホスト構成プロトコル (DHCP) ネットワーク始動を試行するために、ホスト・サーバーの始動(ブート) シーケンスを変更することができます。ホスト始動シーケンスを変更は、ホストが Privileged Access Protection (PAP) の支配下でない場合だけです。詳しくは、50 ページの『PXE ネットワーク・ブート』および 119 ページの『PXE ネットワーク・ブートのセットアップ』を参照してください。  |
|                             | Latest OS Failure Screen | 「Latest OS Failure Screen」ページには、サーバー上で発生した最新のオペレーティング・システム障害の画面イメージ (ある場合) が表示されます。ご使用の IMM2 でオペレーティング・システム障害の画面をキャプチャーするには、オペレーティング・システム・ウォッチドッグが使用可能に設定されている必要があります。詳しくは、50 ページの『最新の OS の障害画面』および 134 ページの『最新の OS 障害画面データのキャプチャー』を参照してください。  |
|                             | Power Management         | 「Server Power Management」ページを使用して、電源関係のポリシーとハードウェアを管理でき、サーバーによって使用された電力量のヒストリーがこのページに表示されます。詳しくは、135 ページの『サーバー電源の管理』を参照してください。   |
| IMM Management<br>(次ページに続く) | IMM Properties           | <p>「IMM Properties」ページでは、次のように、ご使用の IMM2 の各種プロパティ、および設定にアクセスすることができます。「IMM Properties page」ページから使用可能なオプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>「Firmware」タブでは、「Server Management」の「Server Firmware」セクションへのリンクが提供されます。</li> <li>「IMM Date and Time Settings」タブでは、IMM2 の日時設定を表示および構成することができます。</li> <li>「Serial Port」タブでは、IMM2 のシリアル・ポート設定を構成します。これらの設定には、シリアル・ポート・リダイレクト機能で使用されるシリアル・ポートのボー・レート、およびシリアル・リダイレクト・モードと CLI モードの切り替えを行うためのキー・シーケンスなどがあります。</li> </ul> <p>詳しくは、53 ページの『第 4 章 IMM2 の構成』を参照してください。</p> |
|                             | Users                    | 「Users」ページでは、IMM2 ログイン・プロファイルおよびグローバル・ログイン設定を構成します。また、現在 IMM2 にログインしているユーザー・アカウントを表示することもできます。グローバル・ログイン設定には、Lightweight Directory Access Protocol (LDAP) サーバー認証の使用可能化、Web 非アクティブ・タイムアウトの設定、およびアカウント・セキュリティ設定のカスタマイズなどがあります。詳しくは、61 ページの『ユーザー・アカウントの構成』を参照してください。  |

表 1. IMM2 アクション (続き)

| タブ                     | 選択                               | 説明  |
|------------------------|----------------------------------|---|
| IMM Management<br>(続き) | Network                          | <p>「Network Protocol Properties」ページでは、ご使用の IMM2 のネットワーク・プロパティ、状況、および設定にアクセスすることができます。</p> <ul style="list-style-type: none"> <li>「Ethernet」タブでは、IMM2 がイーサネットを使用して通信する方法を管理します。</li> <li>「SNMP」タブでは、SNMPv1 および SNMPv3 エージェントを構成します。</li> <li>「DNS」タブでは、IMM2 が対話する DNS サーバーを構成します。</li> <li>「DDNS」タブでは、IMM2 用の動的 DNS を使用可能または使用不可に設定したり構成したりします。</li> <li>「SMTP」タブでは、E メール経由でのアラートの送信に使用する SMTP サーバー情報を構成します。</li> <li>「LDAP」タブでは、1 つ以上の LDAP サーバーで使用するユーザー認証を構成します。</li> <li>「Telnet」タブでは、IMM2 への Telnet アクセスを管理します。</li> <li>「USB」タブでは、サーバーと IMM2 の間のインバンド通信に使用する USB インターフェースを制御します。これらの設定は、USB リモート制御機能 (キーボード、マウス、大容量ストレージ) には影響しません。</li> <li>「Port Assignments」タブでは、IMM2 上での一部のサービスに使用するポート番号を変更することができます。</li> </ul> <p>詳しくは、70 ページの『ネットワーク・プロトコルの構成』を参照してください。</p> |
|                        | Security                         | <p>「IMM Security」ページでは、次のように、ご使用の IMM2 のセキュリティ・プロパティ、状況、および設定にアクセスすることができます。</p> <ul style="list-style-type: none"> <li>「HTTPS Server」タブでは、HTTPS サーバーを使用可能または使用不可に設定したり、HTTPS サーバーの認証を管理することができます。</li> <li>「CIM Over HTTPS」タブでは、CIM over HTTPS を使用可能または使用不可に設定したり、CIM over HTTPS の認証を管理することができます。</li> <li>「LDAP Client」タブでは、LDAP セキュリティを使用可能または使用不可に設定したり、LDAP セキュリティの認証を管理することができます。</li> <li>「SSH Server」タブでは、SSH サーバーを使用可能または使用不可に設定したり、SSH サーバーの認証を管理することができます。</li> </ul> <p>詳しくは、84 ページの『セキュリティ設定の構成』を参照してください。</p>   |
|                        | IMM Configuration                | <p>「IMM Configuration」ページには、現行の IMM2 構成設定の要約が表示されます。詳しくは、92 ページの『IMM の構成の復元と変更』を参照してください。</p>   |
|                        | Restart IMM                      | <p>「Restart IMM2」ページでは、IMM をリセットすることができます。詳しくは、92 ページの『IMM2 の再始動』を参照してください。</p>   |
|                        | Reset IMM to factory defaults... | <p>「Reset IMM to factory defaults...」ページでは、IMM2 の構成を出荷時のデフォルト値にリセットすることができます。詳しくは、93 ページの『IMM2 の出荷時のデフォルト値へのリセット』を参照してください。</p> <p><b>重要:</b> 「Reset IMM to factory defaults...」をクリックすると、IMM2 に対して行った変更はすべて失われます。</p>   |
|                        | Activation Key Management        | <p>「Activation Key Management」ページでは、オプションの IMM2 またはサーバーの Features on Demand (FoD) 機能のアクティベーション・キーを管理することができます。詳しくは、94 ページの『アクティベーション管理キー』を参照してください。</p>   |

---

## 第 3 章 IMM2 Web ユーザー・インターフェースの概要

この章では、IMM2 Web ユーザー・インターフェース機能の使用法の概要を示します。

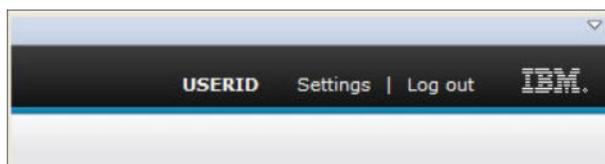
**重要:** このセクションは、IBM BladeCenter および IBM ブレード・サーバーには適用されません。一部の IBM BladeCenter 製品および IBM ブレード・サーバーでは IMM2 が標準ですが、IBM BladeCenter アドバンスド・マネージメント・モジュールは、システム管理機能のための 1 次管理モジュールです。ブレード・サーバー上で IMM2 設定を構成するユーザーは、ブレード・サーバー上で Advanced Settings ユーティリティ (ASU) を使用してこれらのアクションを実行する必要があります。

---

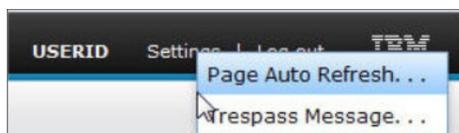
### Web セッションの設定

このセクションでは、Web インターフェース・セッションのメインページの設定について説明します。

IMM2 のメインページでは、Web ページの右上のエリアにメニュー選択項目が表示されます。これらのメニュー項目を使用すると、Web ページの最新表示の動作や、ユーザーがログインするための資格情報を入力したときにユーザーに対して表示するメッセージを構成することができます。次の図は、Web ページの右上のエリアにあるメニュー選択項目を示しています。

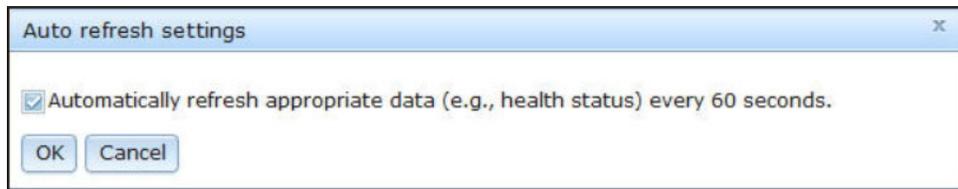


「Settings」項目をクリックすると、次のようなメニュー選択項目が表示されます。



### ページの自動最新表示

Web ページの内容を 60 秒ごとに自動的に最新表示するよう設定するには、Web セッション・ページの右上のエリアにある「Settings」メニュー項目の「Page Auto Refresh」オプションを使用します。ページ内容を 60 秒ごとに最新表示するよう設定するには、「Automatically refresh appropriate data...」チェック・ボックスを選択し、「OK」を押します。ページの自動最新表示を使用不可に設定するには、このチェック・ボックスを選択解除し、「OK」を押します。次の図は、「Auto refresh settings」ウィンドウを示しています。



一部の IMM2 Web ページは、自動最新表示のチェック・ボックスが選択されていない場合でも自動的に最新表示されます。自動的に最新表示される IMM2 Web ページは、次のとおりです。

- **System Status:**

システムと電源の状況は、3 秒ごとに自動的に最新表示されます。

- **Server Power Actions:** (「Server Management」タブの下):

電源の状況は、3 秒ごとに自動的に最新表示されます。

- **Remote Control:** (「Server Management」タブの下):

「Start remote control...」1 の各ボタンは、1 秒ごとに最新表示されます。

「Session List」テーブルは、60 秒に 1 回最新表示されます。

**注:**

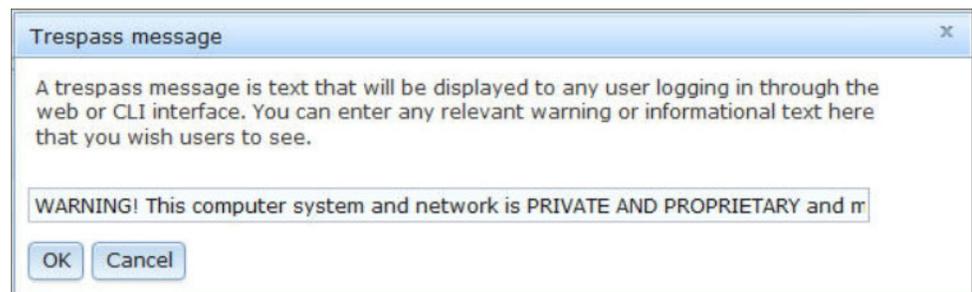
- 自動的に最新表示される Web ページに Web ブラウザーからナビゲートした場合、Web セッションが非アクティブ・タイムアウトで自動的に終了することはありません。
- 「Server Management」の「Remote Control」オプションのページを使用して Remote Control ユーザーに要求を送信した場合は、その Remote Control ユーザーから応答を受信するまで、またはその Remote Control ユーザーがタイムアウトになるまでは、どの Web ページにナビゲートしたかに関係なく、Web セッションはタイムアウトになりません。Remote Control ユーザーからの要求の処理が完了すると、非アクティブ・タイムアウト機能が再開されます。

注: 上記の注は、すべての Web ページに適用されます。

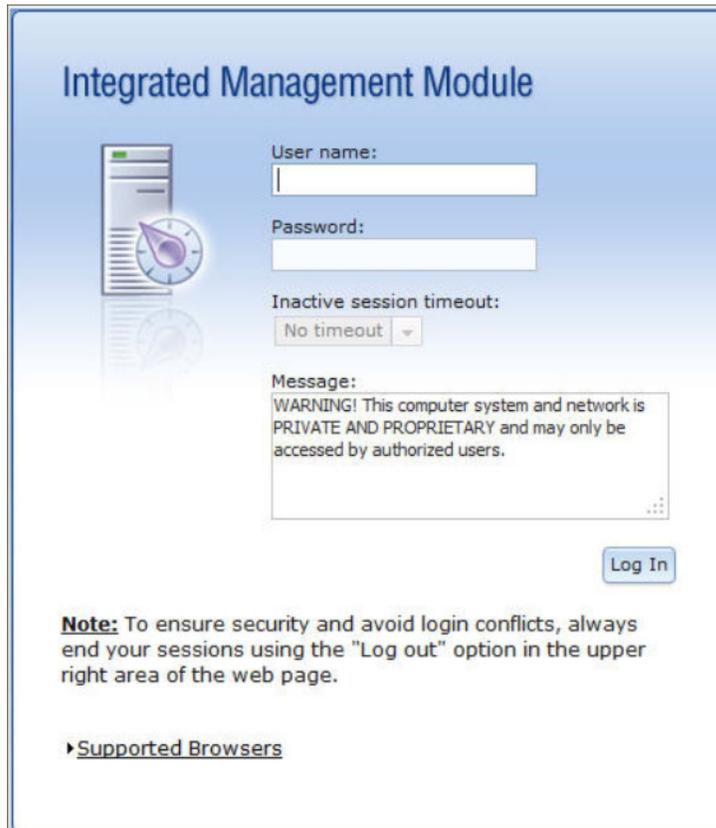
- IMM2 ファームウェアは、最大 6 つの同時 Web セッションをサポートします。他のユーザーにセッションを解放するために、非アクティブ・タイムアウトでセッションが自動的にクローズされるのを待たず、作業が終了した時点で Web セッションからログアウトしてください。自動的に最新表示される IMM2 Web ページ上でブラウザーを放置した場合、Web セッションは非アクティブでも自動的にクローズされません。

## 侵入警告メッセージ

ユーザーが IMM2 サーバーにログインしたときに表示するメッセージをセットアップするには、Web セッション・ページの右上のエリアにある「Settings」メニュー項目の「Trespass Message」オプションを使用します。「Trespass Message」オプションを選択すると、次の画面が表示されます。提供されるフィールドに、ユーザーに対して表示するメッセージ・テキストを入力し、「OK」を押します。



このメッセージは、次の図に示すように、ユーザーがログインしたときに IMM2 ログイン・ページの「Message」エリアに表示されます。



**Integrated Management Module**

User name:

Password:

Inactive session timeout:

Message:  
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.

[Log In](#)

**Note:** To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

[Supported Browsers](#)

## ログアウト

セキュリティを保障するには、作業が終了したら IMM2 Web セッションからログアウトし、開いた可能性がある他の IMM2 Web ブラウザー・ウィンドウがあれば、それらを手動でクローズします。

Web セッションからログアウトするには、Web ページの右上のエリアで「**Log out**」をクリックします。ログイン・ウィンドウが表示されます。

**Integrated Management Module**

User name:

Password:

Inactive session timeout:

Message:  
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.

[Log In](#)

**Note:** To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

[Supported Browsers](#)

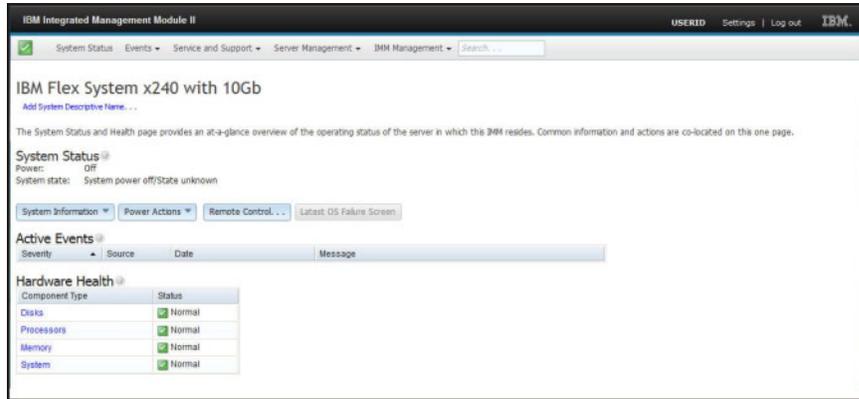
注: IMM2 ファームウェアは、最大 6 つの同時 Web セッションをサポートします。他のユーザーにセッションを解放するために、非アクティブ・タイムアウトでセッションが自動的にクローズされるのを待たず、作業が終了した時点で Web セッションからログアウトしてください。自動的に最新表示される IMM2 Web ページ上でブラウザを放置した場合、Web セッションは非アクティブでも自動的にクローズされません。

---

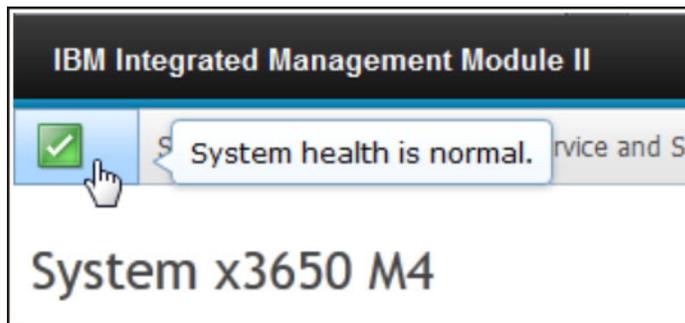
## 「System Status」タブ

このセクションでは、IMM2 Web ユーザー・インターフェースの「System Status」タブの下にあるオプションの使用について説明します。

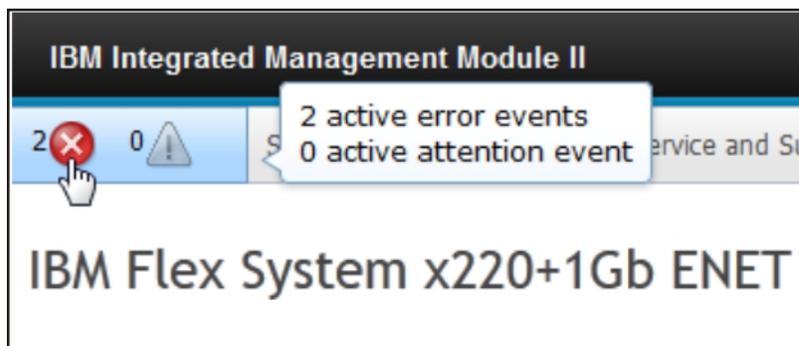
「System Status」ページは、IMM2 Web ユーザー・インターフェースにログインした後、または「System Status」タブをクリックしたときに表示されます。「System Status」ページから、システム状況、アクティブ・システム・イベント、およびハードウェア・ヘルス情報を表示することができます。次の画面は、「System Status」タブをクリックするか、IMM2 Web インターフェースにログインしたときに表示されます。



ページの左上隅にある緑色のアイコン (チェック・マークが付いているもの) をクリックすると、サーバー・ヘルスの要約をすぐに取得できます。チェック・マークは、サーバーが正常に動作していることを示しています。



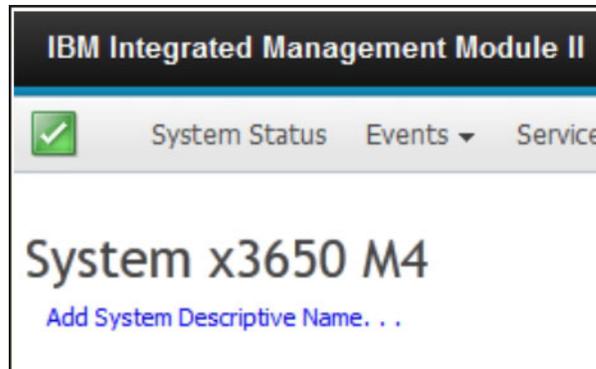
赤い円または黄色の三角形のアイコンが表示された場合、それはエラー状態または警告状態が生じていることを示しています (次の図を参照)。



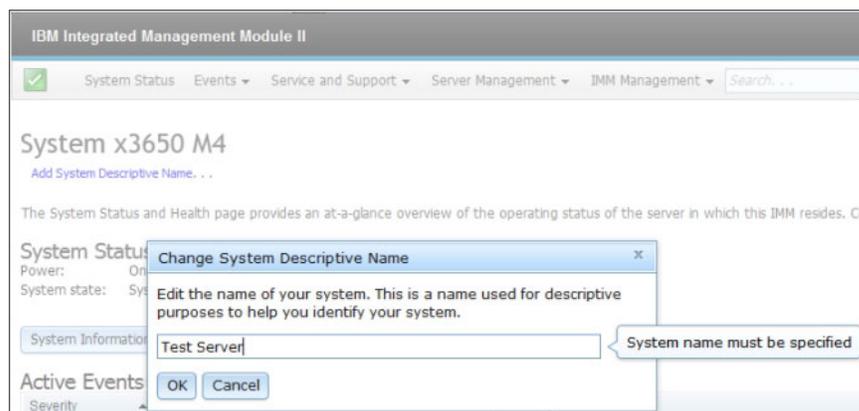
赤い円のアイコンは、サーバーにエラー状態が存在することを示しています。黄色の三角形のアイコンは、警告状態が存在することを示しています。赤い円または黄色の三角形のアイコンが表示された場合は、次の図に示すように、その状態に関連したイベントが「System Status」ページの「Active Events」セクションの下にリストされます。

| Severity | Source | Date                        | Message  |
|----------|--------|-----------------------------|--|
| Error    | System | 16 Jul 2012 01:00:28.000 PM | Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state. |
| Error    | System | 16 Jul 2012 01:00:29.000 PM | Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state. |

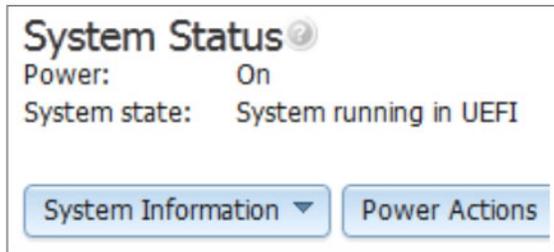
IMM2 サーバーに記述名を追加して、個々の IMM2 サーバーの識別に役立てることができます。IMM2 サーバーに記述名を割り当てるには、サーバー製品名の下にある「**Add System Descriptive Name...**」リンクをクリックします。



「**Add System Descriptive Name...**」リンクをクリックすると、その IMM2 サーバーに関連付ける名前を指定する次のようなウィンドウが表示されます。システム記述名は、いつでも変更できます。



「System Status」ページの「**System Status**」セクションには、サーバーの電源状態と作動状態が表示されます。表示される状況は、「System Status」ページが開かれた時点でのサーバー状態です (次の図を参照)。



サーバーは、以下のいずれかの状態になります。

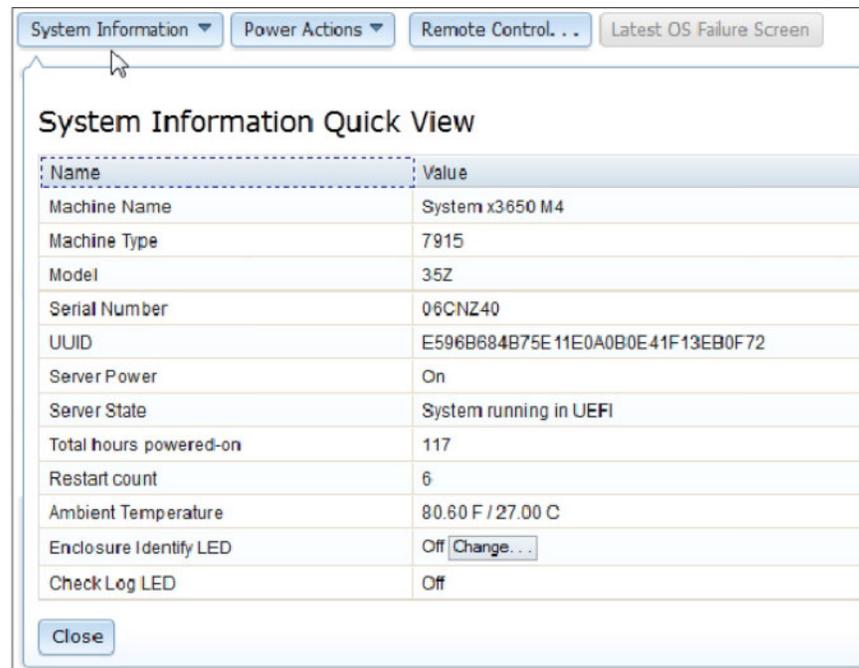
表 2. サーバーの電源状態と作動状態

| サーバー状態                          | 説明  |
|---------------------------------|---|
| System power off/state unknown  | サーバーはオフの状態です。   |
| System on/starting UEFI         | サーバーの電源はオンですが、UEFI は稼働していません。   |
| System running in UEFI          | サーバーの電源はオンで、UEFI が稼働しています。  |
| System stopped in UEFI          | サーバーの電源はオンで、UEFI は問題を検出して実行を停止しています。  |
| Booting OS or in unsupported OS | サーバーは、以下のいずれかの理由でこの状態になる場合があります。 <ul style="list-style-type: none"> <li>オペレーティング・システム・ローダーは始動したが、オペレーティング・システムがまだ稼働していない。</li> <li>IMM2 Ethernet over USB インターフェースが使用不可になっている。</li> <li>オペレーティング・システムに Ethernet over USB インターフェースをサポートするドライバーがロードされていない。</li> </ul> |
| OS booted                       | サーバー・オペレーティング・システムは稼働しています。   |
| Suspend to RAM                  | サーバーは、スタンバイ状態またはスリープ状態に置かれています。   |

「System Status」ページには、「System Information」、「Power Actions」、「Remote Control」、および「Latest OS Failure Screen」の各タブも用意されています。



サーバーに関する情報を表示するには、「System Information」タブをクリックします。



| Name                   | Value                             |
|------------------------|-----------------------------------|
| Machine Name           | System x3650 M4                   |
| Machine Type           | 7915                              |
| Model                  | 35Z                               |
| Serial Number          | 06CNZ40                           |
| UUID                   | E596B684B75E 11E0A0B0E41F13EB0F72 |
| Server Power           | On                                |
| Server State           | System running in UEFI            |
| Total hours powered-on | 117                               |
| Restart count          | 6                                 |
| Ambient Temperature    | 80.60 F / 27.00 C                 |
| Enclosure Identify LED | Off <a href="#">Change...</a>     |
| Check Log LED          | Off                               |

Close

電源オン、電源オフ、および再始動の各アクションによるサーバーの完全なリモート電源制御のために実行できるアクションを表示するには、「Power Actions」タブをクリックします。サーバー電源をリモート側で制御する方法については、104 ページの『サーバーの電源状況の制御』を参照してください。

サーバーをオペレーティング・システム・レベルで制御する方法について情報を得るには、「Remote Control」タブをクリックします。Remote Control 機能については、105 ページの『リモート・プレゼンス機能および Remote Control 機能』を参照してください。

最新の OS 障害画面データをキャプチャーする方法について情報を得るには、「Latest OS Failure Screen」タブをクリックします。最新の OS 障害画面については、134 ページの『最新の OS 障害画面データのキャプチャー』を参照してください。

「System Status」ページの「Hardware Health」セクションの下には、モニター対象となっているハードウェア・コンポーネントとそのヘルス状況のリストがテーブル形式で表示されます。表示されるコンポーネントのヘルスは、テーブルの「Component Type」列のコンポーネントの最もクリティカルな状態を反映している場合があります。例えば、あるサーバーにいくつかの電源モジュールが取り付けら

れており、1 つを除いてすべての電源モジュールが正常に動作している場合があります。その場合、テーブル内の「Power Modules」コンポーネントの状況は、1 つの電源モジュールのために、クリティカルな状況になります (次の画面を参照)。

### Hardware Health

| Component Type                  | Status   |
|---------------------------------|--|
| <a href="#">Cooling Devices</a> |  Normal   |
| <a href="#">Power Modules</a>   |  Critical |
| <a href="#">Disks</a>           |  Normal   |
| <a href="#">Processors</a>      |  Normal   |
| <a href="#">Memory</a>          |  Normal   |
| <a href="#">System</a>          |  Normal   |

各コンポーネント・タイプはリンクになっており、これをクリックすると、さらに詳細な情報を取得できます。コンポーネント・タイプをクリックすると、個々のコンポーネントの状況をリストしたテーブルが表示されます (次の画面を参照)。

### Memory

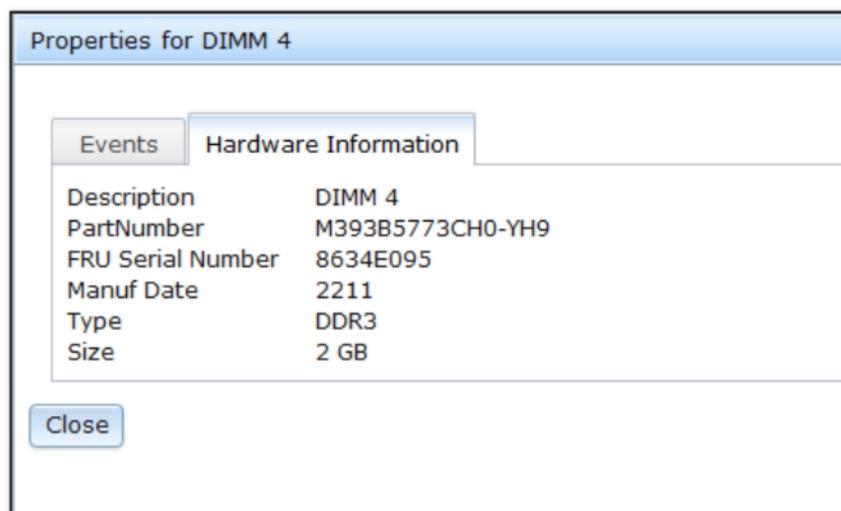
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Eve

| FRU Name                | Status   | Type | Capacity (GB) |
|-------------------------|--|------|---------------|
| <a href="#">DIMM 4</a>  |  Normal | DDR3 | 4             |
| <a href="#">DIMM 9</a>  |  Normal | DDR3 | 4             |
| <a href="#">DIMM 16</a> |  Normal | DDR3 | 4             |
| <a href="#">DIMM 21</a> |  Normal | DDR3 | 4             |

テーブルの「FRU Name」列のコンポーネントをクリックすると、そのコンポーネントの追加情報を取得できます。そのコンポーネントについて、アクティブなすべてのイベントが表示されます。



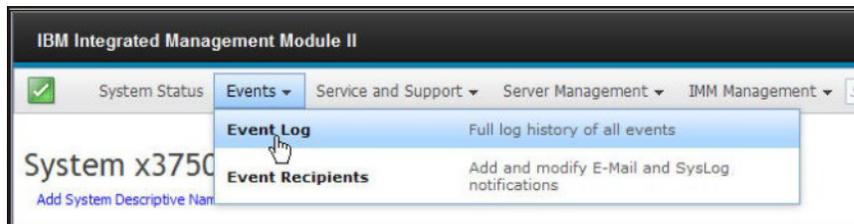
そのコンポーネントの詳細情報を得るには、「**Hardware Information**」タブをクリックします。



## 「Events」タブ

このセクションでは、IMM2 Web ユーザー・インターフェースの「Events」タブの下にあるオプションの使用について説明します。

「Events」タブの下にあるオプションを使用すると、「Event Log」ヒストリーを管理し、Eメール通知および syslog 通知のイベント受信者を管理することができます。次の図は、IMM2 Web ページの「Events」タブの下にあるオプションを示しています。



## イベント・ログ

「Events」タブの下にある「Event Log」を選択すると、「Event Log」ページが表示されます。「Event Log」ページには、IMM2 によって報告されたイベントの重大度とすべてのリモート・アクセス試行および構成変更に関する情報が表示されます。ログ内のすべてのイベントには、IMM2 の日時の設定を使用したタイム・スタンプが付いています。一部のイベントは、アラートも生成します（「Event Recipients」ページでそのように構成された場合）。イベント・ログ内のイベントは、ソートしたりフィルターに掛けたりすることができます。次に、イベント・ログ・ページの図を示します。

| Severity      | Source | Date                      | Event ID           | Message  |
|---------------|--------|---------------------------|--------------------|--|
| Informational | System | 31 1 2013 09:02:42.771 AM | 0x4000000e00000000 | Remote Login Successful. Login ID: USERID from webgpus at IP address 9.111.29.57.  |
| Informational | System | 31 1 2013 09:01:00.297 AM | 0x4000001600000000 | ENET(CR) ep1 DHCP-HSTN-IMM2-5cae8b4e83c5, DN:ox.ibm.com, IP@=9.186.166.78, SW=255.255.255.128, GW@=9.186.166.1, DNS1@=9.0.148.50 |
| Informational | System | 31 1 2013 09:00:58.957 AM | 0x4000001900000000 | LAN: Ethernet(BM ep2) interface is now active.   |
| Informational | System | 31 1 2013 09:00:55.004 AM | 0x4000001700000000 | ENET(CR) ep2 IP-Cy-Hs#name=IMM2-5cae8b4e83c5, IP@=187.254.95.118, NetMtu=255.255.0.0, GW@=9.0.0.0                                |
| Informational | System | 31 1 2013 09:00:53.403 AM | 0x4000003700000000 | ENET(CR) ep1 IPv6-Link-Local-Hs#name=IMM2-5cae8b4e83c5, IP@fe80::5cae8b4e83c5::Pref64  |
| Informational | System | 31 1 2013 09:00:51.592 AM | 0x4000001900000000 | LAN: Ethernet(BM ep1) interface is now active.   |
| Informational | System | 31 1 2013 09:00:47.068 AM | 0x4000001000000000 | Management Controller SHR 05K7N4.9 Network Installation Complete.  |
| Informational | System | 31 1 2013 09:00:02.874 AM | 0x800901282101fff  | Device Low Security Jump has been added.   |
| Informational | Power  | 31 1 2013 09:00:02.304 AM | 0x80900091301fff   | Host Power has been turned off.  |
| Informational | System | 31 1 2013 08:55:11.252 AM | 0x4000001500000000 | Management Controller SHR 05K7N4.9 reset was initiated by user USERID.   |
| Informational | System | 31 1 2013 08:47:59.116 AM | 0x4000002300000000 | Flash of SHR 05K7N4.9 from (##) 9.186.166.119) succeeded for user USERID.  |
| Informational | System | 31 1 2013 08:43:15.666 AM | 0x4000000e00000000 | Remote Login Successful. Login ID: USERID from webgpus at IP address 9.186.166.119.  |
| Informational | System | 31 1 2013 08:43:15.666 AM | 0x4000000e00000000 | Remote Login Successful. Login ID: USERID from webgpus at IP address 9.111.29.57.  |

イベント・ログ内のイベントのソートおよびフィルター操作を行うには、列見出しを選択します (次の図を参照)。

| Severity      | Source | Date                        | Event ID           | Message   |
|---------------|--------|-----------------------------|--------------------|---|
| Informational | System | 31 Jan 2013 09:11:04.024 AM | 0x4000000e00000000 | Remote Login Successful. Login ID: USERID from webgpus at IP address 9.186.166.119. |
| Informational | System | 31 Jan 2013 09:02:42.771 AM | 0x4000000e00000000 | Remote Login Successful. Login ID: USERID from webgpus at IP address 9.111.29.57.   |

「Export」ボタンを使用して、イベント・ログ内のすべてのイベントまたは選択したイベントをファイルに保存できます。特定のイベントを選択するには、「Event Log」のメインページでイベントを 1 つ以上選択し、「Export」ボタンを左クリックします (次の図を参照)。

## Event Log

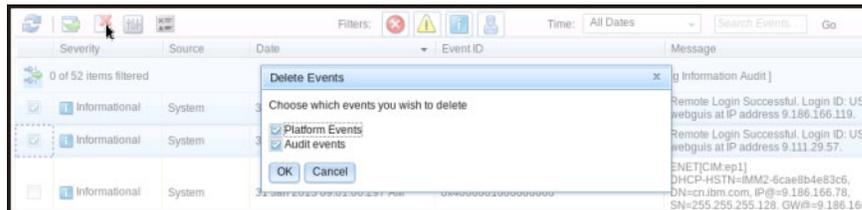
This page displays the contents of the IMM event log, and allows you to export the log entries (sorted by severity, then by time of entry first). For each log entry, the severity of the event is displayed



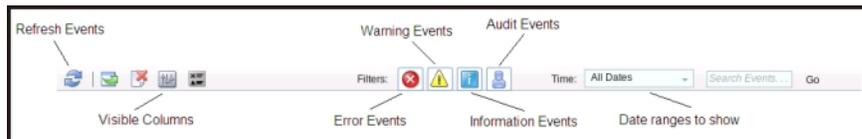
Export Event Logs

|  | Severity  | Source   | Date             |
|--|---|--|------------------|
|  0 of 52 items filtered |   |  2 items selected |                  |
| <input checked="" type="checkbox"/>  |  Informational | System   | 31 Jan 2013 09:1 |
| <input checked="" type="checkbox"/>  |  Informational | System   | 31 Jan 2013 09:0 |

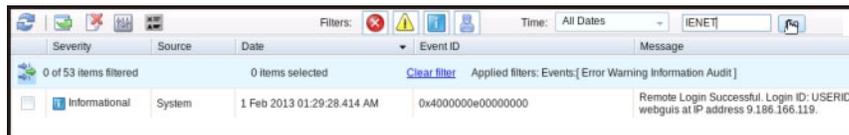
削除するイベントのタイプを選択するには、「Delete Events」ボタンを使用します (次の図を参照)。



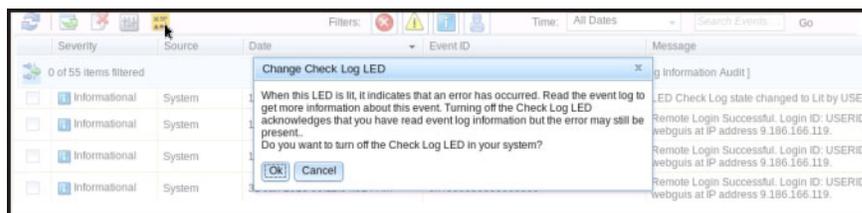
表示するイベント・ログ項目のタイプを選択するには、適切なボタンをクリックします (次の図を参照)。



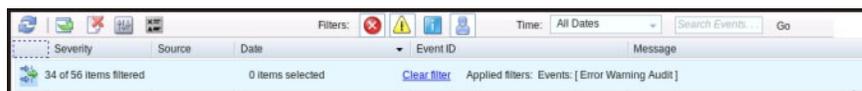
特定のタイプのイベントまたはキーワードを検索するには、「Search Events」ボックスにイベントまたはキーワードのタイプを入力してから、「Go」をクリックします (次の図を参照)。



ログ確認 LED がオンになっていて、関連したイベント・ログが選択されているときに、ログ確認 LED をオフにするには、「Check Log LED Status」ボタンをクリックします (次の図を参照)。

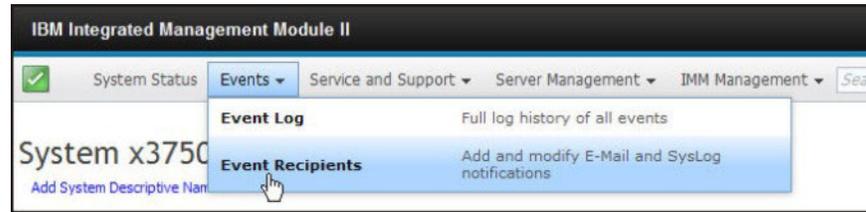


イベント・ログ・ツールバーの「Filter Events」ボタンのいずれかをクリックして、表示するイベントを選択できます。フィルターを消去してすべてのタイプのイベントを表示するには、次の図に示す「Clear Filter」リンクをクリックします。



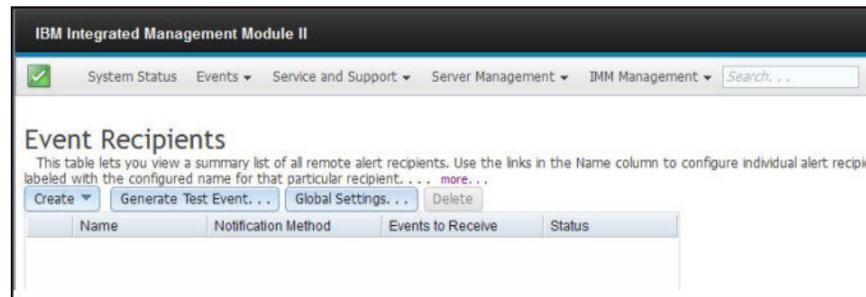
## イベント受信者

「Events」タブの下にある「**Events Recipients**」オプションを使用して、Eメールとsyslogの通知を追加および変更します。

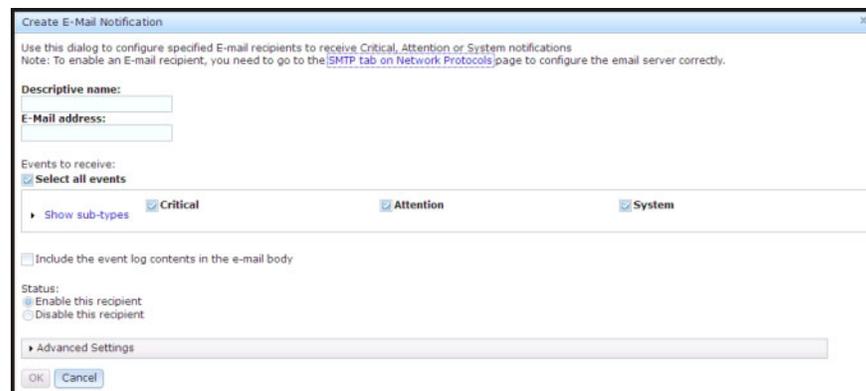


「Event Recipients」オプションを使用すると、システム・イベントの通知先を管理することができます。各受信者を構成したり、すべてのイベント受信者に適用される設定を管理したりすることができます。また、テスト・イベントを生成して、通知機能を確認することもできます。

Eメールとsyslogの通知を作成するには、「**Create**」ボタンをクリックします。

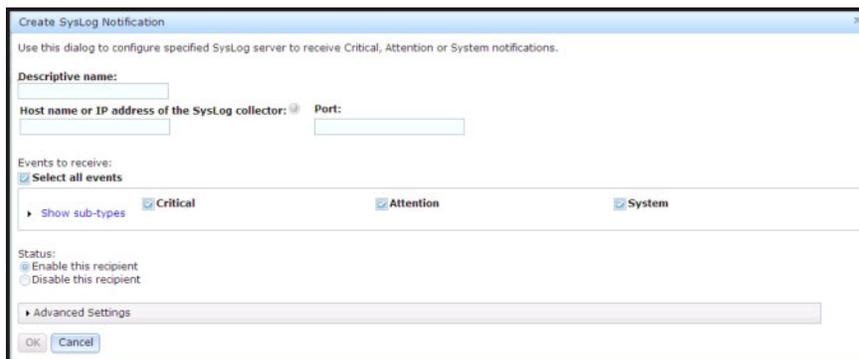


ターゲットのEメール・アドレスをセットアップし、通知するイベントのタイプを選択するには、「**Create E-mail Notification**」オプションを選択します。また、「**Advanced Settings**」をクリックすると、開始索引番号を選択できます。Eメールにイベント・ログを含めるには、「**Include the event log contents in the e-mail body**」チェック・ボックスを選択します。「Create E-mail Notification」ウィンドウの図を次に示します。



SysLogコレクターのホスト名とIPアドレスをセットアップし、通知するイベントのタイプを選択するには、「**Create SysLog Notification**」オプションを選択します。また、「**Advanced Settings**」をクリックすると、開始索引番号を選択できま

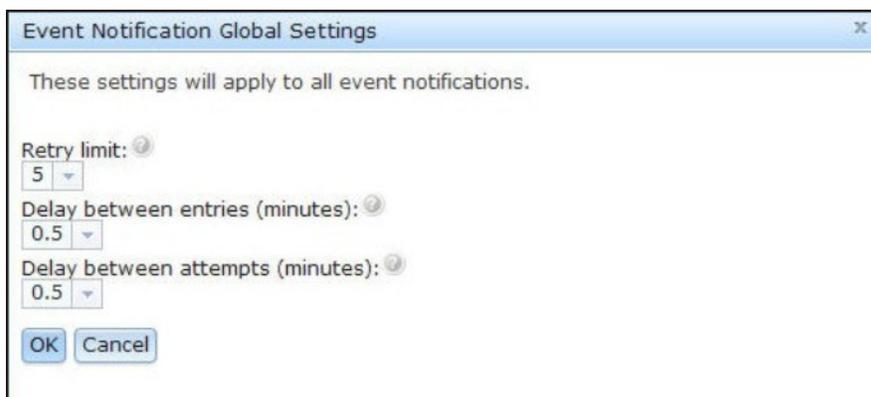
す。このタイプの通知に使用するポートを指定することもできます。「Create SysLog Notification」ウィンドウの図を次に示します。



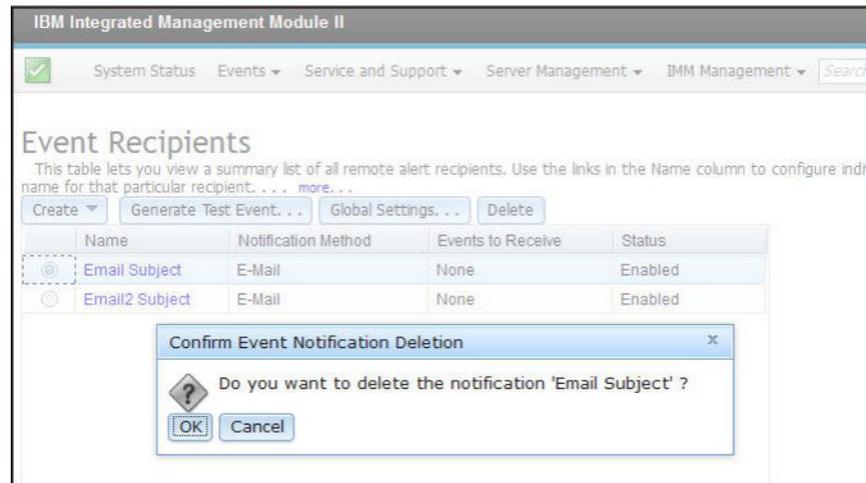
選択した E メール宛先にテスト E メールを送信するには、「**Generate Test Event**」ボタンを選択します (次の図を参照)。



イベント通知を再試行する限度、イベント通知項目間の遅延 (分単位)、および試行間の遅延 (分単位) を設定するには、「**Global Settings**」ボタンを選択します (次の図を参照)。



E メールまたは syslog の通知の宛先を削除するには、「**Delete**」ボタンを選択します。次のウィンドウが開きます。

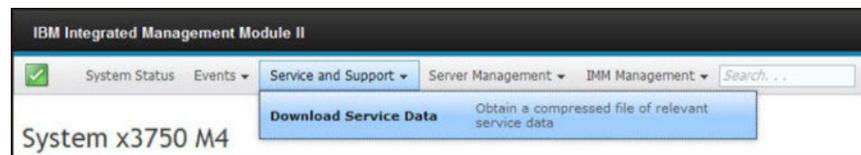


## 「Service and Support」タブ

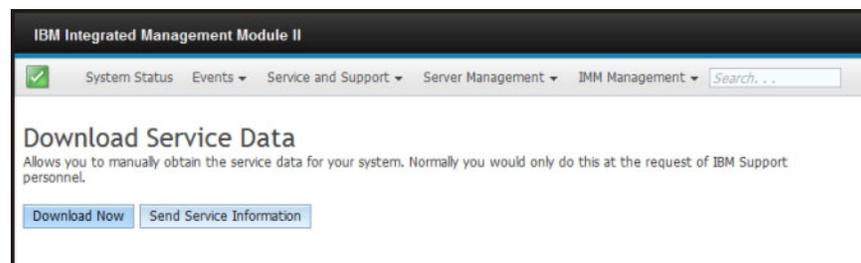
このセクションでは、IMM2 Web ユーザー・インターフェース・ページの「Service and Support」タブの下にあるオプションの使用について説明します。

### サービス・データのダウンロード

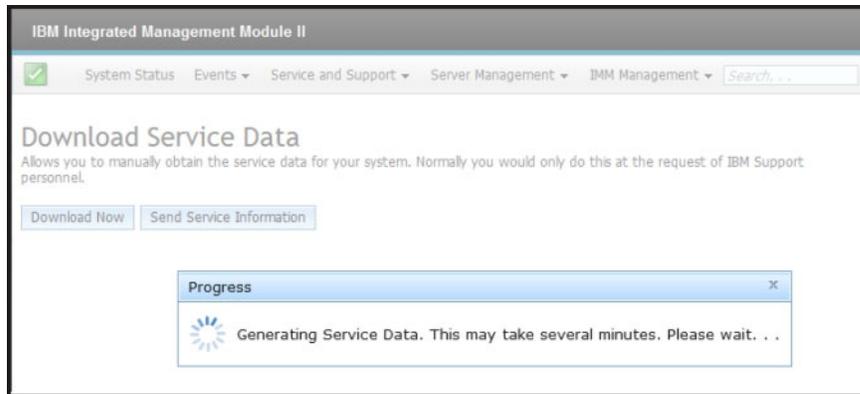
「Service and Support」タブの下にある「**Download Service Data**」オプションを使用すると、サーバーに関する情報を収集して圧縮ファイルを作成し、問題判別を支援するために IBM サポートに送信することができます。



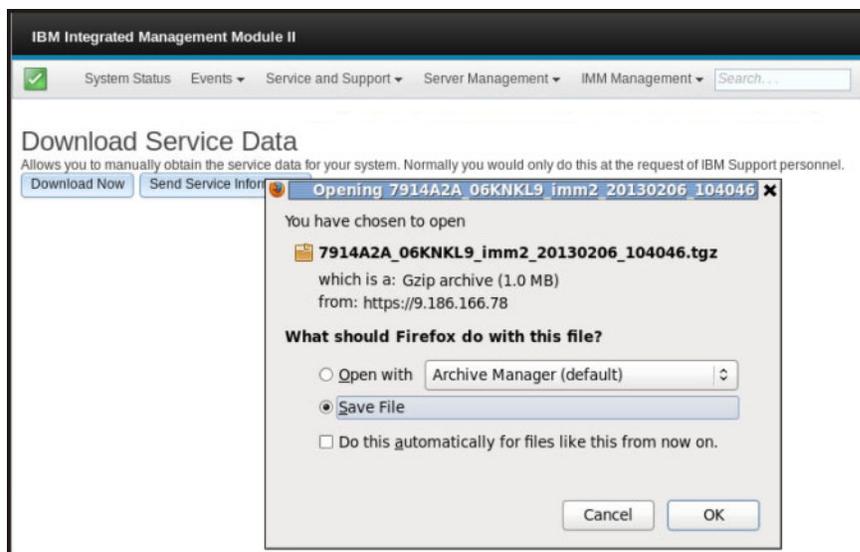
「**Download Now**」ボタンをクリックして、サービスおよびサポートのデータをダウンロードします（次の図を参照）。



データを収集するプロセスが開始されます。このプロセスでは、後でファイルに保存できるサービス・データを生成するために数分かかります。進行状況を示すウィンドウが表示され、データが生成されていることを示します。



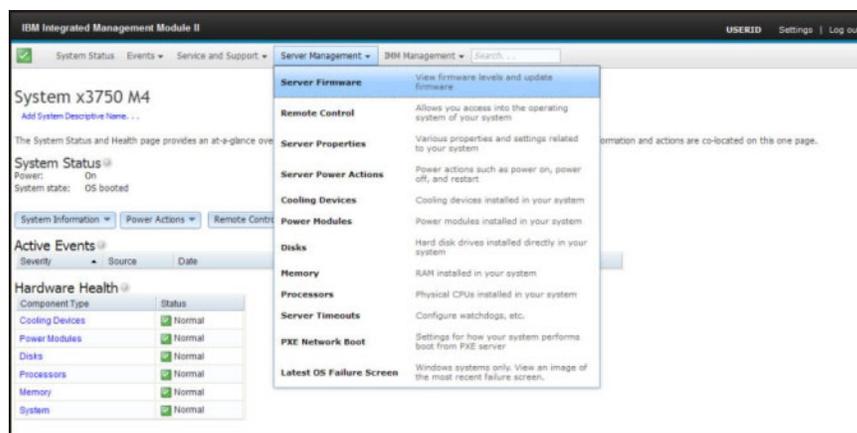
プロセスが完了すると以下のウィンドウが表示され、生成されたファイルの保存場所を入力するプロンプトが出ます。



## 「Server Management」タブ

このセクションでは、IMM2 Web ユーザー・インターフェース・ホーム・ページの「Server Management」タブの下にあるオプションについて説明します。

「Server Management」タブの下にあるオプションを使用すると、サーバー・ファームウェアの状況と制御、Remote Control アクセス、サーバー・プロパティの状況と制御、サーバー電源アクション、冷却装置、電源モジュール、ディスク、メモリー、プロセッサ、サーバー・タイムアウト、PXE ネットワーク・ブート、および最新の OS 障害画面に関する情報を表示することができます (次の図を参照)。



## サーバー・ファームウェア

サーバーにインストールされているファームウェアのレベルを表示したり、ファームウェア更新を適用したりするには、「Server Management」タブの下にある「**Server Firmware**」オプションを選択します。次の図のように、サーバー・ファームウェアのレベルが表示され、DSA、IMM2、および UEFI のファームウェアを更新できます。

| Firmware Type  | Status   | Version | Build     | Release Date |
|----------------|----------|---------|-----------|--------------|
| DSA            | Active   | 9.24    | DSY744B   | 2012-08-10   |
| IMM2           |          |         |           |              |
| IMM2 (Primary) | Active   | 2.15    | 140039G   | 2013-01-28   |
| IMM2 (Backup)  | Inactive | 3.00    | 140039T   | 2013-01-30   |
| UEFI           |          |         |           |              |
| UEFI (Primary) | Active   | 1.20    | 07E120CUB | 2012-08-23   |
| UEFI (Backup)  | Inactive | 1.20    | 07E120CUB | 2012-08-23   |

IMM2、UEFI、および DSA 用ファームウェアの現在の状況とバージョンが表示されます (基本バージョンとバックアップ・バージョンを含めて)。ファームウェア状況には、次の 3 つのカテゴリーがあります。

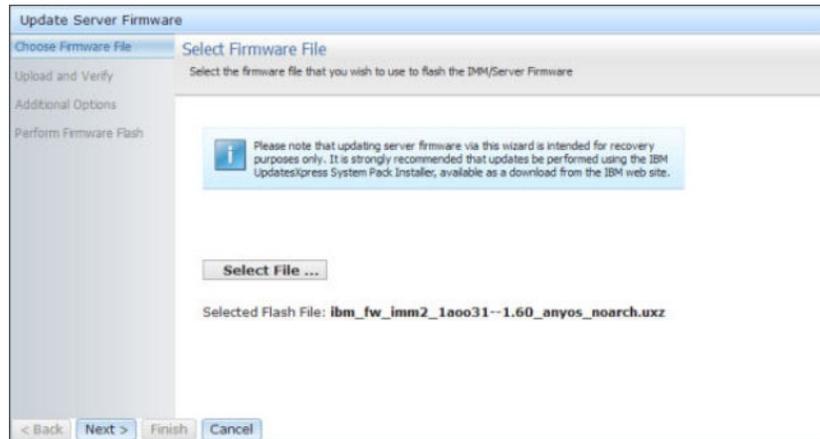
- **アクティブ:** ファームウェアはアクティブです。
- **非アクティブ:** ファームウェアはアクティブではありません。
- **保留:** ファームウェアはアクティブ化を待機しています。

**注意:** 誤ったファームウェア更新をインストールすると、サーバーが誤動作する可能性があります。ファームウェアまたはデバイス・ドライバーの更新をインストールする前に、ダウンロードした更新に付属の **README** または変更履歴・ファイルを読んでください。これらのファイルには、更新に関する重要な情報、および更新をインストールするための手順 (ファームウェアまたはデバイス・ドライバーの旧バージョンから最新バージョンに更新するための特別な手順など) が記載されています。

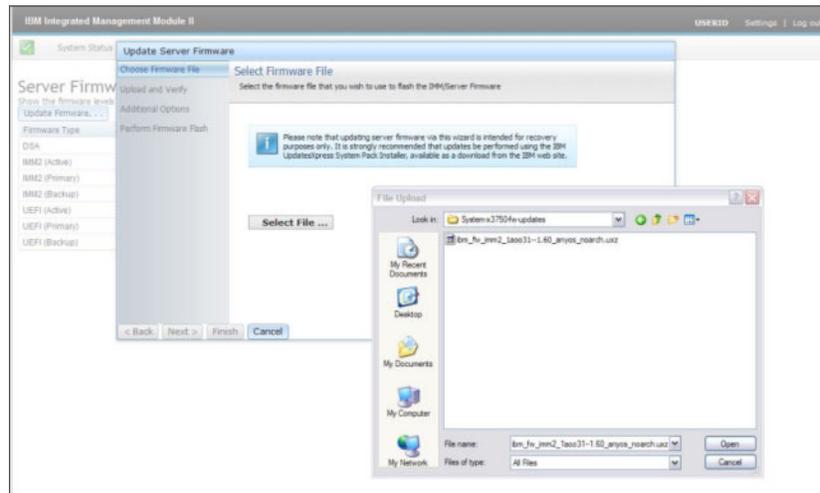
ファームウェアを更新するには、「**Update Firmware...**」ボタンを選択します。「Update Server Firmware」ウィンドウが表示されます。「**Cancel**」をクリックして

前の「Server Firmware」ウィンドウに戻るか、「**Select File...**」ボタンをクリックして、サーバー・ファームウェアをフラッシュするために使用するファームウェア・ファイルを選択することができます。

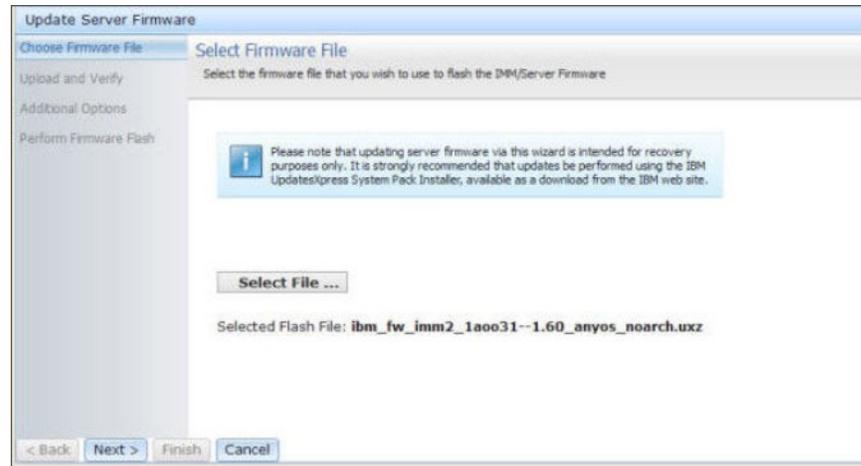
**注:** 「**Select File...**」ボタンをクリックする前に、ウィンドウ・プロンプトに表示される警告を読んでから作業を続けてください。



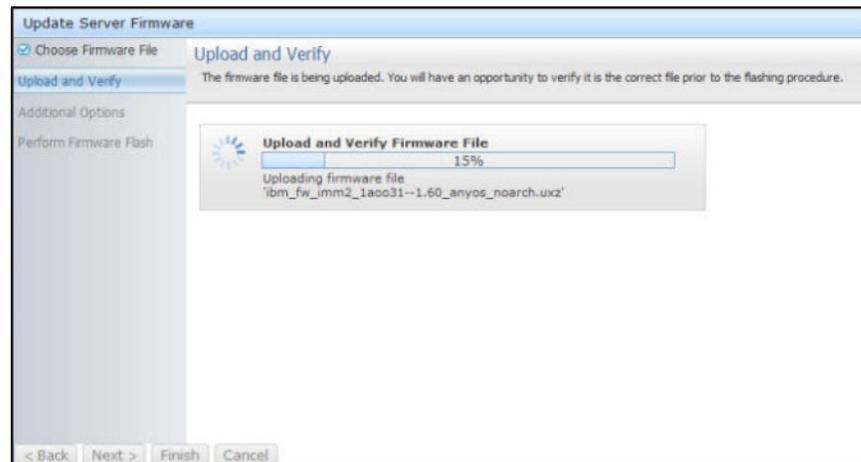
「**Select File...**」ボタンをクリックすると「File Upload」ウィンドウが表示され、目的のファイルを参照できます。



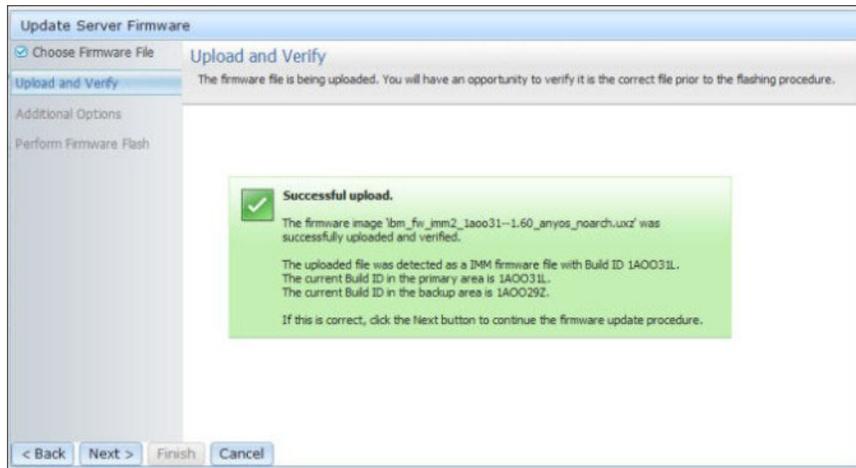
選択するファイルまでナビゲートした後、「**Open**」ボタンをクリックすると「Update Server Firmware」ウィンドウに戻り、選択したファイルが表示されます(次の図を参照)。



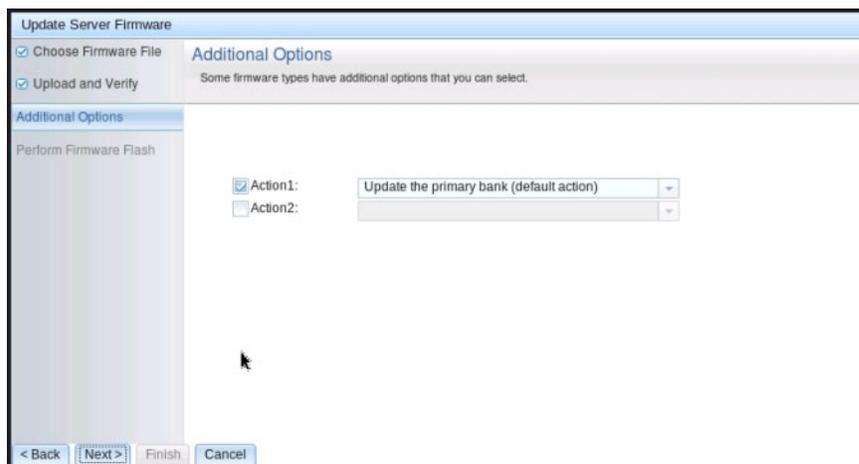
「Next >」 ボタンをクリックして、選択したファイルに対するアップロードと検証のプロセスを開始します (次の図を参照)。ファイルがアップロードされて検証されている間、進行状況メーターが表示されます。



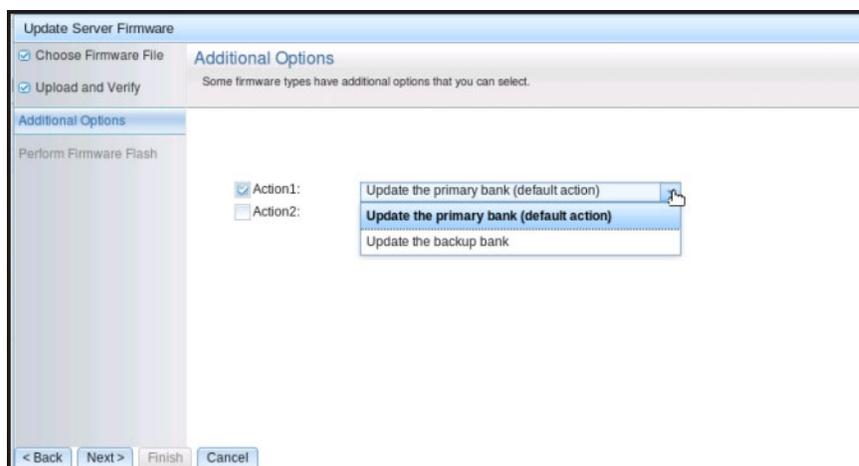
状況ウィンドウ (次の図を参照) が表示されるので、更新用に選択したファイルが正しいファイルであるかどうかを確認できます。このウィンドウには、DSA、IMM2、または UEFI など、更新されるファームウェア・ファイルのタイプに関する情報が示されます。情報が正しければ、「Next >」 ボタンをクリックします。いずれかの選択をやり直す場合は、「< Back」 ボタンをクリックします。



「Next >」 ボタンをクリックすると、一連の追加オプションが表示されます (次の図を参照)。



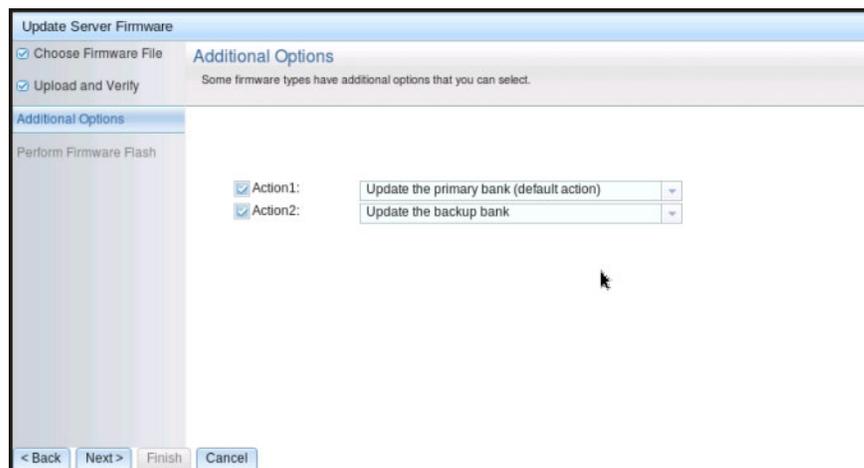
「Action 1」の横のドロップダウン・メニュー (次の図を参照) では、「Update the primary bank (default action)」か「Update the backup bank」を選択できます。



アクションを選択すると、前のウィンドウに戻り、「Action 2」チェック・ボックスをクリックすれば追加のアクションを実行できます。

アクションがロードされると、選択したアクションと新規の「Action 2」ドロップダウン・メニューが表示されます (次の図を参照)。

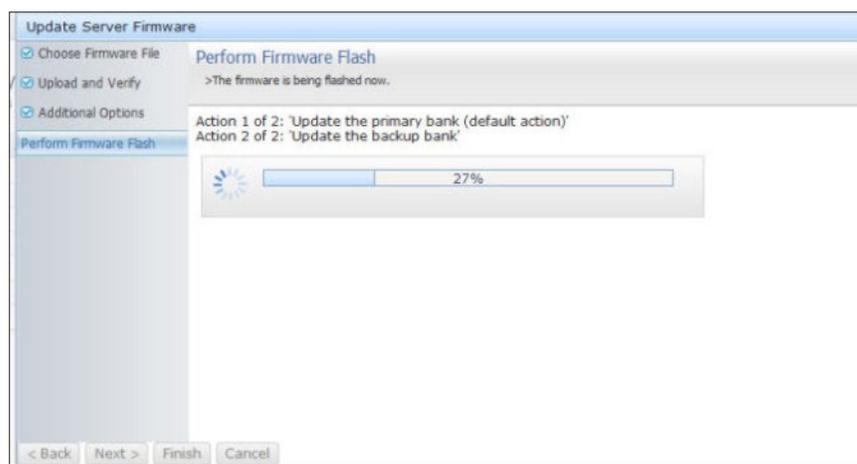
注: アクションを使用不可にするには、関連したアクションの横にあるチェック・ボックスをクリックします。



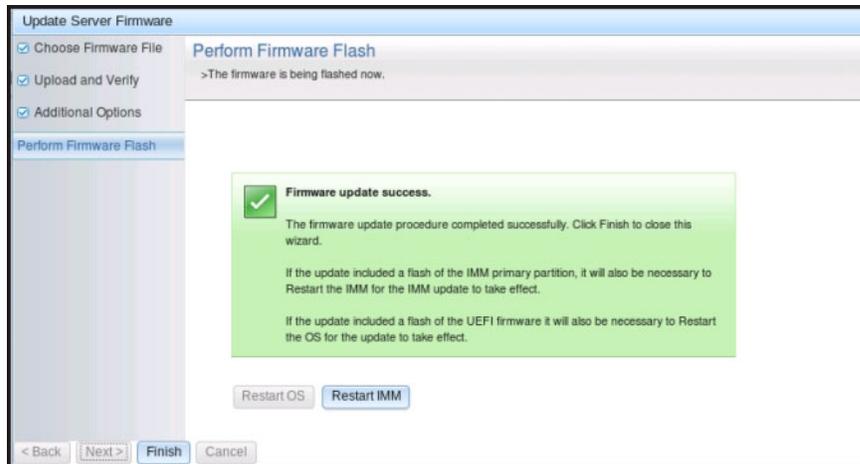
前の画面は、「Action 1」に対して、更新対象として 1 次バンクが選択されていることを示しています。「Action 2」の下で、バックアップ・バンクの更新も選択できます (前のウィンドウを参照)。「Next >」をクリックすると、1 次バンクとバックアップ・バンクが同時に更新されます。

注: 「Action 1」は「Action 2」と異なっている必要があります。

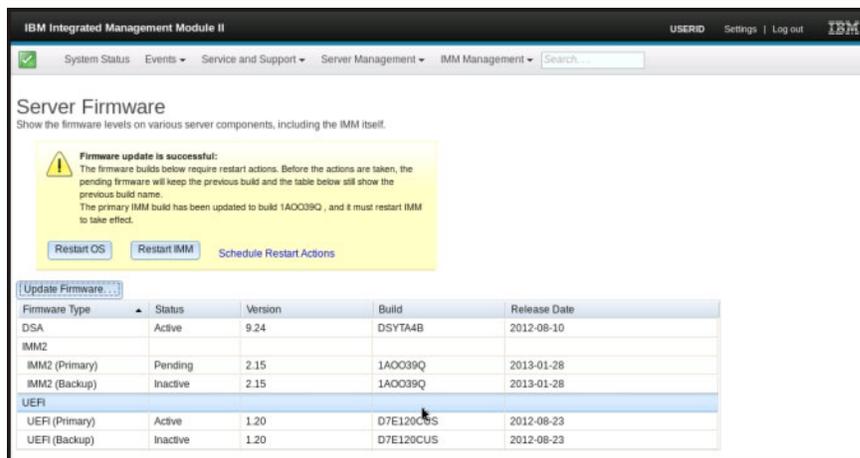
ファームウェア更新の進行状況を示す進行状況メーターが表示されます (次の図を参照)。



ファームウェア更新が正常に完了すると、次のようなウィンドウが開きます。表示される内容に応じて関連した操作を選択して、更新処理を完了します。



1 次ファームウェアの更新が完了しなかった場合は、次のウィンドウが開きます。



## Remote Control

このセクションでは、Remote Control 機能について説明します。

ActiveX クライアントおよび Java クライアントは、サーバーのビデオ表示をリモート側で表示でき、クライアントのキーボードとマウスを使用してそれと対話できるグラフィカル・リモート・コンソールです。

注:

- ActiveX クライアントは、Internet Explorer ブラウザーでのみ使用可能です。
- Java クライアントを使用するには、Java プラグイン 1.5 以降のリリースが必要です。
- Java クライアントは IBM Java 6 SR9 FP2 以降のリリースと互換性があります。

Remote Control 機能は、次に示す 2 つの別個のウィンドウからなっています。

- **Video Viewer**

「Video Viewer」ウィンドウは、リモート・システム管理にリモート・コンソールを使用します。リモート・コンソールはサーバーの対話式グラフィカル・ユー

ザー・インターフェース (GUI) 画面であり、お客様のコンピューター上に表示されます。お客様のモニターにはサーバー・コンソールに表示されるとおりのものが表示され、お客様はコンソールをキーボードとマウスで制御できます。

#### • Virtual Media Session

「Virtual Media Session」ウィンドウには、リモート・ドライブとしてマップ可能なクライアント上のすべてのドライブがリストされ、ISO イメージ・ファイルとディスク・イメージ・ファイルを仮想ドライブとしてマップすることができます。マップされた各ドライブは、読み取り専用としてマークすることができます。CD、DVD ドライブ、および ISO イメージは、常に読み取り専用です。

「Virtual Media Session」ウィンドウは、「Video Viewer」ウィンドウの「Tools」メニュー・バーからアクセスできます。

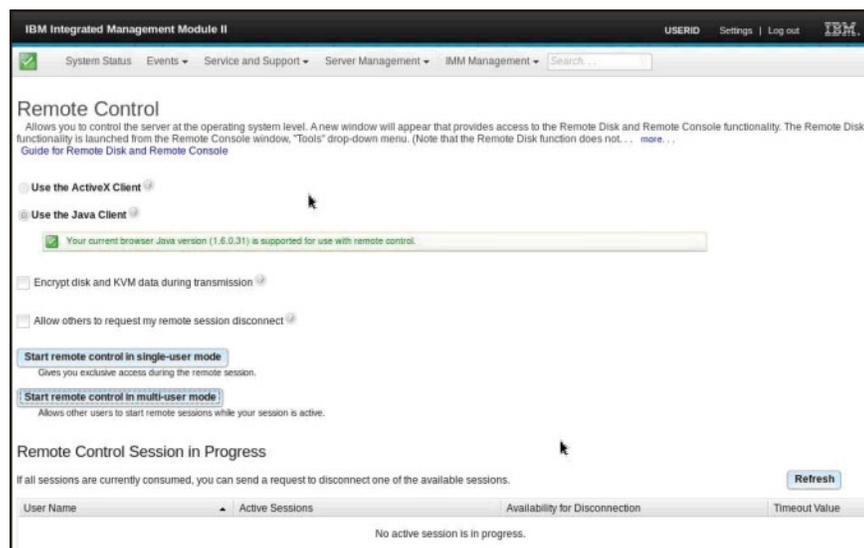
#### 注:

- 「Virtual Media Session」は、一度に 1 つの Remote Control セッション・クライアントが使用できます。
- ActiveX クライアントを使用した場合は親ウィンドウが開きます。このウィンドウは、リモート・セッションを完了するまで開いたままにしておく必要があります。

サーバー・コンソールにリモートでアクセスするには、以下のステップを実行します。

1. IMM2 にログインします (詳しくは、10 ページの『IMM2 へのログイン』を参照)。
2. 以下のいずれかのメニュー選択項目を選択して、「Remote Control」ページにアクセスします。
  - 「Server Management」タブから「Remote Control」をクリックします。
  - 「System Status」ページで「Remote Control...」をクリックします。

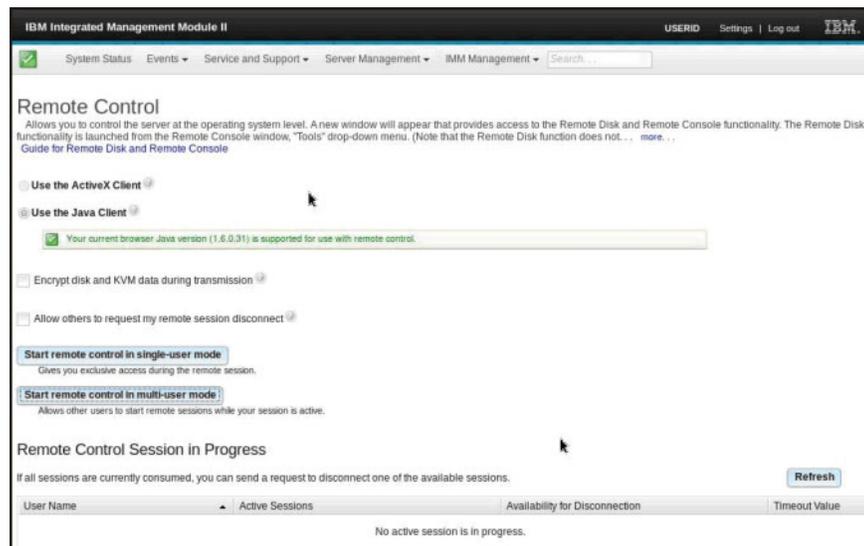
次の図に示すように、「Remote Control」ページが開きます。



3. 「Guide for Remote Disk and Remote Console」リンクをクリックして、追加情報にアクセスできます。次の図は、「Guide for Remote Disk and Remote Console」ウィンドウを示しています。



- a. 「Guide for Remote Disk and Remote Console」ウィンドウから出るには、「Close」をクリックします。
4. 次のいずれかのグラフィカル・リモート・コンソール選択項目を選択します。
- ブラウザーとして Internet Explorer を使用するには、「Use the ActiveX Client」を選択します。
  - Java クライアントを使用するには、次の図に示すように、「Use the Java Client」を選択します。

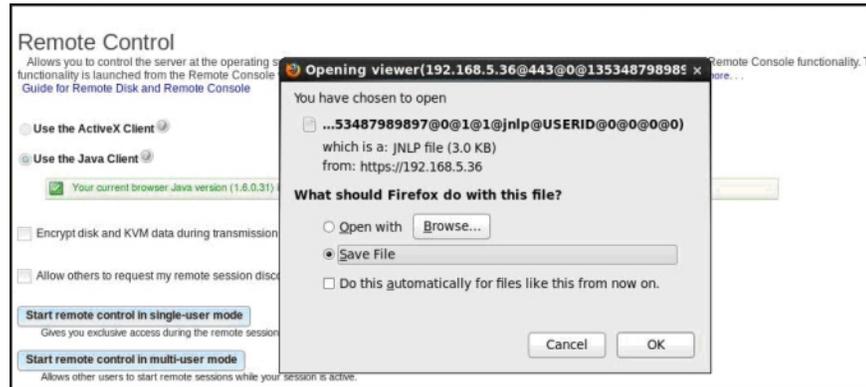


注:

- Internet Explorer ブラウザーを使用していない場合は、Java クライアントだけを選択できます。

- ActiveX クライアントと Java クライアントは、同一の機能性を備えています。
- ご使用のクライアントがサポートされているかどうかを示す状況表示行が表示されます。

次のようなウィンドウが開きます。これは、ブラウザー（例えば、Firefox ブラウザー）がビューアー・ファイルを開くために使用する情報を示しています。



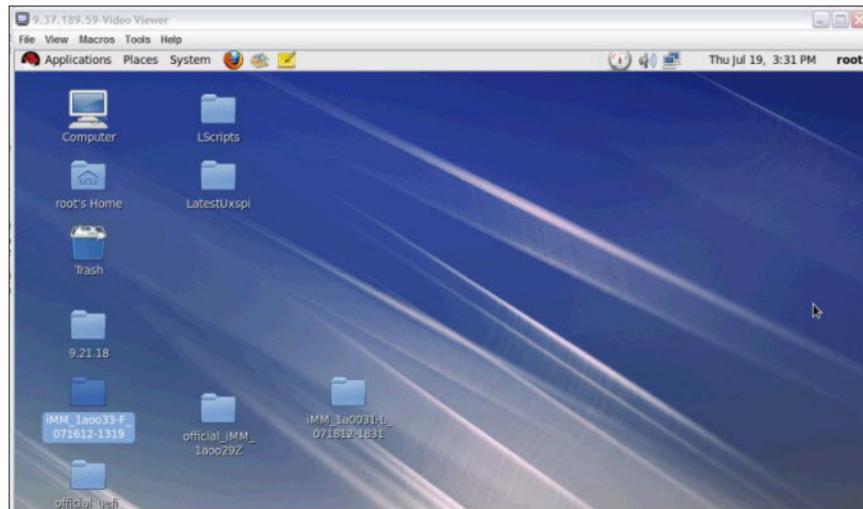
5. ブラウザーがビューアー・ファイルをダウンロードして開いた後、Web サイト証明書の検証に関する警告を表示する確認ウィンドウが開きます（次の図を参照）。「Yes」をクリックして、証明書を受け入れます。



6. サーバーをリモート側で制御するには、次のいずれかのメニュー項目を選択します。
  - セッションで排他的なりモート・アクセス権を持つには、「**Start remote control in single User mode**」をクリックします。
  - 使用しているセッションに他のユーザーからのリモート・コンソール・アクセスを許可するには、「**Start remote control in multi user mode**」をクリックします。

注: 「Video Viewer」ウィンドウが開かれる前に「**Encrypt disk and KVM data during transmission**」チェック・ボックスが選択された場合、ディスク・データはセッション中に ADES 暗号化によって暗号化されます。

「Video Viewer」ウィンドウが開きます (次の図を参照)。このウィンドウで、リモート・コンソール機能にアクセスできます。



7. Remote Control 機能の使用が終了したら、「Video Viewer」ウィンドウと「Virtual Media Session」ウィンドウを閉じます。

**注:**

- Video Viewer は、自動的に「Virtual Media Session」ウィンドウを閉じます。
- リモート・ディスクがマップされている状態で「Virtual Media Session」ウィンドウを閉じない てください。リモート・ディスクのクローズおよびマップ解除の手順については、117 ページの『リモート・ディスク』を参照してください。
- Remote Control 機能を使用しているときにマウスまたはキーボードの問題が生じた場合は、Web インターフェースの「Remote Control」ページから使用できるヘルプを参照してください。
- リモート・コンソールを使用して、Setup ユーティリティー・プログラムで IMM2 の設定を変更すると、サーバーが IMM2 を再始動する場合があります。リモート・コンソールおよびログイン・セッションが失われます。短時間の遅延の後、新しいセッションで再び IMM2 にログインでき、リモート・コンソールを再度開始し、Setup ユーティリティー・プログラムを終了することができます。

**重要:** IMM2 は、Java アプレットまたは ActiveX アプレットを使用してリモート・プレゼンス機能を実行します。IMM2 を最新のファームウェア・レベルに更新した場合は、Java アプレットおよび ActiveX アプレットも最新レベルに更新されます。デフォルトでは、Java は以前に使用されたアプレットをキャッシュに入れます (ローカル側で保管します)。IMM2 ファームウェアのフラッシュ更新の後、サーバーの使用する Java アプレットが最新レベルでない場合もあります。

この問題を修正するには、キャッシングをオフにします。使用方法は、プラットフォームと Java のバージョンによって異なります。以下のステップは、Windows 上の Oracle Java 1.5 用です。

1. 「スタート」 → 「設定」 → 「コントロール パネル」をクリックします。
2. 「Java Plug-in 1.5」ダブルクリックします。「Java Plug-in コントロールパネル」ウィンドウが開きます。

3. 「キャッシュ」タブをクリックします。
4. 次のオプションのいずれかを選択してください。
  - 「キャッシュを有効」チェック・ボックスをクリアし、Java キャッシングが常に使用不可にされているようにします。
  - 「クリア (Clear Caching)」をクリックします。このオプションを選択した場合は、IMM2 ファームウェアを更新するたびに、「クリア (Clear Caching)」をクリックする必要があります。

IMM2 ファームウェアの更新について詳しくは、120 ページの『サーバー・ファームウェアの更新』を参照してください。

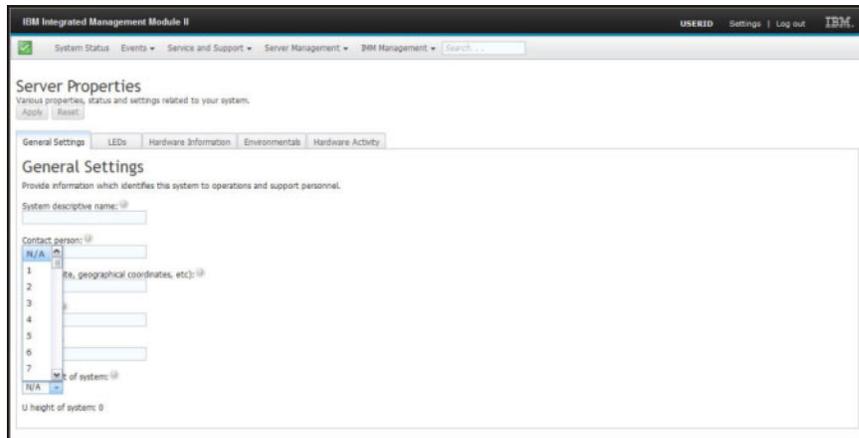
Remote Control 機能について詳しくは、105 ページの『リモート・プレゼンス機能および Remote Control 機能』を参照してください。

## サーバーのプロパティ

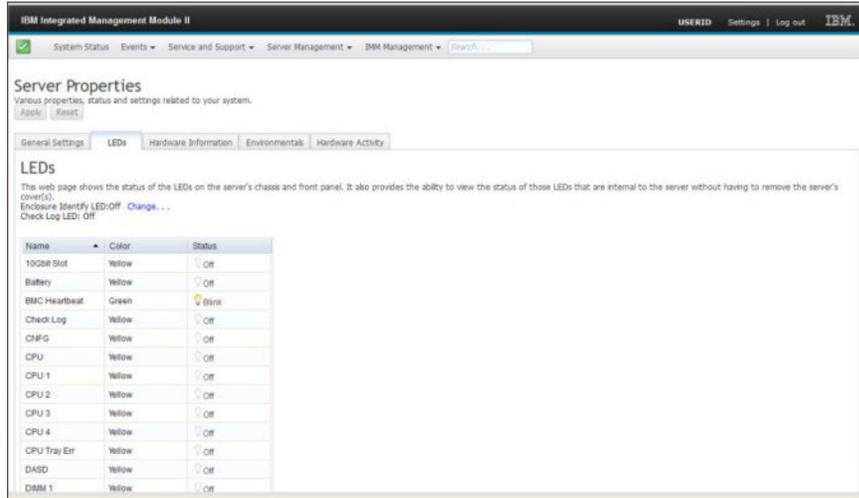
「Server Management」タブの下にある「**Server Properties**」オプションを選択すると、次のようなウィンドウが表示されます。このオプションを使用すると、システムの識別に役立つ各種パラメーターを設定できます。これには、記述名、連絡先の個人、場所などが含まれます。これらのフィールドに入力した情報は、「**Apply**」をクリックすると有効になります。前回変更を適用した後に各フィールドに入力した情報を消去するには、「**Reset**」をクリックします。

The screenshot shows the 'Server Properties' configuration page in the IMM Integrated Management Module 2. The page is titled 'Server Properties' and includes a sub-header 'General Settings'. Below the header, there are several input fields for system identification: 'System descriptive name', 'Contact person', 'Location (site, geographical coordinates, etc.)', 'Room ID', and 'Rack ID'. At the bottom, there are two more fields: 'Lowest unit of system' (currently set to 'N/A') and 'U height of system' (currently set to '0'). The page also features a 'Reset' button and an 'Apply' button (not fully visible).

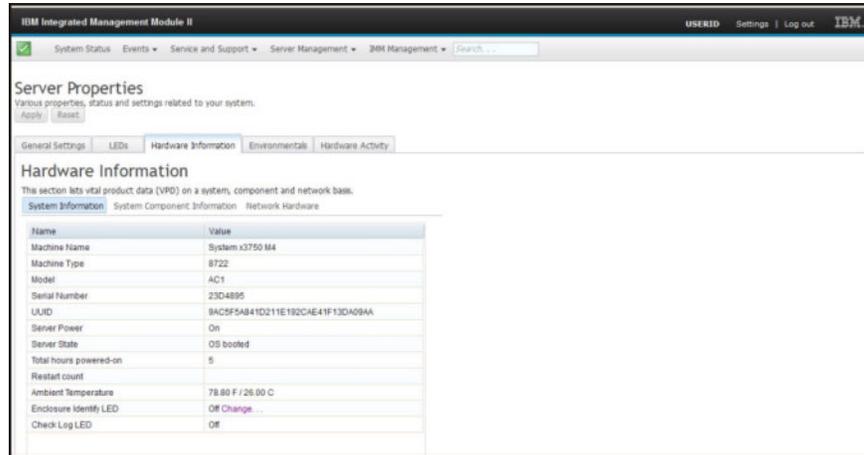
次の図の中では、「**Lowest unit of the system**」を指定できます。「**Lowest unit of the system**」フィールドは、マネージメント・モジュール (例えば、アドバンスト・マネージメント・モジュールまたは CMM) への接続を必要とします。



システム内の LED を表示するには、「LED」タブをクリックします。次のようなウィンドウが開きます。

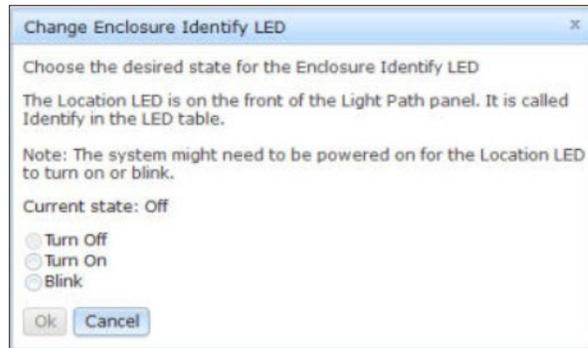


システム情報、システム・コンポーネント情報、およびネットワーク・ハードウェア情報を表示するには、「**Hardware Information**」タブをクリックします。各種の VPD 情報を表示するには、「Hardware Information」タブの中で該当するタブを選択します。「**System Information**」タブは、マシン名、シリアル番号、およびモデルなどの情報を提供します。次の図は、「System Information」ウィンドウを示しています。

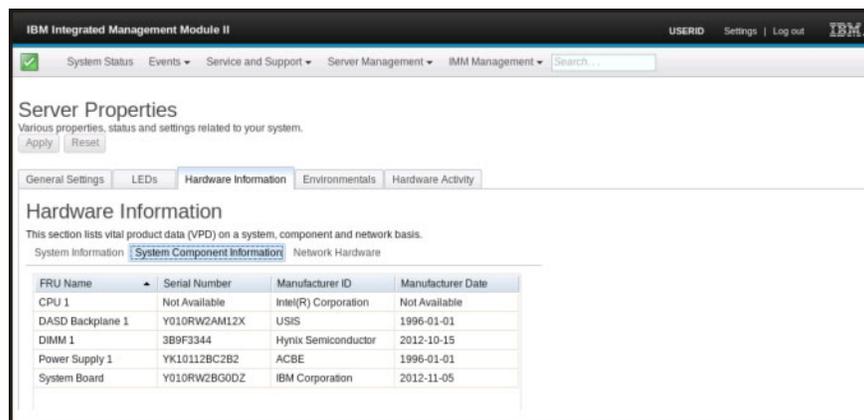


「Enclosure Identify LED」の状況は、「System Information」ウィンドウから表示および変更できます。「Enclosure Identify LED」を変更するには、「Change...」リンクをクリックします。次のようなウィンドウが開きます。

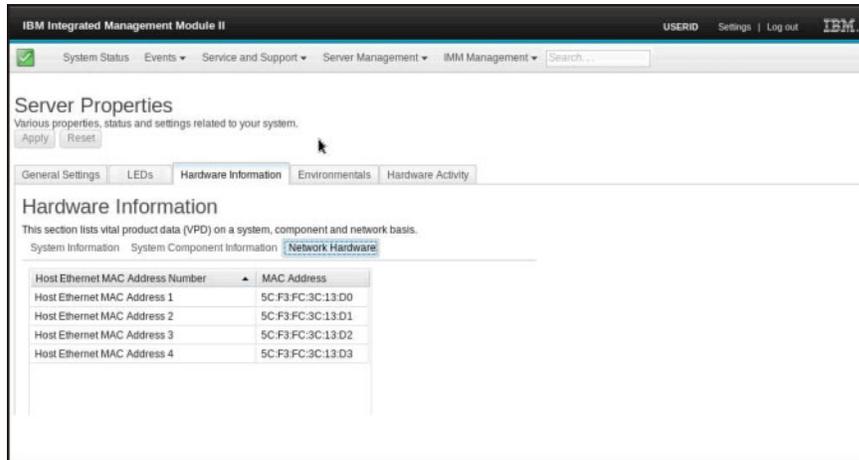
注: 格納装置 ID LED は、Light Path パネルの前面にあります。



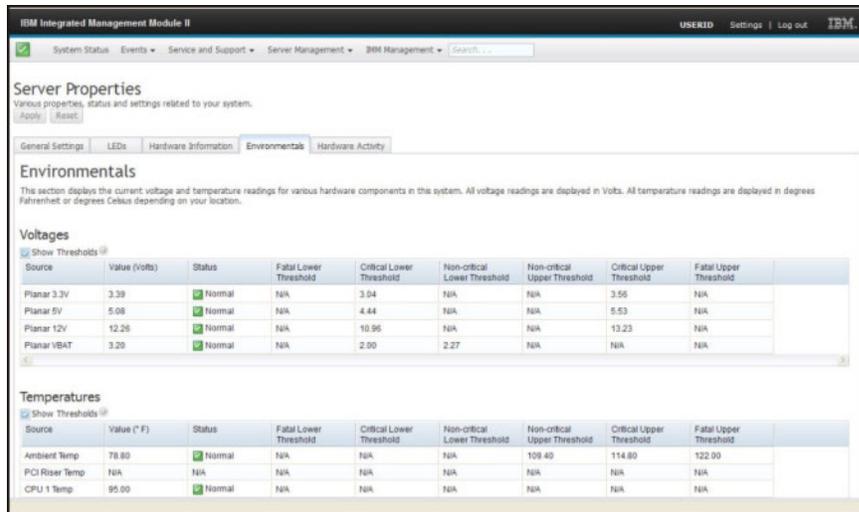
コンポーネント情報を表示するには、「System Component Information」タブを選択します。コンポーネント情報には、FRU 名、シリアル番号、製造元 ID、および製造日が含まれます。次の図は、「System Component Information」タブをクリックしたときに表示される情報を示しています。



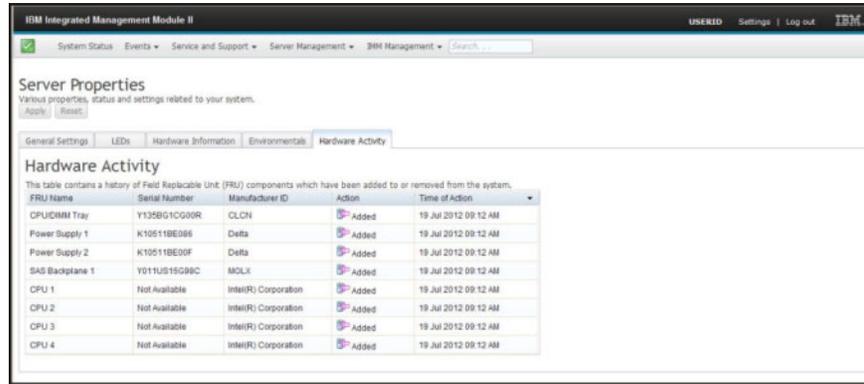
ネットワーク・ハードウェア情報を表示するには、「**Network Hardware**」タブを選択します。ネットワーク・ハードウェア情報には、ホスト・イーサネット MAC アドレス番号と MAC アドレスが含まれます。次の図は、「Network Hardware」タブをクリックしたときに表示される情報を示しています。



システム内のハードウェア・コンポーネントの電圧と温度を表示するには、「Server Properties」ページで「**Environmentals**」タブを選択します。次のようなウィンドウが開きます。テーブルの「**Status**」列には、サーバー内の正常なアクティビティまたは問題のエリアが示されます。



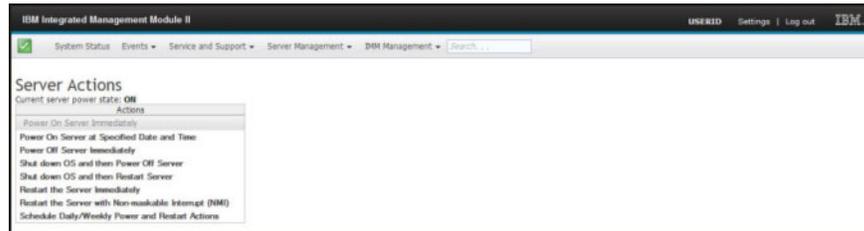
「Server Properties」ページの「**Hardware Activity**」タブは、システムに追加または削除されたハードウェアの履歴を提供します。次の図は、「Hardware Activity」タブをクリックしたときに表示される情報を示しています。



## サーバー電源アクション

このセクションでは、IMM2 Web インターフェース・ホーム・ページの「Server Management」タブの下にある「Server Power Actions」オプションについて説明します。

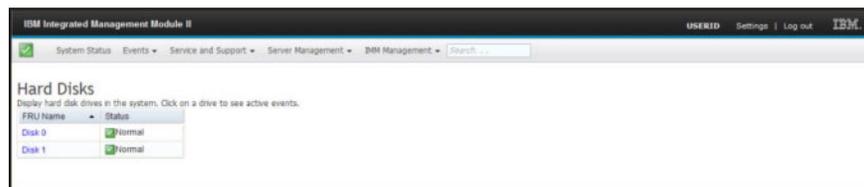
システム電源を制御するために使用できるアクションのリストを表示するには、「Server Management」タブの下にある「**Server Power Actions**」オプションを選択します。「Server Power Actions」ウィンドウの例を次の図に示します。



サーバーの電源を即時にオンにするか、スケジュールした時刻にオンにするかを選択できます。また、オペレーティング・システムのシャットダウンと再始動を選択することもできます。サーバー電源の制御について詳しくは、104 ページの『サーバーの電源状況の制御』を参照してください。

## ディスク

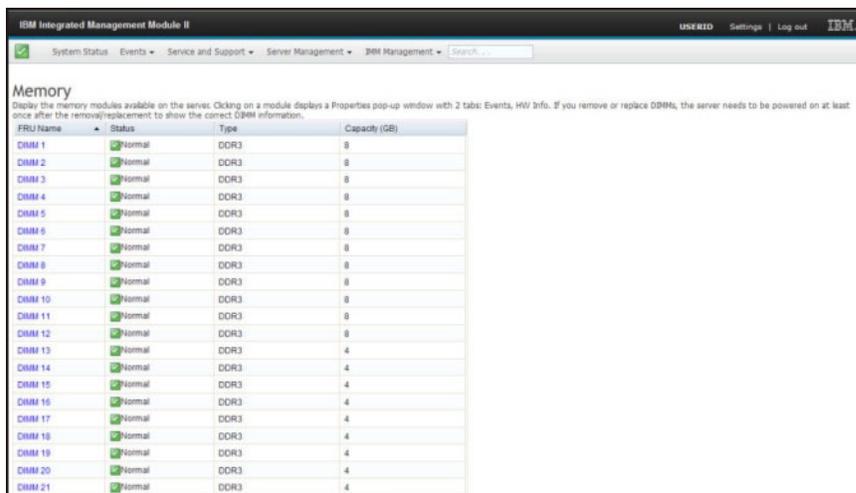
システム内のハード・ディスクを表示するには、「Server Management」タブで「**Disks**」オプションを選択します。次の画面が表示されます。ハード・ディスクに関連したイベントを表示するには、当該のハード・ディスクをクリックします。



## メモリー

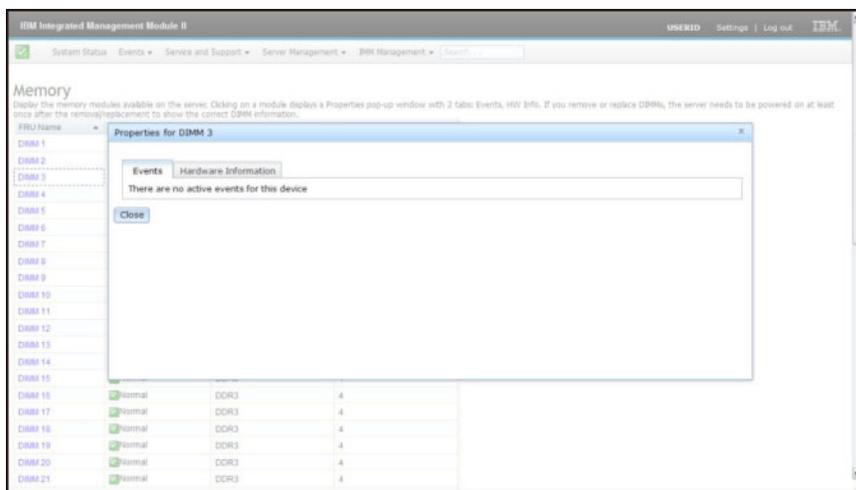
システムに取り付けたメモリー・モジュールに関する情報を表示するには、「Server Management」タブの下にある「Memory」オプションを選択します。次のようなウィンドウが開きます。各メモリー・モジュールはテーブル内にリンクとして表示され、これをクリックすると、そのメモリー・モジュールに関する詳細情報を取得することができます。テーブルには、DIMM の状況、DIMM タイプ、および DIMM 容量も表示されます。

注: DIMM を取り外しまたは交換した場合は、システムを再始動し、システム DIMM に加えた変更に関する更新された DIMM 情報を表示する必要があります。



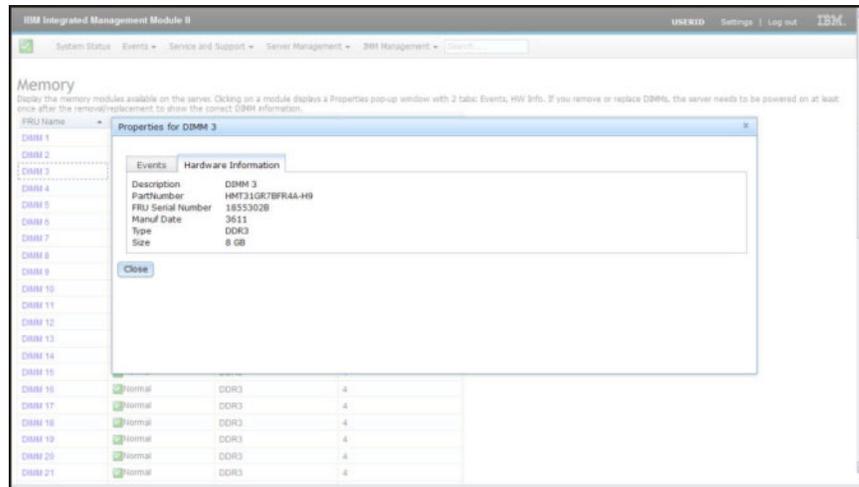
| FRU Name | Status | Type | Capacity (GB) |
|----------|--------|------|---------------|
| DIMM 1   | Normal | DDR3 | 8             |
| DIMM 2   | Normal | DDR3 | 8             |
| DIMM 3   | Normal | DDR3 | 8             |
| DIMM 4   | Normal | DDR3 | 8             |
| DIMM 5   | Normal | DDR3 | 8             |
| DIMM 6   | Normal | DDR3 | 8             |
| DIMM 7   | Normal | DDR3 | 8             |
| DIMM 8   | Normal | DDR3 | 8             |
| DIMM 9   | Normal | DDR3 | 8             |
| DIMM 10  | Normal | DDR3 | 8             |
| DIMM 11  | Normal | DDR3 | 8             |
| DIMM 12  | Normal | DDR3 | 8             |
| DIMM 13  | Normal | DDR3 | 4             |
| DIMM 14  | Normal | DDR3 | 4             |
| DIMM 15  | Normal | DDR3 | 4             |
| DIMM 16  | Normal | DDR3 | 4             |
| DIMM 17  | Normal | DDR3 | 4             |
| DIMM 18  | Normal | DDR3 | 4             |
| DIMM 19  | Normal | DDR3 | 4             |
| DIMM 20  | Normal | DDR3 | 4             |
| DIMM 21  | Normal | DDR3 | 4             |

アクティブ・イベントとコンポーネントの詳細を表示するには、テーブル内の「DIMM」リンクをクリックします (次の画面を参照)。



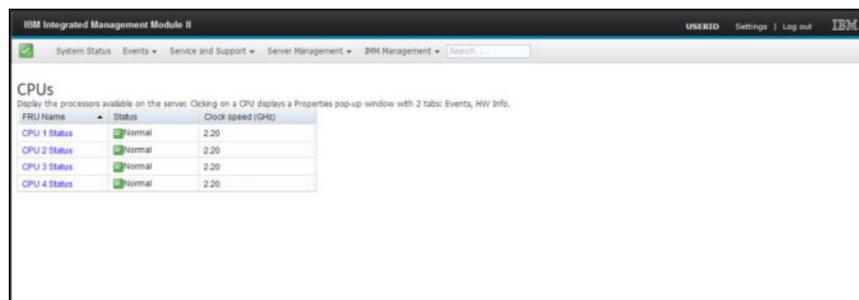
| FRU Name | Status | Type | Capacity (GB) |
|----------|--------|------|---------------|
| DIMM 1   | Normal | DDR3 | 8             |
| DIMM 2   | Normal | DDR3 | 8             |
| DIMM 3   | Normal | DDR3 | 8             |
| DIMM 4   | Normal | DDR3 | 8             |
| DIMM 5   | Normal | DDR3 | 8             |
| DIMM 6   | Normal | DDR3 | 8             |
| DIMM 7   | Normal | DDR3 | 8             |
| DIMM 8   | Normal | DDR3 | 8             |
| DIMM 9   | Normal | DDR3 | 8             |
| DIMM 10  | Normal | DDR3 | 8             |
| DIMM 11  | Normal | DDR3 | 8             |
| DIMM 12  | Normal | DDR3 | 8             |
| DIMM 13  | Normal | DDR3 | 4             |
| DIMM 14  | Normal | DDR3 | 4             |
| DIMM 15  | Normal | DDR3 | 4             |
| DIMM 16  | Normal | DDR3 | 4             |
| DIMM 17  | Normal | DDR3 | 4             |
| DIMM 18  | Normal | DDR3 | 4             |
| DIMM 19  | Normal | DDR3 | 4             |
| DIMM 20  | Normal | DDR3 | 4             |
| DIMM 21  | Normal | DDR3 | 4             |

説明、部品番号、FRU シリアル番号、製造日 (週/年)、タイプ (DDR3 など)、およびギガバイト単位のサイズなど、コンポーネントの詳細を表示するには、「Hardware Information」タブをクリックします (次の図を参照)。

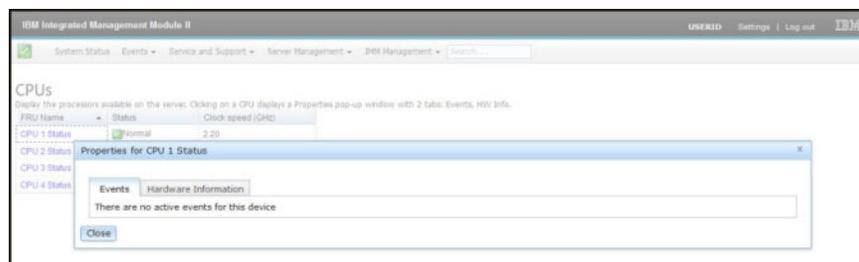


## Processors

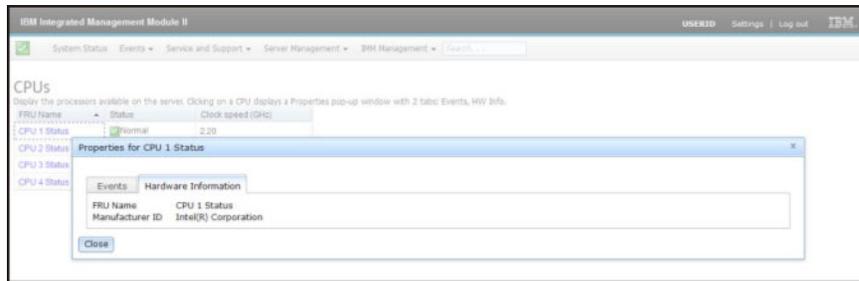
システムに取り付けたマイクロプロセッサに関する情報を表示するには、「Server Management」タブの下にある「Processors」オプションを選択します。次のようなウィンドウが開きます。



アクティブ・イベントとコンポーネントの詳細を表示するには、テーブル内の「CPU」リンクをクリックします (次の図を参照)。



FRU 名や製造元 ID など、コンポーネントの詳細を表示するには、「Hardware Information」タブをクリックします (次の図を参照)。

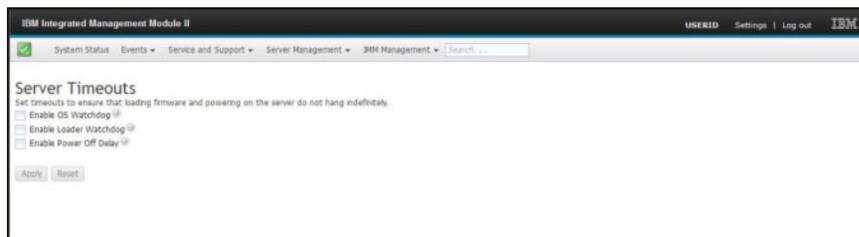


## サーバー・タイムアウト

ファームウェア更新およびシステムの電源オンのときにサーバーが無期限にハングしないようにするには、「Server Management」タブの下の「**Server Timeouts**」オプションを使用してタイムアウトを選択します。この機能は、各オプションに値を設定することで使用可能にできます。

注: サーバー・タイムアウトを使用するには、インバンド USB インターフェース (または LAN over USB) でのコマンドの使用を可能にする必要があります。USB インターフェースの構成について詳しくは、82 ページの『USB の構成』を参照してください。

次の図は、「Server Timeouts」ウィンドウを示しています。



サーバー・タイムアウトについて詳しくは、56 ページの『サーバー・タイムアウトの設定』を参照してください。

## PXE ネットワーク・ブート

次のサーバー再始動時に PXE ネットワーク・ブートを試みるようサーバーをセットアップするには、「Server Management」タブの下にある「**PXE Network Boot**」オプションを選択します。PXE ネットワーク・ブートのセットアップについて詳しくは、119 ページの『PXE ネットワーク・ブートのセットアップ』を参照してください。

## 最新の OS の障害画面

IMM2 に保存されている最新のオペレーティング・システム障害画面データを表示または消去するには、「Server Management」タブで「**Latest OS Failure Screen**」オプションを選択します。IMM2 は最新のエラー・イベント情報のみを保管するため、新規のエラー・イベントが発生すると、古い OS 障害画面データは上書きされます。

次の図は、OS 障害画面の例です。

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

「Latest OS Failure Screen」オプションについて詳しくは、134 ページの『最新の OS 障害画面データのキャプチャー』を参照してください。

---

## 「IMM Management」タブ

このセクションでは、IMM2 Web ユーザー・インターフェース・ホーム・ページの「IMM Management」タブの下にあるオプションについて説明します。

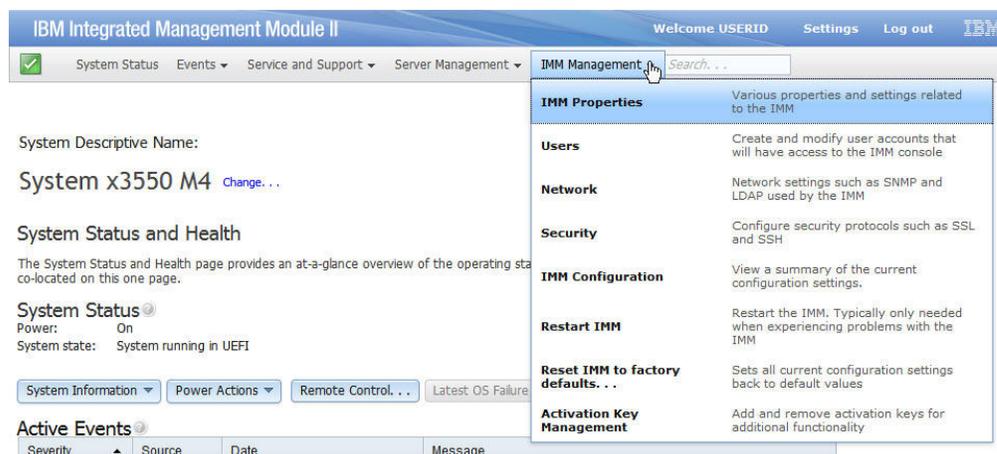
「IMM Management」タブの下にあるオプションを使用すると、IMM2 設定を表示および変更することができます。オプションのリスト、およびそれらのオプションを使用して IMM2 を構成する方法について詳しくは、53 ページの『第 4 章 IMM2 の構成』を参照してください。



## 第 4 章 IMM2 の構成

「IMM Management」タブには、IMM2 を構成するためのオプションが含まれています。IMM2 の設定を表示および変更するには、「IMM Management」タブを使用します。以下のオプションは、「IMM Management」タブの下にリストされます (次の図を参照)。

- IMM Properties
- Users
- Network
- Security
- IMM Configuration
- Restart IMM
- Reset IMM to factory defaults
- Activation Key Management



「Integrated Management Module (IMM) Properties」ページから、以下の機能を実行できます。

- サーバー・ファームウェアの情報へアクセス
- 日付と時刻の設定:
  - IMM2 での時刻の設定方式の選択: 手動または NTP
  - 手動の設定方式の場合の、IMM2 の日時の設定
  - NTP 設定方式の場合の、NTP 情報の設定
  - IMM2 のタイム・ゾーン情報の設定
- IMM2 シリアル・ポート情報へのアクセス:
  - IMM2 シリアル・ポートの構成
  - IMM2 CLI キー・シーケンスの設定

「User Accounts」ページから、以下の機能を実行できます。

- IMM2 ユーザー・アカウントの管理:
  - ユーザー・アカウントの作成
  - ユーザー名をクリックして、そのユーザーのプロパティを編集:
    - ユーザー名の編集
    - ユーザー・パスワードの設定
    - ユーザーの SNMPv3 設定の構成
    - ユーザーの Secure Shell (SSH) 公開認証鍵の管理
  - ユーザー・アカウントの削除
- グローバルなユーザー・ログイン設定の構成:
  - ユーザー認証方式の設定
  - Web の非アクティブ・タイムアウトの設定
  - IMM2 で使用可能なユーザー・アカウントのセキュリティー・レベルの構成
- 現在 IMM2 に接続しているユーザーの表示

「Network Protocol Properties」ページから、以下の機能を実行できます。

- イーサネット設定の構成:
  - イーサネット設定:
    - ホスト名
    - IPv4 および IPv6 の使用可能化、および IPv4 および IPv6 アドレスの設定
  - イーサネットの詳細設定:
    - 自動ネゴシエーションの使用可能化
    - MAC アドレスの管理
    - 最大伝送単位の設定
- SNMP 設定の構成:
  - SNMPv1 の使用可能化、および SNMPv1 の構成:
    - 連絡先情報の設定
    - SNMP トラップの使用可能化、および SNMP トラップの構成
    - コミュニティー管理
  - SNMPv3 の使用可能化、および SNMPv3 の構成:
    - 連絡先情報の設定
    - ユーザー・アカウントの構成
- DNS 設定の構成:
  - DNS アドレッシング設定の指定 (IPv4 または IPv6)
  - DNS サーバーのアドレッシングを追加で使用可能に設定、および DNS サーバーのアドレッシングの構成
- DDNS 設定の構成:
  - DDNS の使用可能化
  - ドメイン・ネームのソースの選択 (カスタムまたは DHCP サーバー)
    - カスタムのドメイン・ネームの設定 (手動で指定したカスタムのソースの場合)
    - DHCP サーバーが指定したドメイン・ネームの表示

- SMTP 設定の構成:
  - SMTP サーバーの IP アドレスまたはホスト名の設定
  - SMTP サーバーのポート番号の設定
  - SMTP 接続のテスト
- LDAP 設定の構成:
  - LDAP サーバー構成の設定 (DNS または事前構成):
    - DNS が LDAP サーバー構成を指定した場合の、検索ドメインの設定:
      - ログイン ID からの検索ドメインの取り出し
      - 検索ドメインおよびサービス名の手動による指定
      - ログイン ID からの検索ドメインの取り出しを試行してから、手動で指定した検索ドメインおよびサービス名を使用
    - 事前構成された LDAP サーバーを使用している場合:
      - LDAP サーバーのホスト名および IP アドレスの設定
      - LDAP サーバーのポート番号の設定
  - LDAP サーバーのルート識別名の設定
  - UID 検索属性の設定
  - バインディング方式の選択 (匿名、構成済みの資格情報を使用、ログイン資格情報を使用):
    - 構成済みの資格情報の場合、クライアントの識別名およびパスワードの設定
  - アクティブ・ディレクトリー・ユーザーを使用可能にするための拡張役割ベース・セキュリティ:
    - 使用不可の場合:
      - グループ・フィルターの設定
      - グループ検索属性の設定
      - ログイン許可属性の設定
    - 使用可能な場合、サーバーのターゲット名の設定
- Telnet 設定の構成:
  - Telnet アクセスの使用可能化
  - Telnet セッションの最大数の設定
- USB 設定の構成:
  - Ethernet over USB の使用可能化
  - 外部イーサネットから Ethernet over USB ポートへの転送の使用可能化および管理
- ポート割り当ての構成:
  - オープン・ポート番号の表示
  - IMM2 サービスが使用するポート番号の設定:
    - HTTP
    - HTTPS
    - Telnet CLI
    - SSH CLI

- SNMP エージェント
- SNMP Traps
- Remote Control
- CIM over HTTPS
- CIM over HTTP

「Security」ページから、以下の機能を実行できます。

- HTTPS サーバーの使用可能化および証明書管理
- CIM over HTTPS の使用可能化および証明書管理
- LDAP セキュリティーの選択および証明書管理
- SSH サーバーの使用可能化および証明書管理

「IMM Configuration」ページから、以下の機能を実行できます。

- IMM2 構成の要約の表示
- IMM2 構成のバックアップまたはリストア
- バックアップまたはリストアの状況表示
- IMM2 構成の出荷時デフォルト設定へのリセット
- IMM2 初期セットアップ・ウィザードへのアクセス

「Restart IMM」ページから、IMM2 をリセットできます。

「Reset IMM2 to factory defaults...」ページから、IMM2 構成を出荷時デフォルト設定にリセットすることができます。

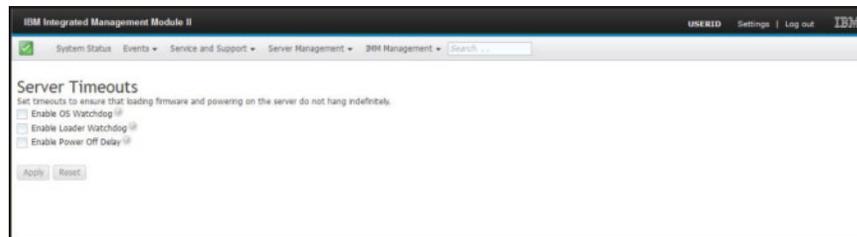
「Activation Key Management」ページから、IMM2 およびサーバーのオプションの Features on Demand (FoD) のアクティベーション・キーを管理することができます。FoD アクティベーション・キーの管理については、141 ページの『第 7 章 Features on Demand』を参照してください。

---

## サーバー・タイムアウトの設定

ファームウェア更新またはサーバーの電源オンのときにサーバーが無期限にハングしないようにするには、「Server Timeouts」オプションを使用してタイムアウトを設定します。この機能は、次の図に示すように、このオプションに値を設定することで使用可能にできます。

**注:** サーバー・タイムアウトを使用するには、インバンド USB インターフェース (または LAN over USB) でのコマンドの使用を可能にする必要があります。USB インターフェースの使用可能化および使用不可化について詳しくは、82 ページの『USB の構成』を参照してください。



サーバー・タイムアウト値を設定するには、以下のステップを実行してください。

1. サーバー・タイムアウトを設定したい IMM2 にログインします。(10 ページの『IMM2 へのログイン』を参照)。
2. 「**Server Management**」をクリックし、次に「**Server Timeouts**」を選択します。

以下のイベントに自動的に応答するように、IMM2 を設定することができます。

- オペレーティング・システムの停止
  - オペレーティング・システムを始動できない
3. IMM2 に自動的に応答させたいイベントに対応するサーバー・タイムアウトを使用可能にします。各選択項目の説明については、『サーバー・タイムアウトの選択項目』を参照してください。
  4. 「**Apply**」をクリックします。

注: すべてのタイムアウトを同時にクリアするために使用できる「**Reset**」ボタンがあります。

## サーバー・タイムアウトの選択項目

### Enable OS Watchdog

「**Enable OS Watchdog**」フィールドを使用して、IMM2 によるオペレーティング・システムのチェックの間隔を分数で指定します。オペレーティング・システムがこれらのチェックの 1 つに回答しないと、IMM2 は OS タイムアウト・アラートを生成し、サーバーを再始動します。サーバーが再始動された後、オペレーティング・システムがシャットダウンされ、サーバーが電源サイクルされるまで、OS ウォッチドッグは使用不可にされます。OS ウォッチドッグ値を設定するには、「**Enable OS Watchdog**」を選択し、メニューから時間間隔を選択します。このウォッチドッグをオフにするには、「**Enable OS Watchdog**」を選択解除します。オペレーティング・システム障害画面をキャプチャーするには、「**Enable OS Watchdog**」フィールドでウォッチドッグを使用可能に設定する必要があります。

### Enable Loader Watchdog

「**Enable Loader Watchdog**」フィールドを使用して、POST の完了からオペレーティング・システムの始動までの間、IMM2 が待つ分数を指定します。この間隔を超えると、IMM2 は、ローダー・タイムアウト・アラートを生成し、サーバーを自動的に再始動します。サーバーが再始動された後、ローダー・タイムアウトは、オペレーティング・システムがシャットダウンされてサーバーが電源サイクルされるまで (または、オペレーティング・システムが始動し、ソフトウェアが正常にロードされるまで)、自動的に使用不可にされます。ローダー・タイムアウト値を設定するには、オペレーティン

グ・システムの始動が完了するまで IMM2 が待てる時間の限度を選択します。このウォッチドッグをオフにするには、メニューから「**Enable Loader Watchdog**」を選択解除します。

#### Enable Power Off Delay

「**Enable Power Off Delay**」フィールドを使用して、IMM2 サブシステムがシステムの電源をオフにする前にオペレーティング・システムのシャットダウンを待つ分数を使用します。電源オフ遅延タイムアウト値を設定するには、IMM2 がオペレーティング・システムの電源オフの後に待つ制限時間を選択します。このウォッチドッグをオフにするには、メニューから「**Enable Loader Watchdog**」を選択解除します。

---

## IMM2 の日付と時刻の設定

注: IMM2 の日付と時刻の設定は、IBM Flex System では変更できません。

IMM2 の日付と時刻を表示または変更するには、「**Date and Time**」タブを選択します。IMM2 は、イベント・ログに記録するすべてのイベントにタイム・スタンプを付けるために、独自のリアルタイム・クロックを使用します。E メールと Simple Network Management Protocol (SNMP) で送信されるアラートには、リアルタイム・クロックの設定を使用してタイム・スタンプが付けられます。クロックの設定は、異なる時間帯にまたがってシステムをリモート側から管理する管理者にとって使いやすくなるよう、グリニッジ標準時 (GMT) のオフセットと夏時間をサポートしています。サーバーの電源がオフにされていたり、サーバーが使用不可にされている場合でも、ユーザーはリモート側からイベント・ログにアクセスできます。

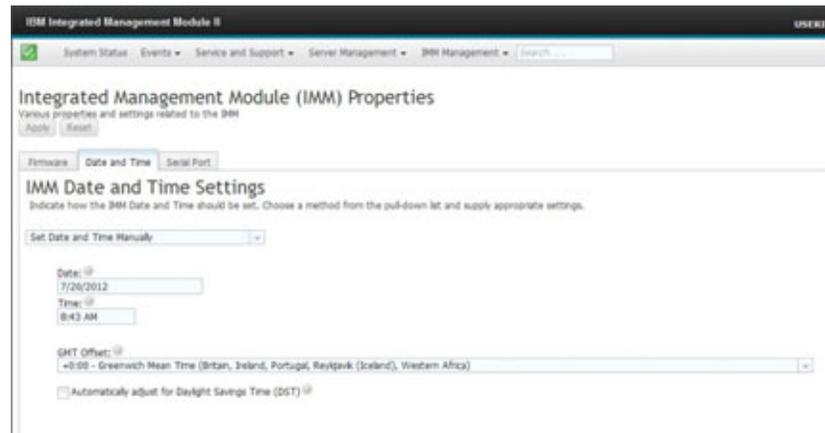
IMM2 日時設定は、IMM2 クロックにのみ影響し、サーバー・クロックには影響しません。IMM2 リアルタイム・クロックとサーバー・クロックは、別個の独立したクロックで、それぞれ別の時刻を設定することができます。

### 時刻と日付の設定の変更 (手動モード)

時刻と日付の設定を手動で変更するには、以下のステップを実行します。

1. 「**Indicate how the IMM date and time should be set**」メニュー・リストから、「**Set Date and Time Manually**」をクリックします。
2. 「**Date**」フィールドに、現在の月、日、および年を入力します。
3. 「**Time**」フィールドで、現在の時間と分に対応する数値を入力します。
  - 時間は、12 時間クロックで表される 1 から 12 の数値であることが必要です。
  - 分は、00 から 59 の数値であることが必要です。
  - 「**AM**」または「**PM**」を選択します。
4. 「**GMT Offset**」フィールドで、GMT からのオフセットを指定する数値を時間単位で選択します。この数値は、サーバーが配置されているタイム・ゾーンに対応する必要があります。
5. 「**Automatically adjust for Daylight Saving Time (DST)**」チェック・ボックスを選択するかクリアして、現地時間が標準時と夏時間の間で変化するとき IMM2 のクロックを自動的に調整するかどうかを指定します。

次の図は、日付と時刻を手動で設定するときの IMM の「Date and Time」タブを示しています。



### 時刻と日付の設定の変更 (NTP サーバー・モード)

IMM2 のクロックをサーバーのクロックと同期させるには、以下のステップを実行します。

1. 「Indicate how the IMM date and time should be set」メニュー・リストから、「Synchronize with an NTP server」をクリックします。
2. 「NTP server host name or IP address」フィールドで、クロックの同期に使用する NTP サーバーの名前を指定します。
3. 「Synchronization frequency (in minutes)」フィールドで、同期要求のおおよその間隔を指定します。3 から 1440 分間の値を入力します。
4. 間隔に指定した時間が経過するのを待たず、(「Apply」をクリックしたときの) 即時同期を要求するには、「Synchronize when these settings are saved」チェック・ボックスにチェック・マークを付けます。
5. 「GMT Offset」フィールドで、サーバーが置かれているタイム・ゾーンに合わせて、GMT からのオフセットを指定する数値を 1 時間単位で選択します。
6. 「Automatically adjust for Daylight Saving Time (DST)」チェック・ボックスを選択するかクリアして、現地時間が標準時と夏時間の間で変化するときに IMM2 のクロックを自動的に調整するかどうかを指定します。

次の図は、サーバーのクロックを使用して同期をとるときの IMM の「Date and Time」タブを示しています。

## シリアル・ポート設定の構成

ホストのシリアル・ポート・リダイレクトを指定するには、「**Serial Port**」オプションを選択します。IMM2 は、シリアル・リダイレクトに使用する 2 つのシリアル・ポートを提供します。

### シリアル・ポート 1 (COM1)

System x サーバー上のシリアル・ポート 1 (COM1) は、IPMI Serial over LAN (SOL) に使用されます。COM1 は、IPMI インターフェースからのみ構成可能です。

### シリアル・ポート 2 (COM2)

ブレード・サーバーでは、シリアル・ポート 2 (COM2) が SOL に使用されます。System x ラック・サーバーおよび IBM Flex System では、COM2 は Telnet または SSH を介してシリアル・リダイレクトに使用されます。COM2 は、IPMI インターフェースから構成することはできません。ラック・マウント型のサーバーおよびタワー型のサーバーでは、COM2 は内部 COM ポートで、外部アクセスはありません。

シリアル・ポート・リダイレクトのためには、次のフィールドに入力します。

#### ボー・レート

このフィールドには、使用するシリアル・ポート接続のデータ転送速度を指定します。ボー・レートを設定するには、使用するシリアル・ポート接続に対応する、9600 と 115200 の間のデータ転送速度を選択します。

#### パリティ

このフィールドには、使用するシリアル・ポート接続のパリティ・ビットを指定します。選択可能なオプションは、None、Odd、または Even です。

#### ストップ・ビット

このフィールドには、使用するシリアル・ポート接続のストップ・ビットの数を指定します。選択可能なオプションは、1 または 2 です。

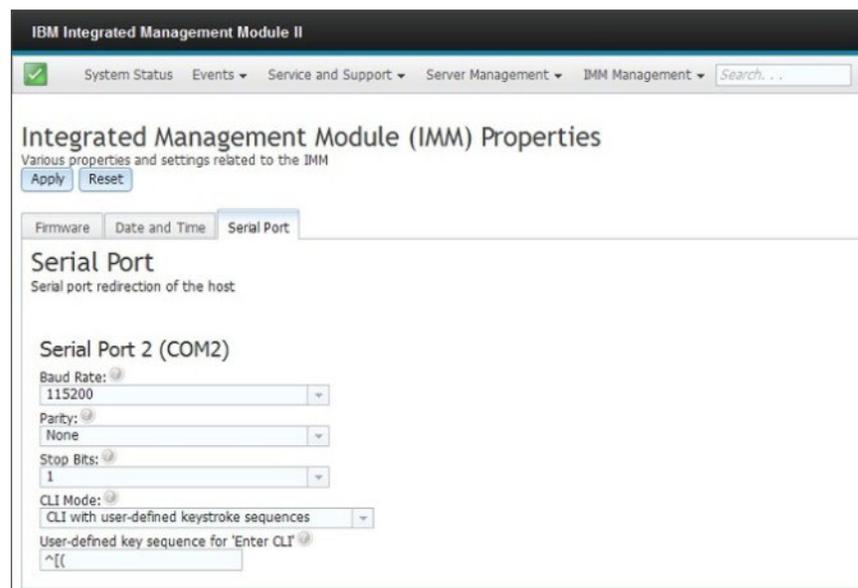
#### CLI モード

このフィールドでは、「**CLI with IMM2 compatible keystroke sequences**」

を選択するか、独自のキー・シーケンスを使用する場合は「**CLI with user defined keystroke sequences**」を選択します。「**CLI with user defined keystroke sequences**」を選択する場合は、「**User-defined key sequence for 'Enter CLI'**」フィールドでキー・シーケンスを定義する必要があります。

シリアル・リダイレクトは、開始されると、終了キー・シーケンスを入力するまで続きます。終了キー・シーケンスが入力されると、シリアル・リダイレクトは停止し、ユーザーは Telnet セッションまたは SSH セッションのコマンド・モードに戻ります。「**User-defined key sequence for 'Enter CLI'**」フィールドを使用して、終了キー・シーケンスを指定します。

次の図は、「Serial Port」タブを示しています。



## ユーザー・アカウントの構成

IMM2 用のユーザー・アカウントを作成および変更し、グループ・プロファイルを表示するには、「IMM Management」タブで「**Users**」オプションを選択します。次のような情報メッセージが表示されます。

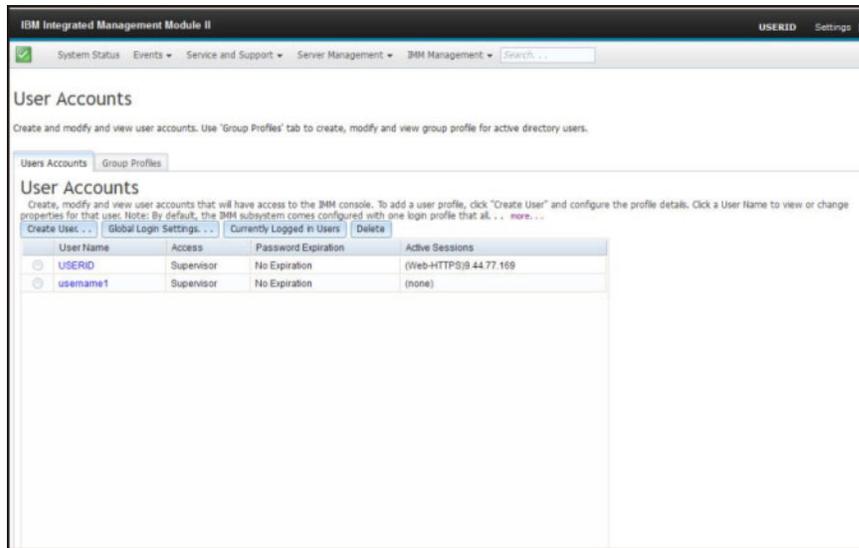
注: IBM Flex System では、IMM2 ユーザー・アカウントは CMM によって管理されます。



## ユーザー・アカウント

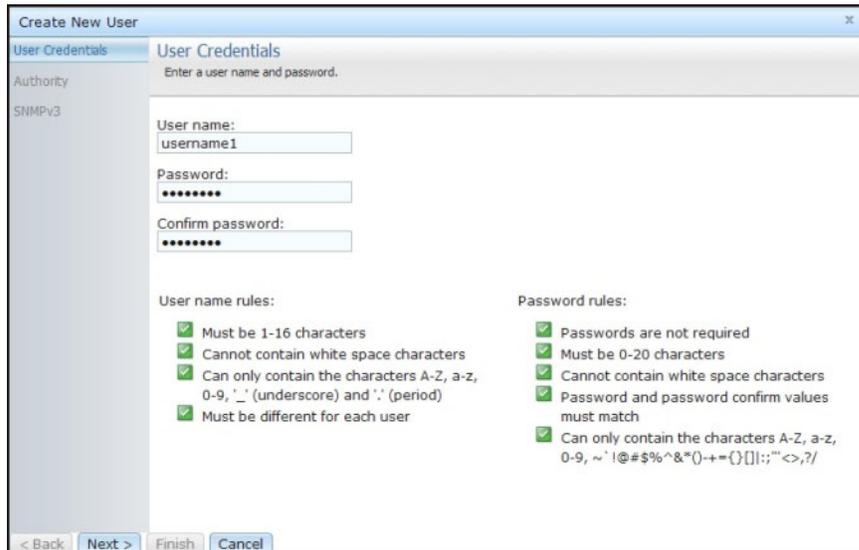
ユーザー・アカウントを作成、変更、および表示するには、次の図に示すように、「**Users Accounts**」タブを選択します。

注: IMM2 サブシステムには、1 つのログイン・プロファイルが付属しています。



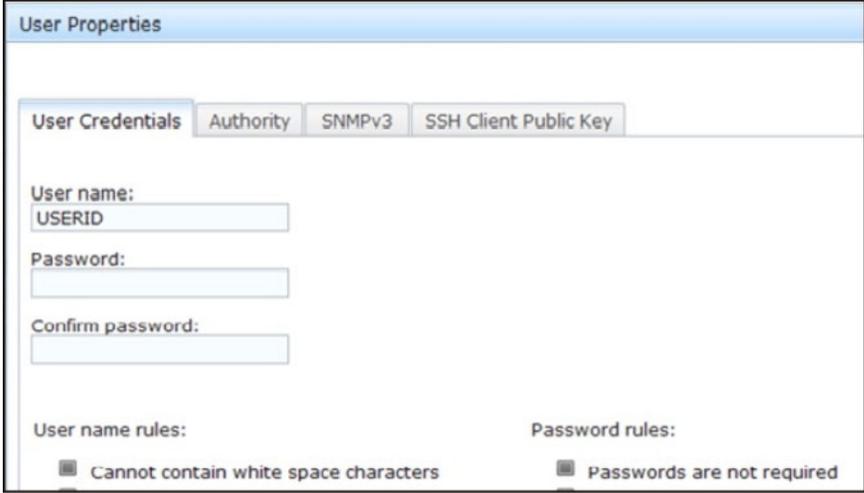
## ユーザーの作成

新規ユーザー・アカウントを作成するには、「**Create User...**」タブをクリックします。「**User name**」、「**Password**」および「**Confirm Password**」の各フィールドに入力します (次の図を参照)。



## ユーザー・プロパティ

既存のユーザー・アカウントを変更するには、「**User Properties**」タブをクリックします (次の図を参照)。



The screenshot shows a window titled "User Properties" with four tabs: "User Credentials", "Authority", "SNMPv3", and "SSH Client Public Key". The "User Credentials" tab is active. It contains the following fields and options:

- User name:** A text box containing "USERID".
- Password:** An empty text box.
- Confirm password:** An empty text box.
- User name rules:** A checkbox labeled "Cannot contain white space characters" which is checked.
- Password rules:** A checkbox labeled "Passwords are not required" which is checked.

## ユーザー権限

ユーザー権限を設定するには、「**Authority**」タブをクリックします。以下のユーザー権限レベルが選択可能です。

### Supervisor

このユーザーには一切の制限がありません。

### Read only

このユーザーには読み取り専用アクセスだけができ、ファイルの転送や電源と再始動のアクション、またはリモート・プレゼンス機能などのアクションを行うことはできません。

### Custom

ユーザーが実行できるアクションの設定で、よりカスタム化されたユーザー権限のプロファイルを使用できます。

## SNMP アクセス権

アカウントの SNMP アクセスを設定するには、「**SNMPv3**」タブをクリックします。以下のユーザー・アクセス・オプションが選択可能です。

### Authentication protocol

認証プロトコルとして、「**HMAC-MD5**」または「**HMAC-SHA**」のいずれかを指定します。これらは、SNMPv3 セキュリティー・モデルが認証に使用するアルゴリズムです。「**Authentication Protocol**」が使用可能に設定されていない場合、どの認証プロトコルも使用されません。

### Privacy protocol

SNMP クライアントとエージェント間のデータ転送は、暗号化を使用して保護することができます。サポートされる方式は、「**DES**」および

「AES」です。プライバシー・プロトコルは、認証プロトコルが  
HMAC-MD5 または HMAC-SHA に設定されている場合にのみ有効です。

#### Privacy password

このフィールドには暗号化パスワードを指定します。

#### Confirm privacy password

確認のために暗号化パスワードを再び指定します。

#### Access type

アクセス・タイプとして「Get」または「Set」を指定します。アクセス・タイプが「Get」の SNMPv3 ユーザーは、照会操作だけを実行できます。アクセス・タイプが「Set」の SNMPv3 ユーザーは、照会操作と設定変更 (例えば、ユーザーのパスワードの設定) を実行できます。

#### Hostname/IP address for traps

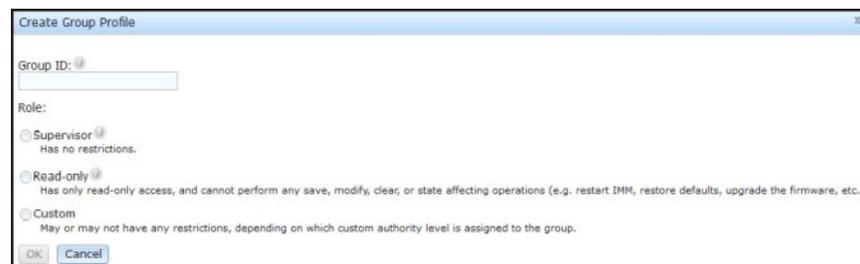
ユーザーのトラップ宛先を指定します。これは、IP アドレスまたはホスト名を指定することができます。トラップを使用して、SNMP エージェントは管理ステーションにイベントを通知します (例えば、プロセッサー温度が制限を超過した場合)。

## グループ・プロファイル

グループ・プロファイルを作成、変更、および表示するには、「Group Profiles」タブを選択します (次の図を参照)。

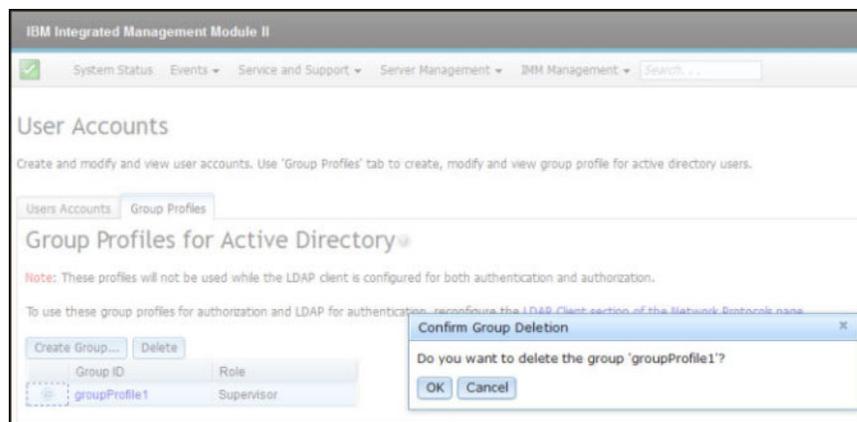


新規のユーザー・グループを作成するには、「Create Group」をクリックします。次の図は、「Create Group Profile」ウィンドウを示しています。



「Group ID」を入力し、「Role」を選択します (ユーザー権限レベルの詳細については、63 ページの『ユーザー権限』を参照してください)。

グループを削除する必要がある場合は、「Delete」をクリックします。次の図は、「Confirm Group Deletion」ウィンドウを示しています。



## グローバル・ログイン設定の構成

すべてのユーザーに適用するログイン設定を構成するには、「Global Login Settings」タブを使用します。

### 一般設定

ユーザーのログインの試行を認証する方法を選択し、非アクティブな Web セッションを切断するまでの IMM2 の待ち時間を分単位で指定するには、「General」タブをクリックします。「User authentication method」フィールドで、ログインを試みるユーザーの認証方法を指定できます。以下のいずれかの認証方式を選択できます。

- **Local only:** ユーザーは IMM2 上に構成されたローカル・ユーザー・アカウントの検索によって認証されます。ユーザー ID とパスワードが一致しない場合、アクセスは拒否されます。
- **LDAP only:** IMM2 は、LDAP サーバーを使用してユーザーの認証を試みます。この認証方式では、IMM2 上のローカル・ユーザー・アカウントは検索に使用されません。
- **Local first, then LDAP:** 最初にローカル認証が試みられます。ローカル認証が失敗すると、LDAP 認証が試みられます。
- **LDAP first, then Local:** 最初に LDAP 認証が試みられます。LDAP 認証が失敗すると、ローカル認証が試みられます。

注:

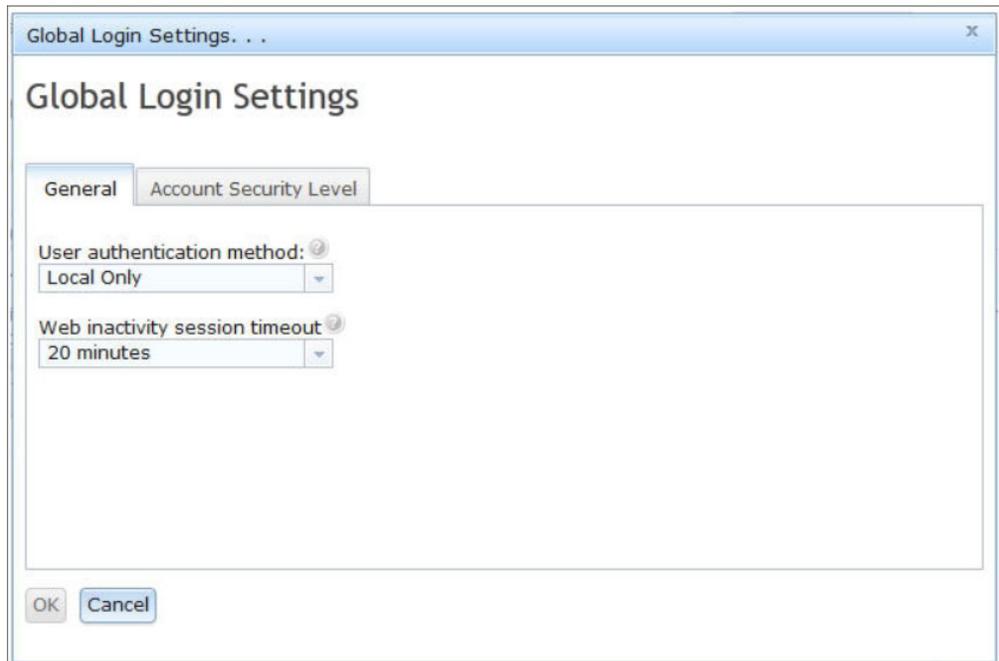
- ローカルで管理されているアカウントだけが、IPMI インターフェースと SNMP インターフェースで共有されます。これらのインターフェースは、LDAP 認証をサポートしていません。

- IPMI ユーザーおよび SNMP ユーザーは、「**User authentication method**」フィールドが「**LDAP only**」に設定されている場合でも、ローカルで管理されているアカウントを使用してログインすることができます。

「**Web inactivity session timeout**」フィールドで、非アクティブな Web セッションを切断するまでの IMM2 の待ち時間を分単位で指定できます。この機能を使用不可にするには、「**No timeout**」を選択します。ログイン・プロセスでのタイムアウト期間を選択するには、「**User picks timeout**」を選択します。

非アクティブ・タイムアウトは、自動的に最新表示されない Web ページにのみ適用されます。ユーザーが自動的に最新表示される Web ページにナビゲートしたときに、Web ブラウザーが絶えず Web ページの更新を要求する場合は、非アクティブ・タイムアウトで自動的にユーザーのセッションが終了することはありません。ユーザーは、60 秒ごとに Web ページのコンテンツを自動的に最新表示するかどうかを選択できます。自動最新表示設定について詳しくは、15 ページの『ページの自動最新表示』を参照してください。

「General」タブを次の図に示します。



一部の IMM2 Web ページは、自動最新表示設定が選択されていない場合でも自動的に最新表示されます。自動的に最新表示される IMM2 Web ページは、次のとおりです。

- **System Status:** システムと電源の状況は、3 秒ごとに自動的に最新表示されます。
- **Server Power Actions:** 電源の状況は、3 秒ごとに自動的に最新表示されます。
- **Remote Control:** 「Start remote control...」の各ボタンは、1 秒ごとに自動的に最新表示されます。「Session List」テーブルは、1 分に 1 回、自動的に最新表示されます。

IMM2 ファームウェアは、最大 6 つの同時 Web セッションをサポートします。他のユーザーが使用できるようにセッションを解放するために、非アクティブ・タイムアウトでセッションが自動的にクローズされるのを待たず、作業が終了した時点で Web セッションからログアウトすることをお勧めします。

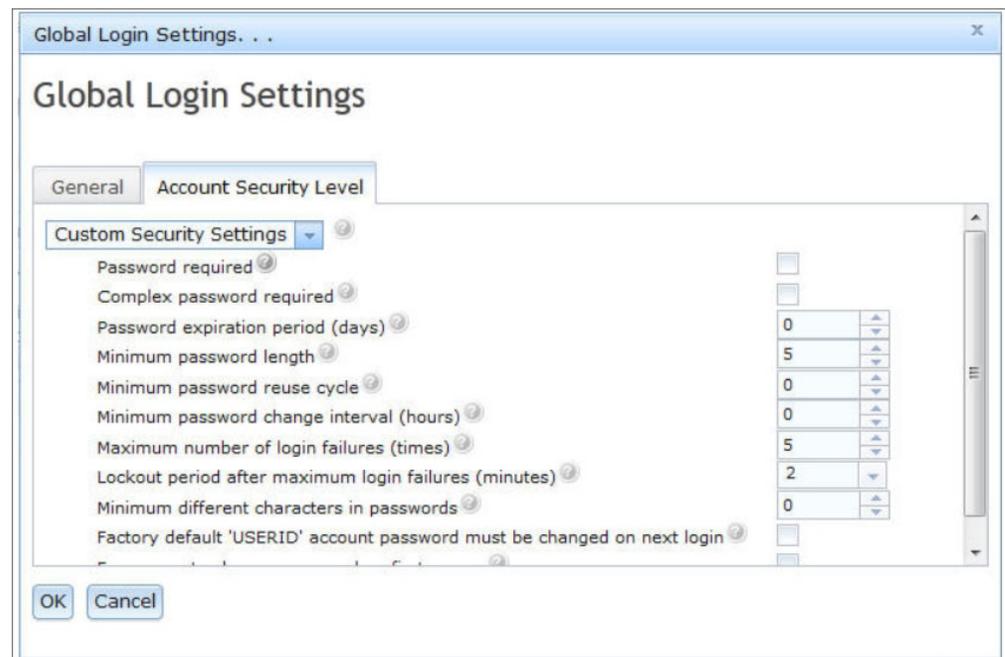
注: 自動的に最新表示される IMM2 Web ページ上でブラウザを開いたまま放置した場合、Web セッションが非アクティブでも自動的にクローズされません。

## アカウントのセキュリティ・ポリシーの設定

アカウントのセキュリティ・ポリシーの設定を選択するには、「Account Security Level」タブをクリックします。アカウントのセキュリティ・ポリシーの設定には、次の 3 つのレベルがあります。

- Legacy Security Settings
- High Security Settings
- Custom Security Settings

「Account Security Level」タブを次の図に示します。



項目リストから、目的のレベルを選択します。「Legacy Security Settings」および「High Security Settings」ではポリシー設定値が事前設定されており、変更することはできません。「Custom Security Settings」では、ユーザーが必要に応じてセキュリティ・ポリシーをカスタマイズすることができます。

次の表に、各レベルのセキュリティ設定の値を示します。

表 3. セキュリティ設定ポリシーの値

| ポリシー設定/フィールド      | Legacy Security Settings | High Security Settings | Custom Security Settings |
|-------------------|--------------------------|------------------------|--------------------------|
| Password required | いいえ                      | はい                     | はい/いいえ                   |

表 3. セキュリティー設定ポリシーの値 (続き)

| ポリシー設定/フィールド  | Legacy Security Settings | High Security Settings | Custom Security Settings |
|---|--------------------------|------------------------|--------------------------|
| Complex password required   | いいえ                      | はい                     | はい/いいえ                   |
| Password expiration period (days)                                       | なし                       | 90                     | 0 - 365                  |
| Minimum password length   | なし                       | 8                      | 5 - 20                   |
| Minimum password reuse cycle  | なし                       | 5                      | 0 - 5                    |
| Minimum password change interval (hours)                                | なし                       | 24                     | 0 - 240                  |
| Maximum number of login failures (times)                                | 5                        | 5                      | 0 - 10                   |
| Lockout period after maximum login failures (minutes)                   | 2                        | 60                     | 0 - 240                  |
| Minimum different characters in passwords                               | なし                       | 2                      | 0 - 19                   |
| Factory default 'USERID' account password must be changed on next login | いいえ                      | はい                     | はい/いいえ                   |
| Force user to change password on first access                           | いいえ                      | はい                     | はい/いいえ                   |

セキュリティー設定の各フィールドの説明を以下に示します。

#### Password required

このフィールドは、パスワードのないログイン ID の作成が許可されるかどうかを示します。「**Password required**」チェック・ボックスを選択した場合、パスワードのない既存のログイン ID は、そのユーザーが次回にログインしたときにパスワードを定義する必要があります。

#### Complex password required

複合パスワードが必要な場合、パスワードは次の規則に従う必要があります。

- パスワードは、長さが 8 文字以上である必要があります。
- パスワードは、次の 4 つのカテゴリの 3 つ以上を含んでいる必要があります。
  - 1 つ以上の英小文字。
  - 1 つ以上の英大文字。
  - 1 つ以上の数字。
  - 1 つ以上の特殊文字。

- スペースまたは空白文字は使用できません。
- パスワードの中で連続して使用できる同じ文字は 3 つまでです (例えば、aaa)。
- 関連付けられているユーザー ID の繰り返しや逆読みをパスワードに使用してはなりません。

複合パスワードが必要でない場合、パスワードは次のとおりです。

- 長さが 5 文字 (または「**Minimum password length**」フィールドで指定された文字数) 以上であることが必要です。
- スペースや空白文字を含むことはできません。
- 数字を 1 つ以上含んでいる必要があります。
- ブランクでもかまいません (「**Password Required**」チェック・ボックスが使用不可の場合)。

#### **Password expiration period (days)**

このフィールドには、パスワードを変更せずに使用することが許可される、パスワードの最大使用日数が入ります。0 から 365 日までの値がサポートされます。このフィールドのデフォルト値は 0 (使用不可) です。

#### **Minimum password length**

このフィールドには、パスワードの最小の長さが入ります。このフィールドでは、5 から 20 文字までがサポートされます。「**Complex password required**」チェック・ボックスにチェック・マークが付いている場合、パスワードの最小の長さは 8 文字であることが必要です。

#### **Minimum password reuse cycle**

このフィールドには、何回前までに使用したパスワードを再使用できないようにするかを指定する回数が入ります。最大 5 回前までのパスワードを比較することができます。0 を選択すると、以前に使用したすべてのパスワードを再使用できます。このフィールドのデフォルト値は 0 (使用不可) です。

#### **Minimum password change interval (hours)**

このフィールドには、パスワードの変更から次の変更までの必要な待ち時間が入ります。0 から 240 時間までの値がサポートされます。このフィールドのデフォルト値は 0 (使用不可) です。

#### **Maximum number of login failures (times)**

このフィールドには、ログイン試行に何回失敗したら、一定期間ロックアウトされるかを指定する失敗回数が入ります。0 から 10 までの値がサポートされます。このフィールドのデフォルト値は 0 (使用不可) です。

#### **Lockout period after maximum login failures (minutes)**

このフィールドは、いずれかのユーザーからの連続した 5 回を超えるログイン失敗を検出した後に、IMM2 サブシステムがすべてのユーザーからのリモート・ログイン試行を使用不可にする時間の長さ (分単位) を指定します。

#### **Minimum different characters in passwords**

このフィールドは、新規パスワードが以前のパスワードと異なっている必要がある文字数を指定します。0 から 19 までの値がサポートされます。

### Factory default 'USERID' account password must be changed on next login

最初にログインに成功した後にデフォルトの USERID プロファイルをリセットするために、製造オプションが提供されます。このチェック・ボックスを使用可能にした場合、アカウントを使用するには、事前にデフォルトのパスワードを変更する必要があります。新規パスワードには、アクティブなすべてのパスワード実施規則が適用されます。

### Force user to change password on first access

デフォルトのパスワードで新規ユーザーをセットアップした後、このチェック・ボックスを選択すると、そのユーザーは、最初にログインするとき自己のパスワードを変更するよう強制されます。

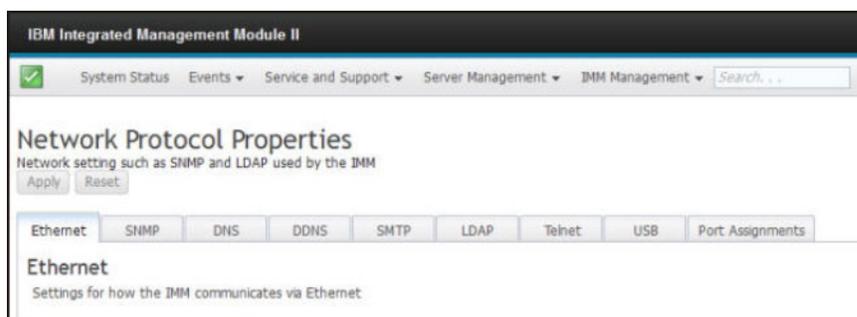
---

## ネットワーク・プロトコルの構成

「IMM Management」タブの下にある「**Network**」オプションをクリックして、ネットワーク設定を表示および設定します。

## イーサネット設定の構成

IMM2 のイーサネット設定を表示または変更するには、「**Ethernet**」タブをクリックします (次の図を参照)。



IPv4 イーサネット接続を使用するには、以下のステップを実行します。

1. 「**IPv4**」オプションを選択します。次に、対応するチェック・ボックスを選択します。

注: イーサネット・インターフェースを使用不可にすることで、外部ネットワークから IMM2 へのアクセスを防ぐことができます。

2. 「**Configure IP address settings**」リストから、以下のいずれかのオプションを選択します。
  - Obtain an IP address from a DHCP server
  - Use static IP address
3. DHCP サーバーに接続できない場合に、IMM2 がデフォルトで固定 IP アドレスを使用するようにするには、対応するチェック・ボックスを選択します。
4. 「**Static address**」フィールドに、IMM2 の IP アドレスを入力します。

注: この IP アドレスには 0 から 255 までの 4 つの整数がピリオドで区切られて入っている必要があり、スペースが含まれてはなりません。

5. 「**Subnet mask**」フィールドに、IMM2 が使用するサブネット・マスクを入力します。

注: このサブネット・マスクには 0 から 255 までの 4 つの整数がピリオドで区切られて入っている必要があり、スペースや連続したピリオドが含まれていてはなりません。デフォルトの設定値は 255.255.255.0 です。

6. 「**Default Gateway**」フィールドに、使用するネットワーク・ゲートウェイ・ルーターを入力します。

注: このゲートウェイ・アドレスには 0 から 255 までの 4 つの整数がピリオドで区切られて入っている必要があり、スペースや連続したピリオドが含まれていてはなりません。

次の図は、「Ethernet」タブを示しています。

The screenshot shows the 'Ethernet' configuration window with the 'Advanced Ethernet' tab selected. The 'Host name' field contains 'IMM2-e41f13d90631'. Under the 'IPv4' tab, the 'Enable IPv4' checkbox is checked. The 'Currently assigned IPv4 address information' section displays the following details:

|                     | Address           |
|---------------------|-------------------|
| Host name           | IMM2-e41f13d90631 |
| IP address          | 9.37.189.59       |
| Subnet mask         | 255.255.240.0     |
| Gateway address     | 9.37.176.1        |
| Domain name         | raleigh.ibm.com   |
| Primary DNS Server  | 9.0.128.50        |
| Second DNS Server   | 9.0.130.50        |
| Tertiary DNS Server | 0.0.0.0           |

The 'Configure IP address settings' section has a dropdown menu set to 'Use static IP address'. Below it, the 'Obtain IP address from DHCP server' option is selected. The 'Static address' field is set to '192.168.70.125', the 'Subnet mask' field is set to '255.255.255.0', and the 'Default gateway' field is set to '0.0.0.0'.

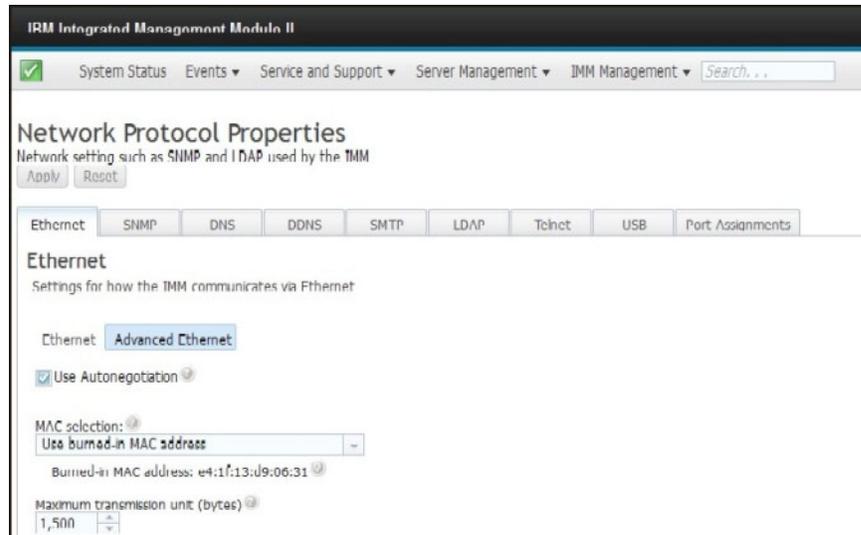
## イーサネットの詳細設定の構成

イーサネットの追加設定を行うには、「**Advanced Ethernet**」タブをクリックします。「**MAC selection**」リストから、以下のいずれかの選択項目を選択します。

- Used burned in MAC address
  - 組み込み MAC アドレス・オプションは、製造元によってこの IMM2 に割り当てられている固有な物理アドレスです。このアドレスは読み取り専用フィールドです。
- Used locally administered MAC address
  - 値を指定した場合は、ローカル管理アドレスが組み込み MAC アドレスをオーバーライドします。ローカル管理アドレスは、000000000000 から FFFFFFFF までの 16 進値である必要があります。この値は、

xx:xx:xx:xx:xx:xx の形式で指定する必要があります。ここで、x は 0 から 9 の数値です。IMM2 はマルチキャスト・アドレスの使用をサポートしません。マルチキャスト・アドレスの最初のバイトは奇数です (最下位ビットが 1 にセットされています)。したがって、最初のバイトは偶数でなければなりません。

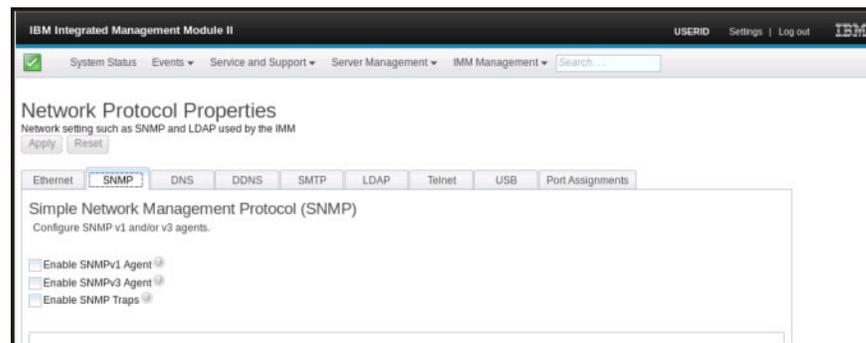
「Maximum transmission unit」フィールドには、使用するネットワーク・インターフェースでのパケットの最大伝送単位 (バイト単位) を指定します。最大伝送単位の範囲は 60 から 1500 までです。このフィールドのデフォルト値は 1500 です。次の図は、「Advanced Ethernet」タブとその関連フィールドを示しています。



## SNMP アラート設定の構成

IMM2 SNMP 設定を構成するには、以下のステップを実行します。

1. 「SNMP」タブをクリックします (次の図を参照)。



2. SNMPv1 エージェント、SNMPv3 エージェント、または SNMP トラップを使用可能にするには、対応するチェック・ボックスにチェック・マークを付けます。
3. SNMPv1 エージェントを使用可能にした場合は、ステップ 4 (73 ページ) に進みます。 SNMPv3 エージェントを使用可能にした場合は、ステップ 5 (73 ページ) に進みます。 SNMP トラップを使用可能にした場合は、ステップ 6 (73 ページ) に進みます。

4. SNMPv1 エージェントを使用可能にした場合は、以下のフィールドに入力します。
  - a. 「**Contact**」タブをクリックします。「**Contact person**」フィールドに、連絡先の個人の名前を入力します。「**Location**」フィールドに、サイト (地理座標) を入力します。
  - b. SNMP エージェントと SNMP マネージャーの間の管理関係を定義するために、「**Communities**」タブをクリックしてコミュニティをセットアップします。少なくとも 1 つのコミュニティを定義する必要があります。

**注:**

- エラー・メッセージ・ウィンドウが表示された場合は、エラー・ウィンドウにリストされるフィールドに対して必要な調整を行ってください。その後、ページの上部までスクロールし、「**Apply**」をクリックして、訂正した情報を保存します。
- この SNMP エージェントを使用可能にするには、少なくとも 1 つのコミュニティを構成する必要があります。

以下のフィールドに入力します。

- 1) 「**Community Name**」フィールドで、ある名前または認証ストリングを入力してコミュニティを指定します。
  - 2) 「**Access type**」フィールドで、アクセス・タイプを選択します。
    - 「**Trap**」を選択して、コミュニティのすべてのホストがトラップを受信できるようにします。
    - コミュニティのすべてのホストがトラップを受信し、管理情報ベース (MIB) オブジェクトを照会できるようにするには、「**Get**」を選択します。
    - コミュニティのすべてのホストがトラップを受信し、MIB オブジェクトを照会および設定できるようにするには、「**Set**」を選択します。
  - c. 「**Host Name**」または「**IP Address**」フィールドで、各コミュニティ・マネージャーのホスト名または IP アドレスを入力します。
  - d. 「**Apply**」をクリックして、加えた変更を適用します。
5. SNMPv3 エージェントを使用可能にした場合は、以下のフィールドに入力します。

- a. 「**Contact**」タブをクリックします。「**Contact person**」フィールドに、連絡先の個人の名前を入力します。「**Location**」フィールドに、サイト (地理座標) を入力します。
- b. コンソール用にローカル・ユーザー・アカウントのリストを表示するには、「**Users**」タブをクリックします。

**注:** これは、「**Users**」オプションにあるのと同じリストです。SNMPv3 アクセス権を必要とするユーザー・アカウントごとに、SNMPv3 を構成する必要があります。

- c. 「**Apply**」をクリックして、加えた変更を適用します。
6. SNMP トラップを使用可能にする場合は、「**Traps**」タブでアラート対象のイベントを構成します。

注: SNMP を構成するとき、入力されていないか誤った値が入力されている必須フィールドは、赤の X で強調表示されます。これを、必須フィールドに入力するためのガイドとして使用できます。

次の図は、SNMPv1 エージェントを構成するときの「SNMP」タブを示しています。

Network Protocol Properties  
Network setting such as SNMP and LDAP used by the IMM  
Apply Reset

Ethernet **SNMP** DNS DDNS SMTP LDAP Telnet USB Port Assignments

Simple Network Management Protocol (SNMP)  
Configure SNMP v1 and/or v2 agents.

Enable SNMPv1 Agent  
 Enable SNMPv3 Agent  
 Enable SNMP Traps

Contact Users **Communities** Traps

SNMPv1 Communities  
Select communities to configure. At least one community must be configured.

Community 1  Enable Community 2  Enable Community 3

Community name: [ ] X  
Access type: Get  
Allow any host to query MIB objects:   
 Accept IPv4 Hosts  
 Accept IPv6 Hosts

## DNS の構成

IMM2 のドメイン・ネーム・システムの設定を表示または変更するには、「DNS」タブをクリックします。「Use additional DNS address servers」チェック・ボックスをクリックした場合は、ネットワーク上にある最大 3 台までのドメイン・ネーム・システム・サーバーの IP アドレスを指定します。各 IP アドレスは、0 から 255 までの整数をピリオドで区切って指定する必要があります (次の図を参照)。

IBM Integrated Management Module II  
System Status Events Service and Support Server Management IMM Management Search ... USERID Settings

Network Protocol Properties  
Network setting such as SNMP and LDAP used by the IMM  
Apply Reset

Ethernet SNMP **DNS** DDNS SMTP LDAP Telnet USB Port Assignments

Domain Name System (DNS)  
Specify whether additional DNS server addresses should be included in the search order for hostname-to-IP address resolution. DNS lookup is always enabled, and other DNS addresses may be automatically assigned by the DHCP server when DHCP is in use.

In order for the 'Additional DNS addresses' to be enabled, at least one must be non-zero. The additional DNS servers are added to the top of the search list, so the hostname lookup is done on these servers before it occurs on a DNS server that is assigned automatically by a DHCP server.

Preferred DNS address type: IPv6  
 Use additional DNS address servers (at least one must be non-zero)

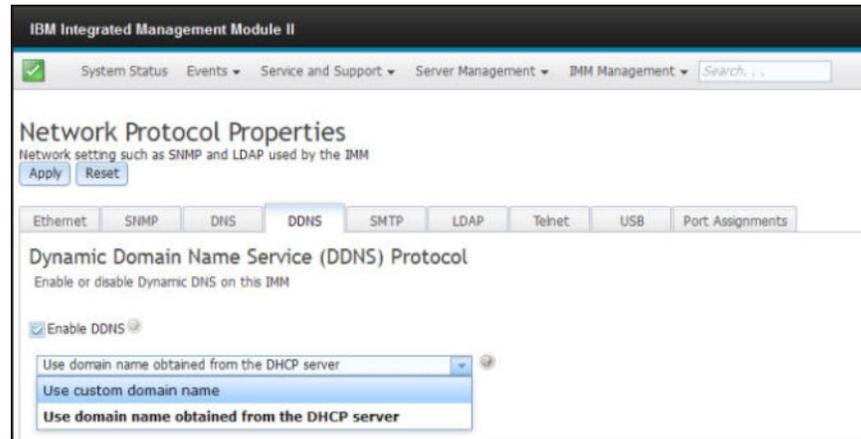
|           | IPv4      | IPv6 |
|-----------|-----------|------|
| Primary   | 0.0.0.0 X | ::   |
| Secondary | 0.0.0.0   | ::   |
| Tertiary  | 0.0.0.0   | ::   |

## DDNS の構成

IMM2 Dynamic Domain Name System の設定を表示または変更するには、「DDNS」タブをクリックします。DDNS を使用可能にするには、「Enable DDNS」チェック・ボックスをクリックします。DDNS を使用可能にすると、IMM2

はドメイン・ネーム・サーバーに対して、構成済みのホスト名、アドレス、またはドメイン・ネーム・サーバーに保管されているその他の情報のアクティブなドメイン・ネーム・サーバー構成をリアルタイムに変更するように通知します。

項目リストからオプションを選択し、IMM2 のドメイン名の選択方法を選択します(次の図を参照)。



## SMTP の構成

IMM2 の SMTP 設定を表示または変更するには、「SMTP」タブをクリックします。SMTP 設定を表示または変更するには、以下のフィールドに入力します。

### IP address or host name

SMTP サーバーのホスト名を入力します。このフィールドで IP アドレスを指定するか、DNS が使用可能にされて構成されている場合は SMTP サーバーのホスト名を指定します。

**Port** SMTP サーバーのポート番号を指定します。デフォルト値は 25 です。

### Test connection

「Test Connection」をクリックすると、SMTP 設定が正しいか確認するために、テスト E メールが送信されます。

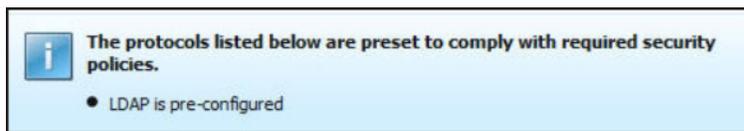
次の図は、「SMTP」タブを示しています。



## LDAP の構成

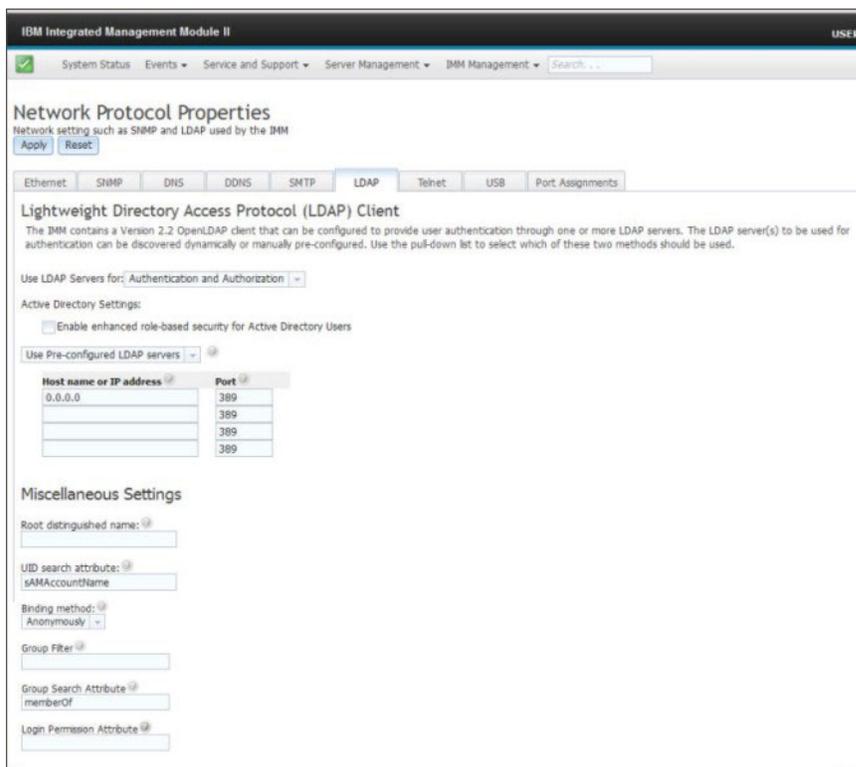
IMM2 の LDAP クライアントの設定を表示または変更するには、「LDAP」タブをクリックします。

注: IBM Flex System では、IMM2 は CMM 上で稼働する LDAP サーバーを使用するようにセットアップされます。LDAP 設定を変更できないことを注意喚起する情報メッセージが表示されます (次の図を参照)。



LDAP サーバーを使用すると、IMM2 は、ローカル・ユーザー・データベースを検索するのではなく、LDAP サーバー上の LDAP ディレクトリーを照会または検索することにより、ユーザーを認証できます。IMM2 は中央 LDAP サーバーを介して、リモート側ですべてのユーザー・アクセスを認証できます。LDAP サーバー上で検出された情報に応じて、権限レベルを割り当てることができます。また、LDAP を使用して、通常のユーザー (パスワード検査) 認証の他に、ユーザーおよび IMM2 をグループに割り当ててグループ認証を行うこともできます。例えば、IMM2 を 1 つ以上のグループに関連付けることができ、ユーザーはこの IMM2 に関連付けられている少なくとも 1 つのグループに属している場合のみ、グループ認証にパスします。

次の図は、「LDAP」タブを示しています。



事前構成された LDAP サーバーを使用するには、以下のフィールドに入力します。

#### LDAP server configuration item list

項目リストから「**Use Pre-Configured LDAP Server**」を選択します。各サーバーのポート番号はオプションです。このフィールドを空白のまま残した場合、デフォルト値の 389 が、非セキュア LDAP 接続に使用されます。セキュア接続の場合、デフォルト値は 636 です。少なくとも 1 つの LDAP サーバーを構成する必要があります。

#### Root distinguished name

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

#### UID search attribute

バインディング方式が「**Anonymously**」または「**With Configured Credentials**」に設定されている場合、LDAP サーバーへの初回バインドの直後に、ユーザーの DN、ログイン許可、およびグループ・メンバーシップなど、ユーザーに関する固有の情報を取得する検索要求が行われます。この検索要求では、そのサーバー上でユーザー ID を表す属性名を指定する必要があります。この属性名は、このフィールドで構成されます。アクティブ・ディレクトリー・サーバーでは、属性名は通常「**sAMAccountName**」です。Novell eDirectory サーバーおよび OpenLDAP サーバーでは、この属性名は「**uid**」です。このフィールドを空白のまま残した場合、デフォルトは「**uid**」です。

#### Binding method

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

- Anonymously
  - DN やパスワードを使用せずにバインドするには、この方式を使用します。ほとんどのサーバーは特定のユーザー・レコードに対する検索要求を許可しないように構成されているため、この方式を使用しないことを強く推奨します。
- With Configured Credentials
  - 構成済みの DN およびパスワードを使用してバインドするには、この方式を使用します。
- With Login Credentials
  - ログイン・プロセスで提供された資格情報を使用してバインドするには、この方式を使用します。DN、完全修飾ドメイン・ネーム、あるいは IMM2 で構成された **UID 検索属性**と一致したユーザー ID から、ユーザー ID を提供することができます。初回のバインドが成功すると、LDAP サーバーでログインするユーザーに属するエントリーの検索が実行されます。必要であれば、2 回目のバインドが試行されます。今回は、ユーザーの LDAP レコードから取得された DN と、ログイン・プロセスで入力されたパスワードが使用されます。この試行が失敗すると、ユーザーはアクセスを拒否されます。2 回目のバイン

ドが実行されるのは、「Anonymous」か「With Configured Credentials」のバインディング方式が使用されている場合だけです。

### Group Filter

「Group Filter」フィールドは、グループ認証に使用されます。グループ認証は、ユーザーの資格情報が正常に確認された後に試行されます。グループ認証が失敗すると、ユーザーのログオン試行は拒否されます。グループ・フィルターが構成されている場合、サービス・プロセッサがどのグループに属しているかを指定するのに使用されます。これは、グループ認証が成功するように構成されたグループの少なくとも 1 つにユーザーが属している必要があることを意味します。「Group Filter」フィールドがブランクのまま残された場合、グループ認証は自動的に成功します。グループ・フィルターが構成されている場合は、リスト内のグループの少なくとも 1 つがユーザーが属しているグループと一致しているか、マッチングが試行されます。一致するグループがない場合、ユーザーは認証に失敗し、アクセスは拒否されます。少なくとも 1 つのグループが一致する場合は、グループ認証は成功します。

この比較は大/小文字を区別します。フィルターは 511 文字が上限で、1 つ以上のグループ名から構成することができます。複数のグループ名を区切る場合は、コロン (:) 文字を使用する必要があります。先頭および末尾のスペースは無視されますが、それ以外のスペースはすべてグループ名の一部として処理されます。グループ名でのワイルドカードの使用を許可するか許可しないかを選択することができます。特定のグループ名 (例えば、IMMWest)、すべてに一致するワイルドカードとして使用されたアスタリスク (\*)、または接頭部付きワイルドカード (例えば、IMM\*) をフィルターとして使用することができます。デフォルトのフィルターは IMM\* です。ご使用のインストール済み環境のセキュリティー・ポリシーでワイルドカードの使用が禁止されている場合、ワイルドカードの使用を許可しないことを選択できます。その場合、ワイルドカード文字 (\*) はワイルドカードでなく通常の文字として扱われます。グループ名は、完全 DN あるいは cn 部分として指定することができます。例えば、DN が `cn=adminGroup,dc=mycompany,dc=com` であるグループは、実際の DN または `adminGroup` を使用して指定することができます。

Active Directory 環境では、グループ・メンバーシップのネストがサポートされます。例えば、ユーザーが GroupA および GroupB のメンバーで、GroupA が GroupC のメンバーである場合、ユーザーは GroupC のメンバーでもあると見なされます。ネストされた検索は、128 個のグループを検索すると停止します。1 つのレベル内のグループが、その下位レベルのグループの前に検索されます。ループは検出されません。

### Group Search Attribute

Active Directory 環境または Novell eDirectory 環境では、「Group Search Attribute」フィールドは、ユーザーの所属先グループを識別するために使用される属性名を指定します。Active Directory 環境では、この属性名は「`memberOf`」です。eDirectory 環境では、この属性名は「`groupMembership`」です。OpenLDAP サーバー環境では、通常、ユーザーは「`objectClass`」が `PosixGroup` であるグループに割り当てられます。そのコンテキストでは、このフィールドは特定の `PosixGroup` のメンバーを識

別するために使用する属性名を指定します。この属性名は「**memberUid**」です。このフィールドがブランクのまま残されると、フィルターの属性名はデフォルトの **memberOf** になります。

#### Login Permission Attribute

ユーザーが LDAP サーバーを通じて正常に認証された場合、ユーザーのログイン許可を取り出す必要があります。ログイン許可を検索するには、サーバーに送信される検索フィルターでログイン許可に関連付けられている属性名を指定する必要があります。「**Login Permission Attribute**」フィールドは、その属性名を指定します。このフィールドをブランクのまま残した場合、ユーザーにはデフォルトの読み取り専用許可が割り当てられ、ユーザーはユーザー認証とグループ認証に合格するものと想定されます。

LDAP サーバーから返される属性値は、キーワード・ストリング **IBMRBSPermissions=** を使用して検索されます。このキーワード・ストリングの直後には、12 個の連続した 0 または 1 として入力されたビット・ストリングが続いている必要があります。各ビットは、各機能の設定を表します。ビットは、その位置に応じて番号付けられています。左端のビットはビット位置 0 で、右端のビットはビット位置 11 です。あるビット位置の値が 1 の場合、そのビット位置に関連付けられた機能は使用可能になります。あるビット位置の値が 0 の場合、そのビット位置に関連付けられた機能は使用不可になります。

ストリング **IBMRBSPermissions=010000000000** は有効な例です。

「**IBMRBSPermissions=**」キーワードを使用すると、このフィールドの任意の位置に配置することが可能になります。これにより、LDAP 管理者は既存の属性を再使用することが可能になるため、LDAP スキーマの拡張を防ぎます。また、これによって属性を元の目的で使うことができるようになります。このフィールドの任意の場所にキーワード・ストリングを追加することができます。使用する属性は、自由な形式のストリングが可能です。属性が正常に取り出された場合、LDAP サーバーから返された値は、以下の表の説明に従って解釈されます。

表 4. 許可ビット

| ビット位置 | 機能             | 説明  |
|-------|----------------|---|
| 0     | 常に拒否           | ユーザーは常に認証に失敗します。この機能は、特定のユーザーまたは特定のグループと関連付けられているユーザーをブロックするために使用されます。                    |
| 1     | スーパーバイザー・アクセス権 | ユーザーに管理者特権が付与されます。ユーザーは、すべての機能に対して読み取り/書き込みアクセス権を持ちます。このビットを設定した場合、他のビットを個別に設定する必要はありません。 |

表4. 許可ビット (続き)

| ビット位置 | 機能                           | 説明  |
|-------|------------------------------|---|
| 2     | 読み取り専用アクセス権                  | ユーザーは読み取り専用のアクセス権を持ち、保守手順 (例えば、再始動、リモート・アクション、またはファームウェア更新など) や変更操作 (例えば、保存、消去、またはリストア機能など) を行うことはできません。ビット位置 2 と他のすべてのビットは相互に排他的で、ビット位置 2 の優先順位が最下位です。他のいずれかのビットが設定されている場合、このビットは無視されます。 |
| 3     | Networking and Security      | ユーザーは、「Security」、「Network Protocols」、「Network Interface」、「Port Assignments」、および「Serial Port」の構成を変更できます。   |
| 4     | ユーザー・アカウント管理                 | このユーザーは、ユーザーの追加、変更、または削除を行うことができ、「Login Profiles」ウィンドウで「Global Login」設定を変更できます。   |
| 5     | リモート・コンソール・アクセス権             | このユーザーは、リモート・サーバーのリモート・サーバー・コンソールにアクセスすることができます。  |
| 6     | リモート・コンソールおよびリモート・ディスク・アクセス権 | このユーザーは、リモート・サーバーのリモート・サーバー・コンソールおよびリモート・ディスク機能にアクセスすることができます。  |
| 7     | リモート・サーバーの電源/再始動アクセス権        | ユーザーは、リモート・サーバーの電源オン機能と再始動機能にアクセスできます。  |
| 8     | アダプターの基本構成                   | ユーザーは、「System Settings」ウィンドウおよび「Alerts」ウィンドウで構成パラメーターを変更できます。   |
| 9     | イベント・ログを消去する権限               | このユーザーはイベント・ログを消去することができます。<br><b>注:</b> すべてのユーザーがイベント・ログを表示できますが、ログを消去するには、ユーザーにこのレベルの権限が必要です。   |

表 4. 許可ビット (続き)

| ビット位置 | 機能         | 説明   |
|-------|------------|--|
| 10    | アダプターの拡張構成 | ユーザーは、IMM2 を構成するときに何も制約を受けません。さらに、ユーザーは IMM2 に対する管理アクセス権限を持ちます。ユーザーは、ファームウェア・アップグレード、PXE ネットワーク・ブート、IMM2 の出荷時デフォルト値のリストア、構成ファイルに入っているアダプター構成の変更とリストア、および IMM2 の再始動とリセットなどの拡張機能を実行することができます。  |
| 11    | 予約済み       | <p>このビット位置は、将来の使用のために予約済みです。セットされたビットがない場合、ユーザーは読み取り専用権限を持ちます。ユーザー・レコードから直接検索されるログイン許可には優先順位があります。</p> <p>ログイン許可属性がユーザーのレコードに入っていない場合は、そのユーザーが属するグループから許可を取り出そうと試みられます。これは、グループ認証フェーズの一部として行われます。このユーザーには、すべてのグループのすべてのビットの包含 OR が割り当てられます。</p> <p>読み取り専用アクセス権限ビット (位置 2) は、他のすべてのビットがゼロに設定された場合にのみ設定されます。「常に拒否」ビット (位置 0) がいずれかのグループに設定されている場合、そのユーザーはアクセスを拒否されます。「常に拒否」ビット (位置 0) は、常に他のすべてのビットに優先します。</p> |

## Telnet の構成

IMM2 の Telnet 設定を表示または変更するには、「**Telnet**」タブを選択します。Telnet 設定を表示または変更するには、以下のフィールドに入力します。

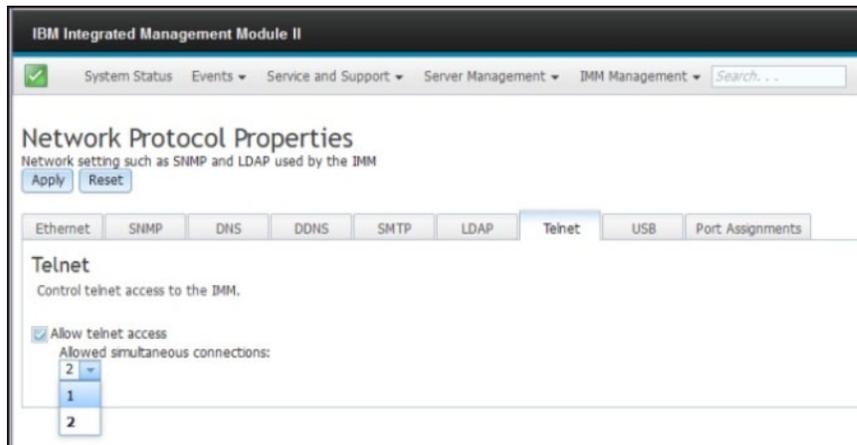
### Allow telnet access

IMM2 による Telnet アクセスが必要かどうかを選択するには、チェック・ボックスにチェック・マークを付けます。

### Allowed simultaneous connections

同時に許可する Telnet 接続の数を選択するには、「**Allowed simultaneous connections**」リストを使用します。

次の図は、「Telnet」タブを示しています。

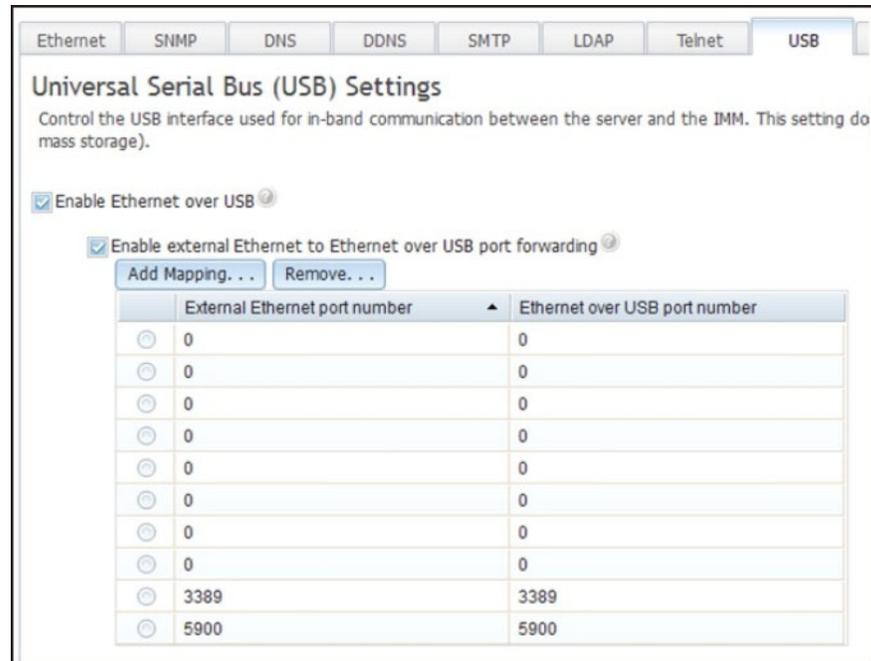


## USB の構成

IMM2 の USB 設定を表示または変更するには、「**USB**」タブを選択します。USB インバンド・インターフェース、あるいは LAN over USB は、IMM2 へのインバンド通信に使用されます。IMM2 Lan over USB インターフェースを使用可能または使用不可に設定するには、「**Enable Ethernet over USB**」チェック・ボックスをクリックします。

**重要:** USB インバンド・インターフェースを使用不可にすると、Linux あるいは Windows フラッシュ・ユーティリティを使用する IMM2 ファームウェア、サーバー・ファームウェア、および DSA ファームウェアのインバンド更新を実行することはできません。USB インバンド・インターフェースが使用不可にされている場合は、「Server Management」タブの下にある「Firmware Server」オプションを使用してファームウェアを更新します。USB インバンド・インターフェースを使用不可にする場合は、サーバーの予期しない再始動を防ぐために、ウォッチドッグ・タイムアウトも使用不可にしてください。

次の図は、「USB」タブを示しています。



外部イーサネット・ポート番号から USB 上のイーサネット・ポート番号へのマッピングを制御するには、「**Enable external Ethernet to Ethernet over USB port forwarding**」チェック・ボックスをクリックして、転送するポートのマッピング情報を入力します。

## ポート割り当ての構成

IMM2 のポート割り当てを表示または変更するには、「**Port Assignments**」タブを選択します。ポート割り当てを表示または変更するには、以下のフィールドに入力します。

**HTTP** このフィールドで、IMM2 の HTTP サーバーのポート番号を指定します。デフォルト値は 80 です。有効なポート番号の値は、1 から 65535 までです。

### HTTPS

このフィールドで、Web インターフェースの HTTPS Secure Sockets Layer (SSL) トラフィックに使用するポート番号を指定します。デフォルト値は 443 です。有効なポート番号の値は、1 から 65535 までです。

### Telnet CLI

このフィールドで、レガシー CLI が Telnet サービスを介してログインするためのポート番号を指定します。デフォルト値は 23 です。有効なポート番号の値は、1 から 65535 までです。

### SSH Legacy CLI

このフィールドで、レガシー CLI が SSH プロトコルを介してログインするために構成されたポート番号を指定します。デフォルト値は 22 です。

### SNMP Agent

このフィールドで、IMM2 上で稼働する SNMP エージェントのポート番号を指定します。デフォルト値は 161 です。有効なポート番号の値は、1 から 65535 までです。

### SNMP Traps

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

### Remote Control

このフィールドで、Remote Control 機能がサーバー・コンソールの表示およびサーバー・コンソールとの対話に使用するポート番号を指定します。ラック・マウント型のサーバーおよびタワー型のサーバーでのデフォルト値は 3900 です。

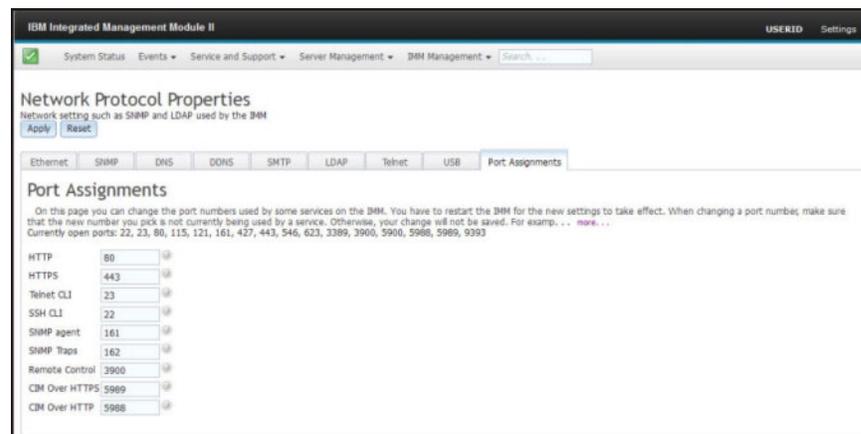
### CIM over HTTP

このフィールドで、CIM over HTTP のポート番号を指定します。デフォルト値は 5988 です。

### CIM over HTTPS

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

次の図は、「Port Assignments」タブを示しています。



## セキュリティ設定の構成

IMM2 のセキュリティのプロパティ、状況、および設定にアクセスし、それらを構成するには、「IMM Management」タブの下にある「**Security**」オプションをクリックします (次の図を参照)。

加えた変更を適用するには、「IMM Security」ウィンドウの左上にある「**Apply**」ボタンをクリックする必要があります。加えた変更をリセットするには、「**Reset Values**」ボタンをクリックする必要があります。

| IMM Management ▾ <input type="text" value="Search..."/> |   |
|---|---|
| <b>IMM Properties</b>                                   | Various properties and settings related to the IMM  |
| <b>Users</b>  | Create and modify user accounts and group profiles that will have access to the IMM console |
| <b>Network</b>  | Network settings such as SNMP and LDAP used by the IMM                                      |
| <b>Security</b>   | Configure security protocols such as SSL and SSH  |
| <b>IMM Configuration</b>                                | View a summary of the current configuration settings.                                       |
| <b>Restart IMM</b>                                      | Restart the IMM. Typically only needed when experiencing problems with the IMM              |
| <b>Reset IMM to factory defaults...</b>                 | Sets all current configuration settings back to default values                              |
| <b>Activation Key Management</b>                        | Add and remove activation keys for additional functionality                                 |

## HTTPS プロトコルの構成

デフォルトの HTTP プロトコルでなく、より安全な HTTPS プロトコルを使用するよう IMM2 Web インターフェースを構成するには、「**HTTPS Server**」タブをクリックします。

注:

- 一度に 1 つのプロトコルだけを使用可能にすることができます。
- このオプションを使用可能にすると、SSL 証明書の追加構成が必要になります。
- プロトコルを変更した場合は、IMM2 Web サーバーを再始動する必要があります。

SSL については、90 ページの『SSL の概要』を参照してください。次の図は、「HTTPS Server」タブを示しています。



注: 一部のサーバーでは、IMM2 セキュリティー・レベルを別の管理システムで制御できる場合があります。そのような環境では、IMM2 Web インターフェースでの上記のアクションを使用不可にすることができます。

## HTTPS 証明書の処理

HTTPS 証明書の処理には、「Actions」メニューにあるオプションを使用します。使用不可になっているオプションを使用可能にするには、最初に別のアクションを実行することが必要な場合もあります。HTTPS 証明書を処理している間は、HTTPS サーバーを使用不可にしてください。証明書の処理について詳しくは、90 ページの『SSL 証明書の処理』を参照してください。

注: 証明書の処理をセットアップした後、変更を有効にするために IMM2 を再始動する必要があります。

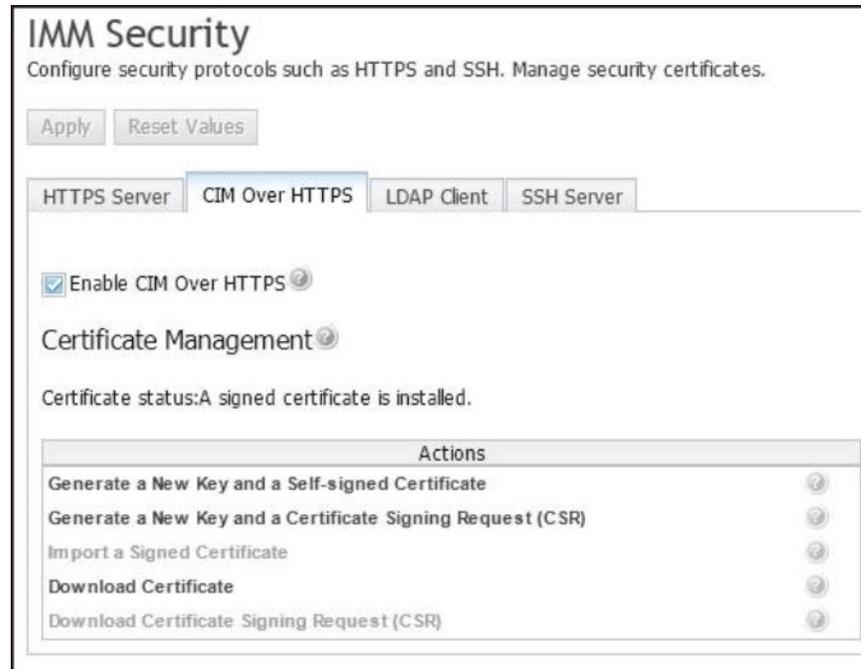
## CIM over HTTPS プロトコルの構成

デフォルトの CIM over HTTP プロトコルでなく、より安全な CIM over HTTPS プロトコルを使用するよう IMM2 Web インターフェースを構成するには、「CIM over HTTPS」タブをクリックします。

注:

- 一度に 1 つのプロトコルだけを使用可能にすることができます。
- このオプションを使用可能にすると、SSL 証明書の追加構成が必要になります。
- プロトコルを変更した場合は、IMM2 Web サーバーを再始動する必要があります。

SSL について詳しくは、90 ページの『SSL の概要』を参照してください。次の図は「CIM over HTTPS」タブを示しています。



## CIM over HTTPS 証明書の処理

CIM over HTTPS 証明書の処理には、「Actions」メニューにあるオプションを使用します。使用不可になっているオプションを使用可能にするには、最初に別のアクションを実行することが必要な場合があります。証明書の処理について詳しくは、90 ページの『SSL 証明書の処理』を参照してください。

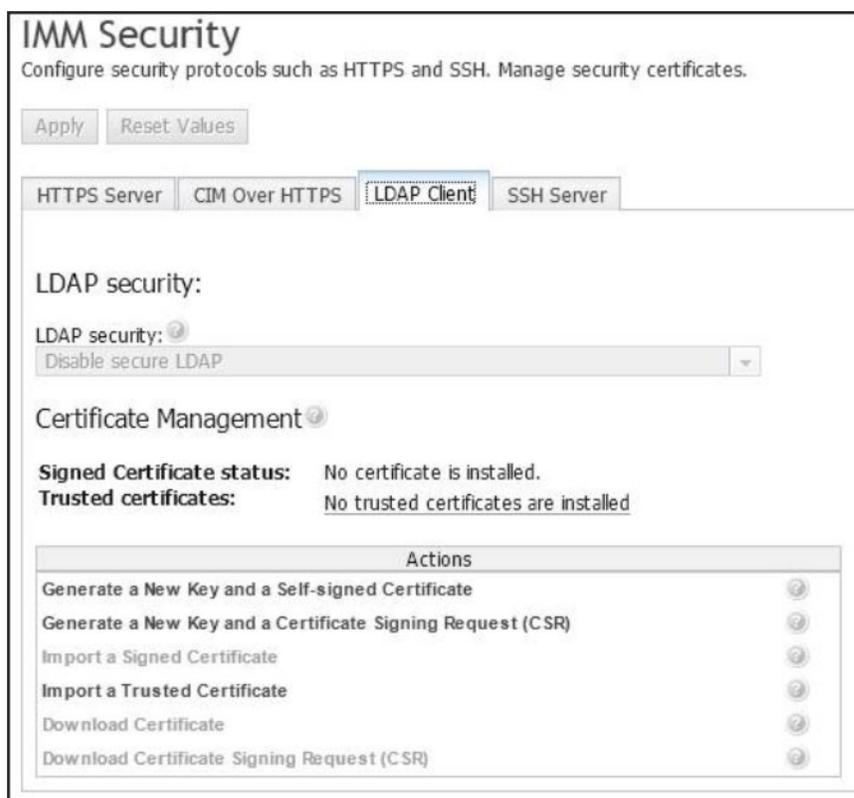
注: 証明書の処理をセットアップした後、変更を有効にするために IMM2 を再始動する必要があります。

## LDAP クライアント・プロトコルの構成

デフォルトの LDAP プロトコルよりも安全な、SSL を介した LDAP プロトコルを使用するには、「LDAP Client」オプションをクリックします。

注: このオプションを使用可能にすると、SSL 証明書の追加構成が必要になります。

SSL について詳しくは、90 ページの『SSL の概要』を参照してください。次の図は、「LDAP Client」タブを示しています。

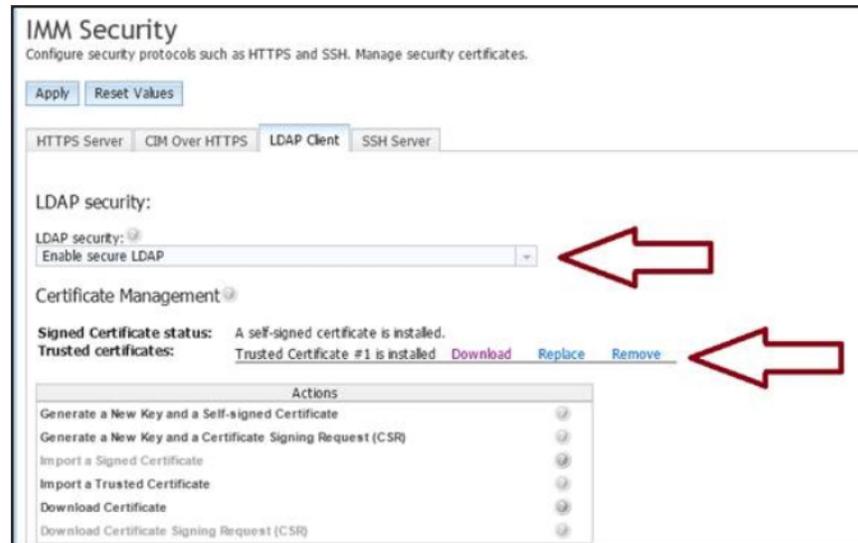


## セキュア LDAP クライアント証明書の処理

SSL を介した LDAP 証明書の処理には、「Actions」メニューにあるオプションを使用します。使用不可になっているオプションを使用可能にするには、最初に別のアクションを実行することが必要な場合もあります。HTTPS 証明書を操作している間は、HTTPS サーバーを使用不可にしてください。証明書の処理について詳しくは、90 ページの『SSL 証明書の処理』を参照してください。トラステッド証明書をインストールした後、次の図に示すように、SSL を介した LDAP を使用可能にすることができます。

### 注:

- IMM2 に対する変更は、即時に有効になります。
- 使用する LDAP サーバーに IMM2 セキュア LDAP クライアントとの互換性を持たせるためには、そのサーバーが Secure Socket Layer 3 (SSL3) またはトランスポート層セキュリティ (TLS) をサポートしている必要があります。



## セキュア・シェル・サーバーの構成

デフォルトの Telnet プロトコルでなく、より安全な SSH プロトコルを使用するよう IMM2 Web インターフェースを構成するには、「SSH Server」タブをクリックします。

注:

- このオプションを使用するのに、証明書管理は必要ありません。
- IMM2 は、最初に SSH サーバー鍵を作成します。新規の SSH サーバー鍵を生成する場合は、「Actions」メニューで「**Generate SSH Server Private Host Key**」をクリックします。
- このアクションを完了した後、変更を有効にするために IMM2 を再始動する必要があります。

「SSH Server」タブを次の図に示します。



## SSL の概要

SSL は、通信プライバシーを提供するセキュリティー・プロトコルです。SSL を使用したクライアント/サーバー・アプリケーションでは、盗聴、不正操作、およびメッセージの偽造が防止されるように設計された方法で通信を行うことができます。IMM2 は、例えば、セキュア Web サーバー (HTTPS)、セキュア LDAP 接続 (LDAPS)、CIM over HTTPS、および SSH サーバーなど、さまざまなタイプの接続に SSL サポートを使用するように構成できます。SSL の設定は、「IMM Management」タブの下にある「Security」オプションから表示または変更することができます。SSL を使用可能あるいは使用不可にしたり、SSL で要求される証明書を管理したりすることもできます。

## SSL 証明書の処理

SSL は、自己署名証明書と一緒に使用するか、第三者認証局によって署名された証明書と一緒に使用することができます。SSL の使用には、自己署名証明書の使用が最も単純な方法ですが、この方法では小さなセキュリティー・リスクが発生します。そのリスクは、SSL クライアントと SSL サーバーの間で試みられる最初の接続で、SSL クライアントに SSL サーバーの ID を検証する手段がないために発生します。例えば、第三者が IMM2 Web サーバーの偽名を使用し、実際の IMM2 Web サーバーとユーザーの Web ブラウザーの間で送受信されるデータを傍受することが可能です。ブラウザーと IMM2 の間の初回接続時に、自己署名証明書がブラウザーの証明書ストアにインポートされると、(初回接続で攻撃により暗号漏えいされなかったことを前提として) その後のすべての通信はそのブラウザーではセキュアです。

より完全なセキュリティーを実現するには、認証局 (CA) が署名する証明書を使用できます。署名付き証明書を取得するには、「Actions」メニューで「**Generate a New Key and a Certificate Signing Request (CSR)**」をクリックします。次に、証明書署名要求 (CSR) を CA に送信して、最終的な証明書を取得する手配を行う必要があります。証明書を受信したら、「Actions」メニューで「**Import a Signed Certificate**」をクリックし、証明書を IMM2 にインポートします。

CA の機能は、IMM2 の ID を検査することです。証明書には、CA および IMM2 のデジタル署名が含まれます。既知の CA が証明書を発行する場合、または CA の証明書が既に Web ブラウザーにインポートされている場合、ブラウザーは証明書を検査することができ、確実に IMM2 の Web サーバーを識別できます。

IMM2 には、HTTPS サーバー、CIM over HTTPS、およびセキュア LDAP クライアントに使用する証明書が必要です。さらに、セキュア LDAP クライアントには、1 つ以上のトラステッド証明書もインポートする必要があります。トラステッド証明書は、セキュア LDAP クライアントが LDAP サーバーを確実に識別するために使用されます。トラステッド証明書は、LDAP サーバーの証明書に署名した CA の証明書です。LDAP サーバーが自己署名証明書を使用する場合、トラステッド証明書を LDAP サーバー自体の証明書とすることもできます。構成の中で複数の LDAP サーバーを使用する場合は、追加のトラステッド証明書をインポートする必要があります。

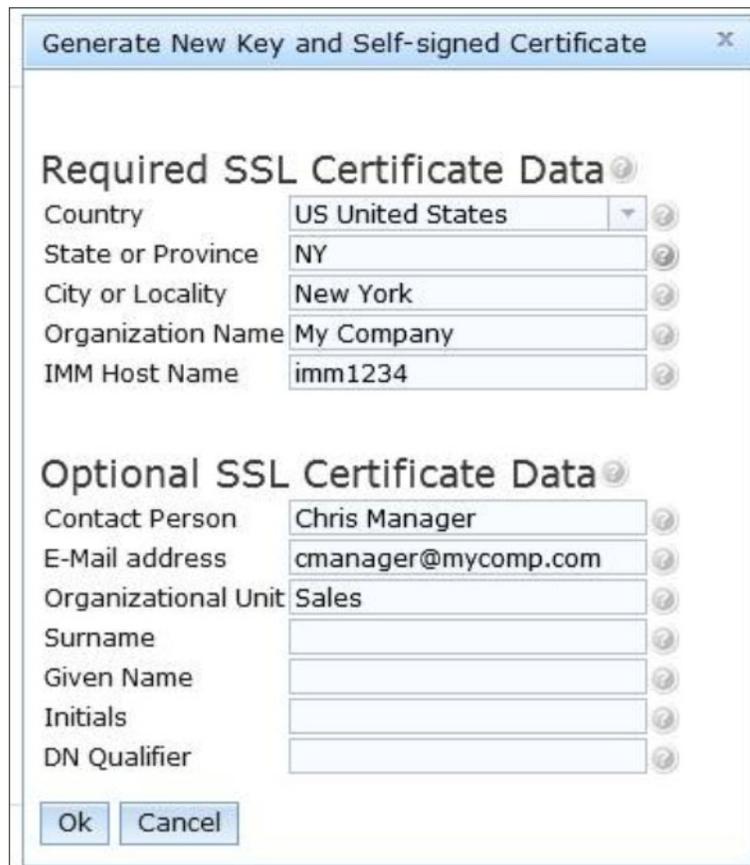
## SSL 証明書管理

IMM2 証明書を管理するときは、アクションのリスト、またはそのサブセットが提示されます (次の図を参照)。



証明書が現在インストール済みである場合は、「Actions」メニューの「**Download Certificate**」アクションを使用して、現在インストール済みの証明書または CSR をダウンロードすることができます。ぼかし表示された証明書は、現在インストール済みではありません。セキュア LDAP クライアントでは、ユーザーはトラステッド証明書をインポートする必要があります。「Actions」メニューで「**Import a Trusted Certificate**」をクリックします。CSR の生成後、「Actions」メニューで「**Import a Signed Certificate**」をクリックします。

いずれかの「Generate」アクションを実行すると、「Generate New Key and Self-signed Certificate」ウィンドウが表示されます (次の図を参照)。



「Generate New Key and Self-signed Certificate」ウィンドウには、必須フィールドとオプション・フィールドへの入力を促すプロンプトが出ます。必須フィールドには、必ず入力する必要があります。情報を入力したら、「**Ok**」をクリックしてタスクを完了します。「Certificate Generated」ウィンドウが開きます (次の図を参照)。



---

## IMM の構成の復元と変更

以下のアクションを実行するオプションについては、「IMM Management」タブから「**IMM Configuration**」オプションを選択します。

- IMM2 構成の要約の表示
- IMM2 構成のバックアップまたはリストア
- バックアップまたはリストアの状況表示
- IMM2 構成の出荷時デフォルト設定へのリセット
- IMM2 初期セットアップ・ウィザードへのアクセス

---

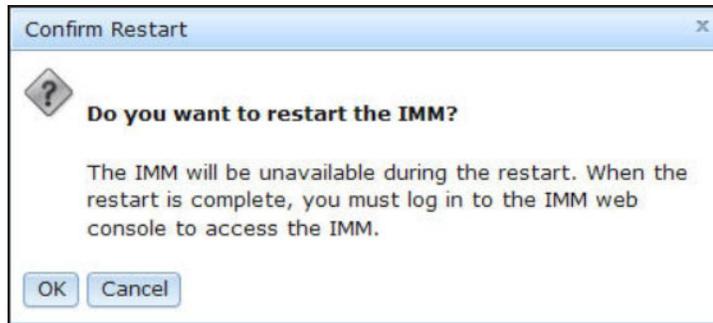
## IMM2 の再始動

IMM2 を再始動するには、「IMM Management」タブから「**Restart IMM**」オプションを選択します。この機能は、監視許可権限を持つユーザーだけが実行できます。イーサネット接続が一時的に除去された場合、IMM2 Web インターフェースにアクセスするには、IMM2 にログインする必要があります。

IMM2 を再始動するには、次の手順に従ってください。

1. IMM2 にログインします。詳しくは、10 ページの『IMM2 へのログイン』を参照してください。
2. 「**IMM Management**」タブをクリックし、次に「**Restart IMM**」をクリックします。
3. 「Confirm Restart」ウィンドウで「**OK**」ボタンをクリックします。IMM2 が再始動されます。

次の図は、「Confirm Restart」ウィンドウを示しています。



IMM2 を再始動すると、TCP/IP 接続またはモデム接続は破壊されます。

次の図は、IMM2 が再始動されるときに表示される通知ウィンドウを示しています。



4. IMM2 Web インターフェースを使用するために、IMM2 に再びログインします (手順については、10 ページの『IMM2 へのログイン』を参照してください)。

---

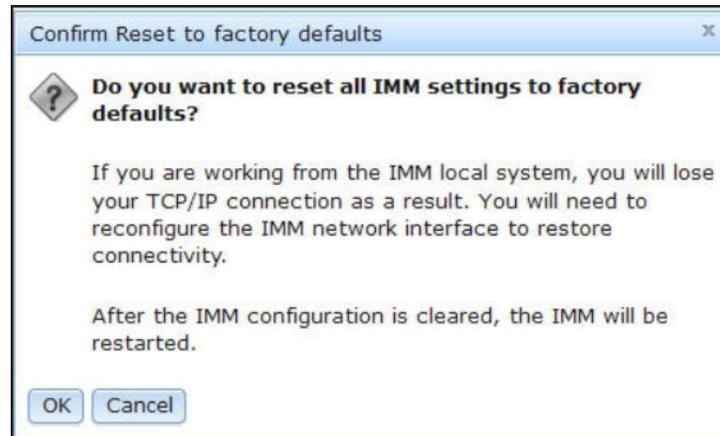
## IMM2 の出荷時のデフォルト値へのリセット

IMM2 を出荷時のデフォルト設定に復元するには、「IMM Management」タブから「Reset IMM to factory defaults...」オプションを選択します。この機能は、監視許可権限を持つユーザーだけが実行できます。イーサネット接続が一時的に除去された場合、IMM2 Web インターフェースにアクセスするには、IMM2 にログインする必要があります。

**重要:** 「Reset IMM to factory defaults」オプションを使用した場合、IMM2 に加えたすべての変更が失われます。

IMM2 の出荷時のデフォルト値を復元するには、以下のステップを実行します。

1. IMM2 にログインします。詳しくは、10 ページの『IMM2 へのログイン』を参照してください。
2. 「IMM Management」タブをクリックし、次に、「IMM Reset to factory defaults...」をクリックします。
3. 「Confirm Reset to factory defaults」ウィンドウで、「OK」ボタンをクリックします (次の図を参照)。



注: IMM2 構成が完了した後、IMM2 は再始動されます。これがローカル・サーバーである場合は、TCP/IP 接続が破壊されるので、接続をリストアするためにネットワーク・インターフェースを再構成する必要があります。

4. IMM2 Web インターフェースを使用するには、IMM2 に再びログインします (手順については、10 ページの『IMM2 へのログイン』を参照してください)。
5. 接続をリストアするために、ネットワーク・インターフェースを再構成します。

---

## アクティベーション管理キー

IMM2 およびサーバーの Features on Demand (FoD) のオプション機能のアクティベーション・キーを管理するには、「IMM Management」タブから「**Activation Key Management**」オプションをクリックします。FoD アクティベーション・キーの管理については、141 ページの『第 7 章 Features on Demand』を参照してください。

## 第 5 章 サーバー状況のモニター

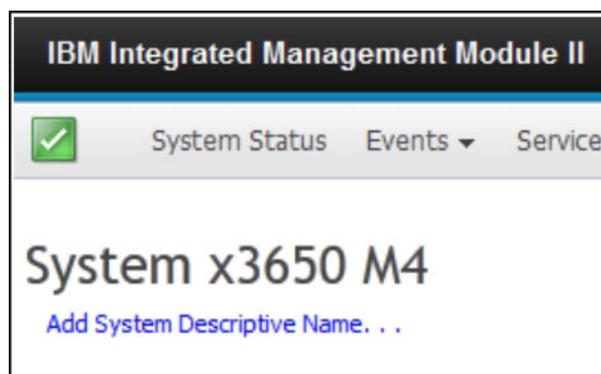
この章では、アクセス先のサーバーの情報を表示およびモニターする方法について説明します。

### システム状況の表示

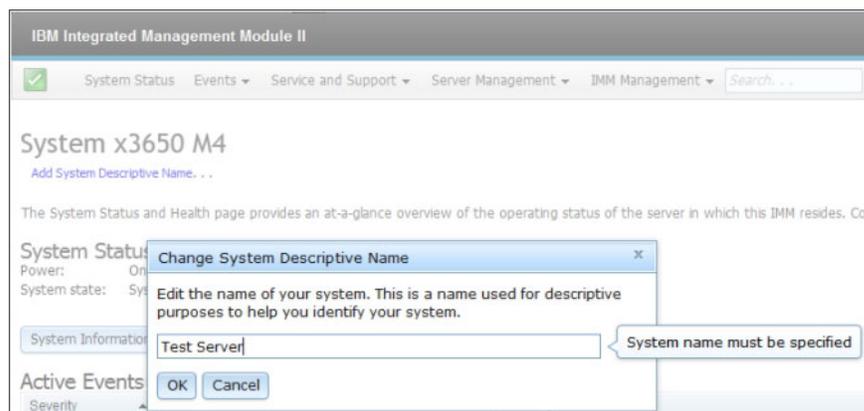
「System Status」ページは、IMM2 サーバーの操作状況の概要を提供します。また、このページにはサーバーのハードウェア・ヘルスのほか、サーバー上で発生しているアクティブ・イベントがあればそれらも表示されます。

注: 「System Status」ページから別のページにアクセスした場合、ページの上にあるメニュー項目から「System Status」をクリックすると、「System Status」ページに戻ることができます。

IMM2 に記述名を追加して、個々の IMM2 の識別に役立てることができます。IMM2 に関連付ける名前を指定するには、サーバー製品名の下にある「Add System Descriptive Name...」リンクをクリックします (次の図を参照)。

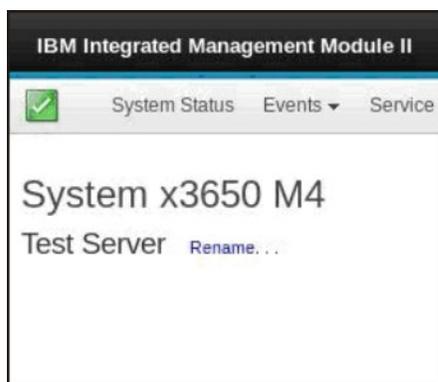


「Change System Descriptive Name」ウィンドウで、IMM2 に関連付ける名前を指定します (次の図を参照)。



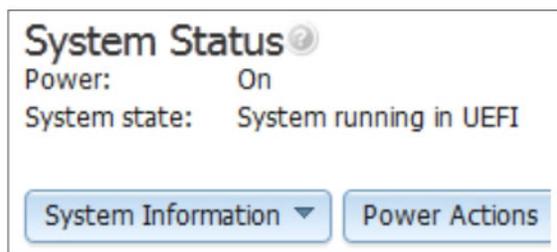
システム記述名を名前変更するには、システム記述名の横にある「**Rename...**」リンクをクリックします。

次の図は、「Rename」リンクを示しています。



「System Status」ページには、サーバーの電源状態と作動状態が表示されます。表示される状況は、「System Status」ページが開かれた時点でのサーバー状態です。

次の図は、「Power」フィールドと「System state」フィールドを示しています。



サーバーは、次の表にリストしたシステム状態のいずれかになります。

表 5. システム状態の説明

| 状態                             | 説明                                   |
|--------------------------------|--------------------------------------|
| System power off/State unknown | サーバーの電源はオフです。                        |
| System on/starting UEFI        | サーバーの電源はオンですが、UEFI は稼働していません。        |
| System running in UEFI         | サーバーの電源はオンで、UEFI が稼働しています。           |
| System stopped in UEFI         | サーバーの電源はオンで、UEFI は問題を検出して実行を停止しています。 |

表 5. システム状態の説明 (続き)

| 状態                              | 説明  |
|---------------------------------|---|
| Booting OS or in unsupported OS | <p>サーバーは、以下のいずれかの理由でこの状態になる場合があります。</p> <ul style="list-style-type: none"> <li>• オペレーティング・システム (OS) ロードが開始されたが、OS が稼働していない。</li> <li>• IMM2 Ethernet over USB インターフェースが使用不可になっている。</li> <li>• OS に Ethernet over USB インターフェースをサポートするドライバーがロードされていない。</li> </ul> |
| OS booted                       | サーバー OS は稼働しています。   |
| Suspend to RAM                  | サーバーは、スタンバイ状態またはスリープ状態に置かれています。   |

以下の「System Status」ページのメニュー選択項目は、追加サーバー情報と、サーバー上で実行できるアクションを提供します。

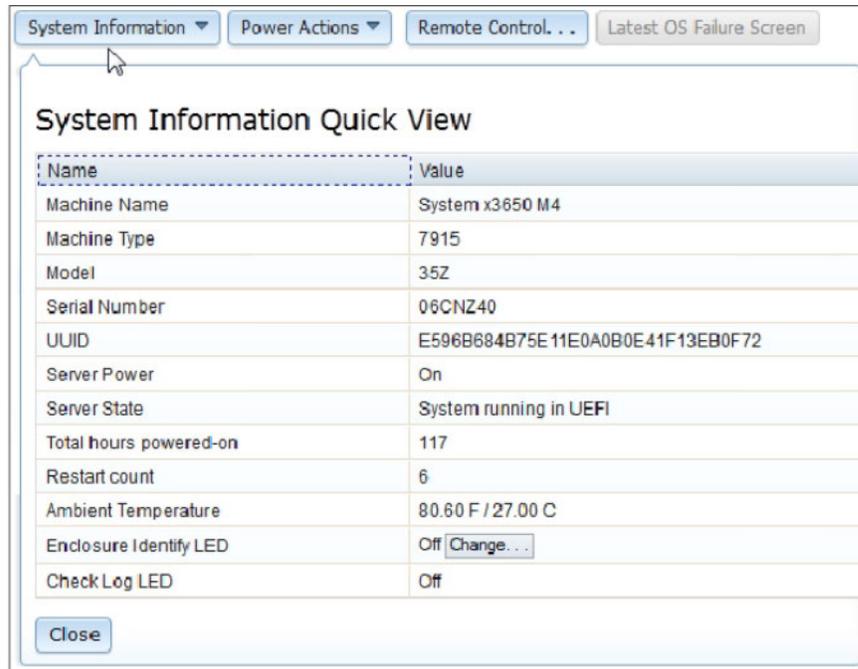
- System Information
- Power Actions
- Remote Control (詳しくは、105 ページの『リモート・プレゼンス機能および Remote Control 機能』を参照)。
- Latest OS Failure Screen (詳しくは、134 ページの『最新の OS 障害画面データのキャプチャー』を参照)。

## システム情報の表示

「System Information」メニューは、一般的なサーバー情報の要約を提供します。以下の情報を表示するには、「System Status」ページの「**System Information**」タブをクリックします。

- マシン名
- マシン・タイプ
- 型式
- シリアル番号
- 汎用固有 ID (UUID)
- サーバー電源
- サーバー状態
- 電源オン合計時間
- 再始動カウント
- 温度
- 筐体 ID LED
- チェック・ログ LED

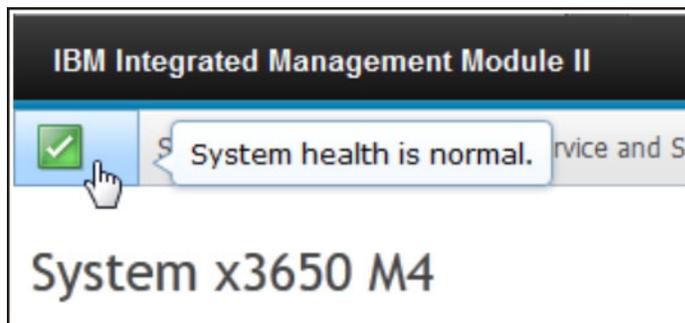
次の図は、「System Information」ウィンドウを示しています。



## サーバー・ヘルスの表示

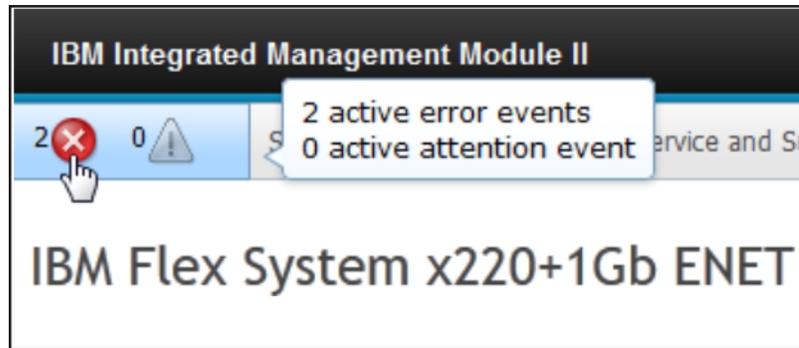
サーバー・ヘルスは「System Status」ページの左上隅のタイトル・バーの下に表示され、アイコンによって指定されます。緑色のチェック・マークは、サーバー・ハードウェアが正常に動作していることを示します。カーソルを緑色のチェック・マークの上に移動すると、サーバー・ヘルスを即時に表示できます。

次の図は、正常な操作モードにあるサーバーの例です。



黄色の三角形のアイコンは、警告状態が存在することを示しています。赤い円のアイコンは、エラー状態が存在することを示しています。

次の図は、エラー・イベントがアクティブであるサーバーの例です。



警告アイコン (黄色の三角形) またはエラー・アイコン (赤い円) が表示された場合は、そのアイコンをクリックして、対応するイベントを「System Status」ページの「Active Events」セクションに表示します。

次の図は、エラー状態での「Active Events」セクションの例です。

| Severity | Source | Date                        | Message  |
|----------|--------|-----------------------------|--|
| Error    | System | 16 Jul 2012 01:00:28.000 PM | Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state. |
| Error    | System | 16 Jul 2012 01:00:29.000 PM | Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state. |

## ハードウェア・ヘルスの表示

「System Status」ページの「Hardware Health」セクションには、サーバー・ハードウェア・コンポーネントがリストされ、IMM2 のモニター対象である各コンポーネントのヘルス状況が表示されます。表示されるコンポーネントのヘルス状況は、あるコンポーネント・タイプについて、すべての個別コンポーネントのうちで最もクリティカルな状態を反映している場合があります。例えば、あるサーバーにいくつかの電源モジュールが取り付けられており、1 つを除いてすべての電源モジュールが正常に動作している場合があります。その場合、「Power Modules」コンポーネントは、正常に動作していない電源モジュールのために、クリティカル状況を示します。

次の図は、「System Status」ページの「Hardware Health」セクションを示しています。

| Hardware Health ⓘ               |            |
|---------------------------------|------------|
| Component Type                  | Status     |
| <a href="#">Cooling Devices</a> | ✓ Normal   |
| <a href="#">Power Modules</a>   | ✗ Critical |
| <a href="#">Disks</a>           | ✓ Normal   |
| <a href="#">Processors</a>      | ✓ Normal   |
| <a href="#">Memory</a>          | ✓ Normal   |
| <a href="#">System</a>          | ✓ Normal   |

各コンポーネント・タイプはリンクとして表示され、これをクリックすると、詳細情報を取得できます。表示するコンポーネント・タイプを選択すると、そのコンポーネント・タイプに属するすべてのコンポーネントの状況をリストしたテーブルが表示されます。

次の図は、「Memory」コンポーネント・タイプのコンポーネントを示しています。

| Memory  |          |      |               |
|---|----------|------|---------------|
| Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Eve |          |      |               |
| FRU Name  | Status   | Type | Capacity (GB) |
| <a href="#">DIMM 4</a>  | ✓ Normal | DDR3 | 4             |
| <a href="#">DIMM 9</a>  | ✓ Normal | DDR3 | 4             |
| <a href="#">DIMM 16</a>   | ✓ Normal | DDR3 | 4             |
| <a href="#">DIMM 21</a>   | ✓ Normal | DDR3 | 4             |

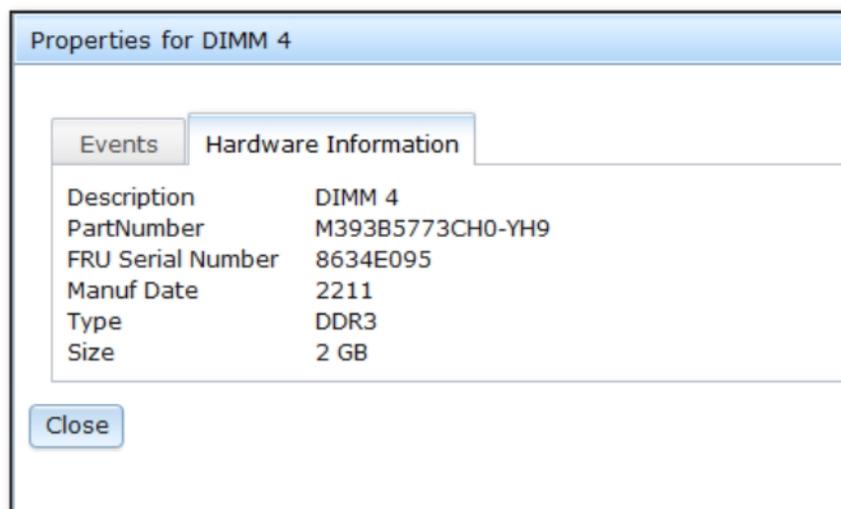
テーブルで個々の現場交換可能ユニット (FRU) のリンクをクリックすると、そのコンポーネントの追加情報を取得できます。その場合、そのコンポーネントのすべてのアクティブ・イベントが「Events」タブに表示されます。

次の図は、DIMM 4 の「Events」タブを示しています。



該当する場合、コンポーネントの追加情報が「Hardware Information」タブで提供されることがあります。

次の図は、DIMM 4 の「Hardware Information」タブを示しています。





---

## 第 6 章 IMM2 タスクの実行

このセクションおよび 15 ページの『第 3 章 IMM2 Web ユーザー・インターフェースの概要』の情報を使用して、以下のタスクを実行し、IMM2 を制御することができます。

「System Status」タブから、以下のタスクを実行できます。

- サーバー・ヘルスを表示する
- マシン名、タイプ、およびシリアル番号など、サーバー情報を表示する
- サーバーの電源および再始動アクティビティを表示する
- サーバーの電源状況をリモートから制御する
- リモート側からサーバー・コンソールにアクセスする
- リモート側でディスクまたはディスク・イメージをサーバーに接続する
- アクティブ・イベントを表示する
- サーバー・コンポーネントのハードウェア・ヘルスを表示する

注: 「System Status」ページは、IMM2 にログインした後に表示されます。このページには、一般的な情報とアクションの両方が示されます。

「Events」タブから、以下のタスクを実行できます。

- イベント・ログ・ヒストリーを管理する
- E メール通知のイベント受信者を管理する
- syslog 通知のイベント受信者を管理する

「Services and Support」タブから、以下のタスクを実行できます。

- サーバーのサービス・データを手動で取得する

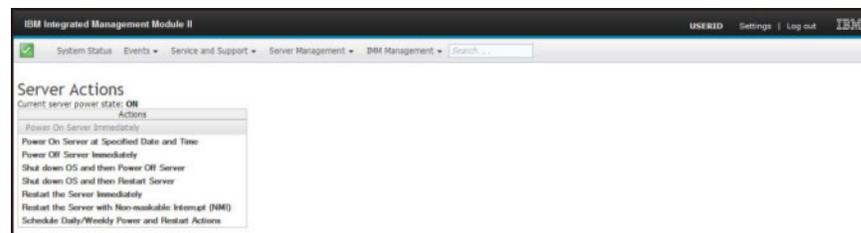
「Server Management」タブから、以下のタスクを実行するためのオプションを選択できます。

- 「Server Firmware」オプションから、サーバー・コンポーネントのファームウェア・レベルを表示および更新する
- 「Remote Control」オプションから、サーバー・コンソールをリモート側で表示し、それと対話する
  - サーバーの電源状況をリモートから制御する
  - リモート側からサーバー・コンソールにアクセスする
  - CD ドライブ、DVD ドライブ、ディスク・ドライブ、USB フラッシュ・ドライブ、またはディスク・イメージを、リモート側でサーバーに接続する
- 「Server Properties」オプションから、サーバーの識別を支援するパラメーターを設定する
- 「Server Power Actions」オプションから、電源オン、電源オフ、再始動などのアクションを実行する

- 「Disks」オプションから、サーバーに取り付けられているハード・ディスクと、それらに関連するイベントを表示する
- 「Memory」オプションから、サーバーに取り付けられているメモリー・モジュールに関する情報を表示する
- 「Processor」オプションから、サーバーに取り付けられているマイクロプロセッサに関する情報を表示する
- 「Server Timeouts」オプションから、ファームウェア更新またはサーバーの電源オンのときにサーバーが無期限にハングしないようにするために、タイムアウトを設定する
- 「PXE Network Boot」オプションから、サーバー実行環境のプリブートの試行をセットアップする
- 「Latest OS Failure Screen」オプションから、OS 障害画面データをキャプチャーし、保管する
- 「Power Management」オプションから、システムの電源使用量と電源機構の容量を表示でき、システムの電源使用に関するパラメーターを設定できます。

## サーバーの電源状況の制御

「Power Actions」オプションには、サーバー電源を制御するために実行できるアクションのリストが含まれています (次の図を参照)。サーバーの電源を即時にオンにするか、スケジュールした時刻にオンにするかを選択できます。また、オペレーティング・システムのシャットダウンと再始動を選択することもできます。



サーバー電源と再始動のアクションを実行するには、以下のステップを実行します。

1. 以下のいずれかのステップを実行して、「Power Actions」メニューにアクセスします。
  - 「System Status」ページで「Power Actions」タブをクリックします。
  - 「Server Management」タブから「Server Power Actions」をクリックします。
2. 「Actions」メニューのリストからサーバー・アクションを選択します。

次の表には、サーバーに対して実行できる電源アクションと再始動アクションの説明が記載されています。

表 6. 電源アクションと説明

| 電源アクション  | 説明  |
|--|---|
| Power on server immediately  | サーバーの電源をオンにし、オペレーティング・システムをブートするには、このアクションを選択します。   |
| Power on server at specified date and time   | 指定した日時にサーバーの電源が自動的にオンになるようスケジュールするには、このアクション項目を選択します。   |
| Power off server immediately   | オペレーティング・システムをシャットダウンせずにサーバーの電源をオフにするには、このアクション項目を選択します。  |
| Shut down operating system and then power off server <sup>1</sup>  | オペレーティング・システムをシャットダウンし、サーバーの電源をオフにするには、このアクション項目を選択します。   |
| Shut down operating system and then restart server <sup>1</sup>  | オペレーティング・システムをリポートするには、このアクション項目を選択します。   |
| Restart the server immediately   | オペレーティング・システムをシャットダウンせずに、即時にサーバーの電源サイクルを実行するには、このアクション項目を選択します。   |
| Restart the server with non-maskable interrupt (NMI)   | 「ハング」したシステムで NMI を強制実行するには、このアクション項目を選択します。このアクション項目を選択すると、プラットフォームのオペレーティング・システムでメモリー・ダンプを行うことができ、これをシステムのハング状態をデバッグするために使用できます。IMM2 ファームウェアは、UEFI F1 からの「Setup」メニューで設定された NMI での自動リポートの設定を使用して、NMI 後のリポートが必要かどうかを判別します。 |
| Schedule daily/weekly power and restart actions  | サーバーの日次および週次の電源アクションと再始動アクションをスケジュールするには、このアクション項目を選択します。   |
| <p>1. 「シャットダウン」要求が試行されたときに、オペレーティング・システムがスクリーン・セーバー・モードまたはロック・モードにあると、IMM2 が正常なシャットダウンを開始できない場合があります。IMM2 は、オペレーティング・システムがまだ稼働中であっても、電源オフ遅延間隔が経過すると、ハード・リセットあるいはシャットダウンを実行します。</p> |   |

## リモート・プレゼンス機能および Remote Control 機能

IMM2 Web インターフェースの IMM2 Remote Control 機能またはリモート・プレゼンス機能を使用して、サーバー・コンソールを表示し、それと対話することができます。ご使用のコンピューター上の CD または DVD ドライブ、ディスクレット・ドライブ、USB フラッシュ・ドライブ、あるいはディスク・イメージを、サーバーに割り当てることができます。リモート・プレゼンス機能は、IMM2 Premium 機能で使用でき、IMM2 Web インターフェースを介してのみ使用可能です。すべての

Remote Control 機能を使用するには、Supervisor アクセス権限を持つユーザー ID を使用して IMM2 にログインする必要があります。IMM2 Standard から IMM2 Premium へのアップグレードについて詳しくは、4 ページの『IMM2 のアップグレード』を参照してください。ご使用の IBM サーバーに取り付けられている IMM2 のレベルについて詳しくは、ご使用のサーバーに付属していた資料を参照してください。

Remote Control 機能は、以下の作業を行うために使用します。

- システムの状態に関係なく、75 Hz で最大 1600 x 1200 のグラフィックス解像度のビデオをリモート側で表示します。
- リモート・クライアントからキーボードとマウスを使用して、リモート側でサーバーにアクセスできます。
- リモート・クライアント上の CD または DVD ドライブ、ディスク・ドライブ、および USB フラッシュ・ドライブをマッピングし、また、ISO イメージ・ファイルおよびディスク・イメージ・ファイルをサーバーが使用できる仮想ドライブとしてマッピングします。
- ディスク・イメージを IMM2 メモリーにアップロードし、これを仮想ドライブとしてサーバーにマッピングします。

## IMM2 ファームウェアおよび Java または ActiveX アプレットの更新

このセクションでは、ファームウェアと Java および ActiveX アプレットの更新について説明します。

**重要:** IMM2 は、Java アプレットまたは ActiveX アプレットを使用してリモート・プレゼンス機能を実行します。IMM2 を最新のファームウェア・レベルに更新した場合は、Java アプレットおよび ActiveX アプレットも最新レベルに更新されます。デフォルトでは、Java は以前に使用されたアプレットをキャッシュに入れます（ローカル側で保管します）。IMM2 ファームウェアのフラッシュ更新の後、サーバーの使用する Java アプレットが最新レベルでない場合もあります。

この問題を修正するには、キャッシングをオフにします。使用方法は、プラットフォームと Java のバージョンによって異なります。以下のステップは、Windows 上の Oracle Java 1.5 用です。

1. 「スタート」 → 「設定」 → 「コントロール パネル」をクリックします。
2. 「Java Plug-in 1.5」ダブルクリックします。「Java Plug-in コントロールパネル」ウィンドウが開きます。
3. 「キャッシュ」タブをクリックします。
4. 次のオプションのいずれかを選択してください。
  - 「キャッシュを有効」チェック・ボックスをクリアし、Java キャッシングが常に使用不可にされているようにします。
  - 「クリア (Clear Caching)」をクリックします。このオプションを選択した場合は、IMM2 ファームウェアを更新するたびに、「クリア (Clear Caching)」をクリックする必要があります。

IMM2 ファームウェアの更新について詳しくは、120 ページの『サーバー・ファームウェアの更新』を参照してください。

## リモート・プレゼンス機能の使用可能化

IMM2 リモート・プレゼンス機能は、IMM2 Premium のみで使用可能です。IMM Standard から IMM Premium へのアップグレードについて詳しくは、4 ページの『IMM2 のアップグレード』を参照してください。

IMM Premium アップグレードのアクティベーション・キーを購入して入手した後、キーをインストールしてください (141 ページの『アクティベーション・キーのインストール』を参照)。

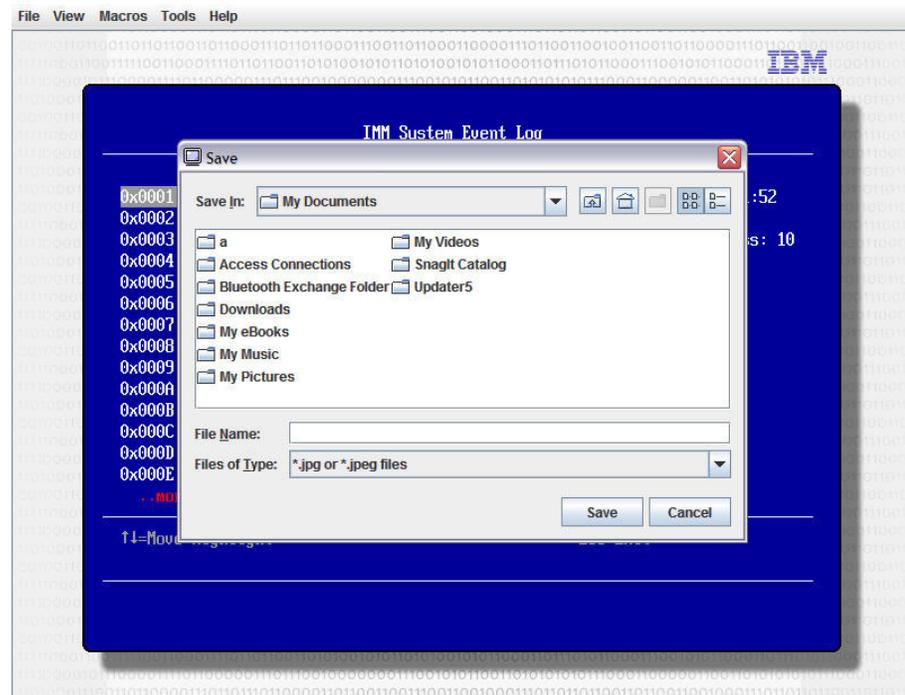
## Remote Control のスクリーン・キャプチャー

「Video Viewer」ウィンドウのスクリーン・キャプチャー機能は、サーバーのビデオ表示内容をキャプチャーします。画面イメージをキャプチャーおよび保管するには、以下のステップを実行します。

1. 「Video Viewer」ウィンドウで「File」をクリックします。
2. メニューから「Capture to File」を選択します。
3. プロンプトが表示されたら、イメージ・ファイルの名前を入力し、ローカル・クライアント上の選択した場所にそのファイルを保存します。

注: Java クライアントは、スクリーン・キャプチャー・イメージを JPG ファイル・タイプとして保存します。ActiveX クライアントは、スクリーン・キャプチャー・イメージを BMP ファイル・タイプとして保存します。

次の図は、イメージ・ファイルの場所を指定し、イメージ・ファイルの名前を入力するウィンドウを示しています。



## Remote Control の Video Viewer モード

「Video Viewer」ウィンドウの表示を変更するには、「**View**」をクリックします。以下のメニュー・オプションが選択可能です。

### Hide Status Bar

Caps Lock キー、Num Lock キー、および Scroll Lock キーの状態を示すステータス・バーを非表示にします。このオプションは、ステータス・バーが表示されている場合にのみ使用可能です。

### Show Status Bar

Caps Lock キー、Num Lock キー、および Scroll Lock キーの状態を示すステータス・バーを表示します。このオプションは、ステータス・バーが非表示の場合にのみ使用可能です。

### Refresh

Video Viewer は、サーバーからのビデオ・データを使用してビデオ表示を再描画します。

### Full Screen

Video Viewer は、クライアントのデスクトップにビデオ表示を全画面表示します。このオプションは、Video Viewer がフルスクリーン・モードでないときにのみ使用可能です。

### Windowed

Video Viewer は、フルスクリーン・モードをウィンドウ表示モードに切り替えます。このオプションは、Video Viewer がフルスクリーン・モードの場合にのみ使用可能です。

**Fit** Video Viewer は、ターゲットのデスクトップを余分な枠やスクロール・バーなしで完全に表示できるようにサイズを変更します。これには、クライアントのデスクトップが、サイズ変更したウィンドウを表示するのに十分な大きさがある必要があります。

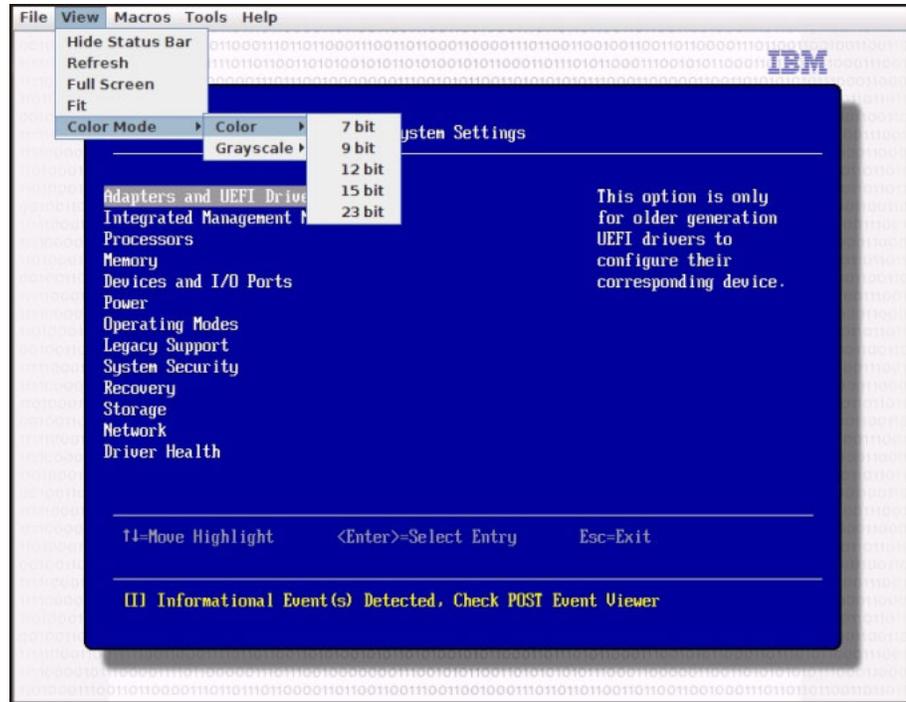
## Remote Control のビデオ・カラー・モード

リモート・サーバーへの接続の帯域幅が制限されている場合、「Video Viewer」ウィンドウのカラー設定を調整することで Video Viewer の帯域幅要求を削減することができます。

**注:** IMM2 には、低帯域幅状態で送信されるデータをカラー階調調整によって削減できるようにするメニュー項目があります。このメニュー項目は、リモート管理アダプター II インターフェースで使用される帯域幅スライダーに代わるものです。

ビデオ・カラー・モードを変更するには、以下のステップを実行します。

1. 「Video Viewer」ウィンドウで「**View**」をクリックします。
2. 「**Color Mode**」をクリックします。2 つのカラー・モード・オプションがあります (次の図を参照)。
  - Color: 7、9、12、15、および 23 bit
  - Grayscale: 16、32、64、および 128 shade



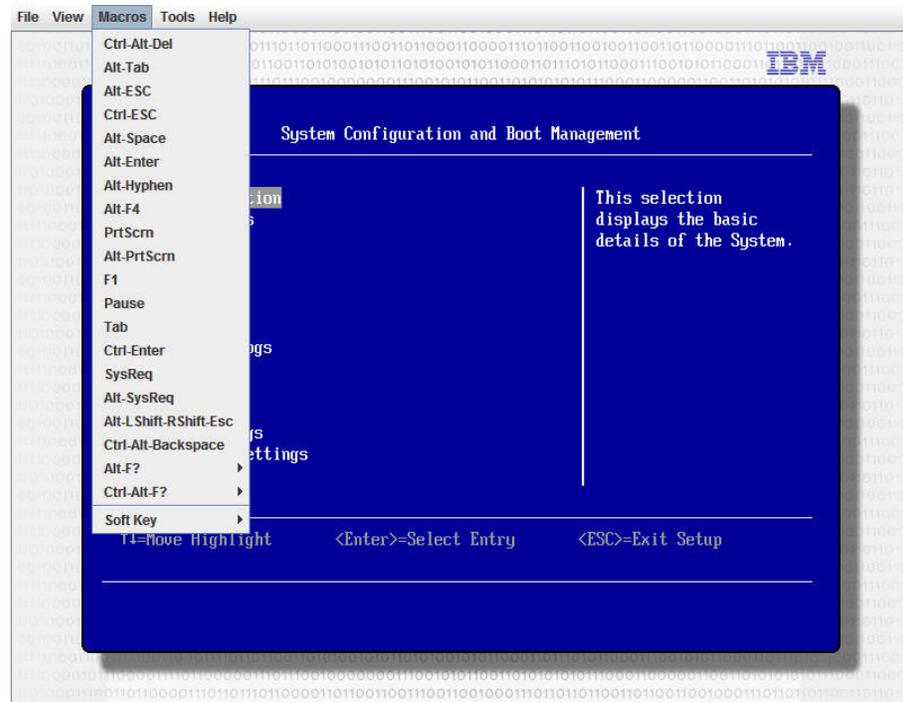
3. カラーあるいはグレースケールの設定を選択します。

## Remote Control のキーボード・サポート

使用しているクライアント・サーバー上のオペレーティング・システムは、特定のキーの組み合わせ（たとえば、Microsoft Windows での Ctrl+Alt+Del）をトラップし、それらをサーバーに伝送しません。その他のキー、たとえば F1 などは、サーバー上のアクションだけでなく、お客様のコンピューター上のアクションも引き起こす場合があります。

リモート・サーバーに影響し、ローカル・クライアントに影響しないキーの組み合わせを使用するには、以下のステップを実行します。

1. 「Video Viewer」ウィンドウで「**Macros**」をクリックします。
2. メニューから事前定義されたキーの組み合わせの 1 つを選択するか、あるいは「**Soft Key**」を選択してユーザー定義のキーの組み合わせを選択または追加します（次の図を参照）。



Video Viewer の「**Macros**」メニュー項目を使用して、サーバーにキー・ストロークを送信するのに使用可能なカスタマイズされたボタンを作成および編集します。

カスタマイズされたボタンを作成および編集するには、以下のステップを実行します。

1. 「Video Viewer」ウィンドウで「**Macros**」をクリックします。
2. 「**Soft Key**」を選択し、次に「**Add**」を選択します。新しいウィンドウが開きます。
3. 「**New**」をクリックして新規のキーの組み合わせを追加するか、あるいはキーの組み合わせを選択して「**Delete**」をクリックし、既存のキーの組み合わせを削除します。
4. 新規の組み合わせを追加する場合は、「**New**」を選択した後に表示されるウィンドウで、定義するキーの組み合わせを入力して「**OK**」をクリックします。
5. 定義あるいはキーの組み合わせの削除が完了したら、「**OK**」をクリックします。

## 多国語キーボードのサポート

Video Viewer は、プラットフォーム固有のネイティブ・コードを使用してキー・イベントを傍受し、物理キー情報に直接アクセスします。クライアントは、物理キー・イベントを検出して、それらをサーバー間で受け渡します。サーバーは、クライアントと同じ物理キー・ストロークを検出し、すべての標準キーボード・レイアウトをサポートします。このときの制限事項は、ターゲットとクライアントが同じキーボード・レイアウトを使用していることのみです。リモート・ユーザーがサーバーと異なるキーボード・レイアウトを使用している場合、サーバーにリモートでアクセスしている間、サーバーのレイアウトを切り替え、後で元に戻すことができます。

## キーボード・パススルー・モード

キーボード・パススルー・モードは、クライアント上でのほとんどの特殊キーの組み合わせの処理を使用不可にすることで、サーバーに直接渡せるようにします。この機能は、マクロの代替として使用できます。

一部のオペレーティング・システムでは、特定のキー・ストロークをアプリケーションの制御の範囲外に定義しているため、パススルー・メカニズムはサーバーとは無関係に動作します。例えば、Linux X セッションでは、Ctrl+Alt+F2 キー・ストロークの組み合わせは仮想コンソール 2 への切り替えを行います。このキー・ストローク・シーケンスを傍受するメカニズムはないため、クライアントがこれらのキー・ストロークをターゲットに直接渡す方法はありません。この場合の唯一のオプションは、この目的で定義されたキーボード・マクロを使用することです。

キーボード・パススルー・モードを使用可能あるいは使用不可にするには、以下のステップを実行します。

1. 「Video Viewer」ウィンドウで「**Tools**」をクリックします。
2. メニューから「**Session Options**」を選択します。
3. 「Session Options」ウィンドウが開いたら、「**General**」タブをクリックします。
4. 「**Pass all keystrokes to target**」チェック・ボックスを選択して、キーボード・パススルー・モードを使用可能または使用不可にします。
5. 「**OK**」をクリックして選択を保存します。

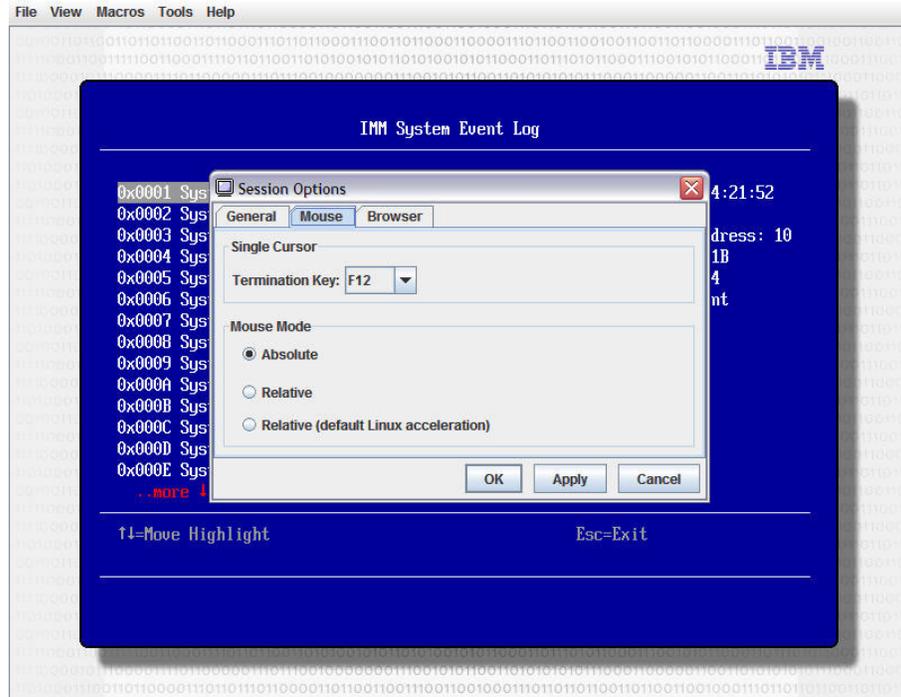
## Remote Control のマウス・サポート

「Video Viewer」ウィンドウは、マウス制御に関するいくつかのオプションを提供します。これには、絶対マウス制御、相対マウス制御、および単一カーソル・モードがあります。

### 絶対マウス制御と相対マウス制御

マウス制御の絶対および相対オプションにアクセスするには、以下のステップを実行します。

1. 「Remote Control」ウィンドウで、「**Tools**」をクリックします。
2. メニューから「**Session Options**」を選択します。
3. 「Session Options」ウィンドウが表示されたら、「**Mouse**」タブをクリックします (次の図を参照)。



4. 以下のいずれかの「**Mouse Modes**」を選択します。

- **Absolute:**

クライアントは、常に表示エリアの原点 (左上のエリア) からの相対位置であるマウス・ロケーション・メッセージをサーバーに送信します。

- **Relative:**

クライアントは、マウス・ロケーションを以前の位置からの相対位置として送信します。

- **Relative (default Linux acceleration):**

クライアントは、加速係数を適用して Linux ターゲット上でマウスをより正確に位置合わせします。加速設定は、Linux ディストリビューションとの互換性を最大化するように選択されています。

## 単一カーソル・モード

一部のオペレーティング・システムでは、ローカルとリモートのカーソルを位置合わせしません。これにより、ローカルとリモートのマウス・カーソルの間にオフセットが生じます。単一カーソル・モードでは、マウスが「Video Viewer」ウィンドウ内にある間は、ローカル・クライアントのカーソルを非表示にします。単一カーソル・モードがアクティブにされている場合、リモート・カーソルのみが表示されます。単一カーソル・モードを使用可能にするには、「Video Viewer」ウィンドウから「Tools」>「Single Cursor」をクリックします。

注: Video Viewer が単一カーソル・モードの場合、ローカル・カーソルがないため、マウスを使用して別のウィンドウに切り替えたり、KVM クライアント・ウィンドウの外側をクリックすることはできません。

単一カーソル・モードを使用不可にするには、「**Defined Termination**」キーをクリックします。定義した終了キーを確認あるいは変更するには、「**Tools > Session Options > Mouse**」をクリックします。

## リモート電源制御

「Video Viewer」ウィンドウから Web ブラウザーに戻ることなく、サーバーに電源および再始動コマンドを送信することができます。Video Viewer を使用してサーバーの電源を制御するには、以下のステップを実行します。

1. 「Video Viewer」ウィンドウで「**Tools**」をクリックします。
2. 「**Power**」をクリックします。以下のコマンドから 1 つを選択します。

**On** サーバーの電源をオンにします。

**off** サーバーの電源をオフにします。

**Reboot**  
サーバーを再始動します。

**Cycle** サーバーの電源をオフにした後、オンに戻します。

## パフォーマンス統計の表示

「Video Viewer」ウィンドウから Video Viewer のパフォーマンス統計を表示するには、「**Tools**」をクリックし、次に「**Stats**」をクリックします。以下の情報が表示されます。

### Frame Rate

フレーム数の実行平均値。クライアントによって 1 秒ごとにデコードされます。

### Bandwidth

クライアントが受信する 1 秒あたりの総キロバイト数の実行平均値。

### Compression

ビデオ圧縮による帯域幅縮小の実行平均値。この値は、100.0% と表示される場合があります。この値は、10% 単位で四捨五入されます。

### Packet Rate

1 秒あたりに受信するビデオ・パケット数の実行平均値。

## リモート・デスクトップ・プロトコルの始動

Windows ベースのリモート・デスクトップ・プロトコル (RDP) クライアントがインストールされている場合、KVM クライアントの代わりに RDP クライアントを使用することができます。リモート・サーバーが RDP 接続を受信するように構成されている必要があります。

## Knock-knock 機能の説明

可能なすべての Remote Control セッションが占有されているとき (1 のシングルユーザー・モード・オプションまたは 4 のマルチユーザー・モード・オプション)、別の Web ユーザーが、Knock-knock 機能を使用可能に設定した Remote Control ユーザー (このユーザーが他の Web ユーザーからの切断要求を処理していない場合) に、切断要求を送信できる場合があります。

Knock-knock 機能を使用可能にした Remote Control ユーザーが、要求を受け入れるかタイムアウト値以内に要求に回答しなかった場合、Remote Control セッションは終了し、要求を送信した Web ユーザー用に予約されます。切断要求を送信した Web ユーザーが、予約された Remote Control セッションを使用して Java または ActiveX の Remote Control セッションを 5 分以内に起動しなかった場合、その Remote Control セッションは、その Web ユーザー用に予約済みでなくなります。

Knock-knock 機能を使用可能にするには、以下のステップを実行します。

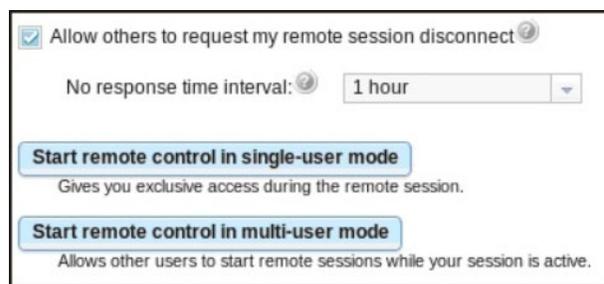
1. 以下のいずれかのメニュー選択項目を選択して、「Remote Control」ページにアクセスします。
  - 「Server Management」タブから「Remote Control」をクリックします。
  - 「System Status」ページで「Remote Control...」をクリックします。
2. 「Allow others to request my remote session disconnect」チェック・ボックスをクリックします。

注: Remote Control 機能を使用するときは、「Allow others to request my remote session disconnect」チェック・ボックスを選択している追加ユーザーが 1 人以上存在する必要があります。

3. 「No response time interval」フィールドから時間間隔を選択します。
4. ユーザー・モードを選択して、Remote Control セッションを開始します。以下のモードから 1 つを選択します。
  - Start remote control in single-user mode
  - Start remote control in multi-user mode

注: Knock-knock 機能は自動的に使用可能に設定されます。

次の図は、ステップ 2 から 4 で説明したフィールドを示しています。



リモート・セッションを要求するには、以下のステップを実行します。

1. 「Refresh」をクリックして、進行中の Remote Control セッションを表示します。

次の図は、「Remote Control Session in Progress」ウィンドウを示しています。

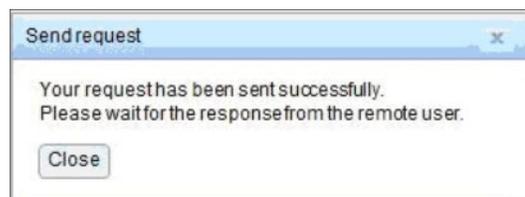


| User Name | Active Sessions | Availability for Disconnection     | Timeout Value |
|-----------|-----------------|------------------------------------|---------------|
| USERID    | 192.168.5.11    | <a href="#">Request to connect</a> | 1 hour        |

「Availability for Disconnection」フィールドに、以下のいずれかの応答が表示されます。

- **Request to connect:** このテキストは、Remote Control ユーザーが Knock-knock 機能を使用可能に設定にしている、別の Web ユーザーからの切断要求を処理していないときに表示されます。現行 Web ユーザーは、Remote Control ユーザーに切断要求を送信していません。
  - **Waiting for response:** このテキストは、Remote Control ユーザーが現行 Web ユーザーからの切断要求を処理しているときに表示されます。現行 Web ユーザーは「Cancel」ボタンをクリックすることにより、Remote Control ユーザーに取消要求を送信できます。
  - **Other request is pending:** このテキストは、以下のいずれかの状態の場合に表示されます。
    - Remote Control ユーザーは、別の Web ユーザーからの切断要求を処理中である。
    - Remote Control ユーザーは Knock-knock 機能を使用可能に設定しており、現行 Web ユーザーは別の Remote Control ユーザーからの切断要求に対する応答を待っている。
  - **Not available:** このテキストは、以下のいずれかの状態にあるときに表示されます。
    - すべての Remote Control セッションが占有されていない。Remote Control ユーザーが Knock-knock 機能を使用可能に設定しているかどうかは、この状態に影響を及ぼしません。
    - すべての Remote Control セッションが占有されており、Remote Control ユーザーは Knock-knock 機能を使用可能に設定していない。
    - この Remote Control 接続は、別のユーザー用に 5 分間予約されている。
2. Remote Control ユーザーに切断要求を送信するには、「Request to connect」をクリックします。

次の図は、要求の送信が正常に完了したときに表示されるウィンドウを示しています。



Remote Control ユーザーが切断要求を受け入れた場合、Web ユーザーは 5 分以内に Remote Control セッションを開始する必要があります。Web ユーザーが 5 分以内にセッションを開始しなかった場合、セッションは予約済みでなくなります。

次の図は、切断要求を受け入れられたときに表示される情報を示しています。

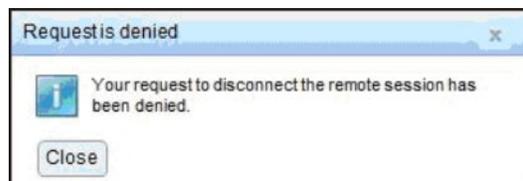
次の図は、予約済み状態にある切断要求を示しています。



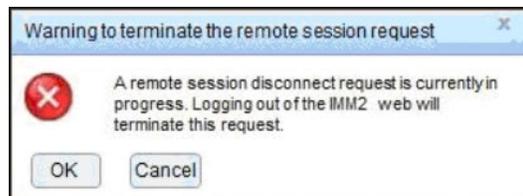
次の図は、予約済みでない状態の切断要求を示しています。



Remote Control ユーザーが切断要求を拒否した場合、切断要求を実行依頼したユーザーは、要求が拒否されたことを知らせる情報を受信します (次の図を参照)。

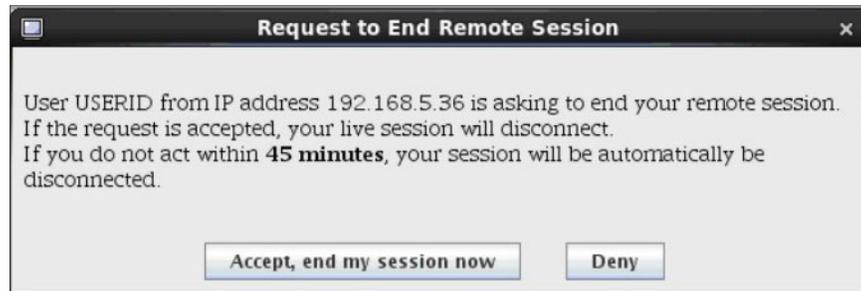


Web ユーザーが、そのユーザーの要求に関するメッセージを受信する前に IMM2 からログアウトした場合、その Web ユーザーはメッセージを受信します (次の図を参照)。

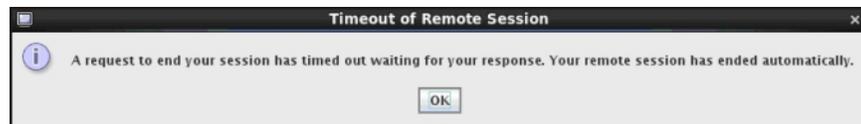


Remote Control ユーザーは、要求を受信した後、Remote Control セッションを開始する前に選択した間隔時間内に、Remote Control セッションを解放するかどうかを決める必要があります。Remote Control ユーザーに残り時間を知らせるために、「Request to End Remote Session」というウィンドウが表示されます。

次の図に、「Request to End Remote Session」ウィンドウを示します。



Remote Control ユーザーが「**Accept, end my session now**」を選択すると、リモート・ビューアーは自動的に終了します。Remote Control ユーザーが「**Deny**」を選択すると、Remote Control ユーザーはリモート・セッションを保持し続けます。「Request to End Remote Session」が終了した後、リモート・セッションは自動的に解放され、次のウィンドウが開きます。



## リモート・ディスク

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

### 注:

- 以下のサーバー・オペレーティング・システムには、USB サポートが搭載されています。USB サポートは、リモート・ディスク機能に必要です。
  - Microsoft Windows Server 2003: Web, Std, Ent, DC (SP2, R2, SBS)
  - Microsoft Windows Server 2008 SP2: Std, SBS, EBS
  - Microsoft Windows Server 2008 R2
  - SUSE Linux Enterprise Server V10 SP3: x86\_64
  - SUSE Linux Enterprise Server V11: x86, \_64
  - Red Hat Enterprise Linux Enterprise Servers V3.7: x86, x86\_64
  - Red Hat Enterprise Linux Enterprise Servers V4.8: x86, x86\_64
  - Red Hat Enterprise Linux Enterprise Servers V5.5: x86, x86\_64
  - Red Hat Enterprise Linux Enterprise Servers V6.0: x86, x86\_64
  - ESX 4.5: 4.0 U1
- クライアント・サーバーには、Java 1.5 プラグインまたはそれ以降が必要です。

- クライアント・サーバーは、700 MHz 以上で作動する Intel Pentium III マイクロプロセッサ以上、またはそれと同等なものを備えている必要があります。

## Remote Control へのアクセス

Remote Control セッションを開始してリモート・ディスクにアクセスするには、以下のステップを実行します。

1. 「Video Viewer」ウィンドウで「**Tools**」をクリックします。
2. 「**Launch Virtual Media**」をクリックします。「Video Viewer」ウィンドウが開きます。

注: 「Video Viewer」ウィンドウが開かれる前に「**Encrypt disk and KVM data during transmission**」チェック・ボックスが選択された場合、ディスク・データは ADES 暗号化によって暗号化されます。

「Virtual Media Session」ウィンドウは、「Video Viewer」ウィンドウとは別に開きます。「Virtual Media Session」ウィンドウは、リモート・ドライブとしてマップ可能なクライアント上のすべてのドライブをリストします。「Virtual Media Session」ウィンドウにより、ISO イメージおよびディスク・イメージ・ファイルを仮想ドライブとしてマップすることができます。マップされた各ドライブは、読み取り専用としてマークすることができます。CD および DVD ドライブと ISO イメージは、常に読み取り専用です。

## ドライブのマッピングおよびマッピング解除

ドライブをマップするには、マップするドライブの横にある「**Select**」チェック・ボックスを選択します。

注: CD または DVD ドライブをマップするには、メディアが入っている必要があります。ドライブが空の場合は、ドライブに CD あるいは DVD を挿入するようにプロンプトが表示されます。

「**Mount Selected**」ボタンをクリックして、選択したドライブをマウントしてマップします。「**Add Image**」をクリックすると、使用可能なドライブのリストにディスク・イメージ・ファイルおよび ISO イメージ・ファイルを追加することができます。ディスク・イメージ・ファイルあるいは ISO イメージ・ファイルが「Virtual Media Session」ウィンドウにリストされると、他のドライブと同様にマップすることができます。ドライブをマップ解除するには、「**Unmount All**」ボタンをクリックします。ドライブをマップ解除する前に、ドライブをマップ解除することを確認する必要があります。

注: ドライブをマップ解除することを確認したら、そのドライブはすべてアンマウントされます。ドライブを個別にアンマウントすることはできません。

イメージがリストに追加され、「**Map**」チェック・ボックスが選択されている場合(イメージが RDOC 機能用の IMM2 メモリーへのロードに適している場合)、ウィンドウが開き、イメージをサーバーに転送するオプションが表示されます。「**Yes**」を選択する場合は、イメージの名前を入力します。

注: 名前にアンパーサンド (&) やスペースなどの特殊文字を入力しないでください。

イメージを IMM2 メモリーにアップロードすることにより、ディスクをサーバーにマウントした状態で残すことが可能になり、IMM2 Web インターフェイス・セッションが終了した後もディスクにアクセスすることができます。IMM2 には複数のイメージを保管できますが、使用する合計スペースが 50 MB を超えることはできません。メモリーからイメージ・ファイルをアンロードするには、「RDOC Setup」ウィンドウで名前を選択して「Delete」をクリックします。

## Remote Control の終了

Remote Control 機能の使用が終了したら、「Video Viewer」ウィンドウと「Virtual Media Session」ウィンドウを閉じます。

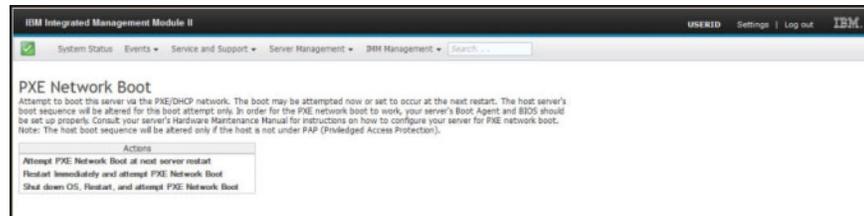
---

## PXE ネットワーク・ブートのセットアップ

サーバー実行環境のプリブートを試行するようセットアップするには、「PXE Network Boot」オプションを使用します。以下のステップを実行して、ご使用のサーバーが次のサーバー再始動時に Preboot Execution Environment ネットワーク・ブートを試行するようセットアップします。

1. IMM2 にログインします。詳しくは、10 ページの『IMM2 へのログイン』の追加情報を参照してください。
2. 「Server Management」をクリックし、次に「PXE Network Boot」を選択します。

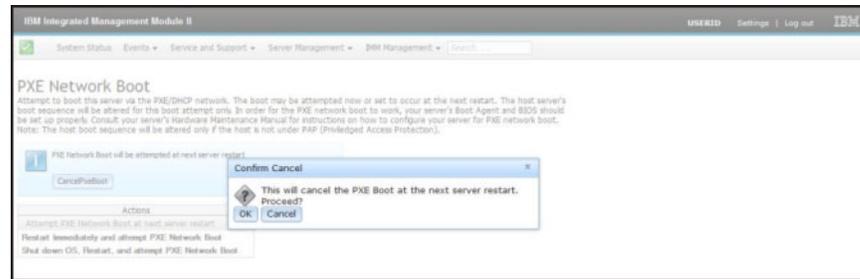
次のようなウィンドウが開きます。



3. 「Action」オプションから「Attempt PXE Network Boot at next server restart」を選択します。次のようなウィンドウが開きます。



選択を取り消すには、「CancelPxeBoot」をクリックします。次の「Confirm Cancel」ウィンドウが開きます。



## サーバー・ファームウェアの更新

「Server Firmware」オプションを使用すると、ファームウェアのレベルを表示し、DSA、IMM2、および UEFI のファームウェアを更新することができます。IMM2、UEFI、および DSA ファームウェアの現行バージョンが表示されます。これには、Active、Primary、Backup の各バージョンがあります。

次の図は、「Server Firmware」ページを示しています。

| Firmware Type  | Status   | Version | Build     | Release Date |
|----------------|----------|---------|-----------|--------------|
| DSA            | Active   | 9.24    | DSY144E   | 2012-08-10   |
| IMM2           |          |         |           |              |
| IMM2 (Primary) | Active   | 2.15    | 140039Q   | 2013-01-28   |
| IMM2 (Backup)  | Inactive | 3.00    | 140039T   | 2013-01-30   |
| UEFI           |          |         |           |              |
| UEFI (Primary) | Active   | 1.20    | D7E120C0S | 2012-08-23   |
| UEFI (Backup)  | Inactive | 1.20    | D7E120C0S | 2012-08-23   |

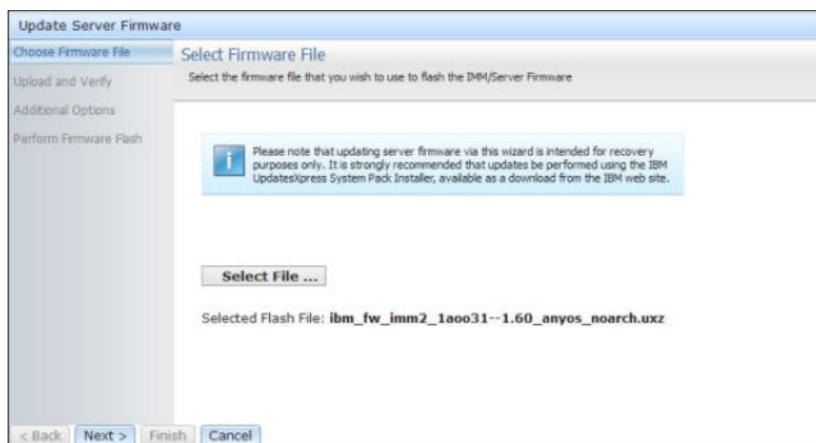
IMM2、UEFI、および DSA 用ファームウェアの現在の状況とバージョンが表示されます (基本バージョンとバックアップ・バージョンを含めて)。ファームウェア状況には、次の 3 つのカテゴリがあります。

- **アクティブ:** ファームウェアはアクティブです。
- **非アクティブ:** ファームウェアはアクティブではありません。
- **保留:** ファームウェアはアクティブ化を待機しています。

**注意:** 誤ったファームウェア更新をインストールすると、サーバーが誤動作する可能性があります。ファームウェアまたはデバイス・ドライバーの更新をインストールする前に、ダウンロードした更新に付属の README または変更履歴・ファイルをすべてお読みください。これらのファイルには、更新に関する重要な情報、および更新をインストールするための手順 (ファームウェアまたはデバイス・ドライバーの旧バージョンから最新バージョンに更新するための特別な手順など) が記載されています。

サーバー・ファームウェアを更新するには、以下のステップを実行します。

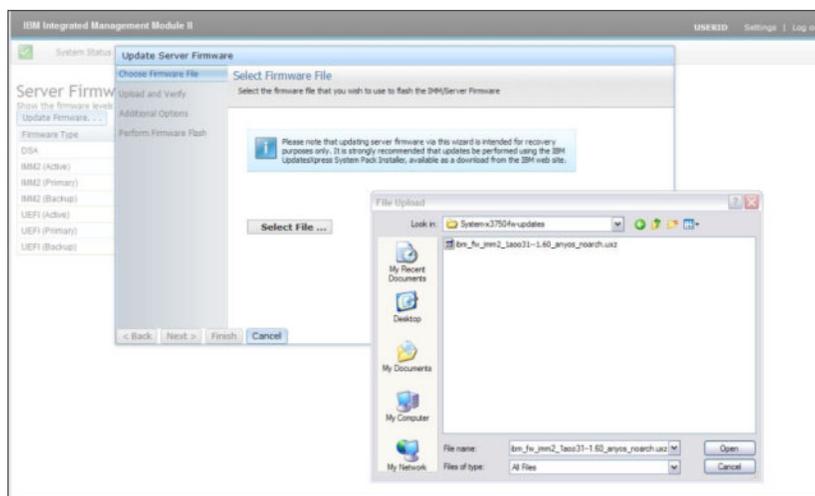
1. 「Server Management」メニュー・リストから「**Server Firmware**」をクリックします。
2. 「**Update Firmware**」をクリックします。「Update Server Firmware」ウィンドウが開きます (次の図を参照)。



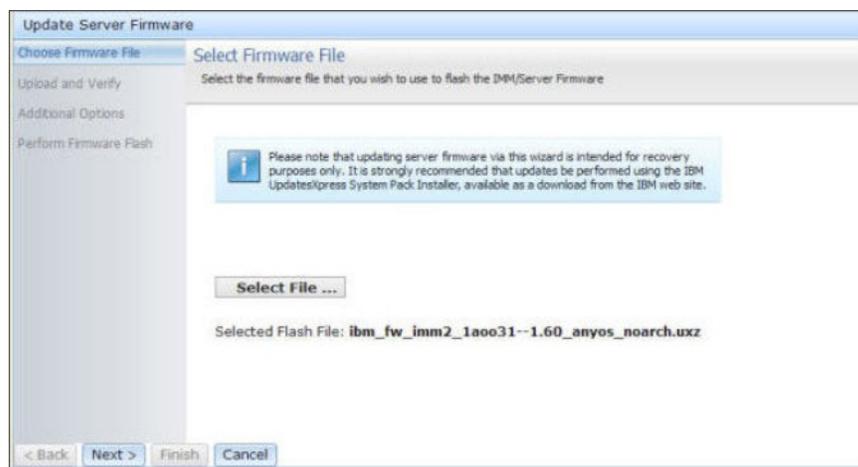
3. 次のステップに進む前に、注意書きをお読みください。
4. 以下のいずれかのステップを実行します。
  - 「**Cancel**」をクリックして、前の「Server Firmware」ウィンドウに戻ります。
  - 「**Select File...**」をクリックして、サーバー・ファームウェアをフラッシュするために使用するファームウェア・ファイルを選択します。

注: 他のすべてのオプションは、「Update Server Firmware」ウィンドウが最初に開いたときはぼかし表示になっています。

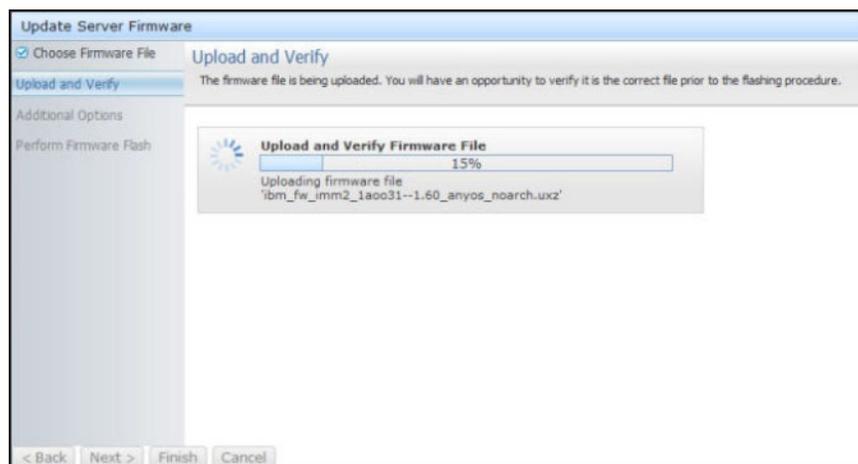
「**Select File...**」をクリックすると、「File Upload」ウィンドウが開きます (次の図を参照)。このウィンドウで、目的のファイルを参照できます。



5. 選択したいファイルまでナビゲートし、「**Open**」をクリックします。「Update Server Firmware」ウィンドウに戻り、選択したファイルが表示されます (次の図を参照)。

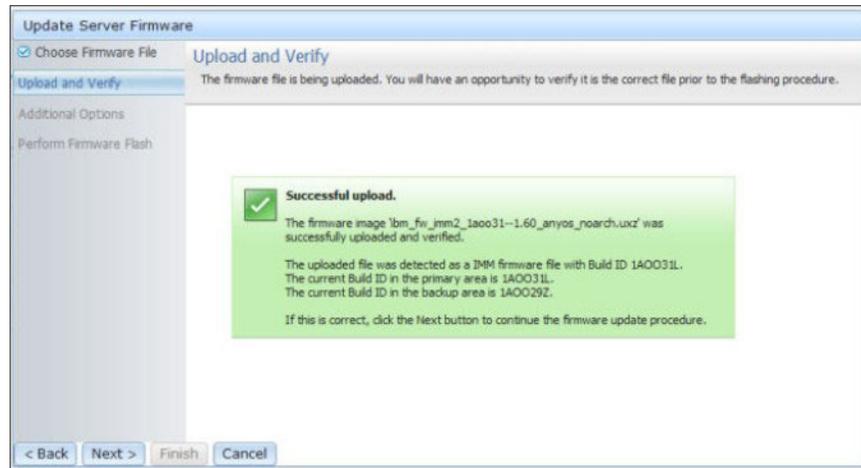


6. 「Next >」をクリックして、選択したファイルに対するアップロードと検証のプロセスを開始します。ファイルがアップロードされて検証されている間、進行状況メーターが表示されます (次の図を参照)。



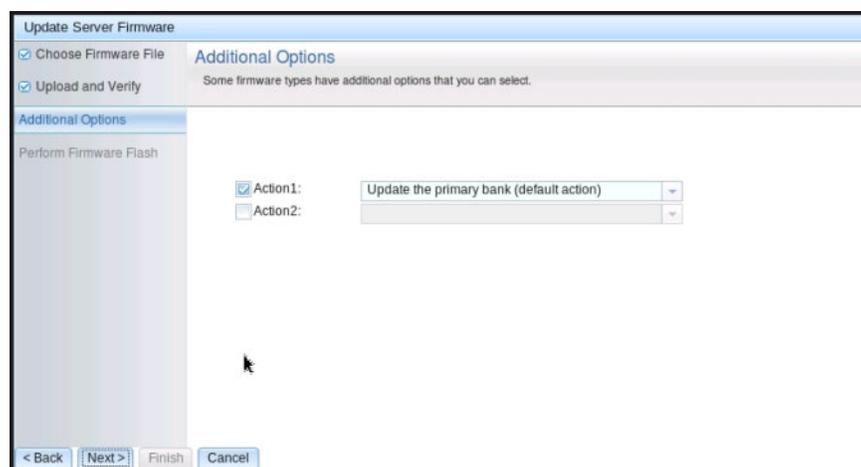
この状況ウィンドウを表示して、更新のために選択したファイルが正しいファイルであることを確認できます。状況ウィンドウには、DSA、IMM、または UEFI など、更新されるファームウェア・ファイルのタイプに関する情報が示されます。

ファームウェア・ファイルが正常にアップロードされて検証された後、「Successful upload」ウィンドウが開きます (次の図を参照)。

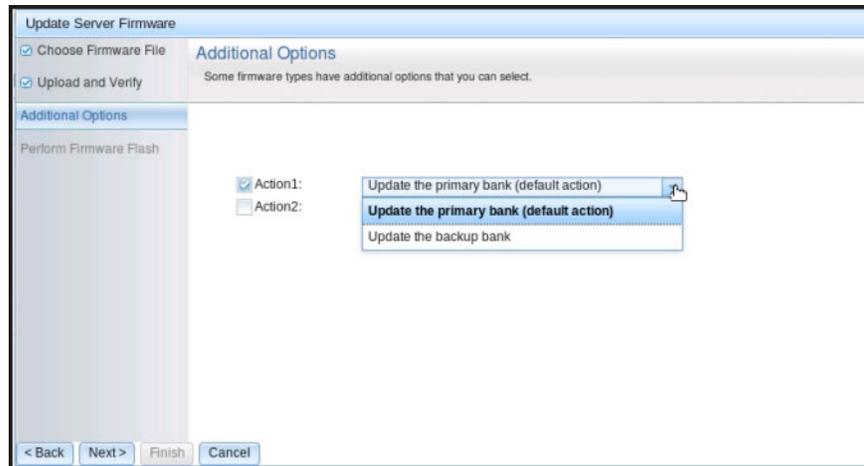


7. 情報が正しい場合は、「**Next >**」をクリックします。いずれかの選択をやり直す場合は、「**< Back**」をクリックします。

「**Next >**」をクリックすると、一連の追加オプションが表示されます (次の図を参照)。



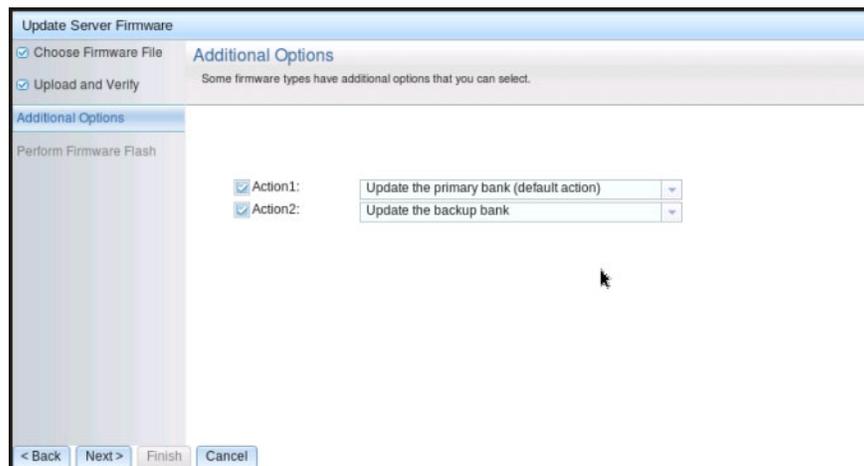
8. 「**Action 1**」フィールドの横にあるドロップダウン・メニューでは、「**Update the primary bank (default action)**」または「**Update the backup bank**」を選択できます (次の図を参照)。



アクションを選択すると、前の画面に戻り、要求した追加アクションが表示されます。

選択したアクションがロードされた後、そのアクションと新しい「**Action 2**」ドロップダウン・メニューが表示されます (次の図を参照)。

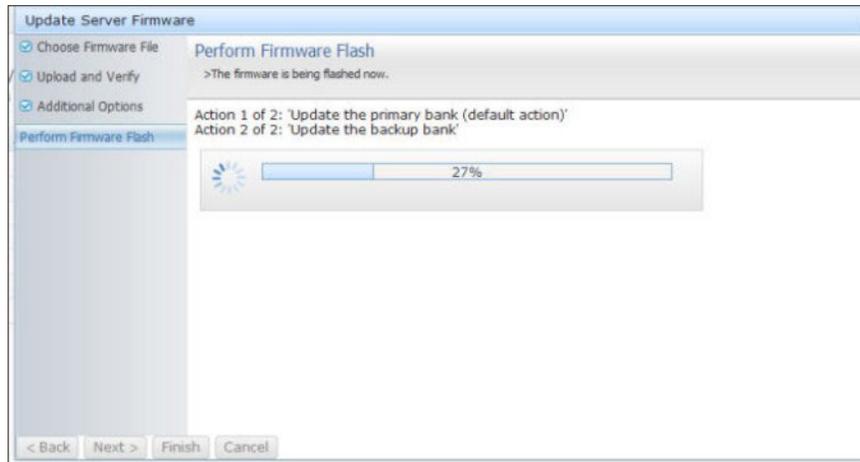
注: アクションを使用不可にして追加オプションの処理を再び開始するには、関連したアクションの横にあるチェック・ボックスをクリックします。



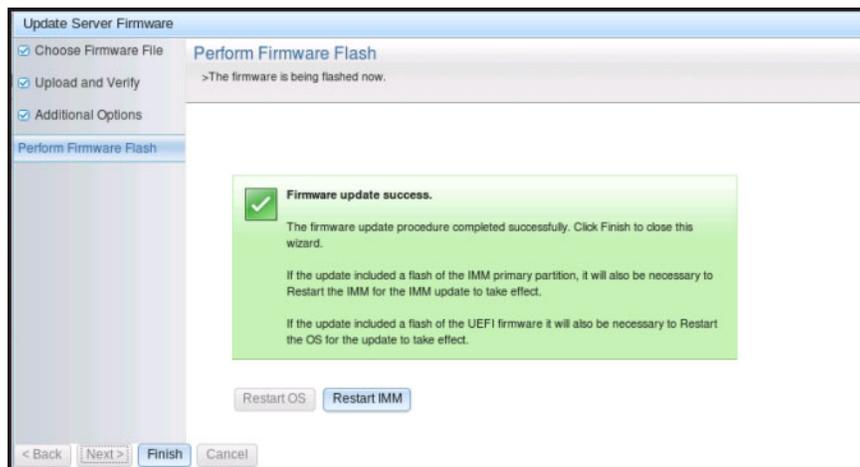
前の画面は、「Action 1」に対して、更新対象として 1 次バンクが選択されていることを示しています。「Action 2」の下で、バックアップ・バンクの更新も選択できます (前の画面を参照)。「**Next >**」をクリックすると、1 次バンクとバックアップ・バンクが同時に更新されます。

注: 「Action 1」は「Action 2」と異なっている必要があります。

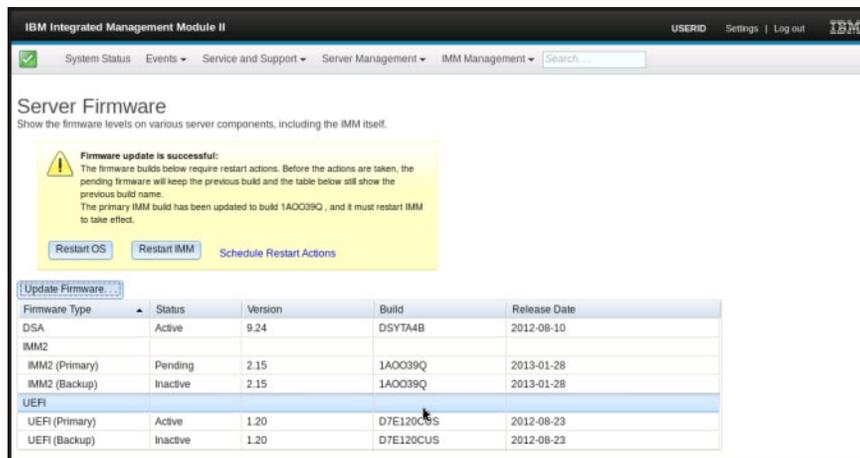
進行状況メーターに 1 次バンクとバックアップ・バンクの更新の進行状況が表示されます (次の図を参照)。



ファームウェア更新が正常に完了すると、次のようなウィンドウが開きます。表示される内容に応じて関連した操作を選択して、更新処理を完了します。



1 次ファームウェアの更新が完了しなかった場合は、「Server Firmware」画面が表示されるときに次のウィンドウが開きます。



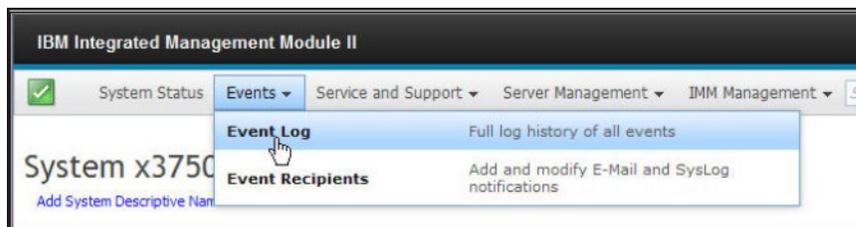
## システム・イベントの管理

「Events」メニューを使用すると、「Event Log」ヒストリーを管理し、Eメール通知および syslog 通知のイベント受信者を管理することができます。

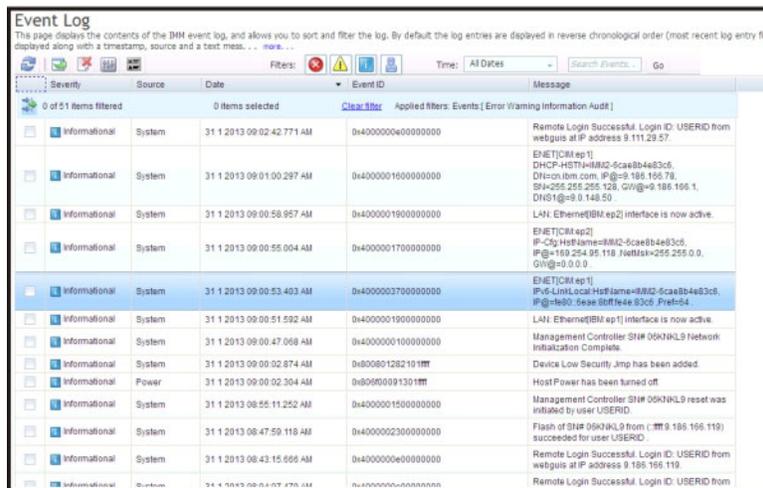
### イベント・ログの管理

「Event Log」ウィンドウを表示するには、「Event Log」オプションをクリックします。「Event Log」ウィンドウには、IMM2 によって報告されたイベントの説明と、すべてのリモート・アクセス試行および構成変更に関する情報が含まれます。ログ内のすべてのイベントには、IMM2 の日時の設定を使用したタイム・スタンプが付いています。一部のイベントは、アラートを生成します（「Event Recipients」ウィンドウでそのように構成された場合）。イベント・ログ内のイベントは、ソートしたりフィルターに掛けたりすることもできます。

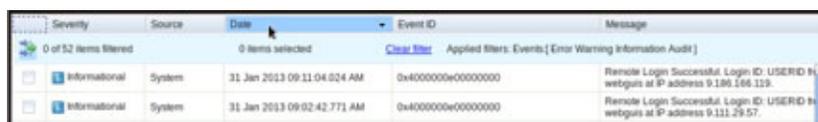
「Event Log」オプションをクリックします。次のようなウィンドウが開きます。



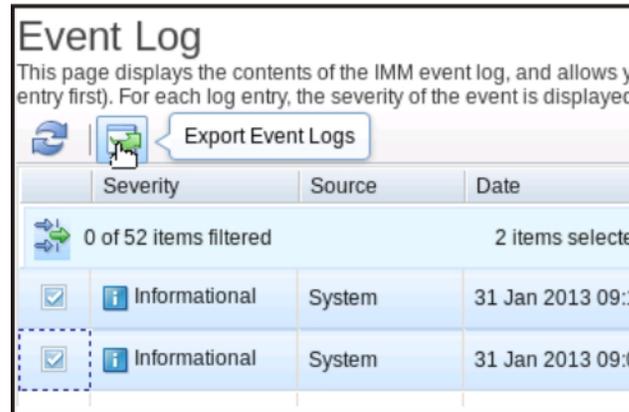
「Event Log」オプションを選択した後、次のウィンドウが開きます。



イベント・ログ内のイベントのソートおよびフィルター操作を行うには、列見出しを選択します（次の図を参照）。

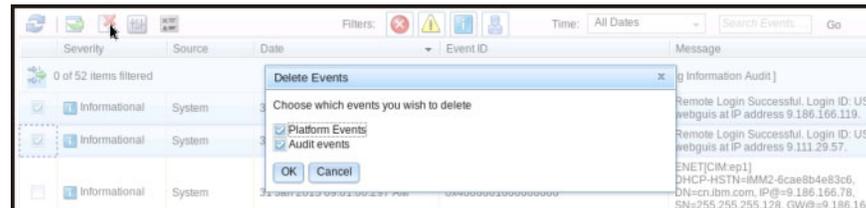


「Export」ボタンを使用して、イベント・ログ内のすべてのイベントまたは選択したイベントをファイルに保存できます。特定のイベントを選択するには、「Event Log」のメインページでイベントを1つ以上選択し、「Export」ボタンを左クリックします (次の図を参照)。

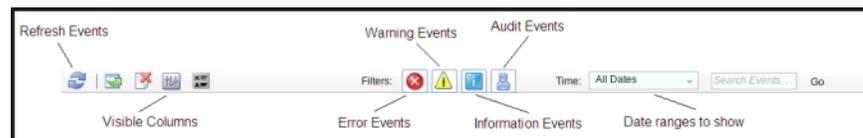


削除するイベントのタイプを選択するには、「Delete Events」をクリックします。削除するイベントのカテゴリを選択する必要があります。

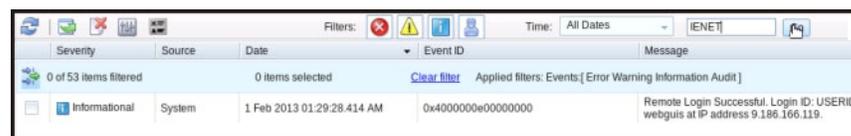
次の図は、「Delete Events」ウィンドウを示しています。



表示するイベント・ログ項目のタイプを選択するには、適切なボタンをクリックします (次の図を参照)。



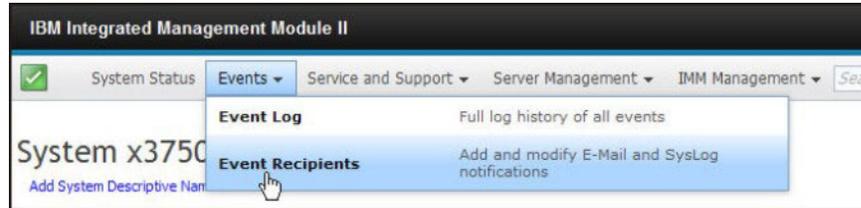
特定のタイプのイベントまたはキーワードを検索するには、「Search Events」フィールドにイベントまたはキーワードのタイプを入力して、「Go」をクリックします (次の図を参照)。



## システム・イベントの通知

E メール通知および syslog 通知を追加および変更するには、「Event Recipients」オプションを選択します。

次の図は、「Event Recipients」オプションの選択を示しています。

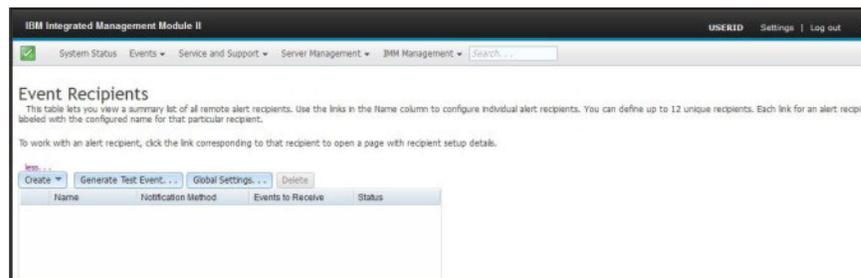


「Event Recipients」オプションを使用すると、システム・イベントの通知先を管理することができます。各受信者を構成したり、すべてのイベント受信者に適用される設定を管理したりすることができます。また、テスト・イベントを生成して、通知機能の操作を確認することもできます。

次の図は、「Event Recipients」ページを示しています。



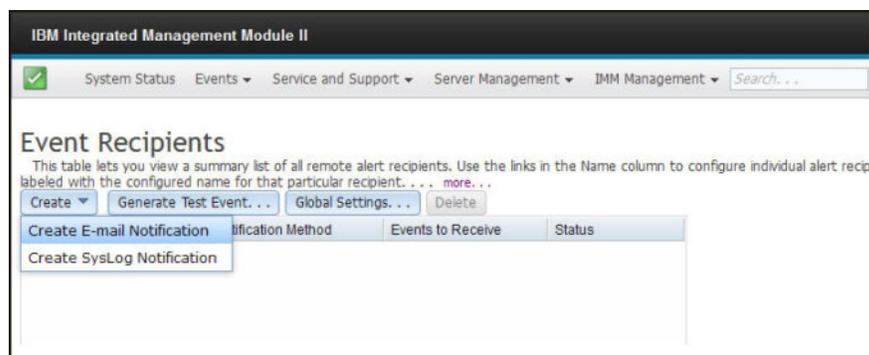
次の図は、「Event Recipients」ページで「more」リンクをクリックしたときに表示される追加情報を示しています。



## E メール通知および syslog 通知の作成

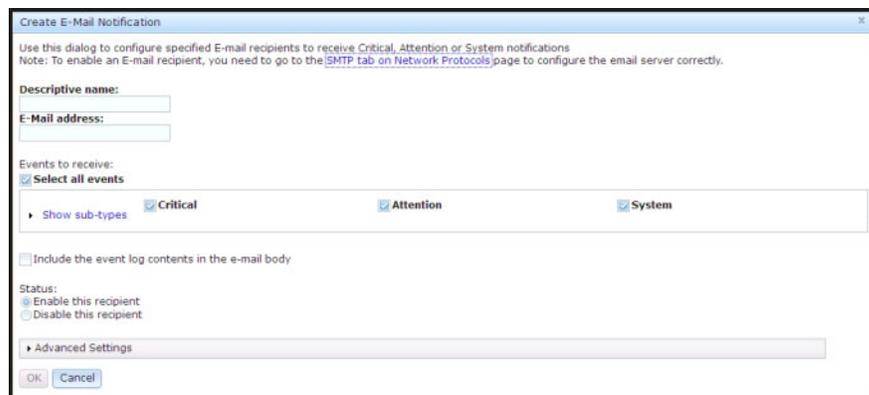
E メールと syslog の通知を作成するには、「Create」タブを選択します。

次の図は、「Create」メニューで選択可能なオプションを示しています。

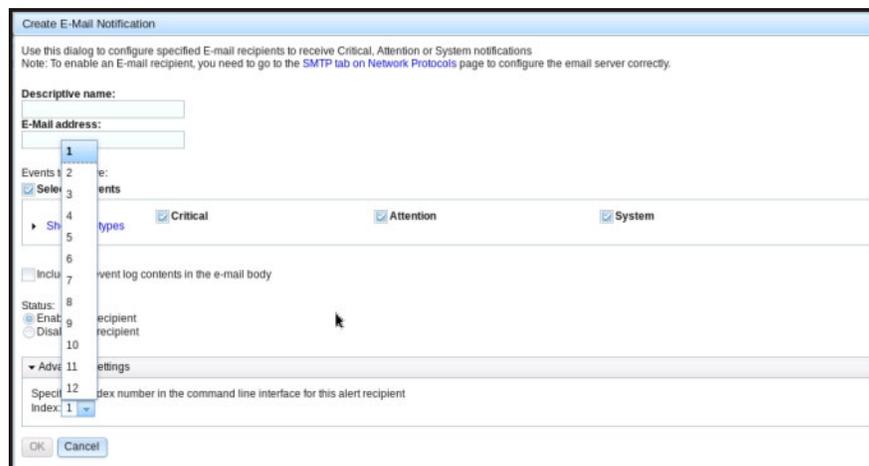


「**Create E-mail Notification**」オプションでは、ターゲットの E メール・アドレスをセットアップし、通知するイベントのタイプを選択できます。また、「**Advanced Settings**」をクリックすると、開始索引番号を選択できます。E メールにイベント・ログを含めるには、「**Include the event log contents in the e-mail body**」チェック・ボックスを選択します。

次の図は、「Create E-mail Notification」画面を示しています。



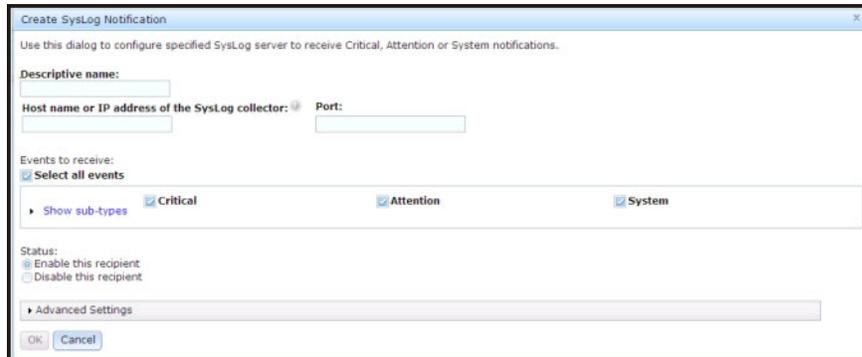
次の図は、「Advance Settings」ペインでの選択を示しています。



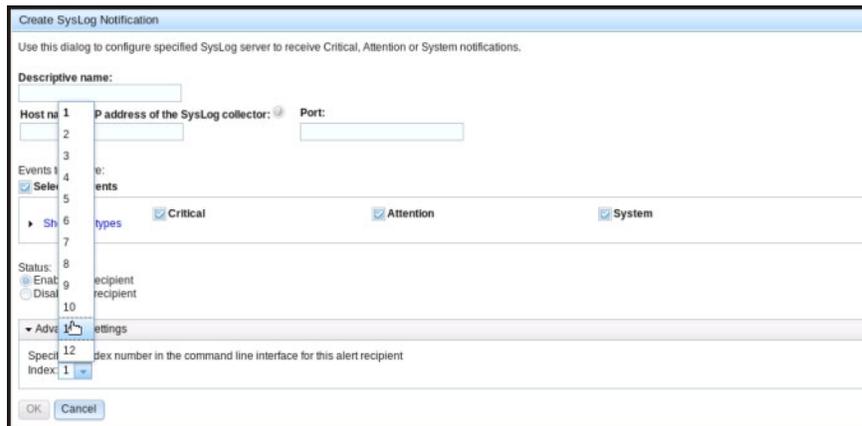
「**Create Syslog Notification**」オプションでは、syslog コレクターのホスト名と IP アドレスをセットアップし、通知するイベントのタイプを選択できます。

「Advanced Settings」をクリックすると、開始索引番号を選択できます。このタイプの通知に使用するポートを指定することもできます。

次の図は、「Create Syslog Notification」画面を示しています。



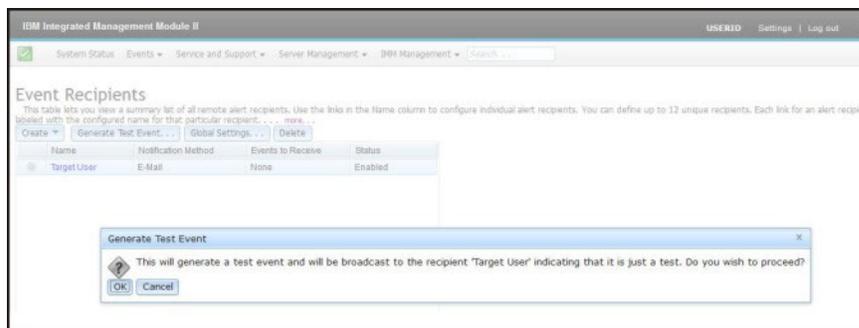
次の図は、「Advance Settings」ペインでの選択を示しています。



## テスト・イベントの生成

選択した E メール宛先にテスト E メールを送信するには、「Generate Test Event...」タブを選択します。イベント通知を選択した後、「OK」をクリックしてテスト・イベントを生成します。テスト・イベントは、これがテストであるという通知と共に受信者へ送信されます。

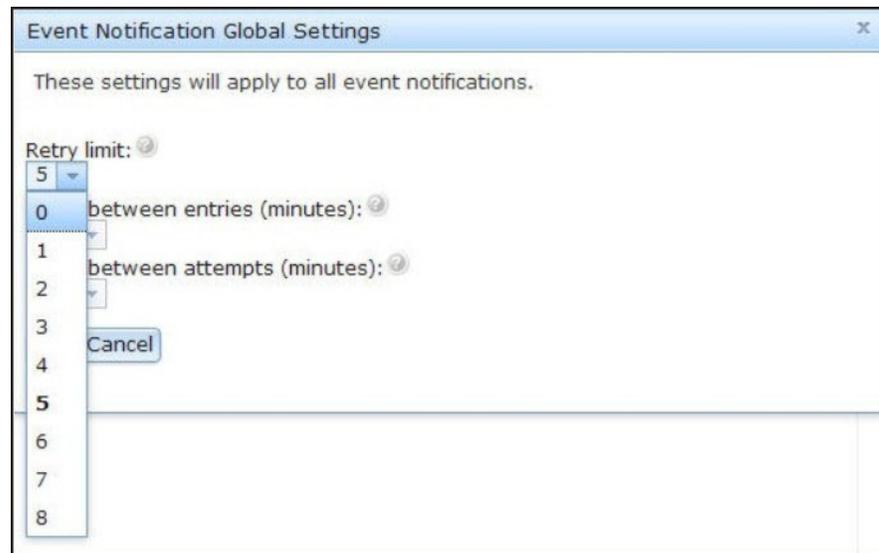
次の図は、「Generate Test Event」ウィンドウを示しています。



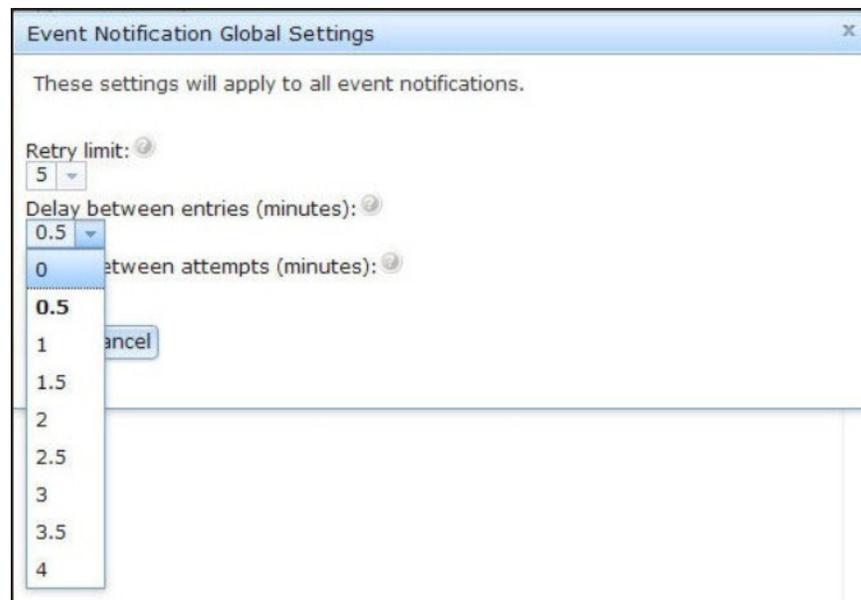
## 再試行通知に対する制限の設定

イベント通知の再試行、イベント通知項目間の遅延 (分単位)、および試行間の遅延 (分単位) に制限を設定するには、「Global Settings...」タブを使用します。

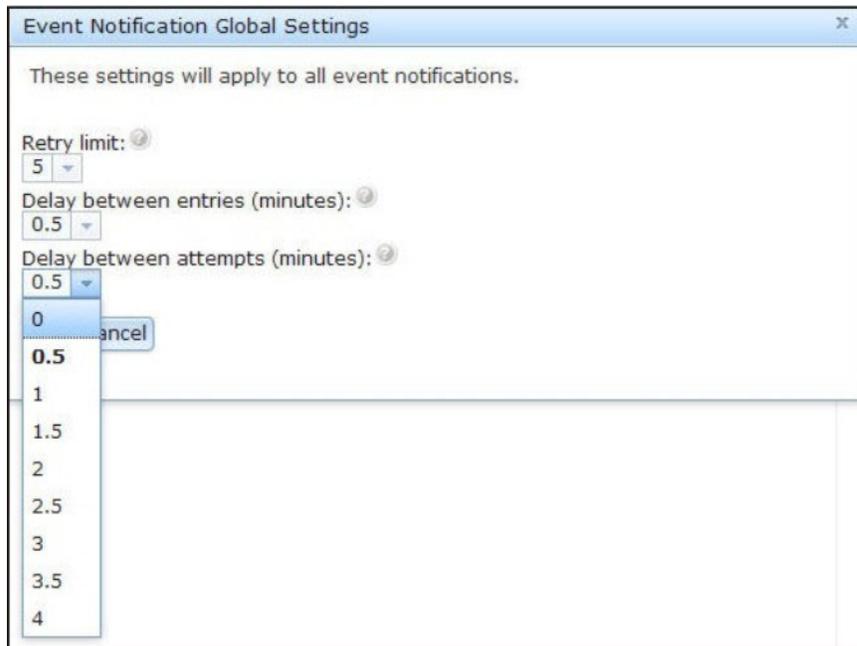
次の図は、「Retry limit」オプションの設定を示しています。



次の図は、「Delay between entries (minutes)」オプションの設定を示しています。



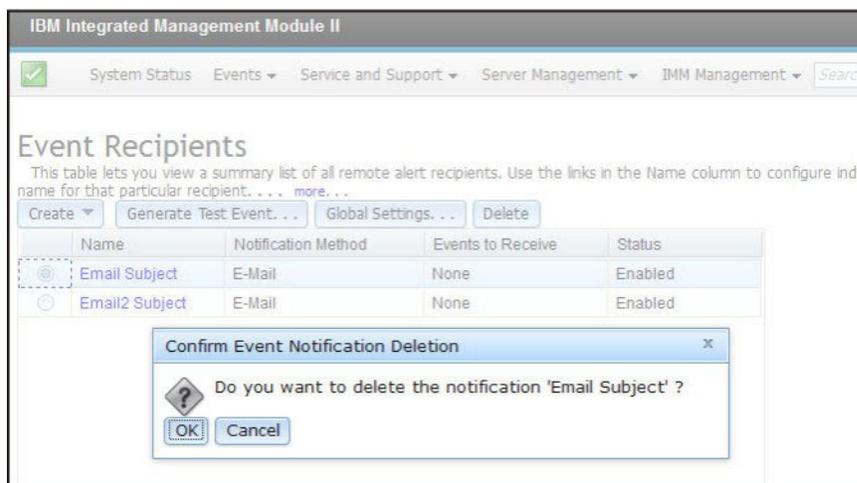
次の図は、「Delay between attempts (minutes)」オプションの設定を示しています。



## E メール通知または syslog 通知の削除

E メールまたは syslog の通知の宛先を削除するには、「Delete」タブを使用します。

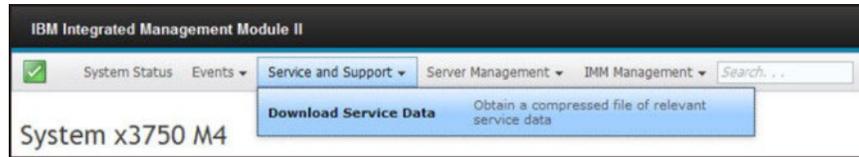
次の図は、「Confirm Event Notification Deletion」ウィンドウを示しています。



## サービスおよびサポート情報の収集

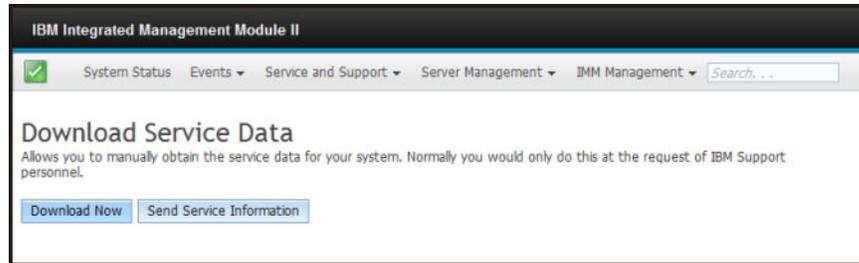
サーバーに関する情報を収集するには、「Service and Support」メニューにある「Download Service Data」オプションをクリックします。この情報を使用して、IBM サポートはお客様の問題の解決を支援することができます。

次の図は、「Service and Support」メニューを示しています。



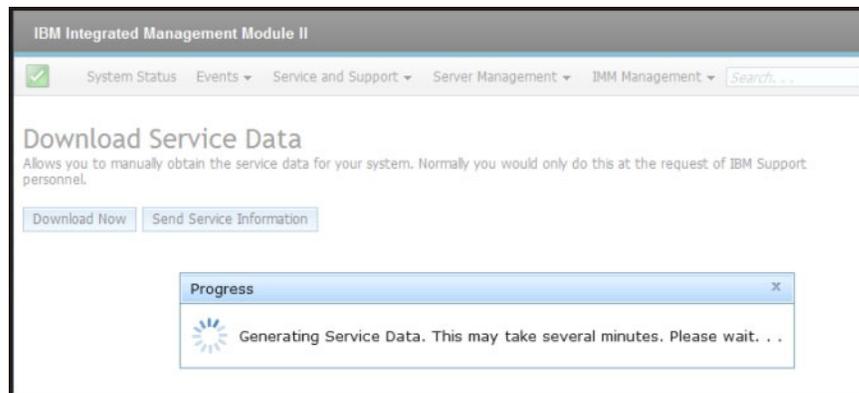
サービスおよびサポート・データをダウンロードするには、「**Download Now**」ボタンをクリックします。

次の図は、「Download Service Data」ウィンドウを示しています。

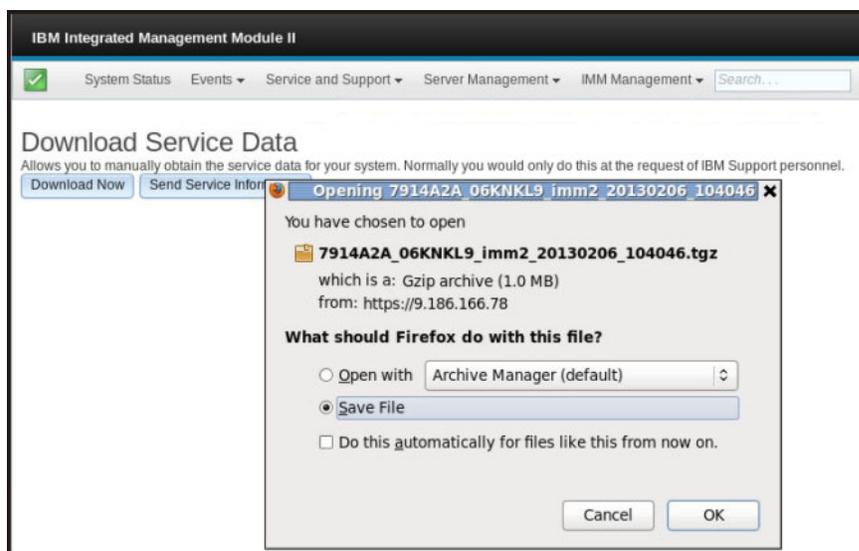


サービスおよびサポート・データを収集するプロセスが開始されます。このプロセスでは、ファイルに保存できるサービス・データを生成するために数分かかります。

サービス・データが生成されている間、次のような進行ウィンドウが表示されます。



プロセスが完了すると、ファイルの保存場所を入力するプロンプトが出ます。例については、次の図を参照してください。



## 最新の OS 障害画面データのキャプチャー

オペレーティング・システムの障害画面データをキャプチャーし、そのデータを保管するには、「Latest OS Failure Screen」オプションを使用します。IMM2 は最新のエラー・イベント情報のみを保管するため、新規のエラー・イベントが発生すると、古い OS 障害画面データは上書きされます。OS 障害画面をキャプチャーするには、OS ウォッチドッグ機能を使用可能にする必要があります。OS の実行を停止する原因となるイベントが発生すると、OS ウォッチドッグ機能が起動されます。OS 障害画面キャプチャーは、IMM2 の拡張レベル機能を使用した場合にだけ使用可能です。ご使用の IBM サーバーに取り付けられている IMM2 のレベルについて詳しくは、ご使用のサーバーの資料を参照してください。

リモート側で OS 障害画面イメージを表示するには、以下のいずれかのメニュー選択項目を選択します。

- 「Server Management」タブの「**Latest OS Failure Screen**」
- 「System Status」ページの「**Latest OS Failure Screen**」タブ

注: OS 障害画面がキャプチャーされていない場合、「System Status」ページの「Latest OS Failure Screen」タブはぼかし表示され、選択できなくなります。

次の図は、OS 障害画面を示しています。

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

---

## サーバー電源の管理

次の作業を行うには、「Power Management」タブを使用します。

- 取り付けられている電源機構に関する情報を表示する。
- 電源機構の「電力」を管理する方法を制御する。
- 全体のシステム電源を制御する。
- 取り付けられている電源機構、および現在の電源機構の容量に関する情報を表示する。
- 電力使用量のヒストリーを表示する。

「Server Management」タブの「Power Management」オプションを選択すると、電源管理に関する情報が表示され、電源管理機能を実行できます (次の図を参照)。

| Server Management ▼             | IMM Management ▼   | Search |
|---------------------------------|--|--------|
| <b>Server Firmware</b>          | View firmware levels and update firmware                               |        |
| <b>Remote Control</b>           | Allows you access into the operating system of your system             |        |
| <b>Server Properties</b>        | Various properties and settings related to your system                 |        |
| <b>Server Power Actions</b>     | Power actions such as power on, power off, and restart                 |        |
| <b>Cooling Devices</b>          | Cooling devices installed in your system                               |        |
| <b>Power Modules</b>            | Power modules installed in your system                                 |        |
| <b>Disks</b>                    | Hard disk drives installed directly in your system                     |        |
| <b>Memory</b>                   | RAM installed in your system   |        |
| <b>Processors</b>               | Physical CPUs installed in your system                                 |        |
| <b>Server Timeouts</b>          | Configure watchdogs, etc.  |        |
| <b>PXE Network Boot</b>         | Settings for how your system performs boot from PXE server             |        |
| <b>Latest OS Failure Screen</b> | Windows systems only. View an image of the most recent failure screen. |        |
| <b>Power Management</b>         | Power devices, policies, and consumption                               |        |

## 電源機構と全体のシステム電源の制御

電源機構の管理方法を制御し、オプションで Active Energy Manager を使用してキャッピング・ポリシーを設定することによってシステム全体の電源を制御するには、「Policies」タブをクリックします (次の図を参照)。

注: 「Policies」タブは、IBM Flex System では使用できません。

The screenshot displays the 'Server Power Management' interface. At the top, it says 'Manage power related policies and hardware'. Below this, there are four tabs: 'Policies', 'Power Modules', 'Power Allocation', and 'Power History'. The 'Policies' tab is selected. Underneath, the section is titled 'Power Policies'. There are two main policy areas:

- Redundant with Throttling:** This section includes a description: 'Set policies for how or if you wish to protect your system in the case of potential power module failure.' The current policy is 'Power Module Redundancy with Throttling Allowed', and there is a 'Change' button next to it.
- Power Limiting/Capping Policy:** This section includes a description: 'Set policies for how or if you wish to limit the total amount of power that the system overall is allowed to consume.' The current policy is 'No Power Limiting', and there is a 'Change' button next to it.

電源モジュール障害が発生する可能性に備えて、サーバーを保護するために使用するポリシーを選択するには、「Power Policies」ウィンドウの「Redundant with Throttling」オプションで、現行ポリシーの「Change」ボタンをクリックします。

注：電源ポリシーを選択することにより、冗長性と使用可能な電源の間でトレードオフを考慮した設定が可能です。

電源ポリシーの選択項目は、次のとおりです。

#### Redundant without Throttling

一方の電源機構が失われてもサーバーが停止せず、スロットルなしで継続して稼働することが保証されている場合に、サーバーのブートを許可します。

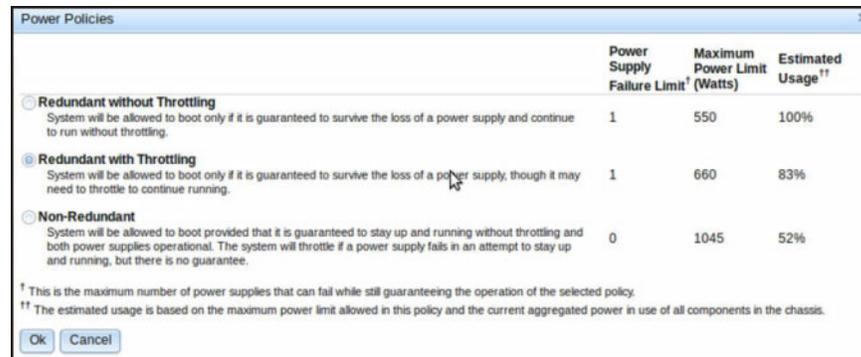
#### Redundant with Throttling

一方の電源機構が失われてもサーバーが停止しないことが保証されていて、ただし稼働を継続するにはサーバーのスロットルが必要になる可能性がある場合に、サーバーのブートを許可します。

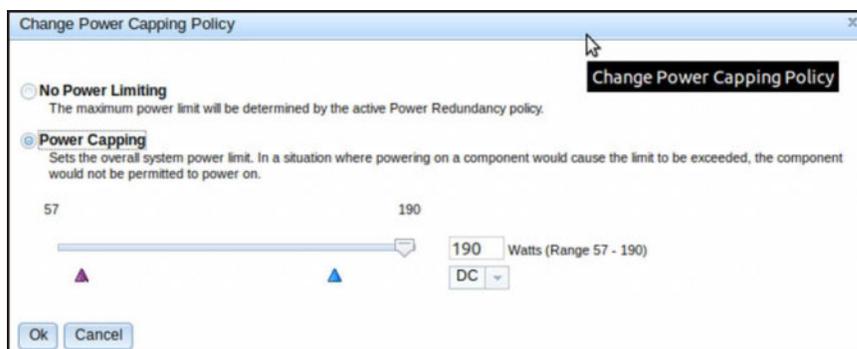
#### Non-Redundant

サーバーがスロットルなしで継続して稼働し、両方の電源機構が作動可能であることが保証されている場合に限って、サーバーのブートを許可します。電源機構が稼働を継続しようとして失敗した場合には、サーバーのスロットルが行われますが、保証はありません。

「Redundant with Throttling」オプションの「Change」ボタンを選択すると、次のウィンドウが開きます。



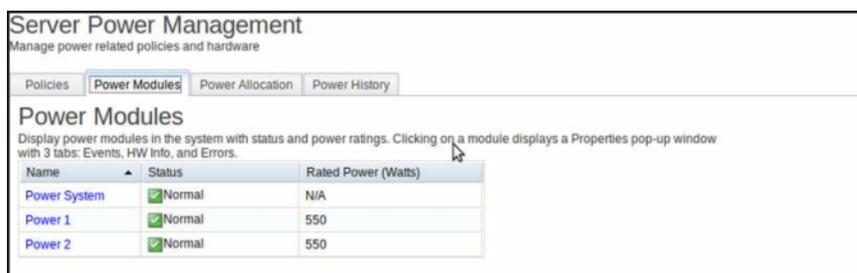
Active Energy Manager を使用して、サーバーが使用できる合計電力量を制限できません。サーバーの電力使用量に制限を設定するには、「Power Policies」ウィンドウの「Power Limiting/Capping Policy」オプションで、現行ポリシーの「Change」ボタンをクリックします。「Change Power Capping Policy」ウィンドウが開きます (次の図を参照)。



「**Power Capping**」ボタンを選択して、スライダー・マークを目的のワット数まで移動します。スライダー・マークの右下にある矢印は、Active Energy Manager が保証できる最小設定値を示しています。スライダー・マークの左下にある矢印は、過去 24 時間で最大のシステム電力使用量を示しています。これら 2 つの矢印は、電力の上限を設定する際の指針になります。

## 現在取り付けられている電源機構の表示

「**Power Modules**」タブをクリックすると、現在取り付けられている電源機構に関する情報が表示されます (次の図を参照)。



サーバー内にあるそれぞれの電源モジュールの名前が、各電源モジュールの状況と電源定格とともに表示されます。電源モジュールに関する追加情報を表示するには、電源モジュールの名前をクリックします。プロパティ・ウィンドウが開き、その特定の電源モジュールに対応する「Events」、「HW Info」、および「Errors」の 3 つのタブが表示されます。

## 電源機構の容量の表示

使用されている電源機構の容量、およびサーバーの現在の DC 電力消費量を表示するには、「**Power Allocation**」タブをクリックします (次の図を参照)。



## 電力使用量のヒストリーの表示

「Power History」タブをクリックすると、選択した期間にわたってシステムによって使用されている電力の量が表示されます。「Power History」ページの「Chart」タブから期間を選択でき、AC または DC の電源を表示するオプションもあります。平均、最小、および最大の電力使用量が表示されます (次の図を参照)。





---

## 第 7 章 Features on Demand

IMM2 Features on Demand (FoD) を使用すると、オプションのサーバーとシステム管理フィーチャーの取り付けおよび管理が可能になります。

IMM2 ファームウェアの機能およびご使用のサーバーで使用可能なフィーチャーには、いくつかのレベルがあります。ご使用のサーバーにインストールされた IMM2 ファームウェア・フィーチャーのレベルは、ハードウェアのタイプによって異なります。ご使用のサーバー内の IMM2 ハードウェアおよびフィーチャーのタイプについては、サーバーに付属の資料を参照してください。

IMM2 の機能は、FoD アクティベーション・キーを購入してインストールするとアップグレードすることができます。FoD についての追加の詳細情報は、「*Features on Demand User's Guide*」(<http://www.ibm.com/systems/x/fod/>) を参照してください。

注: IMM2 基本レベル機能を備えたサーバーでは、IBM Integrated Management Module Advanced Upgrade 機能をインストールする前に、IBM Integrated Management Module Standard Upgrade が必要です。

FoD アクティベーション・キーをオーダーするには、IBM 担当員またはビジネス・パートナーにお問い合わせいただくか、<http://www.ibm.com/systems/x/fod/> にアクセスしてください。

IMM2 Web インターフェースまたは IMM2 CLI を使用して、FoD アクティベーション・キーを手動でインストールします。これにより、購入したオプション・フィーチャーを使用できるようになります。キーをアクティブにする前に、以下のことを確認してください。

- FoD アクティベーション・キーは、IMM2 へのログインに使用するシステム上に存在しなければなりません。
- FoD オプションのオーダーが完了し、その許可コードを郵送または E メールで受け取っていないければなりません。

IMM2 Web インターフェースを使用して FoD アクティベーション・キーを管理するには、『アクティベーション・キーのインストール』、144 ページの『アクティベーション・キーの削除』、または 145 ページの『アクティベーション・キーのエクスポート』を参照してください。IMM2 CLI を使用して FoD アクティベーション・キーを管理するには、175 ページの『keycfg コマンド』を参照してください。

---

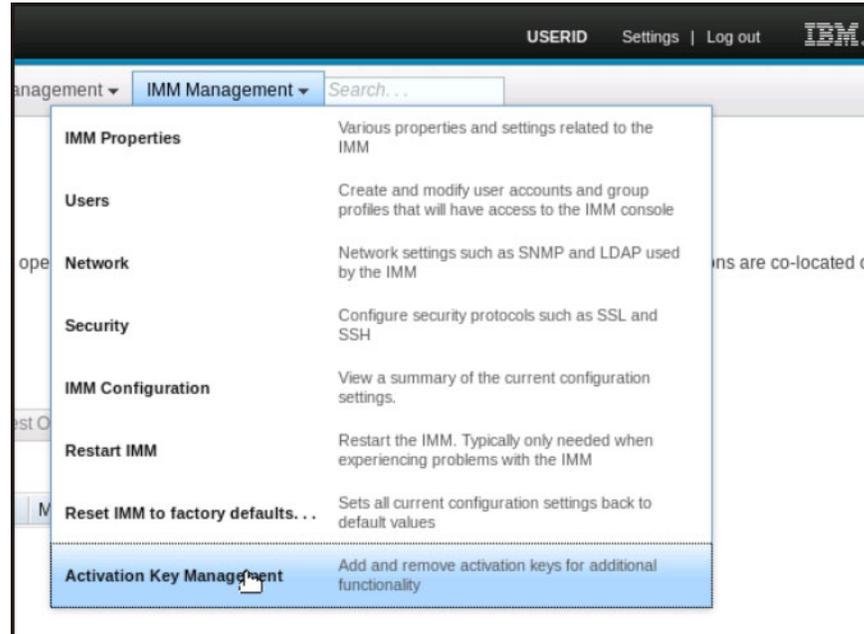
### アクティベーション・キーのインストール

ご使用のサーバーにオプション・フィーチャーを追加するには、FoD アクティベーション・キーをインストールします。

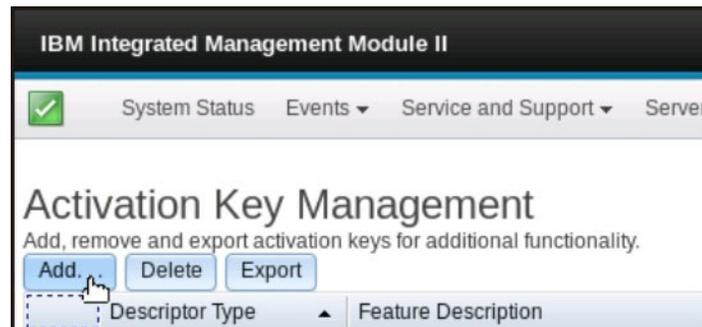
FoD アクティベーション・キーをインストールするには、以下のステップを実行してください。

1. IMM2 にログインします。詳しくは、10 ページの『IMM2 へのログイン』を参照してください。

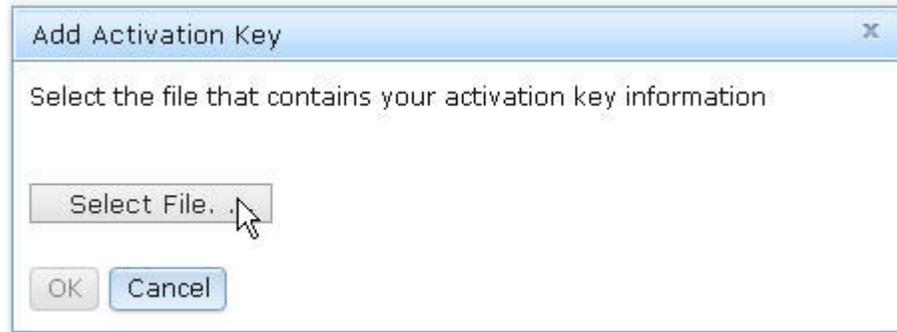
2. IMM2 Web インターフェースから「**IMM Management**」タブをクリックし、次に「**Activation Key Management**」をクリックします。



3. 「Activation Key Management」ページから、「**Add...**」をクリックします。



4. 「Add Activation Key」ウィンドウで「**Select File...**」をクリックします。次に「File Upload」ウィンドウで追加するアクティベーション・キー・ファイルを選択し、「**Open**」をクリックしてそのファイルを追加するか、「**Cancel**」をクリックしてインストールを停止します。キーの追加を完了するには「Add Activation Key」ウィンドウで「**OK**」をクリックするか、「**Cancel**」をクリックしてインストールを停止します。

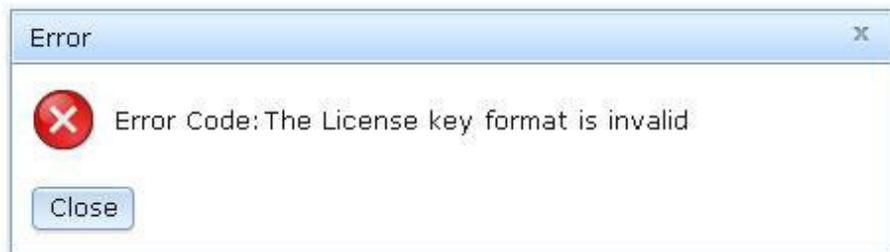


「Success」ウィンドウは、アクティベーション・キーがインストールされたことを示します。

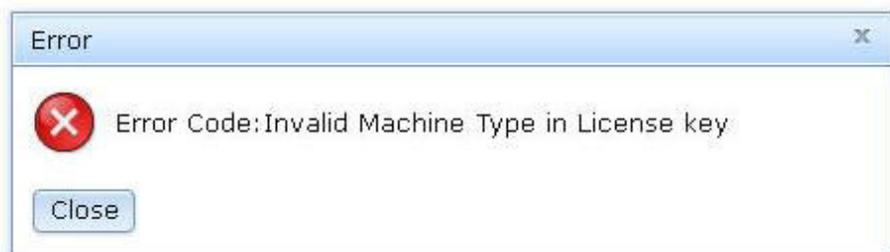


注:

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



- FoD 機能をサポートしないマシン・タイプに、アクティベーション・キーをインストールしようとしている場合、以下のエラー・ウィンドウが表示されず。



5. 「OK」をクリックして「Success」ウィンドウを閉じます。

選択されたアクティベーション・キーはサーバーに追加され、「Activation Key Management」ページに表示されます。



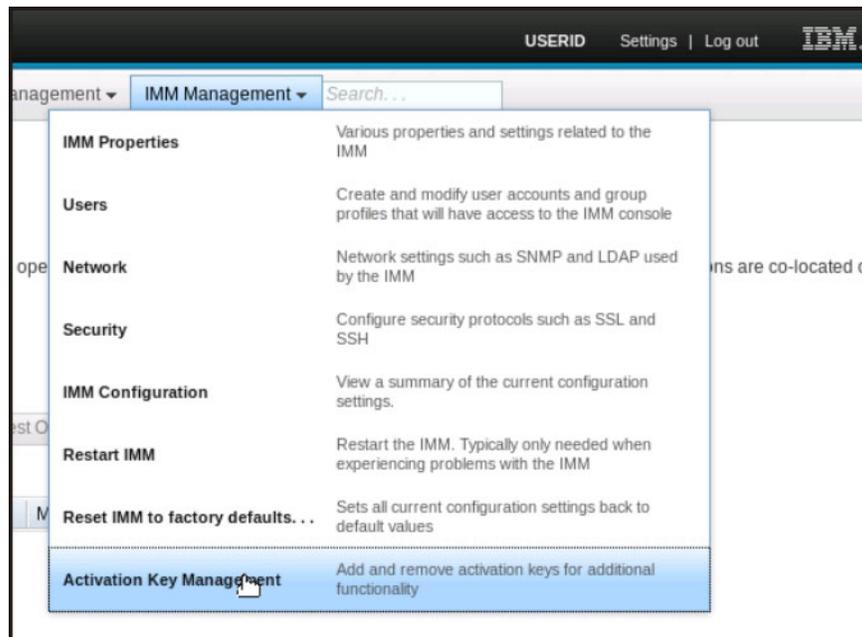
| Descriptor Type | Feature Description                               | Unique IDs  | Constraints    |
|-----------------|---|-------------|----------------|
| 1               | IBM Integrated Management Module Advanced Upgrade | 791406KNKL9 | No Constraints |

## アクティベーション・キーの削除

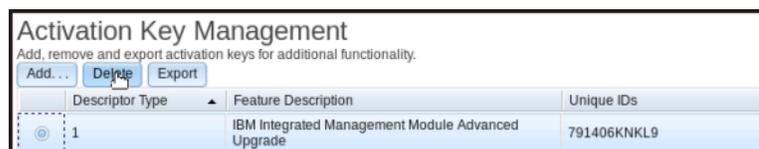
ご使用のサーバーからオプション・フィーチャーを削除するには、FoD アクティベーション・キーを削除します。

FoD アクティベーション・キーを削除するには、以下のステップを実行してください。

1. IMM2 にログインします。詳しくは、10 ページの『IMM2 へのログイン』を参照してください。
2. IMM2 Web インターフェースから「IMM Management」タブをクリックし、次に「Activation Key Management」をクリックします。



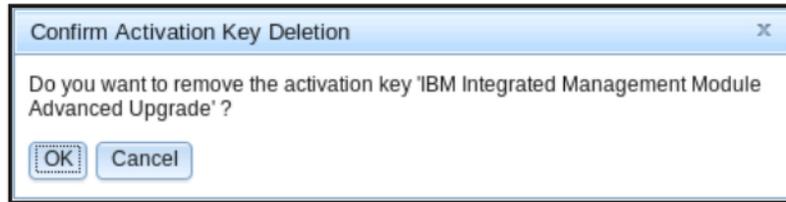
3. 「Activation Key Management」ページから、削除するアクティベーション・キーを選択して、「Delete」をクリックします。



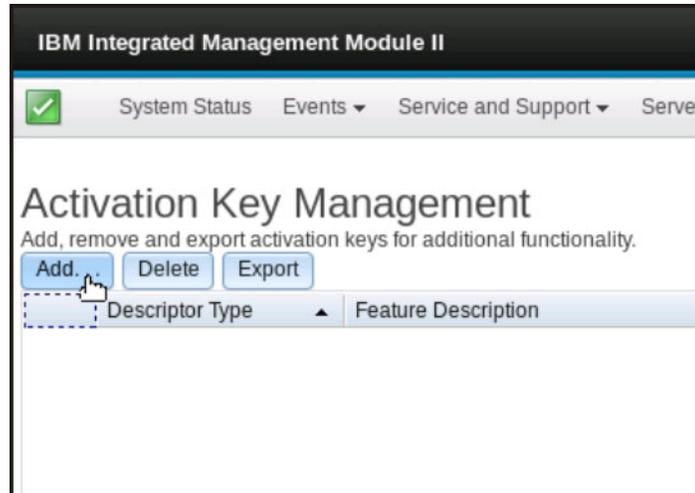
| Descriptor Type | Feature Description                               | Unique IDs  |
|-----------------|---|-------------|
| 1               | IBM Integrated Management Module Advanced Upgrade | 791406KNKL9 |

4. 「Confirm Activation Key Deletion」ウィンドウで、「OK」をクリックしてアクティベーション・キーの削除を確認するか、「Cancel」をクリックしてそのキ

ー・ファイルを保持します。



選択されたアクティベーション・キーはサーバーから削除され、「Activation Key Management」ページには表示されません。



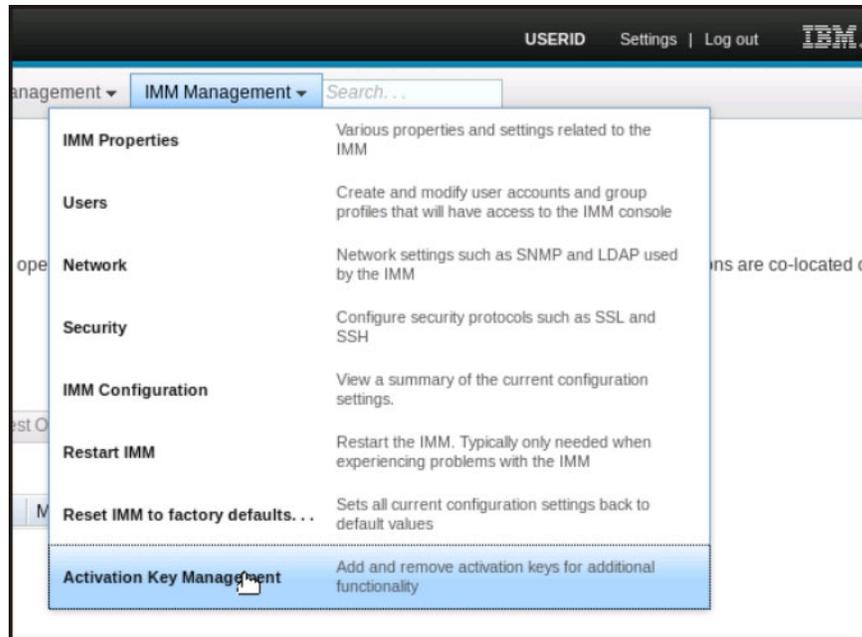
---

## アクティベーション・キーのエクスポート

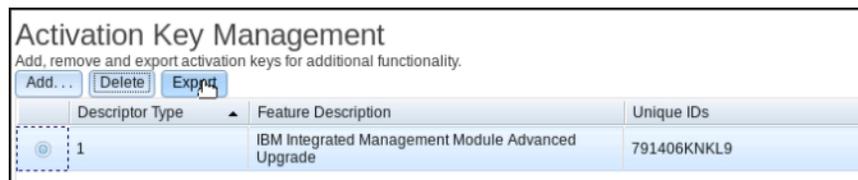
ご使用のサーバーからオプション・フィーチャーをエクスポートするには、FoD アクティベーション・キーをエクスポートします。

FoD アクティベーション・キーをエクスポートするには、次の手順で行います。

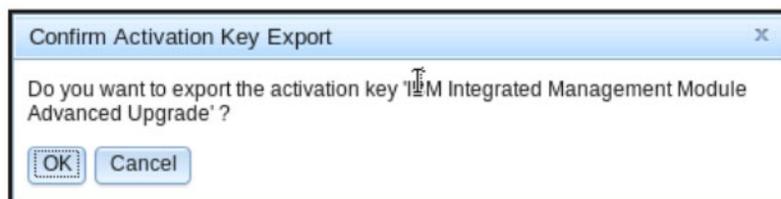
1. IMM2 にログインします。詳しくは、10 ページの『IMM2 へのログイン』を参照してください。
2. IMM2 Web インターフェースから「**IMM Management**」タブをクリックし、次に「**Activation Key Management**」をクリックします。



- 「Activation Key Management」ページから、エクスポートするアクティベーション・キーを選択して、「Export」をクリックします。



- 「Confirm Activation Key Export」ウィンドウで、「OK」をクリックしてアクティベーション・キーのエクスポートを確認するか、「Cancel」をクリックしてキーのエクスポート要求を取り消します。



- ファイルを保存するディレクトリーを選択します。 選択したアクティベーション・キーがサーバーからエクスポートされます。

---

## 第 8 章 コマンド・ライン・インターフェース

IMM2 コマンド・ライン・インターフェースを使用すると、Web インターフェースを使用せずに IMM2 にアクセスすることができます。このインターフェースは、Web インターフェースによって提供される管理機能のサブセットを提供します。

CLI には、Telnet または SSH セッションからアクセスすることができます。CLI コマンドを発行するには、IMM2 に認証されている必要があります。

---

### IPMI を使用した IMM2 の管理

IMM2 は、標準でユーザー ID 1 がユーザー名 USERID、パスワード PASSWORD (英字の O でなくゼロ) に初期設定されています。このユーザーには、Supervisor アクセス権限があります。

**重要:** 拡張セキュリティーを使用するには、初期構成時にこのユーザー名とパスワードを変更してください。

また、IMM2 は以下の IPMI リモート・サーバー管理機能を提供します。

#### コマンド・ライン・インターフェース

CLI では、IPMI 2.0 プロトコルを使用してサーバー管理機能への直接アクセスが可能です。IPMItool を使用して、サーバー電源の制御、サーバー情報の表示、およびサーバーの識別を行うためのコマンドを発行することができます。IPMItool について詳しくは、『IPMItool の使用』を参照してください。

#### Serial over LAN

リモート・ロケーションからサーバーを管理するには、IPMItool を使用して、Serial over LAN (SOL) 接続を確立します。IPMItool について詳しくは、『IPMItool の使用』を参照してください。

### IPMItool の使用

IPMItool は、IPMI システムを管理および構成するのに使用できるさまざまなツールを提供します。IPMItool インバンドまたはアウト・オブ・バンドを使用して、IMM2 を管理および構成することができます。

IPMItool の詳細について、あるいは IPMItool をダウンロードするには、<http://sourceforge.net/> にアクセスしてください。

---

### コマンド・ライン・インターフェースへのアクセス

CLI にアクセスするには、IMM2 の IP アドレスに対して Telnet または SSH セッションを開始します (詳しくは、148 ページの『Serial-to-Telnet または SSH リダイレクトの構成』を参照)。

---

## コマンド・ライン・セッションへのログイン

コマンド・ラインにログインするには、以下のステップを実行します。

1. IMM2 との接続を確立します。
2. ユーザー名プロンプトに、ユーザー ID を入力します。
3. パスワードのプロンプトで、IMM2 へのログインに使用するパスワードを入力します。

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

---

## Serial-to-Telnet または SSH リダイレクトの構成

Serial-to-Telnet または SSH リダイレクトにより、システム管理者が IMM2 をシリアル端末サーバーとして使用できるようになります。シリアル・リダイレクトが使用可能な場合、Telnet または SSH 接続からサーバーのシリアル・ポートにアクセスすることができます。

注:

1. IMM2 では、最大 2 つの Telnet セッションをオープンすることができます。これらの Telnet セッションは、それぞれ独自にシリアル・ポートにアクセスでき、したがって、複数のユーザーが、リダイレクトされたシリアル・ポートの並行ビューを持つことができます。
2. CLI の `console 1` コマンドを使用して、COM ポートとのシリアル・リダイレクト・セッションを開始することができます。

### セッションの例

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
password: ***** (Press Enter.)
system> console 1 (Press Enter.)
```

この時点で、COM2 からのすべてのトラフィックは、Telnet セッションへ経路指定されます。Telnet または SSH セッションからのすべてのトラフィックは、COM2 へ経路指定されます。

ESC (

終了キー・シーケンスを入力して、CLI に戻ります。この例では、Esc を押してから左括弧を入力します。CLI プロンプトが表示され、IMM2 CLI へ戻ることを示します。

```
system>
```

---

## コマンド構文

コマンドを使用する前に、以下のガイドラインをお読みください。

- 各コマンドは、次の形式をとります。

```
command [arguments] [-options]
```

- コマンド構文には大/小文字の区別があります。
- コマンド名は、すべて小文字です。
- すべての引数は、コマンドの直後に置く必要があります。オプションは、引数の直後に置く必要があります。
- 各オプションの前には、必ずハイフン (-) を付けます。オプションには、短いオプション (単一の英字) と長いオプション (複数の英字) があります。
- オプションに引数がある場合は、その引数を必ず指定する必要があります。

```
ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
```

ここで、**ifconfig** はコマンドで、eth0 は引数であり、-i、-g、および -s はオプションです。この例では、3 つのオプションのすべてが引数を備えています。

- ブラケットは、引数またはオプションが省略可能であることを示しています。ブラケットは、入力するコマンドの一部ではありません。

---

## 機能および制限

CLI には、以下の機能と制限事項があります。

- 異なるアクセス方式 (Telnet または SSH) での複数の並行 CLI セッションが許可されます。どの時点でも、最大 2 つの Telnet コマンド・ライン・セッションをアクティブにすることができます。

注: Telnet セッションの数は構成可能で、有効な値は 0、1、および 2 です。値 0 は、Telnet インターフェースが使用不可であることを意味します。

- 1 行 (スペースも含めて 160 文字が限度) につき 1 つのコマンドが許可されます。
- 長いコマンドに継続文字はありません。唯一の編集機能は、入力したばかりの文字を消去する Backspace キーです。
- 上下の矢印キーを使用すると、最後の 8 つのコマンドをブラウズできます。

**history** コマンドを使用すると最後の 8 つのコマンドが入ったリストが表示され、これをショートカットとして使用して、次の例のようにコマンドを実行できます。

```
system > history
0 ifconfig eth0
1 readlog
2 readlog
3 readlog
4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
```

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

- CLI では、出力バッファの限度は 2 KB です。バッファリングはありません。個々のコマンドの出力は、2048 文字を超えることができません。この制限は、シリアル・リダイレクト・モードでは適用されません (シリアル・リダイレクトの間、データはバッファに格納されます)。
- コマンドの実行が完了した後、画面にコマンドの出力が表示されます。このため、コマンドはリアルタイムの実行状況を報告できません。例えば、**flashing** コマンドの詳細モードでは、フラッシュの進行状況はリアルタイムでは表示されません。コマンドの実行が完了した後に表示されます。
- コマンドの実行状況を表すために、次の例のように、単純なテキスト・メッセージが使用されます。

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

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

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

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

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

---

## アルファベット順のコマンド・リスト

すべての IMM2 CLI コマンドの完全なリスト (アルファベット順) は、次のとおりです。

- 162 ページの『`accsecCfg` コマンド』
- 164 ページの『`alertCfg` コマンド』
- 202 ページの『`alertEntries` コマンド』
- 165 ページの『`asu` コマンド』
- 168 ページの『`backup` コマンド』
- 205 ページの『`batch` コマンド』
- 206 ページの『`clearCfg` コマンド』
- 153 ページの『`clearlog` コマンド』

- 206 ページの『clock コマンド』
- 161 ページの『console コマンド』
- 169 ページの『dhcpinfo コマンド』
- 170 ページの『dns コマンド』
- 172 ページの『ethtousb コマンド』
- 152 ページの『exit コマンド』
- 153 ページの『fans コマンド』
- 153 ページの『ffdc コマンド』
- 173 ページの『gprofile コマンド』
- 152 ページの『help コマンド』
- 152 ページの『history コマンド』
- 207 ページの『identify コマンド』
- 173 ページの『ifconfig コマンド』
- 207 ページの『info コマンド』
- 175 ページの『keycfg コマンド』
- 177 ページの『ldap コマンド』
- 154 ページの『led コマンド』
- 178 ページの『ntp コマンド』
- 179 ページの『passwordcfg コマンド』
- 180 ページの『ports コマンド』
- 181 ページの『portcfg コマンド』
- 160 ページの『power コマンド』
- 160 ページの『pxeboot コマンド』
- 156 ページの『readlog コマンド』
- 161 ページの『reset コマンド』
- 208 ページの『resetsp コマンド』
- 182 ページの『restore コマンド』
- 183 ページの『restoredefaults コマンド』
- 183 ページの『set コマンド』
- 157 ページの『show コマンド』
- 184 ページの『smtp コマンド』
- 184 ページの『snmp コマンド』
- 187 ページの『snmpalerts コマンド』
- 208 ページの『spreset コマンド』
- 189 ページの『srcfg コマンド』
- 189 ページの『sshcfcg コマンド』
- 190 ページの『ssl コマンド』
- 191 ページの『sslcfcg コマンド』
- 158 ページの『syshealth コマンド』
- 195 ページの『telnetcfg コマンド』

- 158 ページの『temps コマンド』
- 195 ページの『thermal コマンド』
- 195 ページの『timeouts コマンド』
- 196 ページの『usbeth コマンド』
- 196 ページの『users コマンド』
- 159 ページの『volts コマンド』
- 159 ページの『vpd コマンド』

---

## ユーティリティー・コマンド

ユーティリティー・コマンドは、以下のとおりです。

- 『exit コマンド』
- 『help コマンド』
- 『history コマンド』

### exit コマンド

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

### help コマンド

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

### history コマンド

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

例:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

---

## モニター・コマンド

モニター・コマンドは、以下のとおりです。

- 『clearlog コマンド』
- 『fans コマンド』
- 『ffdc コマンド』
- 154 ページの 『led コマンド』
- 156 ページの 『readlog コマンド』
- 157 ページの 『show コマンド』
- 158 ページの 『syshealth コマンド』
- 158 ページの 『temps コマンド』
- 159 ページの 『volts コマンド』
- 159 ページの 『vpd コマンド』

### clearlog コマンド

**clearlog** コマンドを使用すると、IMM2 のイベント・ログを消去します。このコマンドを使用するには、イベント・ログを消去する権限を持っている必要があります。

### fans コマンド

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

例:

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

### ffdc コマンド

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

**ffdc** コマンドと一緒に使用するコマンドのリストを次に示します。

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

次の表は、オプションの引数を示しています。

| オプション | 説明    | 値   |
|-------|-------|---|
| -t    | タイプ番号 | 1 (プロセッサ・ダンプ) および 4 (サービス・データ)。デフォルトは 1 です。 |

| オプション             | 説明                                   | 値   |
|-------------------|--------------------------------------|---|
| -f <sup>1</sup>   | リモート・ファイル名<br>または sftp ターゲット・ディレクトリー | sftp の場合は、ディレクトリー名 (~/<br>または /tmp/) に絶対パスまたは後書きの / を使用します。デフォルト値は、システムが生成した名前です。 |
| --ip <sup>1</sup> | tftp/sftp サーバーのアドレス                  |   |
| -pn <sup>1</sup>  | tftp/sftp サーバーのポート番号                 | デフォルト値は 69/22 です。   |
| -u <sup>1</sup>   | sftp サーバーのユーザー名                      |   |
| -pw <sup>1</sup>  | sftp サーバーのパスワード                      |   |

1. **generate** コマンドおよび **copy** コマンドの追加引数

構文:

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

例:

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120317-153327.tgz
```

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120926-105320.tgz
system>
```

## led コマンド

**led** コマンドは、LED の状態を表示および設定するために使用します。

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

次の表は、オプションの引数を示しています。

| オプション     | 説明                                   | 値            |
|-----------|--------------------------------------|--------------|
| -l        | システムおよびそのサブコンポーネントにあるすべての LED の状況の取得 |              |
| -chklog   | チェック・ログ LED をオフにする                   | off          |
| -identify | エンクロージャー識別 LED の状態の変更                | off、on、blink |
| -d        | 識別 LED を指定された時間だけオンにする               | 時間 (秒)       |

構文:

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

例:

```
system> led
Fault                Off
Identify              On           Blue
Chklog               Off
Power                Off
```

```
system> led -l
Label                Location          State           Color
Battery              Planar            Off
BMC Heartbeat        Planar            Blink           Green
BRD                  Lightpath Card   Off
Channel A            Planar            Off
Channel B            Planar            Off
Channel C            Planar            Off
Channel D            Planar            Off
Channel E            Planar            Off
Chklog               Front Panel      Off
CNFG                 Lightpath Card   Off
CPU                  Lightpath Card   Off
CPU 1                Planar            Off
CPU 2                Planar            Off
DASD                 Lightpath Card   Off
DIMM                 Lightpath Card   Off
DIMM 1               Planar            Off
DIMM 10              Planar            Off
DIMM 11              Planar            Off
DIMM 12              Planar            Off
DIMM 13              Planar            Off
```

|             |                 |     |      |
|-------------|-----------------|-----|------|
| DIMM 14     | Planar          | Off |      |
| DIMM 15     | Planar          | Off |      |
| DIMM 16     | Planar          | Off |      |
| DIMM 2      | Planar          | Off |      |
| DIMM 3      | Planar          | Off |      |
| DIMM 4      | Planar          | Off |      |
| DIMM 5      | Planar          | Off |      |
| DIMM 6      | Planar          | Off |      |
| DIMM 7      | Planar          | Off |      |
| DIMM 8      | Planar          | Off |      |
| DIMM 9      | Planar          | Off |      |
| FAN         | Lightpath Card  | Off |      |
| FAN 1       | Planar          | Off |      |
| FAN 2       | Planar          | Off |      |
| FAN 3       | Planar          | Off |      |
| Fault       | Front Panel (+) | Off |      |
| Identify    | Front Panel (+) | On  | Blue |
| LINK        | Lightpath Card  | Off |      |
| LOG         | Lightpath Card  | Off |      |
| NMI         | Lightpath Card  | Off |      |
| OVER SPEC   | Lightpath Card  | Off |      |
| PCI 1       | FRU             | Off |      |
| PCI 2       | FRU             | Off |      |
| PCI 3       | FRU             | Off |      |
| PCI 4       | FRU             | Off |      |
| Planar      | Planar          | Off |      |
| Power       | Front Panel (+) | Off |      |
| PS          | Lightpath Card  | Off |      |
| RAID        | Lightpath Card  | Off |      |
| Riser 1     | Planar          | Off |      |
| Riser 2     | Planar          | Off |      |
| SAS ERR     | FRU             | Off |      |
| SAS MISSING | Planar          | Off |      |
| SP          | Lightpath Card  | Off |      |
| TEMP        | Lightpath Card  | Off |      |
| VRM         | Lightpath Card  | Off |      |
| system>     |                 |     |      |

## readlog コマンド

**readlog** コマンドは、IMM2 イベント・ログ項目を一度に 5 つずつ表示するために使用します。項目は、最も新しいものから最も古いものへという順序で表示されます。

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

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

**readlog -f** は、カウンターをリセットし、イベント・ログ内の最初の 5 項目を、最も新しいものから順に表示します。

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

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

**readlog -i ip\_address** は、イベント・ログが保存される TFTP または SFTP サーバーの IPv4 あるいは IPv6 IP アドレスを設定します。**-i** および **-I** コマンド・オプションは一緒に使用され、ロケーションを指定します。

**readlog -l filename** は、イベント・ログ・ファイルのファイル名を設定します。**-i** および **-I** コマンド・オプションは一緒に使用され、ロケーションを指定します。

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

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

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

構文:

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

例:

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
  Login ID: 'USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
  Login ID: 'USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
  being used: 0x00-09-6B-CA-0C-80
system>
```

## show コマンド

**show** コマンドは、シンプルな IMM2 の設定を表示するために使用します。

- **show** コマンドは、**set** コマンドを使用して設定された値を表示します。
- 設定値は、ディレクトリー・ツリーのように編成されます。**show -r** コマンド・オプションを使用すると、完全なツリーを表示します。
- このような一部の設定 (環境変数など) は、CLI によって使用されます。

次の表は、オプションの引数を示しています。

| オプション        | 説明           | 値 |
|--------------|--------------|---|
| <i>value</i> | 表示するパスまたは設定値 |   |
| -r           | 設定を再帰的に表示    |   |

構文:

```
show [options]
option:
  value
  -r
```

## syshealth コマンド

**syshealth** コマンドは、サーバーのヘルスの要約を表示するために使用します。電源状態、システム状態、再始動カウント、および IMM2 ソフトウェア状況が表示されます。

例:

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

## temps コマンド

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

例:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
      WR      W      T      SS      HS
-----
CPU1  65/18  72/22  80/27  85/29  90/32
CPU2  58/14  72/22  80/27  85/29  90/32
DASD1 66/19  73/23  82/28  88/31  92/33
Amb   59/15  70/21  83/28  90/32  95/35
system>
```

注:

- 出力には、次の列見出しがあります。

WR: 警告リセット

W: 警告

T: 温度 (現行値)

SS: ソフト・シャットダウン

HS: ハード・シャットダウン

- 温度値は、すべて華氏/摂氏となっています。

## volts コマンド

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

例:

```
system> volts
      HSL  SSL  WL  WRL  V  WRH  WH  SSH  HSH
-----
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                                3.45
VRM2                                5.45
system>
```

注: 出力には、次の列見出しがあります。

HSL: ハード・シャットダウン低

SSL: ソフト・シャットダウン低

WL: 警告低

WRL: 警告リセット低

V: 電圧 (現行値)

WRH: 警告リセット高

WH: 警告高

SSH: ソフト・シャットダウン高

HSH: ハード・シャットダウン高

## vpd コマンド

**vpd** コマンドは、システム (sys)、IMM2 (imm)、サーバー BIOS (uefi)、サーバーの Dynamic System Analysis Preboot (dsa)、サーバー・ファームウェア (fw)、およびサーバー・コンポーネント (comp) の重要プロダクト・データを表示します。Web インターフェースの場合と同じ情報が表示されます。

構文:

```
vpd [options]
option:
  -sys
  -imm
  -uefi
  -dsa
  -fw
  -comp
```

vpd コマンドを使用すると、サーバーのさまざまな部分の重要プロダクト・データが表示されます。

| オプション | 説明                              |
|-------|---------------------------------|
| -sys  | システムの重要プロダクト・データを表示します。         |
| -imm  | IMM2 コントローラーの重要プロダクト・データを表示します。 |
| -uefi | BIOS の重要プロダクト・データを表示します。        |

| オプション | 説明                              |
|-------|---------------------------------|
| -dsa  | Diag の重要プロダクト・データを表示します。        |
| -fw   | システム・ファームウェアの重要プロダクト・データを表示します。 |
| -comp | システム・コンポーネントの重要プロダクト・データを表示します。 |

例:

```
system> vpd -dsa
Type      Version      Build      ReleaseDate
-----
DSA      9,25        DSYTA5A   2012/07/31
system>
```

## サーバーの電源および再始動制御コマンド

サーバーの電源および再始動コマンドは、以下のとおりです。

- 『power コマンド』
- 『pxeboot コマンド』
- 161 ページの 『reset コマンド』

### power コマンド

**power** コマンドは、サーバーの電源を制御するために使用します。 **power** コマンドと発行するには、電源および再始動アクセス権限を持っている必要があります。

**power on** は、サーバーの電源をオンにします。

**power off** はサーバーの電源をオフにします。 **-s** オプションは、サーバーの電源をオフにする前に、オペレーティング・システムをシャットダウンします。

**power state** は、サーバーの電源の状態 (オンかオフか) と、サーバーの現在の状態を表示します。

**power cycle** はサーバーの電源をいったんオフにしてから、再びオンにします。 **-s** オプションは、サーバーの電源をオフにする前に、オペレーティング・システムをシャットダウンします。

構文:

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

### pxeboot コマンド

**pxeboot** コマンドは、Preboot eXecution Environment の状態を表示および設定するために使用します。

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

| オプション | 説明   | 値                |
|-------|--|------------------|
| -en   | 次回のシステム再始動の際の Preboot eXecution Environment の状態を設定 | enabled、disabled |

構文:

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

例:

```
system> pxeboot
-en disabled
system>
```

## reset コマンド

**reset** コマンドは、サーバーを再始動するために使用します。このコマンドを使用するには、電源および再始動アクセス権限を持っている必要があります。**-s** オプションは、サーバーを再始動する前に、オペレーティング・システムをシャットダウンします。

構文:

```
reset [option]
option:
  -s
```

---

## シリアル・リダイレクト・コマンド

シリアル・リダイレクト・コマンドは『console コマンド』の1つだけです。

### console コマンド

**console** コマンドを使用すると、指定された IMM2 のシリアル・ポートに対するシリアル・リダイレクト・コンソール・セッションが開始されます。

構文:

```
console 1
```

---

## 構成コマンド

構成コマンドは、以下のとおりです。

- 162 ページの『accsecCfg コマンド』
- 164 ページの『alertCfg コマンド』
- 165 ページの『asu コマンド』
- 168 ページの『backup コマンド』
- 169 ページの『dhcpinfo コマンド』
- 170 ページの『dns コマンド』

- 172 ページの『ethtousb コマンド』
- 173 ページの『gprofile コマンド』
- 173 ページの『ifconfig コマンド』
- 175 ページの『keycfg コマンド』
- 177 ページの『ldap コマンド』
- 178 ページの『ntp コマンド』
- 179 ページの『passwordcfg コマンド』
- 180 ページの『ports コマンド』
- 181 ページの『portcfg コマンド』
- 182 ページの『restore コマンド』
- 183 ページの『restoredefaults コマンド』
- 183 ページの『set コマンド』
- 184 ページの『smtp コマンド』
- 184 ページの『snmp コマンド』
- 187 ページの『snmpalerts コマンド』
- 189 ページの『srcfg コマンド』
- 189 ページの『sshcfcg コマンド』
- 190 ページの『ssl コマンド』
- 191 ページの『sslcfcg コマンド』
- 195 ページの『telnetcfg コマンド』
- 195 ページの『thermal コマンド』
- 195 ページの『timeouts コマンド』
- 196 ページの『usbeth コマンド』
- 196 ページの『users コマンド』

## accsecfcg コマンド

**accsecfcg** コマンドは、アカウントのセキュリティー設定を表示および構成するために使用します。

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

| オプション   | 説明                                     | 値 |
|---------|--|---|
| -legacy | アカウント・セキュリティーを事前定義されたデフォルトの legacy に設定 |   |
| -high   | アカウント・セキュリティーを事前定義されたデフォルトの high に設定   |   |

| オプション   | 説明                           | 値   |
|---------|------------------------------|---|
| -custom | アカウント・セキュリティを、ユーザー定義の値に設定    |   |
| -am     | ユーザー認証方式の設定                  | local、ldap、localldap、ldaplocal  |
| -lp     | 最大ログイン失敗回数後のロックアウト期間 (分)     | 0、1、2、5、10、15、20、30、60、120、180、または 240 分。「High Security」が使用可能になっている場合のデフォルト値は 60 で、「Legacy Security」が使用可能になっている場合のデフォルト値は 2 です。値が 0 の場合、この機能は使用不可になります。 |
| -pe     | パスワード有効期限の期間 (日)             | 0 から 365 日  |
| -pr     | パスワードが必要                     | on、off  |
| -pc     | パスワードの複雑性の規則                 | on、off  |
| -pd     | パスワードの最小相違文字数                | 0 から 19 文字  |
| -pl     | パスワードの長さ                     | 1 から 20 文字  |
| -ci     | 最小パスワード変更間隔 (時間)             | 0 から 240 日  |
| -lf     | ログイン失敗の最大回数                  | 0 から 10   |
| -chgdf  | 初回ログイン後のデフォルト・パスワードの変更       | on、off  |
| -chgnew | 初回ログイン後の新規ユーザー・パスワードの変更      | on、off  |
| -rc     | パスワード再利用サイクル                 | 0 から 5  |
| -wt     | Web の非アクティブ・セッションのタイムアウト (分) | 1、5、10、15、20、none、または user  |

構文:

```
accseccfg [options]
option:
  -legacy
  -high
  -custom
  -am authentication_method
  -lp lockout_period
  -pe time_period
  -pr state
  -pc state
  -pd number_characters
  -pl number_characters
  -ci minimum_interval
```

```

-lf number_failures
-chgdft state
-chgnew state
-rc reuse_cycle
-wt timeout

```

例:

```

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

```

## alertcfg コマンド

**alertcfg** コマンドは、IMM2 グローバル・リモート・アラート・パラメーターを表示および構成するために使用します。

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

| オプション | 説明                                       | 値                        |
|-------|--|--------------------------|
| -dr   | IMM2 がアラートを再送するまでの再試行と再試行の間の待ち時間を設定      | 0 から 4.0 分 (0.5 分の増分で設定) |
| -da   | IMM2 が、リストにある次の宛先にアラートを送信するまでの待ち時間を設定    | 0 から 4.0 分 (0.5 分の増分で設定) |
| -rl   | 前回の試行が失敗した場合に、IMM2 がアラートの送信を試行する追加の回数を設定 | 0 から 8                   |

構文:

```

alertcfg [options]
options:
-r| retry_limit
-dr retry_delay
-da agent_delay

```

例:

```
system>alertcfg
-dr 1.0
-da 2.5
-r1 5
system>
```

## asu コマンド

Advanced Settings ユーティリティ・コマンドは、UEFI 設定を設定するために使用します。UEFI 設定の変更を有効にするには、ホスト・システムをリブートする必要があります。

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

表 7. ASU コマンド

| コマンド | 説明   | 値                       |
|------|--|-------------------------|
| 削除   | このコマンドは、設定のインスタンスまたはレコードを削除するために使用します。設定は、削除できるインスタンスである必要があります (例えば、iSCSI.AttemptName.1)。   | <i>setting_instance</i> |
| ヘルプ  | このコマンドは、1 つ以上の設定のヘルプ情報を表示するために使用します。   | 設定                      |
| set  | このコマンドは、設定の値を変更するために使用します。UEFI 設定を、入力された値に設定します。<br><b>注:</b> <ul style="list-style-type: none"> <li>設定/値のペアを 1 つ以上設定します。</li> <li>設定には、単一文字に展開されるワイルドカードを含めることができます。</li> <li>値は、スペースを含む場合は引用符で囲む必要があります。</li> <li>順序リストの値は、等号 (=) で区切ります。例: set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network"</li> </ul> | <i>setting value</i>    |

表 7. ASU コマンド (続き)

| コマンド  | 説明  | 値  |
|---|---|----|
| showgroups  | このコマンドは、選択可能な設定グループを表示するために使用します。このコマンドは、既知のグループの名前を表示します。グループ名は、取り付けたデバイスによって異なる場合があります。   | 設定 |
| show  | このコマンドは、1 つ以上の設定の現行値を表示するために使用します。  | 設定 |
| showvalues  | このコマンドは、1 つ以上の設定について、指定できるすべての値を表示するために使用します。<br><b>注:</b> <ul style="list-style-type: none"> <li>このコマンドは、その設定の許容値に関する情報を表示します。</li> <li>その設定に許容されるインスタンス数の最小値と最大値が表示されます。</li> <li>デフォルト値があれば、それ表示されます。</li> <li>デフォルト値は、開く不等号括弧と閉じる不等号括弧 (&lt; と &gt;) で囲まれます。</li> <li>テキスト値では、最小と最大の長さ、および正規表現が表示されます。</li> </ul> | 設定 |
| <b>注:</b> <ul style="list-style-type: none"> <li>コマンド構文の中で、<i>setting</i> は表示または変更する設定の名前を示し、<i>value</i> は設定に指定する値を示しています。</li> <li><i>setting</i> は複数の名前にすることができます (<b>set</b> コマンドを使用する場合は除く)。</li> <li><i>setting</i> には、例えばアスタリスク (*) や疑問符 (?) などのワイルドカードを含めることができます。</li> <li><i>setting</i> は、グループ、設定名、または <b>all</b> とすることができます。</li> </ul> |   |    |

**asu** コマンド構文のいくつかの例を次のリストに示します。

- **asu** コマンドのすべてのオプションを表示するには、**asu --help** と入力します。
- すべてのコマンドの詳細なヘルプを表示するには、**asu -v --help** と入力します。
- 1 つのコマンドの詳細なヘルプを表示するには、**asu -v set --help** と入力します。
- 値を変更するには、**asu set *setting value*** と入力します。

- 現行値を表示するには、`asu show setting` と入力します。
- 長いバッチ形式で設定を表示するには、`asu show -l -b all` と入力します。
- 設定に指定できるすべての値を表示するには、`asu showvalues setting` と入力します。

**show values** コマンドの例:

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

次の表は、オプションの引数を示しています。

| オプション   | 説明  | 値 |
|---|---|---|
| -b <sup>1</sup>   | バッチ形式で表示します。  |   |
| --help <sup>3</sup>   | コマンドの使用法とオプションを表示します。--help オプションは、例えば <b>asu --help show</b> のように、コマンドの前に置きます。 |   |
| --help <sup>3</sup>   | コマンドのヘルプを表示します。--help オプションは、例えば <b>asu show --help</b> のように、コマンドの後に置きます。       |   |
| -l <sup>1</sup>   | 長形式の設定名 (構成セットを含む)。   |   |
| -m <sup>1</sup>   | 混合形式の設定名 (構成 ID を使用)。   |   |
| -v <sup>2</sup>   | 詳細な出力。  |   |
| 1. -b、-l、および -m の各オプションは、 <b>show</b> コマンドでのみ使用します。<br>2. -v オプションは、 <b>asu</b> とコマンドの間にだけ使用します。<br>3. --help オプションは、すべてのコマンドに使用できます。 |   |   |

構文:

```
asu [options] command [cmdopts]
options:
  -v verbose output
  --help display main help
cmdopts:
  --help help for the command
```

注: 他のコマンド・オプションについては、個々のコマンドの項を参照してください。

asu トランザクション・コマンドは、複数の UEFI 設定を設定し、バッチ・モード・コマンドを作成および実行するために使用します。**tropen** コマンドおよび **trset** コマンドは、適用する複数の設定が入っているトランザクション・ファイルを作成するために使用します。所定の ID を持つトランザクションは、**tropen** コマンドを使用してオープンします。設定は、**trset** コマンドを使用して設定されます。完了し

たトランザクションは、**trcommit** コマンドを使用してコミットされます。トランザクションを終了したら、**trrm** コマンドでトランザクションを削除できます。

**注:** UEFI 設定の復元操作では、ランダムな 3 桁の数値を使用した ID を持つトランザクションが作成されます。

次の表には、**asu** コマンドと一緒に使用できるトランザクション・コマンドが記載されています。

表 8. トランザクション・コマンド

| コマンド                     | 説明   | 値                                      |
|--------------------------|--|--|
| <code>tropen id</code>   | このコマンドは、設定するいくつかの設定が入っている新規トランザクション・ファイルを作成します。                            | <i>Id</i> は識別ストリングで、1 文字から 3 文字の英数字です。 |
| <code>trset id</code>    | このコマンドは、1 つ以上の設定と値のペアをトランザクションに追加します。                                      | <i>Id</i> は識別ストリングで、1 文字から 3 文字の英数字です。 |
| <code>trlist id</code>   | このコマンドは、トランザクション・ファイルの内容を最初に表示します。これは、トランザクション・ファイルが CLI シェルで作成される場合に便利です。 | <i>Id</i> は識別ストリングで、1 文字から 3 文字の英数字です。 |
| <code>trcommit id</code> | このコマンドは、トランザクション・ファイルの内容をコミットおよび実行します。実行の結果とエラー (ある場合) が表示されます。            | <i>Id</i> は識別ストリングで、1 文字から 3 文字の英数字です。 |
| <code>trrm id</code>     | このコマンドは、コミットが済んだトランザクション・ファイルを削除します。                                       | <i>Id</i> は識別ストリングで、1 文字から 3 文字の英数字です。 |

複数の UEFI 設定を確立する例:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.Wo1BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

## backup コマンド

**backup** コマンドは、システム・セキュリティーの現行設定を含むバックアップ・ファイルを作成するために使用します。

次の表は、オプションの引数を示しています。

| オプション           | 説明           | 値        |
|-----------------|--------------|----------|
| <code>-f</code> | バックアップ・ファイル名 | 有効なファイル名 |

| オプション | 説明   | 値                          |
|-------|--|----------------------------|
| -pp   | バックアップ・ファイルの内部でパスワードを暗号化するのに使用するパスワードまたはパスフレーズ | 有効なパスワードまたは引用符で区切られたパスフレーズ |
| -ip   | TFTP/SFTP サーバーの IP アドレス                        | 有効な IP アドレス                |
| -pn   | TFTP/SFTP サーバーのポート番号                           | 有効なポート番号 (デフォルト 69/22)     |
| -u    | SFTP サーバーのユーザー名                                | 有効なユーザー名                   |
| -pw   | SFTP サーバーのパスワード                                | 有効なパスワード                   |
| -fd   | バックアップ CLI コマンドの XML 記述のためのファイル名               | 有効なファイル名                   |

構文:

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

例:

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

## dhcpcinfo コマンド

**dhcpcinfo** コマンドは、インターフェースが DHCP サーバーによって自動的に構成される場合に、DHCP サーバーが eth0 に割り当てた IP 構成を表示するために使用します。**ifconfig** コマンドを使用して、DHCP を使用可能または使用不可にすることができます。

構文:

```
dhcpcinfo eth0
```

例:

```
system> dhcpcinfo eth0

-server : 192.168.70.29
-n      : IMM2A-00096B9E003A
-i      : 192.168.70.202
-g      : 192.168.70.29
-s      : 255.255.255.0
```

```

-d      : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6     : 0::0
-d6     : *
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>

```

次の表は、上記の例からの出力を説明したものです。

| オプション   | 説明                         |
|---------|----------------------------|
| -server | この構成を割り当てた DHCP サーバー       |
| -n      | 割り当てられたホスト名                |
| -i      | 割り当てられた IPv4 アドレス          |
| -g      | 割り当てられたゲートウェイ・アドレス         |
| -s      | 割り当てられたサブネット・マスク           |
| -d      | 割り当てられたドメイン・ネーム            |
| -dns1   | 1 次 IPv4 DNS サーバーの IP アドレス |
| -dns2   | 2 次 IPv4 DNS の IP アドレス     |
| -dns3   | 3 次 IPv4 DNS サーバーの IP アドレス |
| -i6     | IPv6 アドレス                  |
| -d6     | IPv6 ドメイン・ネーム              |
| -dns61  | 1 次 IPv6 DNS サーバーの IP アドレス |
| -dns62  | 2 次 IPv6 DNS の IP アドレス     |
| -dns63  | 3 次 IPv6 DNS サーバーの IP アドレス |

## dns コマンド

**dns** コマンドは、IMM2 の DNS 構成を表示および設定するために使用します。

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

| オプション  | 説明                         | 値                       |
|--------|----------------------------|-------------------------|
| -state | DNS の状態                    | on、off                  |
| -ddns  | DDNS の状態                   | enabled、disabled        |
| -i1    | 1 次 IPv4 DNS サーバーの IP アドレス | IP アドレス (小数点付き 10 進数形式) |
| -i2    | 2 次 IPv4 DNS の IP アドレス     | IP アドレス (小数点付き 10 進数形式) |
| -i3    | 3 次 IPv4 DNS サーバーの IP アドレス | IP アドレス (小数点付き 10 進数形式) |
| -i61   | 1 次 IPv6 DNS サーバーの IP アドレス | IP アドレス (IPv6 形式)       |

| オプション | 説明                         | 値                 |
|-------|----------------------------|-------------------|
| -i62  | 2 次 IPv6 DNS の IP アドレス     | IP アドレス (IPv6 形式) |
| -i63  | 3 次 IPv6 DNS サーバーの IP アドレス | IP アドレス (IPv6 形式) |
| -p    | IPv4/IPv6 の優先順位            | ipv4、ipv6         |

構文:

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

注: 以下の例では、DNS が使用可能にされた場合の IMM2 構成を示しています。

例:

```
system> dns
-state : enabled
-i1    : 192.168.70.202
-i2    : 192.168.70.208
-i3    : 192.168.70.212
-i61   : fe80::21a:64ff:fee6:4d5
-i62   : fe80::21a:64ff:fee6:4d6
-i63   : fe80::21a:64ff:fee6:4d7
-ddns  : enabled
-ddn   : ibm.com
-ddncur : ibm.com
-dnsrc : dhcp
-p     : ipv6
```

system>

次の表は、上記の例からの出力を説明したものです。

| オプション  | 説明                                    |
|--------|---------------------------------------|
| -state | DNS の状態 (on または off)                  |
| -i1    | 1 次 IPv4 DNS サーバーの IP アドレス            |
| -i2    | 2 次 IPv4 DNS の IP アドレス                |
| -i3    | 3 次 IPv4 DNS サーバーの IP アドレス            |
| -i61   | 1 次 IPv6 DNS サーバーの IP アドレス            |
| -i62   | 2 次 IPv6 DNS の IP アドレス                |
| -i63   | 3 次 IPv6 DNS サーバーの IP アドレス            |
| -ddns  | DDNS の状態 (enabled または disabled)       |
| -dnsrc | 優先される DDNS ドメイン・ネーム (dhcp または manual) |
| -ddn   | 手動で指定した DDN                           |

| オプション   | 説明                             |
|---------|--------------------------------|
| -ddncur | 現在の DDN (読み取り専用)               |
| -p      | 優先される DNS サーバー (ipv4 または ipv6) |

## ethtousb コマンド

**ethtousb** コマンドは、イーサネットから Ethernet-over-USB ポートへのマッピングを表示および構成するのに使用します。

このコマンドを使用すると、外部イーサネット・ポート番号を Ethernet-over-USB の異なるポート番号にマップすることができます。

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

| オプション | 説明                    | 値   |
|-------|-----------------------|---|
| -en   | Ethernet-over-USB の状態 | enabled、disabled  |
| -mx   | 索引 $x$ のポート・マッピングを構成  | <p>コロン (:) で区切ったポートのペア (<math>port1:port2</math> の形式)。</p> <p>それぞれのパラメーターの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>ポートの索引番号 <math>x</math> は、コマンド・オプションで 1 から 10 の整数として指定されます。</li> <li>ポート・ペアの <math>port1</math> は、外部イーサネットのポート番号です。</li> <li>ポート・ペアの <math>port2</math> は、Ethernet-over-USB のポート番号です。</li> </ul> |
| -rm   | 指定された索引のポート・マッピングを削除  | <p>1 から 10。</p> <p>ポート・マップの索引は、オプションを指定せずに <b>ethtousb</b> コマンドを使用すると表示されます。</p>  |

構文:

```
ethtousb [options]
option:
  -en state
  -mx port_pair
  -rm map_index
```

例:

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

## gprofile コマンド

**gprofile** コマンドは、IMM2 のグループ・プロファイルを表示および構成するために使用します。

次の表は、オプションの引数を示しています。

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

構文:

```
gprofile [1 - 16 group_profile_slot_number] [options]
```

options:

```
-clear state
```

```
-n group_name
```

```
-a authority level:
```

```
  -nsc network and security
```

```
  -am user account management
```

```
  -rca remote console access
```

```
  -rcvma remote console and remote disk access
```

```
  -pr remote server power/restart access
```

```
  -bc basic adapter configuration
```

```
  -cel ability to clear event logs
```

```
  -ac advanced adapter configuration
```

```
-h help
```

## ifconfig コマンド

**ifconfig** コマンドは、イーサネット・インターフェースを構成するために使用します。現行イーサネット・インターフェース構成を表示するには、`ifconfig eth0` と入力します。イーサネット・インターフェース構成を変更するには、オプションと、それに続けて値を入力します。インターフェース構成を変更するには、少なくとも「アダプター・ネットワーキングおよびセキュリティー構成 (Adapter Networking and Security Configuration)」権限を持っている必要があります。

次の表は、オプションの引数を示しています。

| オプション  | 説明          | 値  |
|--------|-------------|--|
| -state | インターフェースの状態 | disabled、enabled   |
| -c     | 構成方式        | dhcp、static、dthens (dthens は、Web インターフェースの <b>try dhcp server, if it fails use static config</b> オプションに対応します。) |

| オプション          | 説明  | 値  |
|----------------|---|--|
| -i             | 固定 IP アドレス  | 有効なフォーマットのアドレス   |
| -g             | ゲートウェイ・アドレス   | 有効なフォーマットのアドレス   |
| -s             | サブネット・マスク   | 有効なフォーマットのアドレス   |
| -n             | ホスト名  | 63 文字以内のストリング。このストリングには、英字、数字、ピリオド、アンダースコア、およびハイフンを含めることができます。 |
| -r             | Data rate   | 10、100、auto  |
| -d             | 二重モード   | full、half、auto   |
| -m             | MTU   | 60 から 1500 までの数値   |
| -l             | LAA   | MAC アドレス・フォーマット。マルチキャスト・アドレスは許容されません (最初のバイトは偶数である必要があります)。    |
| -dn            | ドメイン・ネーム  | 有効なフォーマットのドメイン・ネーム   |
| -auto          | データ転送速度および二重ネットワークの設定が構成可能かどうかを決定する、自動ネゴシエーションの設定                                     | true、false   |
| -nic           | NIC アクセス  | shared、dedicated   |
| -address_table | 自動生成された IPv6 アドレスと、そのプレフィックスの長さの表<br>注: このオプションは、IPv6 およびステートレス自動構成が使用可能な場合にのみ表示されます。 | この値は読み取り専用であり、構成できません。   |
| -ipv6          | IPv6 の状態  | disabled、enabled   |
| -lla           | リンク・ローカル・アドレス<br>注: リンク・ローカル・アドレスが表示されるのは、IPv6 が使用可能な場合のみです。                          | リンク・ローカル・アドレスは、IMM2 によって決定されます。この値は読み取り専用であり、構成できません。          |
| -ipv6static    | 固定 IPv6 の状態   | disabled、enabled   |
| -i6            | 固定 IP アドレス  | イーサネット・チャンネル 0 の固定 IP アドレス (IPv6 フォーマット)                       |
| -p6            | アドレスのプレフィックスの長さ   | 1 から 128 までの数値   |
| -g6            | ゲートウェイまたはデフォルトのルート  | イーサネット・チャンネル 0 のゲートウェイまたはデフォルトのルートの IP アドレス (IPv6)             |
| -dhcp6         | DHCPv6 の状態  | disabled、enabled   |
| -sa6           | IPv6 ステートレス自動構成の状態  | disabled、enabled   |

構文:

```

ifconfig eth0 [options]
options:
  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
  -l locally_administered_MAC
  -dn domain_name
  -auto state
  -nic state
  -address_table
  -ipv6 state
  -ipv6static state
  -sa6 state
  -i6 static_ipv6_ip_address
  -g6 ipv6_gateway_address
  -p6 length

```

例:

```

system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM2.
system>

```

注: ifconfig 表示の中の **-b** オプションは、組み込み MAC アドレス用です。組み込み MAC アドレスは読み取り専用であり、構成可能ではありません。

## keycfg コマンド

**keycfg** コマンドは、アクティベーション・キーを表示、追加、または削除するために使用します。これらのキーは、オプションの IMM2 Features on Demand (FoD) 機能へのアクセスを制御します。

- オプションを指定せずに **keycfg** を実行すると、インストールされているアクティベーション・キーのリストが表示されます。表示されるキーの情報には、各アクティベーション・キーの索引番号、アクティベーション・キーのタイプ、キーが有効になる日付、残りの使用回数、キーの状況、およびキーの説明などがあります。
- ファイル転送を介して新規アクティベーション・キーを追加します。
- キーの番号またはキーのタイプを指定して、古いキーを削除します。タイプ別にキーを削除する場合、指定されたタイプの最初のキーが削除されます。

次の表は、オプションの引数を示しています。

| オプション    | 説明                                       | 値  |
|----------|--|--|
| -add     | アクティベーション・キーの追加                          | -ip、-pn、-u、-pw、および -f コマンド・オプションの値。        |
| -ip      | 追加するアクティベーション・キーがある TFTP サーバーの IP アドレス   | TFTP サーバーの有効な IP アドレス。                     |
| -pn      | 追加するアクティベーション・キーがある TFTP/SFTP サーバーのポート番号 | TFTP/SFTP サーバーの有効なポート番号 (デフォルト 69/22)。     |
| -u       | 追加するアクティベーション・キーがある SFTP サーバーのユーザー名      | SFTP サーバーの有効なユーザー名。                        |
| -pw      | 追加するアクティベーション・キーがある SFTP サーバーのパスワード      | SFTP サーバーの有効なパスワード。                        |
| -f       | 追加するアクティベーション・キーのファイル名                   | アクティベーション・キー・ファイルの有効なファイル名。                |
| -del     | 索引番号によるアクティベーション・キーの削除                   | <b>keycfg</b> リストにある、有効なアクティベーション・キーの索引番号。 |
| -deltype | キー・タイプによるアクティベーション・キーの削除                 | 有効なキー・タイプの値。                               |

構文:

```
keycfg [options]
option:
  -add
    -ip ip_address
    -pn port_number
    -u username
    -pw password
    -f filename
  -del key_index
  -deltype key_type
```

例:

```
system> keycfg
ID  Type  Valid      Uses  Status  Description
1   4     10/10/2010  5     "valid" "IMM remote presence"
2   3     10/20/2010  2     "valid" "IMM feature"
system>
```

## ldap コマンド

**ldap** コマンドを使用すると、LDAP プロトコル構成パラメーターの表示および構成が可能で

次の表は、オプションの引数を示しています。

| オプション | 説明                                   | 値   |
|-------|--------------------------------------|---|
| -a    | ユーザー認証方式                             | ローカルのみ、LDAP のみ、最初がローカルで次に LDAP、最初が LDAP で次にローカル   |
| -aom  | 認証専用モード                              | enabled、disabled  |
| -b    | バインディング方式                            | 匿名、ClientDN とパスワードを使用したバインド、ログイン資格情報を使用したバインド   |
| -c    | クライアント識別名                            | <i>client_dn</i> の最大 127 文字のストリング   |
| -d    | 検索ドメイン                               | <i>search_domain</i> の最大 63 文字のストリング  |
| -f    | グループ・フィルター                           | <i>group_filter</i> の最大 127 文字のストリング  |
| -fn   | フォレスト名                               | Active Directory 環境用。127 文字以内のストリング。  |
| -g    | グループ検索属性                             | <i>group_search_attr</i> の最大 63 文字のストリング  |
| -l    | ログイン許可属性                             | <i>string</i> の最大 63 文字のストリング   |
| -p    | クライアント・パスワード                         | <i>client_pw</i> の最大 15 文字のストリング  |
| -pc   | クライアント・パスワードの確認                      | <i>confirm_pw</i> の最大 15 文字のストリング<br>コマンドの使用法: <code>ldap -p <i>client_pw</i> -pc <i>confirm_pw</i></code><br>このオプションは、クライアント・パスワードを変更する場合に必要です。このオプションは <i>confirm_pw</i> 引数と <i>client_pw</i> 引数を比較します。引数が一致しない場合、コマンドは失敗します。 |
| -r    | root エントリー識別名 (DN)                   | <i>root_dn</i> の最大 127 文字のストリング   |
| -rbs  | Active Directory ユーザーの拡張役割ベース・セキュリティ | enabled、disabled  |
| -s1ip | サーバー 1 のホスト名/IP アドレス                 | <i>host_name/ip_addr</i> の最大 127 文字のストリングまたは IP アドレス  |
| -s2ip | サーバー 2 のホスト名/IP アドレス                 | <i>host_name/ip_addr</i> の最大 127 文字のストリングまたは IP アドレス  |
| -s3ip | サーバー 3 のホスト名/IP アドレス                 | <i>host_name/ip_addr</i> の最大 127 文字のストリングまたは IP アドレス  |
| -s4ip | サーバー 4 のホスト名/IP アドレス                 | <i>host_name/ip_addr</i> の最大 127 文字のストリングまたは IP アドレス  |
| -s1pn | サーバー 1 のポート番号                        | <i>port_number</i> の最大 5 桁のポート番号  |
| -s2pn | サーバー 2 のポート番号                        | <i>port_number</i> の最大 5 桁のポート番号  |

| オプション | 説明                          | 値  |
|-------|-----------------------------|--|
| -s3pn | サーバー 3 のポート番号               | <i>port_number</i> の最大 5 桁のポート番号   |
| -s4pn | サーバー 4 のポート番号               | <i>port_number</i> の最大 5 桁のポート番号   |
| -t    | サーバーのターゲット名                 | -rbs オプションが使用可能に設定されている場合、このフィールドは、ロール・ベース・セキュリティー (RBS) スナップイン・ツールを使用して Active Directory サーバー上の 1 つ以上の役割に関連付けることができるターゲット名を指定します。 |
| -u    | UID 検索属性                    | <i>search_attrib</i> の最大 63 文字のストリング   |
| -v    | DNS を使用した LDAP サーバー・アドレスの取得 | off、on   |
| -h    | コマンドの使用方法およびオプションの表示        |  |

構文:

```
ldap [options]
options:
-a loc|ldap|loclid|ldloc
-aom enable/disabled
-b anon|client|login
-c client_dn
-d search_domain
-f group_filter
-fn forest_name
-g group_search_attr
-l string
-p client_pw
-pc confirm_pw
-r root_dn
-rbs enable/disabled
-slip host name/ip_addr
-s2ip host name/ip_addr
-s3ip host name/ip_addr
-s4ip host name/ip_addr
-s1pn port_number
-s2pn port_number
-s3pn port_number
-s4pn port_number
-t name
-u search_attrib
-v off|on
-h
```

## ntp コマンド

**ntp** コマンドは、Network Time Protocol (NTP) の表示と構成を行うために使用します。

次の表は、オプションの引数を示しています。

| オプション             | 説明  | 値   |
|-------------------|---|---|
| -en               | Network Time Protocol の使用可能化または使用不可化  | enabled、disabled  |
| -i <sup>1</sup>   | Network Time Protocol サーバーの名前または IP アドレス。これは、Network Time Protocol サーバーの索引番号です。 | クロック同期には NTP サーバーの名前を使用します。NTP サーバーの索引番号の範囲は、-i1 から -i4 までです。 |
| -f                | IMM2 クロックを Network Time Protocol サーバーと同期する頻度 (分単位)                              | 3 から 1440 分   |
| -synch            | Network Time Protocol サーバーとの即時同期の要求   | このパラメーターには値を使用しません。   |
| 1. -i は i1 と同じです。 |   |   |

構文:

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

例:

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

## passwordcfg コマンド

**passwordcfg** コマンドを使用すると、パスワード・パラメーターの表示および構成が可能です。

| オプション   | 説明  |
|---------|---|
| -legacy | アカウント・セキュリティを事前定義されたデフォルトの <b>legacy</b> に設定  |
| -high   | アカウント・セキュリティを事前定義されたデフォルトの <b>high</b> に設定    |
| -exp    | パスワードの最大使用日数 (0 から 365 日)。0 に設定すると有効期限はありません。 |
| -cnt    | 以前に使用したパスワードを再使用できない回数 (0 から 5)               |
| -nul    | パスワードなしのアカウントの許可 (yes または no)                 |
| -h      | コマンドの使用方法およびオプションの表示                          |

構文:

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
```

```
-exp:  
-cnt:  
-nul:  
-h
```

例:

```
system> passwordcfg  
Security Level: Legacy  
system> passwordcfg -exp 365  
ok  
system> passwordcfg -nul yes  
ok  
system> passwordcfg -cnt 5  
ok  
system> passwordcfg  
Security Level: Customize  
-exp: 365  
-cnt: 5  
-nul: allowed
```

## ports コマンド

**ports** コマンドは、IMM2 ポートを表示および構成するために使用します。

オプションを指定せずに **ports** コマンドを実行すると、すべての IMM2 ポートの情報が表示されます。次の表は、オプションの引き数を示しています。

| オプション   | 説明                     | 値                 |
|---------|------------------------|-------------------|
| -open   | オープン・ポートの表示            |                   |
| -reset  | ポートをデフォルトの設定値にリセット     |                   |
| -http   | HTTP ポート番号             | デフォルトのポート番号: 80   |
| -https  | HTTPS ポート番号            | デフォルトのポート番号: 443  |
| -telnet | Telnet のレガシー CLI ポート番号 | デフォルトのポート番号: 23   |
| -ssh    | SSH のレガシー CLI ポート番号    | デフォルトのポート番号: 22   |
| -snmp   | SNMP エージェントのポート番号      | デフォルトのポート番号: 161  |
| -snmptp | SNMP トラップのポート番号        | デフォルトのポート番号: 162  |
| -rpp    | リモート・プレゼンスのポート番号       | デフォルトのポート番号: 3900 |
| -cimhp  | CIM over HTTP ポート番号    | デフォルトのポート番号: 5988 |
| -cimhsp | CIM over HTTPS ポート番号   | デフォルトのポート番号: 5989 |

構文:

```
ports [options]
option:
  -open
  -reset
  -http port_number
  -https port_number
  -telnet port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

例:

```
system> ports
-http 80
-https 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-telnet 23
-cimhp 5988
-cimhsp 5989
system>
```

## portcfg コマンド

**portcfg** コマンドは、シリアル・リダイレクト機能のために IMM2 を構成するのに使用します。

IMM2 の構成は、サーバーの内部シリアル・ポートの設定と一致させる必要があります。シリアル・ポート構成を変更するには、オプションと、それに続けて値を入力します。シリアル・ポート構成を変更するには、少なくとも「アダプター・ネットワークングおよびセキュリティー構成 (Adapter Networking and Security Configuration authority)」権限を持っている必要があります。

**注:** サーバーの外部シリアル・ポートは、IPMI 機能のために IMM2 のみが使用できます。CLI は、シリアル・ポートではサポートされていません。リモート管理アダプター II の CLI に存在していた **serred** オプションと **cliath** オプションは、サポートされていません。

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

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

| オプション | 説明       | 値                                 |
|-------|----------|-----------------------------------|
| -b    | ボー・レート   | 9600, 19200, 38400, 57600, 115200 |
| -p    | パリティ     | none, odd, even                   |
| -s    | ストップ・ビット | 1, 2                              |

| オプション    | 説明      | 値  |
|----------|---------|--|
| -climode | CLI モード | 0, 1, 2<br><br>それぞれのパラメーターの意味は次のとおりです。<br><ul style="list-style-type: none"> <li>• 0 = none: CLI は使用不可になります。</li> <li>• 1 = cliems: CLI は EMS 互換キー・ストローク・シーケンスで使用可能になります。</li> <li>• 2 = cliuser: CLI は、ユーザー定義キー・ストローク・シーケンスで使用可能になります。</li> </ul> |

構文:

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

例:

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

## restore コマンド

**restore** コマンドは、バックアップ・ファイルからシステム設定をリストアするために使用します。

次の表は、オプションの引数を示しています。

| オプション | 説明   | 値                          |
|-------|--|----------------------------|
| -f    | バックアップ・ファイル名                                   | 有効なファイル名                   |
| -pp   | バックアップ・ファイルの内部でパスワードを暗号化するのに使用するパスワードまたはパスフレーズ | 有効なパスワードまたは引用符で区切られたパスフレーズ |
| -ip   | TFTP/SFTP サーバーの IP アドレス                        | 有効な IP アドレス                |
| -pn   | TFTP/SFTP サーバーのポート番号                           | 有効なポート番号 (デフォルト 69/22)     |
| -u    | SFTP サーバーのユーザー名                                | 有効なユーザー名                   |
| -pw   | SFTP サーバーのパスワード                                | 有効なパスワード                   |

構文:

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

例:

```
system> restore -f imm-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

## restoredefaults コマンド

**restoredefaults** コマンドは、IMM2 のすべての設定を出荷時のデフォルト値にリストアするために使用します。

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

構文:

```
restoredefaults
```

例:

```
system> restoredefaults
```

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result. You will need to reconfigure the IMM network interface to restore connectivity. After the IMM configuration is cleared, the IMM will be restarted.

```
Proceed? (y/n)
Y
Restoring defaults...
```

## set コマンド

**set** コマンドは、IMM2 の設定を変更するために使用します。

- 一部の IMM2 設定は、シンプルな **set** コマンドを使用して変更できます。
- このような一部の設定 (環境変数など) は、CLI によって使用されます。
- **show** コマンドは、**set** コマンドを使用して設定された値を表示するのに使用します。

次の表は、オプションの引数を示しています。

| オプション        | 説明                | 値                  |
|--------------|-------------------|--------------------|
| <i>value</i> | 指定されたパスまたは設定の値を設定 | 指定されたパスまたは設定の適切な値。 |

構文:

```
set [options]
option:
  value
```

## smtp コマンド

**smtp** コマンドは、SMTP インターフェースの設定を表示および構成するために使用します。

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

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

構文:

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

例:

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

## snmp コマンド

**snmp** コマンドは、SNMP インターフェースの情報を表示および構成するために使用します。

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

| オプション | 説明            | 値  |
|-------|---------------|--|
| -a    | SNMPv1 エージェント | <p>on、off</p> <p><b>注:</b> SNMPv1 エージェントを使用可能にするには、次の基準を満たす必要があります。</p> <ul style="list-style-type: none"> <li>• IMM2 の連絡先が、-cn コマンド・オプションを使用して指定されている。</li> <li>• IMM2 のロケーションが、-l コマンド・オプションを使用して指定されている。</li> <li>• 少なくとも 1 つの SNMP コミュニティー名が、-cx コマンド・オプションのいずれかを使用して指定されている。</li> <li>• 少なくとも 1 つの有効な IP アドレスが、-cxiy コマンド・オプションのいずれかを使用して各 SNMP コミュニティーに指定されている。</li> </ul> |
| -a3   | SNMPv3 エージェント | <p>on、off</p> <p><b>注:</b> SNMPv3 エージェントを使用可能にするには、次の基準を満たす必要があります。</p> <ul style="list-style-type: none"> <li>• IMM2 の連絡先が、-cn コマンド・オプションを使用して指定されている。</li> <li>• IMM2 のロケーションが、-l コマンド・オプションを使用して指定されている。</li> </ul>   |
| -t    | SNMP トラップ     | on、off   |
| -l    | IMM2 のロケーション  | <p>ストリング (47 文字の制限)。</p> <p><b>注:</b></p> <ul style="list-style-type: none"> <li>• スペースが含まれている引き数は引用符で囲む必要があります。引き数の先頭または末尾にスペースは使用できません。</li> <li>• 引き数を指定しないか、引き数として空ストリングを指定 ("") すると、IMM2 のロケーションがクリアされます。</li> </ul>  |
| -cn   | IMM2 の連絡先名    | <p>ストリング (47 文字の制限)。</p> <p><b>注:</b></p> <ul style="list-style-type: none"> <li>• スペースが含まれている引き数は引用符で囲む必要があります。引き数の先頭または末尾にスペースは使用できません。</li> <li>• 引き数を指定しないか、引き数として空ストリングを指定 ("") すると、IMM2 の連絡先名がクリアされます。</li> </ul>  |

| オプション | 説明  | 値  |
|-------|---|--|
| -cx   | SNMP コミュニティー <i>x</i> の名前                       | <p>ストリング (15 文字の制限)。</p> <p><b>注:</b></p> <ul style="list-style-type: none"> <li>• <i>x</i> はコマンド・オプションで 1、2、または 3 のように指定して、コミュニティ番号を指示します。</li> <li>• スペースが含まれている引き数は引用符で囲む必要があります。引き数の先頭または末尾にスペースは使用できません。</li> <li>• 引き数を指定しないか、引き数として空ストリングを指定 ("") すると、SNMP コミュニティー名がクリアされます。</li> </ul>   |
| -cxiy | SNMP コミュニティー <i>x</i> の IP アドレスまたはホスト名 <i>y</i> | <p>有効な IP アドレスまたはホスト名 (63 文字の制限)。</p> <p><b>注:</b></p> <ul style="list-style-type: none"> <li>• <i>x</i> はコマンド・オプションで 1、2、または 3 のように指定して、コミュニティ番号を指示します。</li> <li>• <i>y</i> はコマンド・オプションで 1、2、または 3 のように指定して、IP アドレスまたはホスト名の番号を指示します。</li> <li>• IP アドレスまたはホスト名に含めることができるのは、ドット、アンダースコア、負符号 (-)、文字、および数字です。組み込みスペースまたは連続したピリオドは許可されません。</li> <li>• 引き数を指定しないと、SNMP コミュニティーの IP アドレスまたはホスト名がクリアされます。</li> </ul> |
| -cax  | SNMPv3 コミュニティー <i>x</i> のアクセス・タイプ               | <p>get、set、trap</p> <p><b>注:</b> <i>x</i> はコマンド・オプションで 1、2、または 3 のように指定して、コミュニティ番号を指示します。</p>  |

#### 構文:

snmp [*options*]

option:

```

-a state
-a3 state
-t state
-l location
-cn contact_name
-c1 snmp_community_1_name
-c2 snmp_community_2_name
-c3 snmp_community_3_name
-cl11 community_1_ip_address_or_hostname_1
-cl12 community_1_ip_address_or_hostname_2
-cl13 community_1_ip_address_or_hostname_3
-c2i1 community_2_ip_address_or_hostname_1
-c2i2 community_2_ip_address_or_hostname_2
-c2i3 community_2_ip_address_or_hostname_3
-c3i1 community_3_ip_address_or_hostname_1
-c3i2 community_3_ip_address_or_hostname_2
-c3i3 community_3_ip_address_or_hostname_3
-ca1 community_1_access_type
-ca2 community_2_access_type
-ca3 community_3_access_type

```

例:

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l RTC,NC
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-ca1 set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>
```

## snmpalerts コマンド

**snmpalerts** コマンドは、SNMP 経由で送信されるアラートを管理するために使用します。

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

| オプション   | 説明                      | 値   |
|---------|-------------------------|---|
| -status | SNMP アラートの状況            | on、off  |
| -crt    | アラートを送信するクリティカル・イベントを設定 | all、none、custom:telvolpoldilfalcplmelinlrelot<br>カスタムのクリティカル・アラート設定は、値をパイプで区切られたリストにして、 <b>snmpalerts -crt custom:telvo</b> の形式で指定します。ここで、カスタム値は以下のとおりです。 <ul style="list-style-type: none"><li>• te: クリティカルな温度しきい値超過</li><li>• vo: クリティカルな電圧しきい値超過</li><li>• po: クリティカルな電源障害</li><li>• di: ハード・ディスク障害</li><li>• fa: ファン障害</li><li>• cp: マイクロプロセッサ障害</li><li>• me: メモリー障害</li><li>• in: ハードウェアの互換性なし</li><li>• re: 電源の冗長性の障害</li><li>• ot: その他すべてのクリティカル・イベント</li></ul> |

| オプション  | 説明                    | 値  |
|--------|-----------------------|--|
| -crten | クリティカル・イベント・アラートを送信   | enabled、disabled   |
| -wrn   | アラートを送信する警告イベントを設定    | all、none、custom:rptelvolpolfalcpmlmet<br><br>カスタムの警告アラート設定は、値をパイプで区切られたリストにして、 <b>snmpalerts -wrn custom:rplte</b> の形式で指定します。ここで、カスタム値は以下のとおりです。<br><br><ul style="list-style-type: none"> <li>• rp: 電源の冗長性の警告</li> <li>• te: 警告の温度しきい値超過</li> <li>• vo: 警告の電圧しきい値超過</li> <li>• po: 警告の電力しきい値超過</li> <li>• fa: クリティカルではないファン・イベント</li> <li>• cp: マイクロプロセッサが機能低下状態</li> <li>• me: メモリーの警告</li> <li>• ot: その他すべての警告イベント</li> </ul>   |
| -wrnen | 警告イベント・アラートを送信        | enabled、disabled   |
| -sys   | アラートを送信するルーチン・イベントを設定 | all、none、custom:loltioltlpolbftilpfllelne<br><br>カスタムのルーチン・アラート設定は、値をパイプで区切られたリストにして、 <b>snmpalerts -sys custom:loltio</b> の形式で指定します。ここで、カスタム値は以下のとおりです。<br><br><ul style="list-style-type: none"> <li>• lo: 正常なりモート・ログイン</li> <li>• tio: オペレーティング・システムのタイムアウト</li> <li>• ot: その他すべての通知イベントおよびシステム・イベント</li> <li>• po: システムの電源オン/オフ</li> <li>• bf: オペレーティング・システムのブート障害</li> <li>• オペレーティング・システム・ローダーのウォッチドッグ・タイムアウト</li> <li>• pf: 障害予知 (PFA)</li> <li>• el: イベント・ログ 75% フル</li> <li>• ne: ネットワーク変更</li> </ul> |
| -sysen | ルーチン・イベント・アラートを送信     | enabled、disabled   |

構文:

```
snmpalerts [options]
options:
  -status status
  -crt event_type
  -crten state
```

```

-wrn event_type
-wrnen state
-sys event_type
-sysen state

```

## srcfg コマンド

**srcfg** コマンドは、シリアル・リダイレクト・モードから CLI に入るキー・シーケンスを示すために使用します。シリアル・リダイレクト構成を変更するには、オプションと、それに続けて値を入力します。シリアル・リダイレクト構成を変更するには、少なくとも「アダプター・ネットワークングおよびセキュリティー構成 (Adapter Networking and Security Configuration authority)」権限を持っている必要があります。

**注:** IMM2 ハードウェアは、シリアル・ポートからシリアル・ポートのパススルー機能を備えていません。したがって、リモート管理アダプター II の CLI に存在する `-passthru` オプションと `entercliseq` オプションはサポートされていません。

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

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

構文:

```

srcfg [options]
options:
-entercliseq entercli_keyseq

```

例:

```

system> srcfg
-entercliseq ^[Q
system>

```

## sshcfg コマンド

**sshcfg** コマンドは、SSH パラメーターを表示および構成するために使用します。

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

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

構文:

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

例:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

## ssl コマンド

**ssl** コマンドは、SSL パラメーターを表示および構成するために使用します。

注: SSL クライアントを使用可能にするには、クライアント証明書がインストールされている必要があります。

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

| オプション | 説明  | 値      |
|-------|---|--------|
| -ce   | SSL クライアントの使用可能化または使用不可化                  | on、off |
| -se   | SSL サーバーの使用可能化または使用不可化                    | on、off |
| -cime | SSL サーバー上での CIM over HTTPS の使用可能化または使用不可化 | on、off |

構文:

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

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

#### **Server secure transport enable**

この状況表示は読み取り専用で、直接設定することはできません。

#### **Server Web/CMD key status**

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

Private Key and Cert/CSR not available  
Private Key and CA-signed cert installed  
Private Key and Auto-gen self-signed cert installed  
Private Key and Self-signed cert installed  
Private Key stored, CSR available for download

#### **SSL server CSR key status**

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

Private Key and Cert/CSR not available  
Private Key and CA-signed cert installed  
Private Key and Auto-gen self-signed cert installed  
Private Key and Self-signed cert installed  
Private Key stored, CSR available for download

#### **SSL client LDAP key status**

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

Private Key and Cert/CSR not available  
Private Key and CA-signed cert installed  
Private Key and Auto-gen self-signed cert installed  
Private Key and Self-signed cert installed  
Private Key stored, CSR available for download

#### **SSL client CSR key status**

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

Private Key and Cert/CSR not available  
Private Key and CA-signed cert installed  
Private Key and Auto-gen self-signed cert installed  
Private Key and Self-signed cert installed  
Private Key stored, CSR available for download

## **sslcfg コマンド**

**sslcfg** コマンドは、IMM2 の SSL を表示および構成し、証明書を管理するために使用します。

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

| オプション   | 説明                      | 値   |
|---------|-------------------------|---|
| -server | SSL サーバー状況              | enabled、disabled<br>注: SSL サーバーは、有効な証明書が提供されている場合にのみ使用可能にすることができます。   |
| -client | SSL クライアントの状況           | enabled、disabled<br>注: SSL クライアントは、有効なサーバーまたはクライアントの証明書が提供されている場合にのみ使用可能にすることができます。   |
| -cim    | CIM over HTTPS の状況      | enabled、disabled<br>注: CIM over HTTPS は、有効なサーバーまたはクライアントの証明書が提供されている場合にのみ使用可能にすることができます。  |
| -cert   | 自己署名証明書の生成              | server、client、sysdir<br>注:<br><ul style="list-style-type: none"> <li>自己署名証明書を生成する際には、<b>-c</b>、<b>-sp</b>、<b>-cl</b>、<b>-on</b>、および <b>-hn</b> コマンド・オプションの値は必須です。</li> <li>自己署名証明書を生成する際には、<b>-cp</b>、<b>-ea</b>、<b>-ou</b>、<b>-s</b>、<b>-gn</b>、<b>-in</b>、および <b>-dq</b> コマンド・オプションの値はオプションです。</li> </ul>                   |
| -csr    | CSR の生成                 | server、client、sysdir<br>注:<br><ul style="list-style-type: none"> <li>CSR を生成する際には、<b>-c</b>、<b>-sp</b>、<b>-cl</b>、<b>-on</b>、および <b>-hn</b> コマンド・オプションの値は必須です。</li> <li>CSR を生成する際には、<b>-cp</b>、<b>-ea</b>、<b>-ou</b>、<b>-s</b>、<b>-gn</b>、<b>-in</b>、<b>-dq</b>、<b>-cpwd</b>、および <b>-un</b> コマンド・オプションの値はオプションです。</li> </ul> |
| -i      | TFTP/SFTP サーバーの IP アドレス | 有効な IP アドレス<br>注: 証明書のアップロード、または証明書あるいは CSR のダウンロードの際には、TFTP または SFTP サーバーの IP アドレスを指定する必要があります。  |
| -pn     | TFTP/SFTP サーバーのポート番号    | 有効なポート番号 (デフォルト 69/22)  |
| -u      | SFTP サーバーのユーザー名         | 有効なユーザー名  |
| -pw     | SFTP サーバーのパスワード         | 有効なパスワード  |
| -l      | 証明書ファイル名                | 有効なファイル名<br>注: 証明書または CSR をダウンロードあるいはアップロードする際には、ファイル名は必須です。ダウンロードを行う場合にファイル名が指定されないと、ファイルのデフォルト名が使用され、表示されます。  |

| オプション | 説明                        | 値  |
|-------|---------------------------|--|
| -dnld | 証明書ファイルのダウンロード            | このオプションには引き数を使用しませんが、 <b>-cert</b> または <b>-csr</b> コマンド・オプション (ダウンロードする証明書のタイプによって異なる) にも値を指定する必要があります。このオプションには引き数を使用しませんが、 <b>-i</b> コマンド・オプション、および <b>-I</b> (オプション) コマンド・オプションにも値を指定する必要があります。 |
| -upld | 証明書ファイルのインポート             | このオプションには引き数を使用しませんが、 <b>-cert</b> 、 <b>-i</b> 、および <b>-I</b> コマンド・オプションは指定する必要があります。  |
| -tcx  | SSL クライアントの信頼証明書 <i>x</i> | import、download、remove<br>注: 信頼証明書の番号 <i>x</i> は、コマンド・オプションで 1 から 3 の整数として指定されます。  |
| -c    | Country                   | 国別コード (2 文字)<br>注: 自己署名証明書または CSR を生成するには必須です。   |
| -sp   | 都道府県/州                    | 引用符で区切ったストリング (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するには必須です。   |
| -cl   | 市区町村または地方                 | 引用符で区切ったストリング (最大 50 文字)<br>注: 自己署名証明書または CSR を生成するには必須です。   |
| -on   | 組織名                       | 引用符で区切ったストリング (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するには必須です。   |
| -hn   | IMM2 ホスト名                 | ストリング (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するには必須です。   |
| -cp   | 連絡先担当者                    | 引用符で区切ったストリング (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するにはオプションです。  |
| -ea   | 連絡先担当者の E メール・アドレス        | 有効な E メール・アドレス (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するにはオプションです。   |
| -ou   | 組織単位                      | 引用符で区切ったストリング (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するにはオプションです。  |
| -s    | 姓                         | 引用符で区切ったストリング (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するにはオプションです。  |
| -gn   | 名                         | 引用符で区切ったストリング (最大 60 文字)<br>注: 自己署名証明書または CSR を生成するにはオプションです。  |
| -in   | イニシャル                     | 引用符で区切ったストリング (最大 20 文字)<br>注: 自己署名証明書または CSR を生成するにはオプションです。  |

| オプション | 説明           | 値  |
|-------|--------------|--|
| -dq   | ドメイン・ネームの修飾子 | 引用符で区切った文字列 (最大 60 文字)<br>注: 自己署名証明書または CSR を生成する際にはオプションです。 |
| -cpwd | チャレンジ・パスワード  | 文字列 (最小 6 文字、最大 30 文字)<br>注: CSR を生成する際にはオプションです。            |
| -un   | 非構造化名        | 引用符で区切った文字列 (最大 60 文字)<br>注: CSR を生成する際にはオプションです。            |

構文:

```

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

```

例:

```

system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
  A self-signed certificate is installed
SSL Client Certificate status:
  A self-signed certificate is installed
SSL CIM Certificate status:
  A self-signed certificate is installed
SSL Client Trusted Certificate status:
  Trusted Certificate 1: Not available
  Trusted Certificate 2: Not available
  Trusted Certificate 3: Not available
  Trusted Certificate 4: Not available
system>

```

## telnetcfg コマンド

**telnetcfg** コマンドは、Telnet の設定を表示および構成するために使用します。

オプションを指定せずに **telnetcfg** コマンドを実行すると、Telnet の状態が表示されます。次の表は、オプションの引き数を示しています。

| オプション | 説明         | 値   |
|-------|------------|---|
| -en   | Telnet の状態 | disabled、1、2<br>注: 使用不可にされていない場合、1 人または 2 人のユーザーで、Telnet が使用可能です。 |

構文:

```
telnetcfg [options]
option:
  -en state
```

例:

```
system> telnetcfg
-en 1
system>
```

## thermal コマンド

**thermal** コマンドは、ホスト・システムのサーマル・モード・ポリシーを表示および構成するために使用します。

オプションを指定せずに **thermal** コマンドを実行すると、サーマル・モード・ポリシーが表示されます。次の表は、オプションの引き数を示しています。

| オプション | 説明          | 値                  |
|-------|-------------|--------------------|
| -mode | サーマル・モードの選択 | normal、performance |

構文:

```
thermal [options]
option:
  -mode thermal_mode
```

例:

```
system> thermal
-mode normal
system>
```

## timeouts コマンド

**timeouts** コマンドは、タイムアウト値の表示または変更を行うために使用します。タイムアウトを表示するには、**timeouts** と入力します。タイムアウト値を変更するには、オプションと、それに続けて値を入力します。タイムアウト値を変更するには、少なくとも「アダプター構成 (Adapter Configuration)」権限を持っている必要があります。

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

| オプション | タイムアウト               | 単位 | 値   |
|-------|----------------------|----|---|
| -f    | 電源オフ遅延               | 分  | disabled、0.5、1、2、3、4、5、7.5、10、15、20、30、60、120                 |
| -l    | ローダー・タイムアウト          | 分  | disabled、0.5、1、1.5、2、2.5、3、3.5、4、4.5、5、7.5、10、15、20、30、60、120 |
| -o    | オペレーティング・システムのタイムアウト | 分  | disabled、2.5、3、3.5、4  |

構文:

```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
```

例:

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

## usbeth コマンド

**usbeth** コマンドを使用すると、インバンド LAN over USB インターフェイスを使用可能または使用不可にすることができます。

構文:

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

例:

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

## users コマンド

**users** コマンドは、すべてのユーザー・アカウントとその権限レベルにアクセスするために使用します。また、**users** コマンドは、新規ユーザー・アカウントの作成、および既存のアカウントの変更を行うためにも使用します。

オプションを指定せずに **users** コマンドを実行すると、ユーザーと、ユーザーの一部の基本情報のリストが表示されます。次の表は、オプションの引き数を示しています。

| オプション       | 説明                      | 値  |
|-------------|-------------------------|--|
| -user_index | ユーザー・アカウントの索引番号         | 1 から 12、またはすべてのユーザーの場合は all。   |
| -n          | ユーザー・アカウント名             | 数字、文字、ピリオド、およびアンダースコアのみを含む固有のストリング。最小で 4 文字、最大で 16 文字です。   |
| -p          | ユーザー・アカウントのパスワード        | 少なくとも 1 文字の英字と 1 文字の英字以外の文字を含むストリング。最小で 6 文字、最大で 20 文字です。NULL は、初回ログイン時にユーザーが設定する必要がある、パスワードなしのアカウントを作成します。  |
| -a          | ユーザー権限レベル               | super、ro、custom<br><br>それぞれのパラメーターの意味は次のとおりです。<br><ul style="list-style-type: none"> <li>• super (スーパーバイザー)</li> <li>• ro (読み取り専用)</li> <li>• custom の後にはコロンと、パイプ ( ) で区切られた値のリストが続きます (custom:am rca の形式)。これらの値は、いかなる組み合わせでも使用できます。<br/> am (ユーザー・アカウント管理アクセス)<br/> rca (リモート・コンソール・アクセス)<br/> rcvma (リモート・コンソールおよび仮想メディア・アクセス)<br/> pr (リモート・サーバー電源/再始動アクセス)<br/> cel (イベント・ログを消去する機能)<br/> bc (アダプター構成 - 基本)<br/> nsc (アダプター構成 - ネットワークおよびセキュリティ)<br/> ac (アダプター構成 - 拡張)</li> </ul> |
| -ep         | 暗号化パスワード (バックアップ/リストア用) | 有効なパスワード   |
| -clear      | 指定されたユーザー・アカウントの削除      | 削除するユーザー・アカウントの索引番号を、以下の形式で指定する必要があります。<br><br>users -clear -user_index  |
| -curr       | 現在ログイン中のユーザーの表示         |  |
| -sauth      | SNMPv3 認証プロトコル          | HMAC-MD5、HMAC-SHA、none   |
| -spriv      | SNMPv3 プライバシー・プロトコル     | CBC-DES、AES、none   |

| オプション   | 説明   | 値  |
|---------|--|--|
| -spw    | SNMPv3 プライバシー・パスワード                                | 有効なパスワード   |
| -sepw   | SNMPv3 プライバシー・パスワード (暗号化)                          | 有効なパスワード   |
| -sacc   | SNMPv3 アクセス・タイプ                                    | get、set  |
| -strap  | SNMPv3 トラップ・ホスト名                                   | 有効なホスト名  |
| -pk     | ユーザーの SSH 公開鍵の表示                                   | ユーザー・アカウントの索引番号<br><b>注:</b><br><ul style="list-style-type: none"> <li>該当するユーザーに割り当てられている各 SSH 鍵が、識別するための鍵の索引番号と一緒に表示されます。</li> <li>SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー索引 (-userindex オプション) の後で使用する必要があります (users -2 -pk の形式)。</li> <li>すべての鍵は、OpenSSH フォーマットです。</li> </ul> |
| -e      | OpenSSH フォーマットで、全体の SSH 鍵を表示<br><br>(SSH 公開鍵オプション) | このオプションでは引き数を使用せず、他のすべての users -pk オプションと同時に使用することはできません。<br><b>注:</b> SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー索引 (-userindex オプション) の後で使用する必要があります (users -2 -pk -e の形式)。  |
| -remove | SSH 公開鍵のユーザーからの削除<br><br>(SSH 公開鍵オプション)            | 削除する公開鍵の索引番号は、該当するユーザーに割り当てられているすべての鍵で、固有の -key_index または -all として指定する必要があります。<br><b>注:</b> SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー索引 (-userindex オプション) の後で使用する必要があります (users -2 -pk -remove -1 の形式)。   |

| オプション | 説明  | 値   |
|-------|---|---|
| -add  | <p>ユーザーの SSH 公開鍵の追加</p> <p>(SSH 公開鍵オプション)</p>     | <p>OpenSSH フォーマットの引用符で区切られた鍵</p> <p>注:</p> <ul style="list-style-type: none"> <li>• -add オプションは、他のすべての users -pk コマンド・オプションと同時に使用することはできません。</li> <li>• SSH 公開鍵のオプションを使用する場合、以下の例のように、-pk オプションはユーザー索引 (-userindex オプション) の後で使用する必要があります。</li> </ul> <pre>users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEAvmfTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaN0y400ICEKCqjKEhrYymtAoVtFKApvY39GpnSGRC/qcLGWLM4cmi rKL5kxHNOqIcwbT1NPceoKHj46X7E+mq1fWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DPHJU1tzCjy68mEAnI rzjUoR98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUi upA1Yd8PSSMgdukASKEd3eRRZTB13SAtMucUsTkYj1Xcqex10Qz4+N50R6MbNcw1sx+mTEAvvcPJhuga70UNPGhLJM16k7jeJiQ8Xd2p Xb0ZQ=="</pre> |
| -upld | <p>SSH 公開鍵のアップロード</p> <p>(SSH 公開鍵オプション)</p>       | <p>鍵のロケーションを指定するには、-i および -l オプションが必要です。</p> <p>注:</p> <ul style="list-style-type: none"> <li>• -upld オプションは、他のすべての users -pk コマンド・オプション (-i および -l を除く) と同時に使用することはできません。</li> <li>• 鍵を新しい鍵と置き換えるには、-key_index を指定する必要があります。現行の鍵のリストの最後に鍵を追加する場合は、鍵の索引を指定しないでください。</li> <li>• SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー索引 (-userindex オプション) の後で使用する必要があります (users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key の形式)。</li> </ul>  |
| -dnld | <p>指定された SSH 公開鍵のダウンロード</p> <p>(SSH 公開鍵オプション)</p> | <p>ダウンロードする鍵を指定するには -key_index オプションが必要で、TFTP サーバーを稼働している別のコンピューター上のダウンロード・ロケーションを指定するには -i および -l オプションが必要です。</p> <p>注:</p> <ul style="list-style-type: none"> <li>• -dnld オプションは、他のすべての users -pk コマンド・オプション (-i、-l、および -key_index を除く) と同時に使用することはできません。</li> <li>• SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー索引 (-userindex オプション) の後で使用する必要があります (users -2 -pk -dnld -i tftp://9.72.216.40/ -l file.key の形式)。</li> </ul>  |

| オプション | 説明   | 値  |
|-------|--|--|
| -i    | 鍵ファイルをアップロードまたはダウンロードするための TFTP/SFTP サーバーの IP アドレス<br><br>(SSH 公開鍵オプション) | 有効な IP アドレス<br>注: users -pk -upld および users -pk -dnld コマンド・オプションでは、-i オプションが必須です。  |
| -pn   | TFTP/SFTP サーバーのポート番号<br><br>(SSH 公開鍵オプション)                               | 有効なポート番号 (デフォルト 69/22)<br>注: users -pk -upld および users -pk -dnld コマンド・オプションのオプション・パラメーター。  |
| -u    | SFTP サーバーのユーザー名<br><br>(SSH 公開鍵オプション)                                    | 有効なユーザー名<br>注: users -pk -upld および users -pk -dnld コマンド・オプションのオプション・パラメーター。  |
| -pw   | SFTP サーバーのパスワード<br><br>(SSH 公開鍵オプション)                                    | 有効なパスワード<br>注: users -pk -upld および users -pk -dnld コマンド・オプションのオプション・パラメーター。  |
| -l    | TFTP または SFTP 経由で鍵ファイルをアップロードまたはダウンロードするためのファイル名<br><br>(SSH 公開鍵オプション)   | 有効なファイル名<br>注: users -pk -upld および users -pk -dnld コマンド・オプションでは、-l オプションが必須です。   |
| -af   | ホストからの接続を受け入れる<br><br>(SSH 公開鍵オプション)                                     | ホスト名および IP アドレスのコンマ区切りリスト (最大で 511 文字)。有効な文字には、英数字、コンマ、アスタリスク、疑問符 (?)、感嘆符、ピリオド、ハイフン、コロン、および % 記号があります。   |
| -cm   | コメント<br><br>(SSH 公開鍵オプション)   | 最大 255 文字の、引用符で区切ったストリング。<br>注: SSH 公開鍵のオプションを使用する場合、-pk オプションはユーザー索引 (-userindex オプション) の後で使用する必要があります (users -2 -pk -cm "This is my comment." の形式)。. |

構文:

```
users [options]
options:
  -user_index
  -n username
  -p password
  -a authority_level
  -ep encryption_password
  -clear
  -curr
```

```

-sauth protocol
-spriv protocol
-spw password
-sepw password
-sacc state
-strap hostname

users -pk [options]
options:
-e
-remove index
-add key
-upld
-dnld
-i ip_address
-pn port_number
-u username
-pw password
-l filename
-af list
-cm comment

```

例:

```

system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
4. <not used>
5. jacybyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSWORD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID Read/Write
Password Expires: no expiration
2. test Read/Write
Password Expires: no expiration
3. test2 Read/Write
Password Expires: no expiration
4. <not used>
5. jacybyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>

```

---

## IMM2 制御コマンド

IMM2 制御コマンドは、以下のとおりです。

- 202 ページの『alertentries コマンド』
- 205 ページの『batch コマンド』
- 206 ページの『clearcfg コマンド』
- 206 ページの『clock コマンド』

- 207 ページの『identify コマンド』
- 207 ページの『info コマンド』
- 208 ページの『resetsp コマンド』
- 208 ページの『spreset コマンド』

## alertentries コマンド

**alertentries** コマンドを使用すると、アラートの受信者を管理することが可能です。

- オプションを指定しない **alertentries** では、すべてのアラート項目の設定が表示されます。
- **alertentries -number -test** では、指定された受信者の索引番号にテスト・アラートが生成されます。
- **alertentries -number** (ここで **number** は 0 から 12) では、指定された受信者の索引番号に対するアラート項目の設定が表示されるか、その受信者のアラート設定の変更が可能になります。

次の表は、オプションの引数を示しています。

| オプション   | 説明                           | 値                  |
|---------|------------------------------|--------------------|
| -number | 表示、追加、変更、または削除するアラート受信者の索引番号 | 1 から 12            |
| -status | アラート受信者状況                    | on、off             |
| -type   | アラート・タイプ                     | email、syslog       |
| -log    | アラート E メールにイベント・ログを含める       | on、off             |
| -n      | アラート受信者名                     | ストリング              |
| -e      | アラート受信者の E メール・アドレス          | 有効な E メール・アドレス     |
| -ip     | Syslog の IP アドレスまたはホスト名      | 有効な IP アドレスまたはホスト名 |
| -pn     | Syslog ポート番号                 | 有効なポート番号           |
| -del    | 指定された受信者の索引番号を削除             |                    |
| -test   | 指定された受信者の索引番号に対するテスト・アラートを生成 |                    |

| オプション  | 説明                      | 値  |
|--------|-------------------------|--|
| -crt   | アラートを送信するクリティカル・イベントを設定 | <p>all、none、custom:telvolpoldilfalcpmlinlrelot</p> <p>カスタムのクリティカル・アラート設定は、値をパイプで区切られたリストにして、<b>alertentries -crt custom:telvo</b> の形式で指定します。ここで、カスタム値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• te: クリティカルな温度しきい値超過</li> <li>• vo: クリティカルな電圧しきい値超過</li> <li>• po: クリティカルな電源障害</li> <li>• di: ハード・ディスク障害</li> <li>• fa: ファン障害</li> <li>• cp: マイクロプロセッサ障害</li> <li>• me: メモリー障害</li> <li>• in: ハードウェアの互換性なし</li> <li>• re: 電源の冗長性の障害</li> <li>• ot: その他すべてのクリティカル・イベント</li> </ul> |
| -crten | クリティカル・イベント・アラートを送信     | enabled、disabled   |
| -wrn   | アラートを送信する警告イベントを設定      | <p>all、none、custom:rpltelvolpolfalcpmlmet</p> <p>カスタムの警告アラート設定は、値をパイプで区切られたリストにして、<b>alertentries -wrn custom:rplte</b> の形式で指定します。ここで、カスタム値は以下のとおりです。</p> <ul style="list-style-type: none"> <li>• rp: 電源の冗長性の警告</li> <li>• te: 警告の温度しきい値超過</li> <li>• vo: 警告の電圧しきい値超過</li> <li>• po: 警告の電力しきい値超過</li> <li>• fa: クリティカルではないファン・イベント</li> <li>• cp: マイクロプロセッサが機能低下状態</li> <li>• me: メモリーの警告</li> <li>• ot: その他すべての警告イベント</li> </ul>   |
| -wrnen | 警告イベント・アラートを送信          | enabled、disabled   |

| オプション  | 説明                    | 値   |
|--------|-----------------------|---|
| -sys   | アラートを送信するルーチン・イベントを設定 | all、none、custom:loltiotlotlpolbftillpfllelne<br><br>カスタムのルーチン・アラート設定は、値をパイプで区切られたリストにして、 <b>alertentries -sys custom:loltio</b> の形式で指定します。ここで、カスタム値は以下のとおりです。<br><br><ul style="list-style-type: none"> <li>• lo: 正常なりモート・ログイン</li> <li>• tio: オペレーティング・システムのタイムアウト</li> <li>• ot: その他すべての通知イベントおよびシステム・イベント</li> <li>• po: システムの電源オン/オフ</li> <li>• bf: オペレーティング・システムのブート障害</li> <li>• オペレーティング・システム・ローダーのウォッチドッグ・タイムアウト</li> <li>• pf: 障害予知 (PFA)</li> <li>• el: イベント・ログ 75% フル</li> <li>• ne: ネットワーク変更</li> </ul> |
| -sysen | ルーチン・イベント・アラートを送信     | enabled、disabled  |

構文:

```

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

```

例:

```

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

```

12. <not used>

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

## batch コマンド

**batch** コマンドは、同一のファイルに含まれている 1 つ以上の CLI コマンドを実行するために使用します。

- バッチ・ファイルのコメント行は、# で始まります。
- バッチ・ファイルを実行する際、失敗したコマンドは、失敗の戻りコードとともに返されます。
- 認識されないコマンド・オプションを含むバッチ・ファイル・コマンドでは、警告が生成される場合があります。

次の表は、オプションの引数を示しています。

| オプション | 説明                      | 値                      |
|-------|-------------------------|------------------------|
| -f    | バッチ・ファイル名               | 有効なファイル名               |
| -ip   | TFTP/SFTP サーバーの IP アドレス | 有効な IP アドレス            |
| -pn   | TFTP/SFTP サーバーのポート番号    | 有効なポート番号 (デフォルト 69/22) |
| -u    | SFTP サーバーのユーザー名         | 有効なユーザー名               |
| -pw   | SFTP サーバーのパスワード         | 有効なパスワード               |

構文:

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

例:

```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg -client -dnld -ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

## clearcfg コマンド

**clearcfg** コマンドは、IMM2 の構成を出荷時のデフォルト値に設定するために使用します。このコマンドを発行するには、少なくとも「拡張アダプター構成 (Advanced Adapter Configuration)」権限を持っている必要があります。IMM2 の構成がクリアされた後、IMM2 は再始動されます。

## clock コマンド

**clock** コマンドは、IMM2 クロックと GMT オフセットに従って現在の日時を表示するために使用します。日付、時刻、GMT オフセット、および夏時間調整の設定値を設定できます。

以下の情報に注意してください。

- +2、-7、-6、-5、-4、または -3 の GMT オフセットでは、以下のように特殊な夏時間の設定が必要です。
  - +2 の場合、夏時間オプションには、off、ee (東欧)、mik (ミンスク)、tky (トルコ)、bei (バイルート)、amm (アンマン)、jem (エルサレム) があります。
  - -7 の場合、夏時間の設定には、off、mtn (山岳部標準時)、maz (マサトラン) があります。
  - -6 の場合、夏時間の設定には、off、mex (メキシコ)、cna (中央/北アメリカ) があります。
  - -5 の場合、夏時間の設定には、off、cub (キューバ)、ena (アメリカ北東部) があります。
  - -4 の場合、夏時間の設定には、off、asu (アスンシオン)、cui (クイアバ)、san (サンティアゴ)、cat (カナダ - 大西洋岸) があります。
  - -3 の場合、夏時間の設定には、off、gtb (ゴットホープ)、moo (モンテビデオ)、bre (ブラジル - 東部) があります。
- 年は、2000 以上 2089 以下であることが必要です。
- 月、日、時、分、秒は、1 桁の値 (たとえば、09:50:25 でなく 9:50:25) にすることができます。
- GMT オフセットのフォーマットは、正のオフセットの場合には、+2:00、+2、または 2 とすることができ、負のオフセットの場合には -5:00 または -5 とすることができます。

構文:

```
clock [options]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

例:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2011
ok
system> clock
12/31/2011 13:15:30 GMT-5:00 dst on
```

## identify コマンド

**identify** コマンドを使用すると、シャーシ識別 LED を点灯、または消灯、あるいは点滅させることができます。 **-d** オプションを **-s on** と一緒に使用すると、**-d** パラメーターで指定した秒数だけ LED を点灯させることができます。その秒数を経過すると、LED は消灯します。

構文:

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

例:

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

## info コマンド

**info** コマンドは、IMM2 に関する情報を表示および構成するために使用します。

オプションを指定せずに **info** コマンドを実行すると、IMM2 のロケーションおよび連絡先のすべての情報が表示されます。次の表は、オプションの引き数を示しています。

| オプション              | 説明              | 値      |
|--------------------|-----------------|--------|
| -name              | IMM2 名          | ストリング  |
| -contact           | IMM2 の連絡先担当者の氏名 | ストリング  |
| -location          | IMM2 のロケーション    | ストリング  |
| -room <sup>1</sup> | IMM2 のルーム ID    | ストリング  |
| -rack <sup>1</sup> | IMM2 のラック ID    | ストリング  |
| -rup <sup>1</sup>  | ラック内での IMM2 の位置 | ストリング  |
| -ruh               | ラック・ユニットの高さ     | 読み取り専用 |
| -bbay              | ブレード・ベイのロケーション  | 読み取り専用 |

1. IMM2 が IBM Flex System 環境にある場合、値は読み取り専用であり、リセットすることができません。

構文:

```
info [options]
option:
-name imm_name
-contact contact_name
-location imm_location
-room room_id
```

```
-rack rack_id  
-rup rack_unit_position  
-ruh rack_unit_height  
-bbay blade_bay
```

## resetsp コマンド

**resetsp** コマンドは、IMM2 を再始動するために使用します。このコマンドを発行するには、少なくとも「拡張アダプター構成 (Advanced Adapter Configuration)」権限を持っている必要があります。

## spreset コマンド

**spreset** コマンドは、IMM2 を再始動するために使用します。このコマンドを発行するには、少なくとも「拡張アダプター構成 (Advanced Adapter Configuration)」権限を持っている必要があります。

---

## 付録 A. ヘルプおよび技術サポートの入手

ヘルプ、サービス、技術サポート、または IBM 製品に関する詳しい情報が必要な場合は、IBM がさまざまな形で提供しているサポートをご利用いただけます。

以下の情報を使用して、IBM と IBM 製品に関する追加情報の入手先、IBM システムまたはオプション装置で問題が発生した場合の対処方法、およびサービスが必要になった場合の連絡先を知ることができます。

---

### 依頼する前に

連絡する前に、以下の手順を実行して、必ずお客様自身で問題の解決を試みてください。

ご使用の IBM 製品において IBM が保証サービスを実行する必要があると確信する場合は、お客様に連絡前の準備をしていただくことで、IBM サービス技術員がより効果的な支援を行うことができます。

- ケーブルがすべて接続されていることを確認します。
- 電源スイッチをチェックして、システムおよびすべてのオプション製品の電源がオンになっていることを確認します。
- ご使用の IBM 製品用のソフトウェア、ファームウェア、およびオペレーティング・システムのデバイス・ドライバが更新されていないかを確認します。IBM 保証条件は、IBM 製品の所有者であるお客様の責任で、製品のソフトウェアおよびファームウェアの保守および更新を行う必要があることを明記しています (追加の保守契約によって保証されていない場合)。お客様の IBM サービス技術員は、問題の解決策がソフトウェアのアップグレードで文書化されている場合、ソフトウェアおよびファームウェアをアップグレードすることを要求します。
- ご使用の環境で新しいハードウェアを取り付けたり、新しいソフトウェアをインストールした場合、<http://www.ibm.com/systems/info/x86servers/serverproven/compat/us> でそのハードウェアおよびソフトウェアがご使用の IBM 製品によってサポートされていることを確認してください。
- <http://www.ibm.com/supportportal> にアクセスして、問題の解決に役立つ情報があるか確認してください。
- IBM サポートに提供するために、次の情報を収集してください。IBM サポートは、このデータを使用してお客様の問題に対する解決策を迅速に提供し、また、お客様の契約に基づく適切なレベルのサービスを保証できるようになります。
  - ハードウェアおよびソフトウェアの保守契約番号 (該当する場合)
  - マシン・タイプ番号 (IBM の 4 桁のマシン ID)
  - 型式番号
  - シリアル番号
  - 現行のシステム UEFI およびファームウェアのレベル
  - その他の関連する情報 (エラー・メッセージおよびログなど)

- [http://www.ibm.com/support/entry/portal/Open\\_service\\_request](http://www.ibm.com/support/entry/portal/Open_service_request) にアクセスして、Electronic Service Request を送信してください。Electronic Service Request を送信すると、IBM サポートが迅速に、そして効果的に関連情報を使用できるようになることで、お客様の問題の解決策を判別するプロセスが開始されます。IBM サービス技術員は、お客様が Electronic Service Request を完了および送信するとすぐに、解決策の作業を開始します。

多くの問題は、オンライン・ヘルプおよびご使用のサーバーに付属の資料に記載のトラブルシューティング手順を実行することで、外部の支援なしに解決することができます。IBM システムに付属の資料には、ユーザーが実行できる診断テストについても記載されています。ほとんどのシステム、オペレーティング・システム、およびプログラムには、トラブルシューティング手順やエラー・メッセージおよびエラー・コードに関する資料が付属しています。ソフトウェアの問題が疑われる場合は、オペレーティング・システムまたはプログラムの資料を参照してください。

---

## 資料の使用

IBM システム、およびプリインストール・ソフトウェア、あるいはオプション装置に関する情報は、製品に付属の資料に記載されています。資料には、印刷された説明書、オンライン資料、README ファイル、およびヘルプ・ファイルがあります。

診断プログラムの使用方法については、システム資料にあるトラブルシューティングに関する情報を参照してください。トラブルシューティング情報または診断プログラムを使用した結果、デバイス・ドライバーの追加や更新、あるいは他のソフトウェアが必要になることがあります。IBM は WWW に、最新の技術情報を入手したり、デバイス・ドライバーおよび更新をダウンロードできるページを設けています。これらのページにアクセスするには、<http://www.ibm.com/supportportal>に進んでください。

---

## ヘルプおよび情報を WWW から入手する

IBM 製品およびサポートに関する最新情報は、WWW から入手可能です。

WWW 上の <http://www.ibm.com/supportportal> では、IBM システム、オプション装置、サービス、およびサポートについての最新情報が提供されています。IBM System x 情報は、<http://www-06.ibm.com/systems/jp/x/> にあります。IBM BladeCenter 情報は、<http://www-06.ibm.com/systems/jp/bladecenter/> にあります。IBM IntelliStation 情報は、<http://www-06.ibm.com/jp/products/workstations/intellistation/product/list.shtml> にあります。

---

## IBM への DSA データの送信方法

IBM に診断データを送信するには、IBM Enhanced Customer Data Repository を使用します。

診断データを IBM に送信する前に、<http://www.ibm.com/de/support/ecurep/terms.html> の利用条件をお読みください。

以下のいずれかの方法を使用して、診断データを IBM に送信することができます。

- 標準アップロード:[http://www.ibm.com/de/support/ecurep/send\\_http.html](http://www.ibm.com/de/support/ecurep/send_http.html)
- システムのシリアル番号を使用した標準アップロード:[http://www.ecurep.ibm.com/app/upload\\_hw](http://www.ecurep.ibm.com/app/upload_hw)
- セキュア・アップロード:[http://www.ibm.com/de/support/ecurep/send\\_http.html#secure](http://www.ibm.com/de/support/ecurep/send_http.html#secure)
- システムのシリアル番号を使用したセキュア・アップロード:  
[https://www.ecurep.ibm.com/app/upload\\_hw](https://www.ecurep.ibm.com/app/upload_hw)

---

## 個別設定したサポート Web ページの作成

目的の IBM 製品を特定して、個別設定したサポート Web ページを作成することができます。

個別設定したサポート Web ページを作成するには、<http://www.ibm.com/support/mynotifications> にアクセスします。この個別設定したページから、最新の技術文書に関する E メール通知を毎週購読したり、情報やダウンロードを検索したり、さまざまな管理サービスにアクセスしたりすることができます。

---

## ソフトウェアのサービスとサポート

IBM Support Line を使用すると、IBM 製品の使用方法、構成、およびソフトウェアの問題について、電話による援助を有料で受けることができます。

サポート・ラインおよび各種の IBM サービスについて詳しくは、<http://www.ibm.com/services> をご覧になるか、あるいは <http://www.ibm.com/planetwide> でサポート電話番号をご覧ください。米国およびカナダの場合は、1-800-IBM-SERV (1-800-426-7378) に電話してください。

---

## ハードウェアのサービスとサポート

ハードウェアの保守は、IBM 販売店か IBM サービスを通じて受けることができます。

IBM により許可された保証サービスを提供する販売店を見つけるには、<http://www.ibm.com/partnerworld/jp/> にアクセスしてから、ページの右サイドで「パートナーを探す」をクリックしてください。IBM サポートの電話番号については、<http://www.ibm.com/planetwide> を参照してください。米国およびカナダの場合は、1-800-IBM-SERV (1-800-426-7378) に電話してください。

米国およびカナダでは、ハードウェア・サービスおよびサポートは、1 日 24 時間、週 7 日ご利用いただけます。英国では、これらのサービスは、月曜から金曜までの午前 9 時から午後 6 時までご利用いただけます。



---

## 付録 B. 特記事項

本書は米国IBM が提供する製品およびサービスについて作成したものであり、本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510  
東京都中央区日本橋箱崎町19番21号  
日本アイ・ビー・エム株式会社  
法務・知的財産  
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

---

## 商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。

現時点での IBM の商標リストについては、<http://www.ibm.com/legal/us/en/copytrade.shtml> をご覧ください。

Adobe および PostScript は、Adobe Systems の米国およびその他の国における登録商標です。

Cell Broadband Engine, Cell/B.E は、米国およびその他の国における Sony Computer Entertainment, Inc. の商標であり、同社の許諾を受けて使用しています。

Intel、Intel Xeon、Itanium、および Pentium は、Intel Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

UNIX は、The Open Group の米国およびその他の国における登録商標です。

---

## 重要事項

プロセッサの速度とは、マイクロプロセッサの内蔵クロックの速度を意味しますが、他の要因もアプリケーション・パフォーマンスに影響します。

CD または DVD のドライブ・スピードは、読み取り速度が変動します。実際の速度は記載された速度と異なる場合があります、最大可能な速度よりも遅いことがあります。

主記憶装置、実記憶域と仮想記憶域、またはチャンネル転送量を表す場合、KB は 1024 バイト、MB は 1,048,576 バイト、GB は 1,073,741,824 バイトを意味します。

ハード・ディスクの容量、または通信ボリュームを表すとき、MB は 1,000,000 バイトを意味し、GB は 1,000,000,000 バイトを意味します。ユーザーがアクセス可能な総容量は、オペレーティング環境によって異なる可能性があります。

内蔵ハード・ディスクの最大容量は、IBM から入手可能な現在サポートされている最大のドライブを標準ハード・ディスクの代わりに使用し、すべてのハード・ディスク・ベイに取り付けることを想定しています。

最大メモリーは標準メモリーをオプション・メモリー・モジュールと取り替える必要があることもあります。

各ソリッド・ステート・メモリー・セルには、そのセルが耐えられる固有の有限数の組み込みサイクルがあります。したがって、ソリッド・ステート・デバイスには、可能な書き込みサイクルの最大数が決められています。これを「書き込み合計バイト数」(TBW) と呼びます。この制限を超えたデバイスは、システム生成コマンドに応答できなくなる可能性があります、また書き込み不能になる可能性があります。

IBM は、正式に公開された仕様に文書化されているプログラム/消去のサイクルの最大保証回数を超えたデバイスについては責任を負いません。

IBM は、ServerProven<sup>®</sup> に登録されている他社製品およびサービスに関して、商品性、および特定目的適合性に関する黙示的な保証も含め、一切の保証責任を負いません。これらの製品は、第三者によってのみ提供および保証されます。

IBM は、他社製品に関して一切の保証責任を負いません。他社製品のサポートがある場合は、IBM ではなく第三者によって提供されます。

いくつかのソフトウェアは、その小売り版 (利用可能である場合) とは異なる場合があります、ユーザー・マニュアルまたはすべてのプログラム機能が含まれていない場合があります。

---

## サーバーの廃棄・譲渡時のハード・ディスク上のデータ消去に関するご注意

これらのサーバーの中のハード・ディスクという記憶装置に、お客様の重要なデータが記録されています。従ってそのサーバーを譲渡あるいは廃棄するときには、これらの重要なデータ内容を消去するということが必要となります。

ところがこのハード・ディスク内に書き込まれたデータを消去するというのは、それほど簡単ではありません。「データを消去する」という場合、一般に

- データを「ゴミ箱」に捨てる
- 「削除」操作を行う
- 「ゴミ箱を空にする」コマンドを使って消す
- ソフトウェアで初期化 (フォーマット) する
- 付属のリカバリー・プログラムを使い、工場出荷状態に戻す

などの作業をすすると思いますが、これらのことをしても、ハード・ディスク内に記録されたデータのファイル管理情報が変更されるだけで、実際にデータが消された状態ではありません。つまり、一見消去されたように見えますが、Windows<sup>®</sup> などの OS のもとで、それらのデータを呼び出す処理ができなくなっただけで、本来のデータは残っているという状態にあるのです。

従いまして、特殊なデータ回復のためのソフトウェアを利用すれば、これらのデータを読みとることが可能な場合があります。このため、悪意のある人により、このサーバーのハード・ディスク内の重要なデータが読みとられ、予期しない用途に利用されるおそれがあります。

サーバーの廃棄・譲渡等を行う際に、ハード・ディスク上の重要なデータが流出するというトラブルを回避するためには、ハード・ディスクに記録された全データを、お客様の責任において消去することが非常に重要となります。消去するためには、ハード・ディスク上のデータを金槌や強磁気により物理的・磁氣的に破壊して読めなくする、または、専用ソフトウェアあるいはサービス (共に有償) をご利用になられることを推奨します。

なお、ハード・ディスク上のソフトウェア (オペレーティング・システム、アプリケーション・ソフトウェアなど) を削除することなくサーバーを譲渡すると、ソフトウェア・ライセンス使用許諾契約に抵触する場合がありますため、十分な確認を行う必要があります。

データ消去支援サービスまたは機器リサイクル支援サービスについての詳細は、弊社営業担当員または「ダイヤル IBM」044-221-1522 へお問い合わせ下さい。

## 粒子汚染

**重要:** 浮遊微小粒子 (金属片や微粒子を含む) や反応性ガスは、単独で、あるいは湿気や気温など他の環境要因と組み合わせられることで、本書に記載されている装置にリスクをもたらす可能性があります。

過度のレベルの微粒子や高濃度の有害ガスによって発生するリスクの中には、装置の誤動作や完全な機能停止の原因となり得る損傷も含まれます。以下の仕様では、このような損傷を防止するために設定された微粒子とガスの制限について説明しています。以下の制限を、絶対的な制限としてみなしたり、使用したりしてはなりません。微粒子や環境腐食物質、ガスの汚染物質移動が及ぼす影響の度合いは、温度や空気中の湿気など他の多くの要因によって左右されるからです。本書で説明されている具体的な制限がない場合は、人体の健康と安全の保護を脅かすことのない微粒子とガスのレベルを維持するよう、実践していく必要があります。お客様の環境の微粒子あるいはガスのレベルが装置損傷の原因であると IBM が判断した場合、IBM は、装置または部品の修理あるいは交換の条件として、かかる環境汚染を改善する適切な是正措置の実施を求める場合があります。かかる是正措置は、お客様の責任で実施していただきます。

表9. 微粒子およびガスの制限

| 汚染物質 | 制限   |
|------|--|
| 微粒子  | <ul style="list-style-type: none"> <li>室内の空気は、ASHRAE Standard 52.2 に従い、大気粉塵が 40% のスポット効率で継続してフィルタリングされなければならない (MERV 9 準拠)<sup>1</sup>。</li> <li>データ・センターに取り入れる空気は、MIL-STD-282 に準拠する HEPA フィルターを使用し、99.97% 以上の粒子捕集率効果のあるフィルタリングが実施されなければならない。</li> <li>粒子汚染の潮解相対湿度は、60% を超えていなければならない<sup>2</sup>。</li> <li>室内には、亜鉛ウイスキーのような導電性汚染があってはならない。</li> </ul> |
| ガス   | <ul style="list-style-type: none"> <li>銅: ANSI/ISA 71.04-1985 準拠の Class G1<sup>3</sup></li> <li>銀: 腐食率は 30 日間で 300 Å 未満</li> </ul>   |

<sup>1</sup> ASHRAE 52.2-2008 - 一般的な換気および空気清浄機器について、微粒子の大きさごとの除去効率をテストする方法。Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

<sup>2</sup> 粒子汚染の潮解相対湿度とは、水分を吸収した塵埃が、十分に濡れてイオン導電性を持つようになる湿度のことです。

<sup>3</sup> ANSI/ISA-71.04-1985。プロセス計測およびシステム制御のための環境条件: 気中浮遊汚染物質。Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

## 通信規制の注記

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks.

本製品は、電気通信事業者の通信回線への直接、またはそれに準ずる方法での接続を目的とするものではありません。

---

## 電波障害自主規制特記事項

この装置にモニターを接続する場合は、モニターに付属の指定のモニター・ケーブルおよび電波障害抑制装置を使用してください。

### Federal Communications Commission (FCC) statement

**Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

### Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

### Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

### Australia and New Zealand Class A statement

**Attention:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

### European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any

failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

**Attention:** This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

International Business Machines Corp.  
New Orchard Road  
Armonk, New York 10504  
914-499-1900

European Community contact:

IBM Deutschland GmbH  
Technical Regulations, Department M372  
IBM-Allee 1, 71139 Ehningen, Germany  
Telephone: +49 7032 15 2941  
Email: lugi@de.ibm.com

## Germany Class A statement

### **Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit**

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:  
"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

### **Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten**

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

## Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.  
New Orchard Road  
Armonk, New York 10504  
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH  
Technical Regulations, Abteilung M372  
IBM-Allee 1, 71139 Ehningen, Germany  
Telephone: +49 7032 15 2941  
Email: lugi@de.ibm.com

### Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

## VCCI クラス A 情報技術装置

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

## Korea Communications Commission (KCC) statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

## Russia Electromagnetic Interference (EMI) Class A statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.  
В жилых помещениях оно может создавать радиопомехи, для  
снижения которых необходимы дополнительные меры

## People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声明

此为A类产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

## Taiwan Class A compliance statement

警告使用者：  
這是甲類的資訊產品，在  
居住的環境中使用時，可  
能會造成射頻干擾，在這  
種情況下，使用者會被要  
求採取某些適當的對策。

# 索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

## [ア行]

### アクセス

Remote Control 118

Telnet 55, 195

### アクティブ・ディレクトリー・ユーザー

LDAP 55, 196

### アクティベーション・キー

インストール 141, 175

エクスポート 145

管理 56, 175

削除 144, 175

### アドバンスド・マネージメント・モジュール

1, 4, 7

### アルファベット順のコマンド・リスト

150

### イーサネット

構成 54, 173

### イーサネットの詳細

設定 70

### イベント

ログ 126

### イベント通知

### イベント・ログ

管理 126

### インストール

アクティベーション・キー 141, 175

### インフォメーション・センター

210

### エクスポート

アクティベーション・キー 145

### エクスポート機能

Features on Demand 145

FoD 145

### オープン・ポートの表示

55, 180

### 汚染、粒子およびガス

216

### オプション

IMM management (IMM 管理) タブ

51

server management (サーバー管理) タブ

32

### オペレーティング・システムのスクリーン・キャプチャー

107

### オペレーティング・システム要件

4

### オンライン資料

エラー・コード情報 1

### オンライン資料 (続き)

資料更新情報 1

ファームウェア更新情報 1

## [カ行]

### 概要

download service data (サービス・データのダウンロード) 31

ssl 90

### 拡張役割ベース・セキュリティ

LDAP 55, 196

### 拡張レベル機能

3

### ガス汚染

カスタム・サポート Web ページ 211

### 管理

アクティベーション・キー 56, 175

ユーザー 54, 196

DDNS 54, 170

Features on Demand 56, 175

FoD 56, 175

MAC アドレス 54, 173

SNMPv1 コミュニティー 54, 184

### 基本レベル機能

3

### クライアント識別名

LDAP サーバー 55, 177

### クラス A 電波障害自主規制ステートメント

219

### グループ検索属性

LDAP 55, 177

### グループの削除

使用可能にする、使用不可にする 173

### グループ・フィルター

LDAP 55, 177

### グループ・プロファイル

管理 64

### グローバル・ログイン

設定 65

### グローバル・ログイン設定

account security level (アカウント・セキュリティ・レベル) タブ 67

general (一般) タブ 65

### 検索ドメイン

LDAP サーバー 55, 177

### 更新

ActiveX アプレット 106

Java アプレット 106

### 構成

イーサネット 54, 173

イーサネット設定 70

グローバル・ログイン設定 65

### 構成 (続き)

シリアル・ポート 53, 60, 181

セキュリティ 56

セキュリティ設定 84

ネットワーク・プロトコル 70

ポート 55, 180

ポート割り当て 83

ユーザー・アカウントのセキュリティ

レベル 54, 162

CIM over HTTPS プロトコル 86

DDNS 54, 170

DDNS 設定 74

DNS 54, 170

DNS 設定 74

Ethernet over USB 55, 172

HTTPS プロトコル 85

IMM2 56

IPv4 54, 173

IPv6 54, 173

LDAP 55, 177

LDAP クライアント・プロトコル 87

LDAP サーバー 55, 177

LDAP 設定 76

Serial-to-SSH リダイレクト 148

Serial-to-Telnet リダイレクト 148

SMTP 55, 184

SMTP 設定 75

SNMP アラート設定 72

SNMPv1 54, 184

SNMPv1 トラップ 54, 184

SNMPv3 のユーザー・アカウント 54,

196

ssh サーバー 89

Telnet 195

Telnet 設定 55, 81

USB 55, 172

USB 設定 82

### 構成コマンド

161

### 構成サマリー、表示

11

### 構成のバックアップ

IMM2 56

### 構成の表示

IMM2 56

### 構成の復元

IMM2 56, 182

### 構成のリストア

IMM2 56, 182

### 構成のリセット

IMM 183

IMM2 56

固定 IP アドレス、デフォルト 8

個別設定したサポート Web ページの作成

211

コマンド

電源 160

復元 182

ヘルプ 152

ポート 180

accsecfg 162

alertcfg 164

alertentries 202

asu 165

backup 168

batch 205

clearcfg 206

clearlog 153

clock 206

console 161

dhcpinfo 169

dns 170

ethtousb 172

exit 152

fans 153

ffdc 153

gprofile 173

history 152

identify 207

ifconfig 173

info 207

keycfg 175

ldap 177

led 155

ntp 178

passwordcfg 179

portcfg 181

pxeboot 160

readlog 156

reset 161

resetsp 208

restoredefaults 183

set 183

show 157

smtp 184

snmp 184

snmpalerts 187

sreset 208

srcfg 189

sshcfg 189

ssl 190

sslcfg 192

syshealth 158

telnetcfg 195

temps 158

thermal 195

timeouts 195

usbeth 196

users 196

コマンド (続き)

volts 159

vpd 159

コマンド、アルファベット順リスト 150

コマンド、タイプ

構成 161

サーバーの電源および再始動 160

シリアル・リダイレクト 161

モニター 153

ユーティリティ 152

IMM2 制御 201

コマンド・ライン・インターフェース

(CLI)

アクセス 147

機能および制限 149

コマンド構文 149

説明 147

ログイン 148

## [サ行]

サーバー状況

モニター 95

サーバー状況のモニター 95

サーバー電源

制御 104

サーバーのターゲット名

LDAP 55, 177

サーバーの電源および再始動

コマンド 160

サーバー・アドレッシング

DNS 54, 170

サーバー・タイムアウト

選択 56

サーバー・タイムアウトの設定 56

サービスおよびサポート

依頼する前に 209

ソフトウェア 211

ハードウェア 211

サービスおよびサポート・データ

収集 132

ダウンロード 132

サービスおよびサポート・データの収集

132

再始動

IMM 208

IMM2 56

最大セッション数

Telnet 55, 195

最大伝送単位

設定 54, 173

作業

イベント・ログのイベント 26

削除

アクティベーション・キー 144, 175

ユーザー 54, 196

削除 (続き)

E メール通知 128

syslog 通知 128

作成

ユーザー・アカウント 54, 196

E メール通知 128

syslog 通知 128

サポート Web ページ、カスタム 211

支援、入手 209

識別名、クライアント

LDAP サーバー 55, 177

識別名、ルート

LDAP サーバー 55, 177

事項、重要 214

時刻

設定 53, 206

システム状況 95

システム情報 97

表示 97

システム・イベント

再試行通知 128

通知 128

システム・イベント通知 29

システム・ヘルス 98

事前構成

LDAP サーバー 55, 177

実行

IMM2 タスク 103

始動シーケンスの変更 11

自動ネゴシエーション

設定 54, 173

「重要」の注記 214

使用

ActiveX クライアント 38

Java クライアント 38

商標 214

証明書管理

CIM over HTTPS 56, 190, 192

HTTPS サーバー 56, 190, 192

LDAP 56, 190, 192

SSH サーバー 56, 189

証明書の処理

セキュア LDAP クライアント 87

CIM over HTTPS 86

シリアル・ポート

構成 53, 60, 181

シリアル・リダイレクト・コマンド 161

資料

使用 210

セキュリティ

構成 56

CIM over HTTPS 56, 190, 192

CIM over HTTPS プロトコル 86

HTTPS サーバー 56, 190, 192

HTTPS プロトコル 85

LDAP 56, 190, 192

セキュリティ (続き)  
LDAP クライアント 87  
SSH サーバー 56, 189  
ssh サーバー 89  
SSL 証明書管理 91  
SSL 証明書の処理 90  
SSL の概要 90  
セッション、最大数  
Telnet 55, 195  
絶対マウス制御 111  
設定  
イーサネット 70  
グローバル・ログイン 65  
account security level (アカウント・セキュリティ・レベル) タブ 67  
general (一般) タブ 65  
最大伝送単位 54, 173  
時刻 53, 206  
自動ネゴシエーション 54, 173  
詳細 70  
セキュリティ 84  
日付 53, 206  
ポート割り当て 83  
ホスト名 54, 173  
ユーザー認証方式 54, 162  
CIM over HTTP ポート 56, 180  
CIM over HTTPS 86  
CIM over HTTPS ポート 56, 180  
CLI キー・シーケンス 53, 181  
DDNS 74  
DNS 74  
HTTP ポート 55, 180  
HTTPS 85  
HTTPS ポート 55, 180  
IMM2 の日付と時刻 58  
LDAP 76  
LDAP クライアント・プロトコル 87  
LDAP サーバー・ポート 55, 177  
MTU 54, 173  
Remote Control ポート 56, 180  
SMTP 75  
SNMP アラート 72  
SNMP エージェント・ポート 56, 180  
SNMP トラップ・ポート 56, 180  
SNMPv1 の連絡先 54, 184  
SNMPv3 の連絡先 54, 184  
SSH CLI ポート 55, 180  
ssh サーバー 89  
Telnet 81  
Telnet CLI ポート 55, 180  
USB 82  
Web セッションの 15  
Web の非アクティブ・タイムアウト 54, 162  
設定、ポート番号 55, 180

セットアップ  
アラート受信者 29  
セットアップ ウィザード  
IMM2 56  
相対マウス制御 111  
ソフトウェアのサービスおよびサポートの  
電話番号 211

## [夕行]

ターゲット名、サーバー  
LDAP 55, 177  
単一カーソル・モード 112  
注記 6  
ツール  
IPMItool 147  
通信規制の注記 216  
粒子汚染 216  
ディスク、リモート 117  
テスト  
SMTP 55  
テスト・イベント  
生成 128  
デフォルト構成  
IMM 183  
IMM2 56  
デフォルトの固定 IP アドレス 8  
電源管理  
active energy manager 136  
chart タブ 139  
policies タブ 136  
power allocation タブ 138  
power history タブ 139  
power modules タブ 138  
電源管理オプション  
Server Management (サーバー管理) タブの  
電源デバイス 135  
電源ポリシー 135  
電力使用量 135  
電源機構  
容量 138  
電源状況の制御  
サーバー 104  
電話番号 211  
ドメイン・ネーム、カスタム  
DDNS 54, 170  
ドメイン・ネーム、DHCP サーバーが指定  
DDNS 54, 170  
ドメイン・ネームのソース  
DDNS 54, 170  
ドライブ  
マッピング 118  
マッピング解除 118  
ドライブのマッピング 118

ドライブのマッピング解除 118  
取り付けられている電源機構  
電源管理 138  
power modules タブ 138

## [ナ行]

日時、IMM2  
設定 58  
ネットワーク接続 8  
固定 IP アドレス、デフォルト 8  
デフォルトの固定 IP アドレス 8  
IP アドレス、デフォルトの固定 8

## [ハ行]

ハードウェアのサービスおよびサポートの  
電話番号 211  
バイインディング方式  
LDAP サーバー 55, 177  
パスワード  
ユーザー 54, 196  
LDAP サーバー 55, 177  
バックアップ、構成  
IMM2 56  
バックアップ状況の表示  
IMM 56  
IMM2 56  
日付  
設定 53, 206  
表示  
システム状況 95  
システム・ヘルス 98  
ハードウェア・ヘルス 99  
表示、現在データ  
users 54, 196  
ファームウェア  
表示、サーバー 53, 159  
ファームウェア、サーバー  
更新 120  
ファームウェア情報の表示  
サーバー 53, 159  
ファームウェアの更新 106  
フィーチャーのインストール  
Features on Demand 141, 175  
FoD 141, 175  
フィーチャーの除去  
Features on Demand 144, 175  
FoD 144, 175  
ブラウザの要件 4  
ブルー・スクリーン・キャプチャー 107  
ブレード・サーバー 1, 4, 7  
ベースボード管理コントローラー  
(BMC) 1

ヘルプ  
ソース 209  
ワールド・ワイド・ウェブ (WWW) からの 210  
IBM への診断データの送信 210

ポート  
オープン の表示 55, 180  
構成 55, 180  
番号 の設定 55, 180

ポート転送  
Ethernet over USB 55, 172

ポート番号  
設定 55, 180  
LDAP サーバー 55, 177  
SMTP サーバー 55, 184

ホスト名  
設定 54, 173  
LDAP サーバー 55, 177  
SMTP サーバー 55, 184

ホスト・サーバーの始動シーケンスの変更 11

## [マ行]

マウス制御  
絶対 111  
相対 111  
デフォルト Linux 加速を使用する相対 111

モニター・コマンド 153

## [ヤ行]

役割ベースのレベル  
operator 173  
rbs 173  
supervisor 173

役割ベース・セキュリティ、拡張  
LDAP 55, 196

ユーザー  
管理 54, 196  
削除 54, 196  
パスワード 54, 196  
SNMPv3 設定 54, 196  
SSH 鍵 54, 196

ユーザー認証方式  
設定 54, 162

ユーザー・アカウント  
管理 61  
グループ・プロファイル 64  
構成 61  
作成 54, 196

ユーザー・アカウントのセキュリティ・レベル  
構成 54, 162

ユーティリティー・コマンド 152

要件  
オペレーティング・システム 4  
Web ブラウザー 4

## [ラ行]

リストア状況の表示  
IMM2 56

リモート管理アダプター II 1

リモート電源制御 113

リモート・アクセス 2

リモート・ディスク 117, 118

リモート・デスクトップ・プロトコル (RDP)  
起動 113

リモート・ブート 117

リモート・プレゼンス機能 105  
使用可能化 107

ルート識別名  
LDAP サーバー 55, 177

ログイン許可属性  
LDAP 55, 177

## A

accsecfcfg コマンド 162

active energy manager  
policies タブ 136

ActiveX アプレット  
更新 106

Advanced Settings ユーティリティー (ASU) 1

alertcfg コマンド 164

alertentries コマンド 202

asu コマンド 165

Australia Class A statement 217

## B

backup コマンド 168

batch コマンド 205

BIOS (基本入出力システム) 1

BladeCenter 1, 4, 7

## C

Canada Class A electronic emission statement 217

China Class A electronic emission statement 220

CIM over HTTP ポート  
設定 56, 180

CIM over HTTPS  
証明書管理 56, 190, 192

CIM over HTTPS (続き)  
セキュリティ 56, 190, 192

CIM over HTTPS ポート  
設定 56, 180

Class A electronic emission notice 217

clearcfg コマンド 206

clearlog コマンド 153

CLI キー・シーケンス  
設定 53, 181

clock コマンド 206

console コマンド 161

## D

DDNS  
カスタムのドメイン・ネーム 54, 170  
管理 54, 170  
構成 54, 170  
ドメイン・ネームのソース 54, 170  
DHCP サーバーが指定したドメイン・ネーム 54, 170

dhcpinfo コマンド 169

disks (ディスク) オプション  
Server Management (サーバー管理) タブの 47

DNS  
構成 54, 170  
サーバー・アドレッシング 54, 170  
IPv4 アドレッシング 54, 170  
IPv6 アドレッシング 54, 170  
LDAP サーバー 55, 177

dns コマンド 170

download service data (サービス・データのダウンロード)  
オプション、概要 31

DSA、IBM へのデータの送信 210

## E

E メール受信者  
セットアップ 29

electronic emission Class A notice 217

Ethernet over USB  
構成 55, 172  
ポート転送 55, 172

ethtousb コマンド 172

European Union EMC Directive  
conformance statement 218

event recipient (イベント受信者) 29

event recipients (イベント受信者)  
管理 126

event (イベント) タブ  
ログ 26

events  
受信者 128

events (イベント) タブ  
 概要 25  
events (イベント) メニュー 126  
exit コマンド 152

## F

fans コマンド 153  
FCC Class A notice 217  
feature  
  Knock-knock 113  
Features on Demand 141  
  エキスポート機能 145  
  管理 56, 175  
  フィーチャーのインストール 141,  
  175  
  フィーチャーの除去 144, 175  
ffdc コマンド 153  
FoD 141  
  エキスポート機能 145  
  管理 56, 175  
  フィーチャーのインストール 141,  
  175  
  フィーチャーの除去 144, 175

## G

Germany Class A statement 218  
gprofile コマンド 173

## H

hardware health (ハードウェア・ヘルス)  
  99  
help コマンド 152  
history コマンド 152  
HTTP ポート  
  設定 55, 180  
HTTPS サーバー  
  証明書管理 56, 190, 192  
  セキュリティ 56, 190, 192  
HTTPS ポート  
  設定 55, 180

## I

IBM BladeCenter 1, 4, 7  
IBM System x サーバー・ファームウェア  
  説明 1  
  Setup ユーティリティ 8  
IBM ブレード・サーバー 1, 4, 7  
IBM への診断データの送信 210  
identify コマンド 207  
ifconfig コマンド 173

IMM  
  構成 56  
  構成の復元 182  
  構成のリセット 183  
  再始動 208  
  デフォルト構成 183  
  reset 208  
  spreset 208  
IMM management  
  アクティベーション管理キー 94  
  セキュリティ設定 84  
  ネットワーク・プロトコルの構成 70  
  ユーザー  
    アカウント 61  
    group profiles (グループ・プロファイ  
    イル) 64  
  ユーザー・アカウントの構成 61  
IMM properties  
  シリアル・ポート設定 60  
IMM 構成  
  IMM 構成のリストアと変更 92  
  restart IMM2 (IMM2 の再始動) 92  
IMM management (IMM 管理) タブ 51  
IMM2  
  アクションの説明 11  
  アクティベーション管理キー 94  
  機能 2  
  構成オプション 53  
  構成のバックアップ 56  
  構成の表示 56  
  構成の復元 56  
  構成のリストア 56, 182  
  構成のリセット 56  
  再始動 56, 92  
  シリアル・リダイレクト 148  
  新機能 1  
  セットアップ ウィザード 56  
  説明 1  
  デフォルト構成 56  
  ネットワーク接続 8  
  バックアップ、構成 56  
  バックアップ状況の表示 56  
  リストア状況の表示 56  
  IMM2 の拡張レベル 2  
  IMM2 の基本レベル 2  
  IMM2 の標準レベル 2  
  reset 56, 93  
  Web インターフェース 7  
  Web ユーザー・インターフェースの概  
  要 15  
IMM2 Web セッション  
  ログアウト 18  
IMM2 Web ユーザー・インターフェース  
  概要 15  
  events (イベント) タブ  
  オプションの概要 25

IMM2 Web ユーザー・インターフェース  
 (続き)  
  service and support (サービスおよびサ  
  ポート) タブ  
    オプションの概要 31  
  system status (システム状況) タブ  
  概要 19  
IMM2 管理  
  IMM properties  
    日時 58  
  IMM2 のリセット 93  
IMM2 制御コマンド 201  
IMM2 セッションからのログアウト 18  
IMM2 タスク 103  
IMM2 の機能 2  
  拡張レベル 3  
  基本レベル 3  
IMM2 の機能標準レベル機能  
  標準レベル 3  
IMM2 の構成  
  構成のオプション  
  IMM2 53  
IMM2 へのログイン 10  
info コマンド 207  
IP address  
  構成 7  
  IPv4 7  
  IPv6 7  
  LDAP サーバー 55, 177  
  SMTP サーバー 55, 184  
IP アドレス、デフォルトの固定 8  
IPMI  
  リモート・サーバー管理 147  
IPMItool 147  
IPv4  
  構成 54, 173  
IPv4 アドレッシング  
  DNS 54, 170  
IPv6 7  
  構成 54, 173  
IPv6 アドレッシング  
  DNS 54, 170  
**J**  
Java 4, 117  
Java アプレット  
  更新 106  
**K**  
keycfg コマンド 175  
Knock-knock 機能  
  使用可能に設定 113

Knock-knock 機能 (続き)  
ユーザー・モード  
    シングル 113  
    マルチ 113  
リモート・セッションの要求 113  
Korea Class A electronic emission  
statement 219

## L

latest OS failure screen (最新の OS 障害画面) オプション  
    Server Management (サーバー管理) タブの 50  
LDAP  
    アクティブ・ディレクトリー・ユーザー 55, 196  
    拡張役割ベース・セキュリティ 55, 196  
    グループ検索属性 55, 177  
    グループ・フィルター 55, 177  
    構成 55, 177  
    サーバーのターゲット名 55, 177  
    証明書管理 56, 190, 192  
    セキュリティ 56, 190, 192  
    役割ベース・セキュリティ、拡張 55, 196  
    ログイン許可属性 55, 177  
ldap コマンド 177  
LDAP サーバー  
    クライアント識別名 55, 177  
    検索ドメイン 55, 177  
    構成 55, 177  
    事前構成 55, 177  
    バインディング方式 55, 177  
    パスワード 55, 177  
    ポート番号 55, 177  
    ホスト名 55, 177  
    ルート識別名 55, 177  
    DNS 55, 177  
    IP address 55, 177  
    UID 検索属性 55, 177  
LDAP サーバー・ポート  
    設定 55, 177  
led コマンド 155  
Linux (デフォルト Linux 加速) での相対マウス制御 111

## M

MAC アドレス  
    管理 54, 173  
memory (メモリー) オプション  
    Server Management (サーバー管理) タブの 48

MTU  
    設定 54, 173

## N

network protocol properties (ネットワーク・プロトコルのプロパティ)  
    イーサネット設定 70  
    ポート割り当て 83  
    DDNS 74  
    DNS 74  
    LDAP 76  
    SMTP 75  
    SNMP アラート設定 72  
    Telnet 81  
    USB 82  
New Zealand Class A statement 217  
notices 213  
    electronic emission 217  
    FCC, Class A 217  
ntp コマンド 178

## O

OS 障害画面データ  
    収集 134

## P

page auto refresh (ページの自動最新表示) オプション 15  
passwordcfg コマンド 179  
People's Republic of China Class A electronic emission statement 220  
portcfg コマンド 181  
ports コマンド 180  
power actions (電源アクション) 104  
power allocation タブ  
    電源管理 138  
    電源機構 138  
power コマンド 160  
processors (プロセッサ) オプション  
    Server Management (サーバー管理) タブの 49  
PXE network boot (PXE ネットワーク・ブート) オプション  
    Server Management (サーバー管理) タブの 50  
PXE ネットワーク・ブート  
    セットアップ 119  
PXE ブート・エージェント 11  
pxeboot コマンド 160

## R

readlog コマンド 156  
Remote Control  
    アクセス 118  
    キーボード・サポート 109  
    キーボード・パススルー・モード 111  
    終了 119  
    スクリーン・キャプチャー 107  
    絶対マウス制御 111  
    相対マウス制御 111  
    多国語キーボードのサポート 110  
    単一カーソル・モード 112  
    電源および再始動コマンド 113  
    パフォーマンス統計 113  
    ビデオ・ビューアー 105  
    マウス・サポート 111  
Linux (デフォルト Linux 加速) での相対マウス制御 111  
Video Viewer 108  
Virtual Media Session 117  
virtual media session (仮想メディア・セッション) 105  
Remote Control 機能 38, 105  
Remote Control での多国語キーボードのサポート 110  
Remote Control のキーボード・サポート 109  
Remote Control のキーボード・パススルー・モード 111  
Remote Control のビデオ・カラー・モード 108  
Remote Control の表示モード 108  
Remote Control のマウス・サポート 111  
Remote Control ポート  
    設定 56, 180  
Remote Control、ウィンドウ  
    ビデオ・ビューアー 38  
    virtual media session (仮想メディア・セッション) 38  
reset  
    IMM 208  
    IMM2 56  
reset コマンド 161  
resetsp コマンド 208  
restore コマンド 182  
restoredefaults コマンド 183  
Russia Class A electronic emission statement 220

## S

Serial over LAN 147  
Serial-to-SSH リダイレクト 148  
Serial-to-Telnet リダイレクト 148

server firmware (サーバー・ファームウェア) 更新 120

server firmware (サーバー・ファームウェア) オプション  
Server Management (サーバー管理) タブの 33

Server Management  
disks (ディスク) オプション 47  
latest OS failure screen (最新の OS 障害画面) オプション 50  
memory (メモリー) オプション 48  
processors (プロセッサ) オプション 49  
PXE network boot (PXE ネットワーク・ブート) オプション 50  
server firmware (サーバー・ファームウェア) オプション 33  
server power actions (サーバー電源アクション) オプション 47  
server properties (サーバーのプロパティ) オプション 43  
server timeouts (サーバー・タイムアウト) オプション 50

server management (サーバー管理)  
サーバー・タイムアウト、設定 56  
OS 障害画面データ 134  
PXE ネットワーク・ブート 119  
server firmware (サーバー・ファームウェア) 120

server management (サーバー管理) タブ 32

server power actions (サーバー電源アクション) オプション  
Server Management (サーバー管理) タブの 47

server properties (サーバーのプロパティ)  
environmentals (環境) タブ 43  
general settings (一般設定) タブ 43  
hardware activity (ハードウェア・アクティビティ) タブ 43  
hardware information (ハードウェア情報) タブ  
network hardware (ネットワーク・ハードウェア) タブ 43  
system component information (システム・コンポーネント情報) タブ 43  
system information (システム情報) タブ 43  
LED タブ 43

server properties (サーバーのプロパティ) オプション  
Server Management (サーバー管理) タブの 43

server timeouts (サーバー・タイムアウト) オプション  
Server Management (サーバー管理) タブの 50

service and support (サービスおよびサポート) タブ  
概要 31

set コマンド 183

show コマンド 157

SMTP  
構成 55, 184  
サーバーの IP アドレス 55, 184  
サーバーのポート番号 55, 184  
サーバーのホスト名 55, 184  
テスト 55

smtp コマンド 184

SNMP エージェント・ポート  
設定 56, 180

snmp コマンド 184

SNMP トラップ・ポート  
設定 56, 180

snmpalerts コマンド 187

SNMPv1  
構成 54, 184

SNMPv1 コミュニティ  
管理 54, 184

SNMPv1 トラップ  
構成 54, 184

SNMPv1 の連絡先  
設定 54, 184

SNMPv3 設定  
ユーザー 54, 196

SNMPv3 のユーザー・アカウント  
構成 54, 196

SNMPv3 の連絡先  
設定 54, 184

sreset コマンド 208

srcfg コマンド 189

SSH CLI ポート  
設定 55, 180

SSH 鍵  
ユーザー 54, 196

SSH サーバー  
証明書管理 56, 189  
セキュリティ 56, 189

sshcfg コマンド 189

SSL  
証明書管理 91  
証明書の処理 90

ssl コマンド 190

sslcfg コマンド 192

syshealth コマンド 158

system status (システム状況) タブ  
概要 19

system status (システム状況) ページ、概要 19

## T

Taiwan Class A electronic emission statement 220

### Telnet

アクセス 55, 195  
構成 195  
最大セッション数 55, 195

### Telnet CLI ポート

設定 55, 180

### Telnet 設定

構成 55

telnetcfg コマンド 195

temps コマンド 158

thermal コマンド 195

timeouts コマンド 195

trespass message (侵入警告メッセージ) オプション 17

## U

### UID 検索属性

LDAP サーバー 55, 177

United States FCC Class A notice 217

### USB

構成 55, 172

usbeth コマンド 196

### users

現在の表示 196

表示、現在データ 54

users コマンド 196

## V

### Video Viewer

キーボード・パススルー・モード 111

終了 119

スクリーン・キャプチャー 107

絶対マウス制御 111

相対マウス制御 111

多国語キーボードのサポート 110

単一カーソル・モード 112

電源および再始動コマンド 113

パフォーマンス統計 113

ビデオ・カラー・モード 108, 109

表示モード 108

マウス・サポート 111

Linux (デフォルト Linux 加速) での相対マウス制御 111

### Virtual Light Path 11

### Virtual Media Session

起動 118

終了 119

ドライブのマップ 118

ドライブのマップ解除 118

リモート・ディスク 117

volts コマンド 159

vpd コマンド 159

## W

Web インターフェース

Web インターフェースへのログイン

10

Web インターフェースの開始および使用

7

Web セッションの設定 15

Web の非アクティブ・タイムアウト

設定 54, 162

Web ブラウザーの要件 4





部品番号: 47C9126

Printed in Japan

(1P) P/N: 47C9126



**日本アイ・ビー・エム株式会社**

〒103-8510 東京都中央区日本橋箱崎町19-21