



統合管理モジュール I
ユーザーズ・ガイド





統合管理モジュール I 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 I
User's Guide

発行： 日本アイ・ピー・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6版第1刷 2013.6

© Copyright IBM Corporation 2013.

目次

表	vii
-------------	-----

第 1 章 概要 1

IMM の機能	3
IMM Standard から IMM Premium へのアップグレード	5
IMM と System x サーバー内の他のシステム管理ハードウェアの比較	6
IMM と BladeCenter アドバンスド・マネージメント・モジュールの使用	10
Web ブラウザーとオペレーティング・システムの要件	11
本書で使用される注記	11

第 2 章 IMM Web インターフェースの開始および使用 13

IMM Web インターフェースへのアクセス	13
IBM System x サーバー・ファームウェアの Setup ユティリティを使用した IMM ネットワーク接続のセットアップ	13
IMM へのログイン	16
IMM のアクションの説明	17

第 3 章 IMM の構成 21

システム情報の設定	22
サーバー・タイムアウトの設定	23
IMM の日付と時刻の設定	24
ネットワーク内のクロックの同期	25
USB インバンド・インターフェースの使用不可化	26
ログイン・プロファイルの作成	28
ログイン・プロファイルの削除	32
グローバル・ログイン設定の構成	33
リモート・アラート設定の構成	34
リモート・アラート受信者の構成	35
グローバル・リモート・アラート設定の構成	36
SNMP アラート設定の構成	37
シリアル・ポート設定の構成	38
Serial-to-Telnet または SSH リダイレクトの構成	39
ポート割り当ての構成	39
ネットワーク・インターフェースの構成	41
イーサネット設定の構成	42
IPv4 設定の構成	45
IPv6 設定の構成	46
ネットワーク・プロトコルの構成	47
SNMP の構成	48
DNS の構成	49
Telnet の構成	50
SMTP の構成	51
LDAP の構成	51
ユーザー・スキーマの例	52

Novell eDirectory スキーマ・ビュー	53
LDAP サーバーの参照	62
Microsoft Windows Server 2003 Active Directory スキーマ・ビュー	64
LDAP クライアントの構成	70
セキュリティの構成	89
セキュア Web サーバー、IBM Systems Director、およびセキュア LDAP	90
SSL 証明書の概要	90
SSL サーバー証明書管理	91
HTTPS 上でセキュア Web サーバーまたは IBM Systems Director を使用するための SSL の使用可能化	96
SSL クライアント証明書管理	96
SSL クライアントのトラステッド証明書管理	96
LDAP クライアント用の SSL を使用可能にする	97
セキュア・シェル・サーバーの構成	97
セキュア・シェル・サーバー鍵の生成	98
セキュア・シェル・サーバーの使用可能化	98
セキュア・シェル・サーバーの使用	99
IMM の構成の復元と変更	99
構成ファイルの使用	100
現行構成のバックアップ	100
IMM の構成の復元と変更	101
デフォルトのリストア	102
IMM の再始動	102
スケーラブル・パーティショニング	102
Service Advisor 機能	103
Service Advisor の構成	103
Service Advisor の使用	106
ログオフ	108

第 4 章 サーバー状況のモニター 109

システム状況の表示	109
Virtual Light Path の表示	114
イベント・ログの表示	114
Web インターフェースからのシステム・イベント・ログの表示	115
Setup ユティリティからのイベント・ログの表示	116
サーバーを再始動しないイベント・ログの表示	117
重要プロダクト・データの表示	119

第 5 章 IMM タスクの実行 121

サーバーの電源および再始動アクティビティの表示	121
サーバーの電源状況の制御	122
リモート・プレゼンス	123
IMM ファームウェアおよび Java または ActiveX アプレットの更新	124
リモート・プレゼンス機能の使用可能化	124

Remote Control	125
Remote Control のスクリーン・キャプチャー	126
Remote Control の Video Viewer の表示モード	127
Remote Control のビデオ・カラー・モード	127
Remote Control のキーボード・サポート	128
Remote Control のマウス・サポート	130
リモート電源制御	132
パフォーマンス統計の表示	132
リモート・デスクトップ・プロトコルの始動	132
リモート・ディスク	132
PXE ネットワーク・ブートのセットアップ	135
ファームウェアの更新	136
Setup ユーティリティを使用した IMM のリセッ ト	137
IMM および IBM System x サーバー・ファームウ ェア対応の管理ツールおよびユーティリティ	138
IPMITool の使用	138
OSA システム管理ブリッジの使用	138
IBM Advanced Settings ユーティリティの使用	139
IBM フラッシュ・ユーティリティの使用	139
IMM を管理する他の方法	139

第 6 章 LAN over USB 141

LAN over USB インターフェースとの競合の可能性	141
IMM LAN over USB インターフェースとの競合の 解決	141
LAN over USB インターフェースの手動構成	142
デバイス・ドライバのインストール	142
Windows IPMI デバイス・ドライバのインスト ール	142
LAN over USB の Windows デバイス・ドライ バのインストール	143
LAN over USB の Linux デバイス・ドライバ のインストール	144

第 7 章 コマンド・ライン・インターフ ェース 145

IPMI を使用した IMM の管理	145
コマンド・ラインへのアクセス	145
コマンド・ライン・セッションへのログイン	146
コマンド構文	146
機能および制限	146
ユーティリティ・コマンド	148
exit コマンド	148
help コマンド	148
history コマンド	148
モニター・コマンド	148
clearlog コマンド	149
fans コマンド	149
readlog コマンド	149
syshealth コマンド	149
temps コマンド	150
volts コマンド	150
vpd コマンド	151
サーバーの電源および再始動制御コマンド	151
power コマンド	151

reset コマンド	152
シリアル・リダイレクト・コマンド	152
console コマンド	152
構成コマンド	152
dhcpcfg コマンド	153
dns コマンド	153
gprofile コマンド	154
ifconfig コマンド	155
ldap コマンド	157
ntp コマンド	159
passwordcfg コマンド	159
portcfg コマンド	160
srcfg コマンド	161
ssl コマンド	161
timeouts コマンド	163
usbeth コマンド	163
users コマンド	164
IMM 制御コマンド	165
clearcfg コマンド	165
clock コマンド	165
identify コマンド	166
resetsp コマンド	166
update コマンド	166
Service Advisor コマンド	167
autoftp コマンド	168
chconfig コマンド	168
chlog コマンド	170
chmanual コマンド	170
events コマンド	171
sdemail コマンド	171

付録 A. ヘルプおよび技術サポートの入 手 173

依頼する前に	173
資料の使用	174
ヘルプおよび情報を WWW から入手する	174
IBM への DSA データの送信方法	174
個別設定したサポート Web ページの作成	175
ソフトウェアのサービスとサポート	175
ハードウェアのサービスとサポート	175

付録 B. 特記事項 177

商標	177
重要事項	178
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	179
粒子汚染	180
通信規制の注記	180
電波障害自主規制特記事項	181
Federal Communications Commission (FCC) statement	181
Industry Canada Class A emission compliance statement	181
Avis de conformité à la réglementation d'Industrie Canada	181
Australia and New Zealand Class A statement	181

European Union EMC Directive conformance	
statement	181
Germany Class A statement	182
VCCI クラス A 情報技術装置	183
Korea Communications Commission (KCC)	
statement	183
Russia Electromagnetic Interference (EMI) Class A	
statement	184

People's Republic of China Class A electronic	
emission statement	184
Taiwan Class A compliance statement.	184
索引	185

表

1. IMM 機能と System x サーバーの BMC および リモート管理アダプター II を結合した機能との 比較	6	11. グループ・プロファイル情報	75
2. IMM アクション	17	12. 各種パラメーター	81
3. 予約済みポート番号	41	13. 許可ビット	87
4. 「Advanced Ethernet Setup」ページの設定	44	14. IMM の SSL 接続サポート	90
5. ユーザーからグループへのマッピング	53	15. 連絡先情報	104
6. 許可ビット	57	16. イベント・ログを表示する方法	118
7. UserLevelAuthority 属性の例と説明	59	17. マシン・レベルの重要プロダクト・データ	119
8. ユーザー・グループに割り当てられた UserAuthorityLevel	61	18. コンポーネント・レベルの重要プロダクト・ データ	120
9. 権限レベルとグループ・メンバーシップの検査	70	19. コンポーネントのアクティビティ・ログ	120
10. 各種パラメーター	73	20. IMM、UEFI、および DSA ファームウェア重 要プロダクト・データ	120
		21. 微粒子およびガスの制限	180

第 1 章 概要

統合管理モジュール (IMM) は、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・プレゼンス機能をシステム・ボード上の単一のチップに統合しています。IMM は、IBM® System x サーバーのベースボード管理コントローラー (BMC) およびリモート管理アダプター II (RSA) に置き換わるものです。

IBM サーバーで IMM が使用される前は、ベースボード管理コントローラー (BMC) および基本入出力システム (BIOS) が標準のシステム管理ハードウェアおよびファームウェアでした。System x サーバーは、BMC サービス・プロセッサを使用してシステム管理ソフトウェアとプラットフォーム・ハードウェアの間のインターフェースを管理していました。リモート管理アダプター II およびリモート管理アダプター II SlimLine は、アウト・オブ・バンドによるサーバー管理のためのオプションのコントローラーでした。

重要: 一部の IBM BladeCenter 製品および IBM ブレード・サーバーでは IMM が標準ですが、BladeCenter アドバンスド・マネージメント・モジュールは、BladeCenter およびブレード・サーバーの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 次管理モジュールとして残っています。IMM Web インターフェースとコマンド・ライン・インターフェースに関連した内容は、IBM BladeCenter とブレード・サーバーには適用されません。ブレード・サーバー上で IMM 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。

IMM は、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。

- 専用あるいは共有イーサネット接続の選択。専用イーサネット接続は、ブレード・サーバーあるいは一部の System x サーバーでは選択できません。

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、IMM の設定で使用可能なのは、共有の設定のみです。

- 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、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)。
- 更新処理を開始するためにサーバーを再始動することなく、他のエンティティをローカルあるいはリモートで更新することが可能。
- 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、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 IMM 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。ブレード・サーバーでは、インバンド IMM 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、ブレード・サーバーには適用されません。

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、System x サーバーおよび IBM ブレード・サーバーの 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 2.1 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 IMM の機能の使用方法について説明しています。IMM は、IBM System x サーバー・ファームウェアと連動し、System x および BladeCenter サーバーのシステム管理機能を提供します。

本書には、エラーあるいはメッセージの説明は含まれません。IMM エラーおよびメッセージは、ご使用のサーバーに付属の「問題判別の手引き」で説明されています。IBM[®] サポート・ポータルで本書あるいは IBM ホワイト・ペーパー「*Transitioning to UEFI and IMM*」の最新バージョンを検索するには、以下のステップを実行します。

注: IBM サポート・ポータルに初めてアクセスする際、ご使用のサーバーの製品カテゴリ、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、「**Documentation**」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. 「**Documentation**」ボックスで、「**More results**」をクリックします。
7. 「**Category**」ボックスで、「**Integrated Management Module (IMM)**」チェック・ボックスを選択します。IMM および UEFI 資料へのリンクが表示されます。

ファームウェア更新が使用可能な場合は、IBM Web サイトからダウンロードすることができます。IMM には、資料に記載されていない機能が備わっている場合があります。資料は、そのような情報を記載するために時々更新されることがあります。あるいは、IMM 資料に記載されていない追加情報を提供するための技術更新が使用可能になることもあります。

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、ご使用のサーバーの製品カテゴリ、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。

IMM の機能

IMM は以下の機能を提供します。

- 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
- 標準の Web ブラウザーを使用した Web ベースの管理

IMM は、2 つのタイプ (IMM Standard 機能と IMM Premium 機能) の IMM 機能を提供します。ご使用のサーバー内の IMM ハードウェア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。

IMM Standard 機能

注: 以下の機能の一部は、ブレード・サーバーには適用されません。

- クリティカル・サーバー設定値へのアクセス
- サーバーの重要プロダクト・データ (VPD) へのアクセス
- 拡張障害予知 (PFA) サポート
- 自動通知およびアラート
- 連続ヘルス・モニターおよび制御
- 専用あるいは共有イーサネット接続の選択 (適用可能な場合)。

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。

- ドメイン・ネーム・システム (DNS) サーバー・サポート
- 動的ホスト構成プロトコル (DHCP) サポート
- E-mail アラート
- 組み込み Dynamic System Analysis (DSA)
- 拡張ユーザー権限レベル
- IMM とのインバンド通信用の LAN over USB
- タイム・スタンプがあり、IMM に保管され、E-mail アラートに添付できるイベント・ログ
- 業界標準のインターフェースおよびプロトコル
- OS ウォッチドッグ
- Advanced Settings ユーティリティー (ASU) を使用したリモート構成
- リモート・ファームウェア更新
- リモート電源制御
- シームレス・リモート・アクセラレーション・グラフィックス
- セキュアな Web サーバー・ユーザー・インターフェース
- Serial over LAN
- サーバー・コンソール・リダイレクト
- Simple Network Management Protocol (SNMP) のサポート
- Lightweight Directory Access Protocol (LDAP) サーバーへのセキュア接続を使用するユーザー認証

IMM Premium 機能

注: 以下の機能の一部は、ブレード・サーバーには適用されません。

- クリティカル・サーバー設定値へのアクセス
- サーバーの重要プロダクト・データ (VPD) へのアクセス
- 拡張障害予知 (PFA) サポート
- 自動通知およびアラート
- 連続ヘルス・モニターおよび制御
- 専用あるいは共有イーサネット接続の選択 (適用可能な場合)。

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。

- ドメイン・ネーム・システム (DNS) サーバー・サポート
 - 動的ホスト構成プロトコル (DHCP) サポート
 - E-mail アラート
 - 組み込み Dynamic System Analysis (DSA)
 - 拡張ユーザー権限レベル
 - IMM とのインバンド通信用の LAN over USB
 - タイム・スタンプがあり、IMM に保管され、E-mail アラートに添付できるイベント・ログ
 - 業界標準のインターフェースおよびプロトコル
 - OS ウォッチドッグ
 - Advanced Settings ユーティリティ (ASU) を使用したリモート構成
 - リモート・ファームウェア更新
 - リモート電源制御
 - シームレス・リモート・アクセラレーション・グラフィックス
 - セキュアな Web サーバー・ユーザー・インターフェース
 - Serial over LAN
 - サーバー・コンソール・リダイレクト
 - Simple Network Management Protocol (SNMP) のサポート
 - Lightweight Directory Access Protocol (LDAP) サーバーへのセキュア接続を使用するユーザー認証
 - サーバーのリモート制御を含むリモート・プレゼンス
 - オペレーティング・システム障害のスクリーン・キャプチャーおよび Web インターフェースを介した表示
 - サーバーへのディスク・ドライブ、CD/DVD ドライブ、USB フラッシュ・ドライブ、あるいはディスク・イメージの接続を可能にするリモート・ディスク
- 注: 以下のリモート管理アダプター II の機能は、IMM にはありません。
- サーバー MAC アドレスの表示
 - 複数の NTP サーバーのエントリ

IMM Standard から IMM Premium へのアップグレード

ご使用のサーバーが IMM Standard 機能を備えている場合、仮想メディア・キーを購入してサーバーのシステム・ボードに取り付けることで、IMM Premium にアップグレードすることが可能です。新規のファームウェアは不要です。

仮想メディア・キーを注文するには、<http://www-06.ibm.com/systems/jp/x/> にアクセスします。

注: 仮想メディア・キーの取り付けについては、ご使用のサーバーに付属の資料を参照してください。

注文の際にヘルプが必要な場合は、最寄りの IBM 担当員にお問い合わせください。

IMM と System x サーバー内の他のシステム管理ハードウェアの比較

次の表は、IMM の機能と IBM System x サーバー BMC およびリモート管理アダプター II の機能との比較を示しています。

注: BMC と同様に、IMM は標準の IPMI 仕様を使用します。

表 1. IMM 機能と System x サーバーの BMC およびリモート管理アダプター II を結合した機能との比較

説明	リモート管理アダプター II 付きの BMC	IMM
ネットワーク接続	BMC は、サーバーと共有のネットワーク接続と、リモート管理アダプター II とは別の IP アドレスを使用します。 リモート管理アダプター II は、専用のシステム管理ネットワーク接続と、BMC とは別の IP アドレスを使用します。	IMM は、BMC およびリモート管理アダプター II 両方の機能を、同一のネットワーク接続を介して提供します。1 つの IP アドレスを両方に使用します。ご使用のサーバーに、専用のシステム管理ネットワーク・ポートが備わっている場合、専用または共有ネットワーク接続のいずれ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、IMM の設定で使用可能なのは、共有の設定のみです。
更新機能	各サーバーごとに固有の BMC およびリモート管理アダプターの更新が必要です。 BIOS および診断ツールは、インバンドで更新することができます。	適用可能なすべてのサーバーに対して、1 つの IMM ファームウェア・イメージを使用することができます。 IMM ファームウェア、System x サーバー・ファームウェア、および Dynamic System Analysis (DSA) ファームウェアは、インバンドおよびアウト・オブ・バンドのどちらでも更新することができます。 IMM は、IMM 自体、サーバー・ファームウェア、および DSA ファームウェアを、サーバーを再始動して更新処理を開始することなく、ローカルまたはリモートのいずれかで更新することができます。

表 1. IMM 機能と System x サーバーの BMC およびリモート管理アダプター II を結合した機能との比較 (続き)

説明	リモート管理アダプター II 付きの BMC	IMM
構成機能	ASU を使用した構成変更は、インバンドでのみ可能です。システムは、BMC、リモート管理アダプター II、および BIOS の個別の構成を要求します。	ASU はインバンドあるいはアウト・オブ・バンドのいずれかで実行することも可能で、IMM およびサーバー・ファームウェアの両方を構成することができます。ASU を使用して、ブート順序、iSCSI、および VPD (マシン・タイプ、シリアル番号、UUID、および資産 ID) を変更することもできます。 サーバー・ファームウェア構成の設定は、IMM によって保持されます。そのため、サーバーの電源がオフの間、あるいはオペレーティング・システムの稼働中にサーバー・ファームウェア構成を変更することができ、それらの変更は、次にサーバーが始動すると有効になります。 IMM 構成の設定は、以下の IMM ユーザー・インターフェースを介して、インバンドまたはアウト・オブ・バンドで構成することができます。 • Web インターフェース • コマンド・ライン・インターフェース • IBM Systems Director インターフェース • SNMP
オペレーティング・システムのスクリーン・キャプチャー	スクリーン・キャプチャーは、オペレーティング・システム障害が発生したときに、リモート管理アダプター II によって実行されます。スクリーン・キャプチャーの表示には、Java アプレットが必要です。	この機能は、IMM Premium でのみ使用可能です。IMM Standard から IMM Premium へのアップグレードについては、5 ページの『IMM Standard から IMM Premium へのアップグレード』を参照してください。 スクリーン・キャプチャーは、Web ブラウザーによって Java アプレットなしで直接表示されます。

表 1. IMM 機能と System x サーバーの BMC およびリモート管理アダプター II を結合した機能との比較 (続き)

説明	リモート管理アダプター II 付きの BMC	IMM
エラー・ログ	BMC は、BMC システム・イベント・ログ (IPMI イベント・ログ) を提供します。 リモート管理アダプター II は、BMC が報告したイベントの説明を含むテキスト・ベースのログを提供します。このログには、リモート管理アダプター II によって検出された情報あるいはイベントも含まれます。	IMM には、次の 2 つのイベント・ログがあります。 1. システム・イベント・ログは、IPMI インターフェースから使用可能です。 2. シャーシ・イベント・ログは、その他の IMM インターフェースから使用可能です。シャーシ・イベント・ログは、Distributed Management Task Force 仕様 DSP0244 および DSP8007 によって生成されたテキスト・メッセージを表示します。 注: 特定のイベントあるいはメッセージの説明については、ご使用のサーバーに付属の「問題判別の手引き」を参照してください。
モニター	リモート管理アダプター II 付きの BMC には、以下のモニター機能があります。 ・ サーバーとバッテリーの電圧、サーバーの温度、ファン、パワー・サプライ、およびプロセッサと DIMM の状況のモニター。 ・ ファン速度の制御 ・ 障害予知機能 (PFA) のサポート ・ システム診断 LED の制御 (電源、ハード・ディスク、アクティビティ、アラート、ハートビート) ・ 自動サーバー再始動 (ASR) ・ 自動 BIOS リカバリー (ABR)	IMM は、BMC およびリモート管理アダプター II と同じモニター機能を提供します。 RAID 構成で使用される場合は、ディスク・ドライブ PFA を含む拡張されたハード・ディスク状況が IMM によってサポートされます。

表 1. IMM 機能と System x サーバーの BMC およびリモート管理アダプター II を結合した機能との比較 (続き)

説明	リモート管理アダプター II 付きの BMC	IMM
リモート・プレゼンス	リモート管理アダプター II 付きの BMC には、以下のリモート・プレゼンス機能があります。 • LAN 経由でのグラフィカル・コンソール・リダイレクト • リモート仮想ディスクおよび CD-ROM • PCI ビデオ、キーボード、マウスの高速リモート・リダイレクト • 70 Hz で最大 1024 x 768 のビデオ解像度をサポート • データ暗号化	この機能は、IMM Premium でのみ使用可能です。IMM Standard から IMM Premium へのアップグレードについては、5 ページの『IMM Standard から IMM Premium へのアップグレード』を参照してください。 リモート管理アダプター II のリモート・プレゼンス機能に加えて、IMM には以下の機能もあります。 注: IMM を使用するには、Java ランタイム環境 1.5 以降、あるいは Windows で Internet Explorer を使用している場合は ActiveX が必要です。 • 75 Hz で最大 1280 x 1024 のビデオ解像度をサポート • 仮想キーボード、マウス、および大容量ストレージ・デバイス用に USB 2.0 をサポート • 15 ビット・カラー階調 • 絶対あるいは相対マウス・モードの選択 • USB フラッシュ・ドライブのサポート • Remote Control ウィンドウでのサーバーの電源およびリセットの制御 • Remote Control ウィンドウでのビデオのファイルへの保存が可能 IMM は、2 つの別個のクライアント・ウィンドウを提供します。1 つはビデオとキーボードとマウスの対話用、もう 1 つは仮想メディア用です。 IMM Web インターフェースには、低帯域幅状態で送信されるデータを削減するためのカラー階調調整を可能にするためのメニュー項目があります。リモート管理アダプター II インターフェースには、帯域幅スライダーがあります。
Security	リモート管理アダプター II には、Secure Sockets Layer (SSL) および暗号化を含む拡張セキュリティ機能があります。	IMM には、リモート管理アダプター II と同じセキュリティ機能があります。

表 1. IMM 機能と System x サーバーの BMC およびリモート管理アダプター II を結合した機能との比較 (続き)

説明	リモート管理アダプター II 付きの BMC	IMM
シリアル・リダイレクト	IPMI Serial over LAN (SOL) 機能は、BMC の標準機能です。 リモート管理アダプター II は、サーバーのシリアル・データを Telnet あるいは SSH セッションにリダイレクトすることが可能です。 注: この機能は、一部のサーバーでは使用できません。	COM1 ポートは、System x サーバー上の 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。 COM2 ポートは、Telnet あるいは SSH を介したシリアル・リダイレクトに使用されません。COM2 は、IPMI インターフェースを除くすべての IMM インターフェースから構成可能です。COM2 ポートは、ブレード・サーバー上の SOL に使用されます。 両方の COM ポート構成は、8 データ・ビット、NULL パリティ、1 ストップ・ビット、およびボー・レート選択 (9600、19200、38400、57600、115200、または 230400) に制限されます。 ブレード・サーバーでは、COM2 ポートは内部 COM ポートで、外部アクセスはありません。IPMI シリアル・ポートは、ブレード・サーバーでは共用できません。 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、IMM COM2 ポートは内部ポートで、外部アクセスはありません。
SNMP	SNMP サポートは、SNMPv1 に制限されます。	IMM は、SNMPv1 および SNMPv3 をサポートします。

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

BladeCenter アドバンスト・マネージメント・モジュールは、IBM BladeCenter および IBM ブレード・サーバー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 および IBM ブレード・サーバーには IMM が組み込まれていますが、アドバンスト・マネージメント・モジュールは、BladeCenter およびブレード・サーバーのシステム管理機能およびキーボード、ビデオ、マウス (KVM) 多重方式のための管理モジュールとして残っています。BladeCenter では、IMM への外部ネットワーク・インターフェースは使用できません。

ブレード・サーバーには、IMM への外部ネットワーク・アクセスはありません。アドバンスト・マネージメント・モジュールは、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。IMM は、過去のブレード・サーバー製品における 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

IMM 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 6.0 以降 (最新の Service Pack を適用済み)
- Mozilla Firefox バージョン 1.5 以降

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

注: IMM の Web インターフェースは、2 バイト文字セット (DBCS) 言語をサポートしません。

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。
- **重要:** また、これらの注記は、プログラム、デバイス、またはデータに損傷を及ぼすおそれのあることを示します。「重要」の注記は、損傷を起こすおそれのある指示や状態の記述の直前に書かれています。

第 2 章 IMM Web インターフェースの開始および使用

IMM 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。IMM Web インターフェースを使用してリモートで IMM 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、IMM 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。

IMM Web インターフェースへのアクセス

IMM 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。IMM 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。IMM 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。

IMM は IPv6 もサポートしますが、IMM 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 IMM 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。IMM 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 IMM 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
```

IMM 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。

IMM 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、IMM の設定で使用可能なのは、共有の設定のみです。

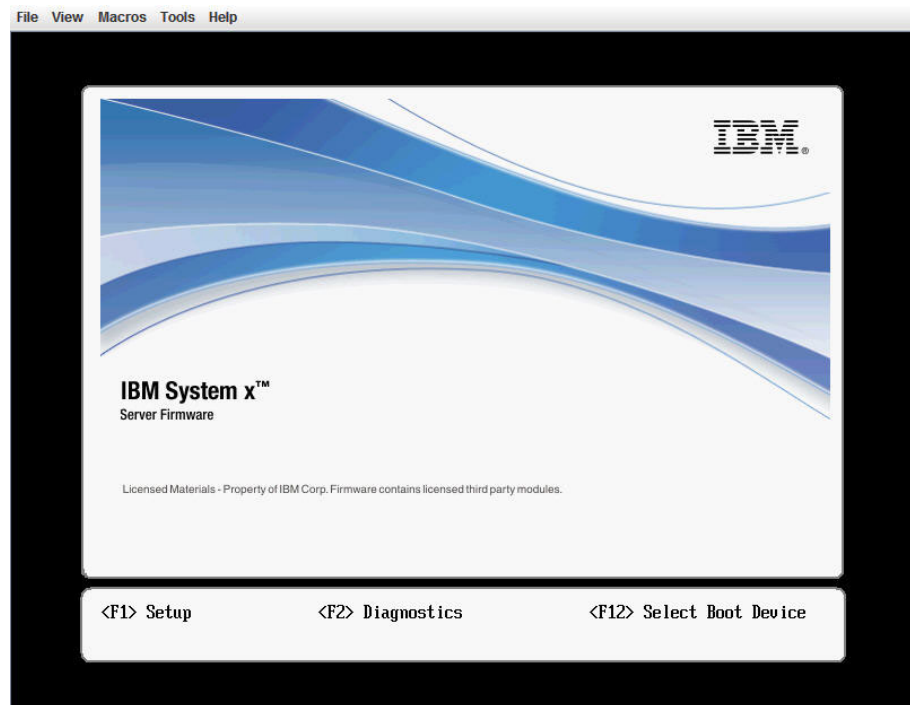
IBM System x サーバー・ファームウェアの Setup ユーティリティを使用した IMM ネットワーク接続のセットアップ

サーバーを始動した後、Setup ユーティリティを使用して IMM ネットワーク接続を選択することができます。IMM ハードウェアを搭載したサーバーは、動的ホスト構成プロトコル (DHCP) サーバーに接続するか、あるいはサーバー・ネットワ

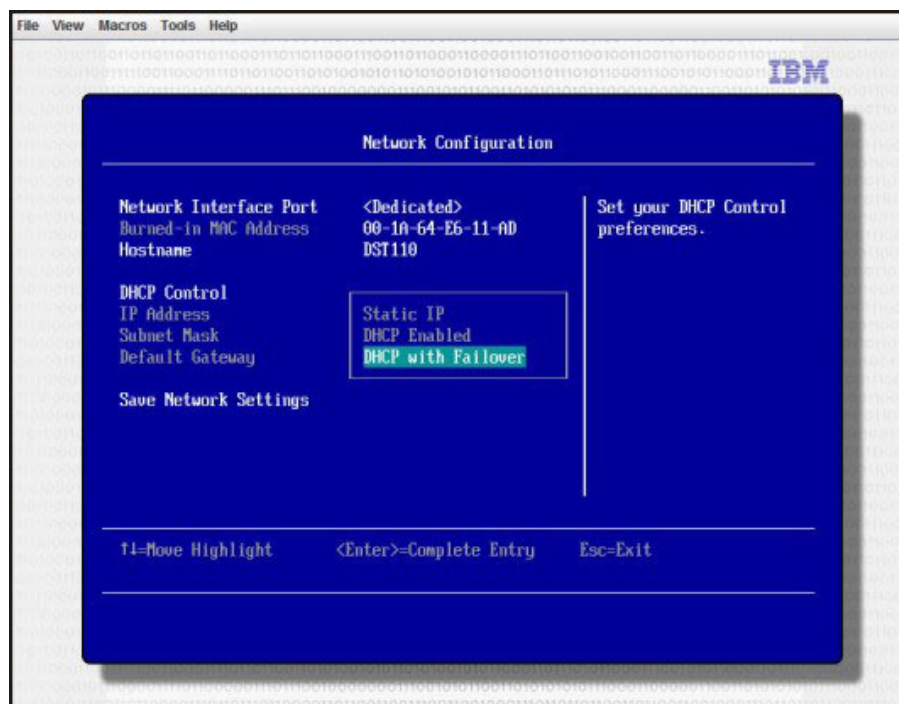
ークが IMM 固定 IP アドレスを使用するように構成されている必要があります。
Setup ユーティリティを使用して IMM ネットワーク接続をセットアップするには、以下のステップを実行します。

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: サーバーを AC 電源に接続してから約 2 分後に、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 IMM 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 IMM 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、IMM 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。
- IMM 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. 「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:

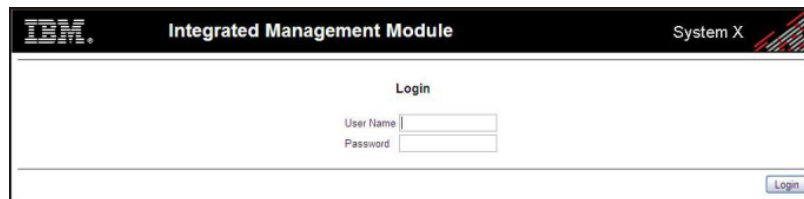
- サーバー・ファームウェアが再度機能するには、変更が有効になるまで約 1 分間待つ必要があります。
- IMM Web インターフェースから IMM ネットワーク接続を構成することもできます。詳しくは、41 ページの『ネットワーク・インターフェースの構成』を参照してください。

IMM へのログイン

重要: IMM 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、初期構成時にこのデフォルト・パスワードを変更してください。

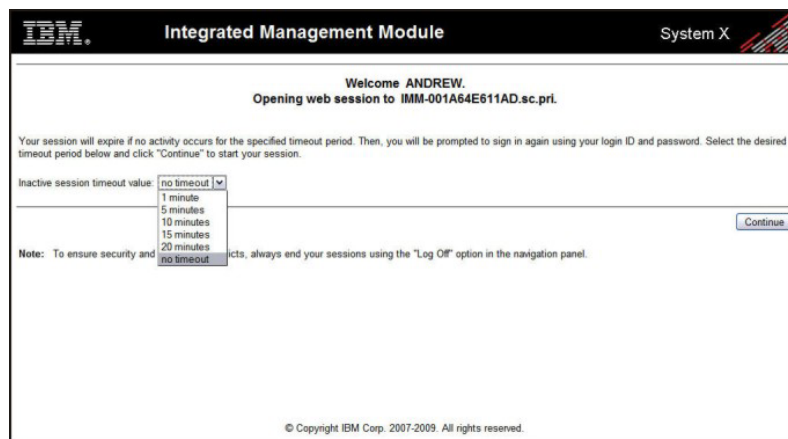
IMM Web インターフェースで IMM にアクセスするには、以下の手順に従ってください。

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 IMM サーバーの IP アドレスまたはホスト名を入力します。

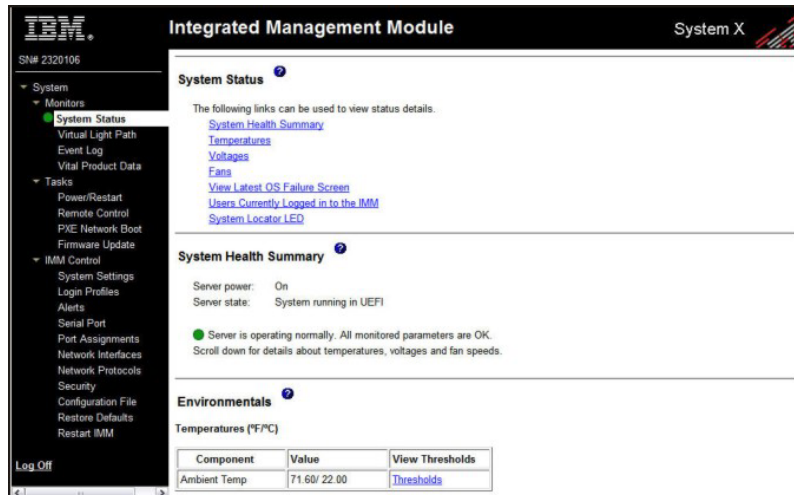
The image shows the login page of the Integrated Management Module (IMM). The header includes the IBM logo, the text "Integrated Management Module", and "System X". The main content area is titled "Login" and contains two input fields: "User Name" and "Password". A "Login" button is located at the bottom right of the form.

2. IMM 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。IMM 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。
3. 「Welcome」Web ページで、提供されるフィールドのドロップダウン・リストから、タイムアウト値を選択します。ご使用のブラウザがその分数の間、非アクティブの場合、IMM はユーザーを Web インターフェースからログオフさせます。

注: システム管理者がグローバル・ログイン設定をどのように構成したかに応じて、タイムアウト値は固定値になる場合があります。

The image shows the "Welcome" page of the Integrated Management Module (IMM). The header includes the IBM logo, the text "Integrated Management Module", and "System X". The main content area is titled "Welcome ANDREW." and "Opening web session to IMM-001A64E611AD.sc.pri." Below this, there is a message: "Your session will expire if no activity occurs for the specified timeout period. Then, you will be prompted to sign in again using your login ID and password. Select the desired timeout period below and click 'Continue' to start your session." There is a dropdown menu for "Inactive session timeout value" with options: "no timeout", "1 minute", "5 minutes", "10 minutes", "15 minutes", "20 minutes", and "no timeout" (selected). A "Continue" button is located at the bottom right of the form. A note at the bottom states: "Note: To ensure security and privacy, always end your sessions using the 'Log Off' option in the navigation panel." The footer contains the copyright notice: "© Copyright IBM Corp. 2007-2009. All rights reserved."

4. 「Continue」をクリックしてセッションを開始します。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のヘルスの要約を素早く見ることができます。



IMM Web インターフェースの左のナビゲーション・ペインにあるリンクから実行できるアクションについては、『IMM のアクションの説明』を参照してください。次に、21 ページの『第 3 章 IMM の構成』へ進みます。

IMM のアクションの説明

表 2 は、IMM にログインしたときに使用できるアクションのリストです。

表 2. IMM アクション

リンク	アクション	説明
System Status	サーバーのヘルスを表示し、オペレーティング・システムの障害の画面取りを表示し、IMM にログインしたユーザーを表示する	「System Health」ページでは、サーバーの電源およびヘルス状態、サーバーの温度、電圧、およびファンの状況をモニターすることができます。また、前回のオペレーティング・システム障害の画面取りイメージと、IMM にログインしたユーザーを表示することもできます。
Virtual Light Path	サーバー Light Path のすべての LED の名前、色、および状況を表示する	「Virtual Light Path」ページでは、サーバー上の LED の現在の状況を表示します。
Event Log	リモート・サーバーのイベント・ログを表示する	「Event Log」ページには、現在シャーシ・イベント・ログに保管されているエントリが含まれます。このログには、BMC によって報告されたイベントのテキスト記述に加えて、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、IMM 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（「Alerts」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。
Vital Product Data	サーバーの重要プロダクト・データ (VPD) の表示	IMM は、サーバー情報、サーバー・ファームウェア情報、およびサーバー・コンポーネントの VPD を収集します。このデータは「Vital Product Data」ページで入手できます。

表 2. IMM アクション (続き)

リンク	アクション	説明
Power/Restart	リモート側でサーバーの電源を入れるか再始動を行う	IMM 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を提供し、パワーオン、パワーオフ、および再始動のアクションがあります。そのほかに、パワーオンおよび再始動の統計がキャプチャーされて表示され、ハードウェアの可用性を示します。
Remote Control	サーバー・ビデオ・コンソールをリダイレクトし、ご使用のコンピューターのディスク・ドライブまたはディスク・イメージをサーバー上のドライブとして使用する	「Remote Control」ページから、Remote Control 機能を開始することができます。Remote Control を使用すると、ご使用のコンピューターからサーバー・コンソールを表示し、ご使用の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・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。ご使用のマウスおよびキーボードを使用して、サーバーと対話したり、サーバーを制御したり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。
PXE Network Boot	次回の再始動で 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みるために、ホスト・サーバーの始動 (ブート) シーケンスを変更する	サーバー・ファームウェアおよび PXE ブート・エージェント・ユーティリティーが正しく定義されていると、「PXE Network Boot」ページからホスト・サーバーの始動 (ブート) シーケンスを変更し、次回の再始動で PXE/DHCP ネットワーク始動を試みることができます。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。次回の再始動が行われた後、「PXE Network Boot」ページ上のチェック・ボックスは消去されます。
Firmware Update	IMM 上のファームウェアを更新する	「Firmware Update」ページの各オプションを使用して、IMM 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できます。
System Settings	IMM サーバーの設定を表示し、変更する	「System Settings」ページから、サーバーの位置および一般情報 (IMM の名前、サーバー・タイムアウト設定、IMM の連絡先情報など) を構成することができます。
	IMM のクロックを設定する	イベント・ログ内の項目にタイム・スタンプを付けるために使用される IMM のクロックを設定できます。
	USB インバンド・インターフェースを使用可能または使用不可にする	USB インバンド (または LAN over USB) インターフェースを使用可能または使用不可にすることができます。
Login Profiles	IMM のログイン・プロファイルおよびグローバル・ログイン設定を構成する	IMM へアクセスできるようにする最大 12 個までのログイン・プロファイルを定義できます。また、Lightweight Directory Access Protocol (LDAP) サーバー認証の使用可能化およびアカウント・セキュリティ・レベルのカスタマイズを含む、すべてのログイン・プロファイルに適用されるグローバル・ログイン設定を定義することもできます。

表 2. IMM アクション (続き)

リンク	アクション	説明
Alerts	リモート・アラートおよびリモート・アラート受信者名を構成する	IMM は、さまざまなイベントについてアラートを生成して転送するように構成できます。「Alerts」ページでは、モニター対象とするアラートと、その通知先とする受信者を構成できます。
	Simple Network Management Protocol (SNMP) イベントを構成する	SNMP トラップを送信する対象のイベント・カテゴリを設定することができます。
	アラート設定を構成する	アラートの再試行回数や再試行間の遅延時間など、すべてのリモート・アラート受信者に適用するグローバル設定を確立できます。
Serial Port	IMM シリアル・ポート設定を構成する	「Serial Port」ページから、シリアル・リダイレクト機能で使用するシリアル・ポート・ボー・レートを構成することができます。また、シリアル・リダイレクトとコマンド・ライン・インターフェース (CLI) モードを切り替えるのに使用するキー・シーケンスを構成することもできます。
Port assignments	IMM プロトコルのポート番号を変更する	「Port Assignments」ページから、IMM プロトコル (HTTP、HTTPS、Telnet、および SNMP) に割り当てられたポート番号を表示して変更できます。
Network Interfaces	IMM のネットワーク・インターフェースを構成する	「Network Interfaces」ページから、IMM 上のイーサネット接続に関するネットワーク・アクセス設定を構成できます。
Network Protocols	IMM のネットワーク・プロトコルを構成する	「Network Protocols」ページから、IMM に使用する Simple Network Management Protocol (SNMP)、ドメイン・ネーム・システム (DNS)、および Simple Mail Transfer Protocol (SMTP) の設定を構成できます。また、LDAP パラメーターを構成することもできます。
Security	Secure Sockets Layer (SSL) を構成する	SSL を使用可能にするか使用不可能にすることができ、使用される SSL 証明書を管理できます。また、LDAP サーバーへの接続に SSL 接続を使用できるようにすることも設定できます。
	セキュア・シェル (SSH) アクセスを使用可能にする	IMM への SSH アクセスを使用可能にすることができます。
Configuration File	IMM の構成のバックアップとリストアを行う	「Configuration File」ページから、IMM の構成のバックアップ、変更、およびリストアができるほか、構成の要約を表示できます。
Restore Default Settings	IMM デフォルト設定を復元する	重要: 「 Restore Defaults 」をクリックすると、IMM に加えたすべての変更が失われます。 IMM の構成を出荷時のデフォルト値にリセットできます。
Restart IMM	IMM を再始動する	IMM を再始動することができます。
Scalable Partitioning	スケーラブル・マルチノード・システム内のパーティションとしてサーバーを構成する	サーバーがスケーラブル・マルチノード・システム内で構成されている場合、IMM を使用してマルチノード・システム内のシステムを制御することができます。スケーラブルなサーバーに問題がある場合、IMM がエラーを報告します。

表 2. IMM アクション (続き)

リンク	アクション	説明
Service Advisor	保守可能イベント・コードを IBM サポートに転送する	Service Advisor を使用可能に設定することで、さらにトラブルシューティングを行うために IMM によって保守可能イベント・コードが IBM サポートに転送されます。 注: ご使用のサーバーがこの機能をサポートしているかを確認するには、サーバーの資料を参照してください。
Log off	IMM をログオフする	IMM への接続をログオフすることができます。

ほとんどのページの右上隅にある「**View Configuration Summary**」リンクをクリックすると、IMM の構成をすぐに表示することができます。

第 3 章 IMM の構成

ナビゲーション・ペインの「**IMM Control**」の下にあるリンクを使用すると、IMM を構成できます。

「System Settings」ページから、次のことができます。

- サーバー情報を設定する
- サーバー・タイムアウトを設定する
- IMM の日付と時刻を設定する
- USB インターフェース上のコマンドを使用可能または使用不可にする

「Login Profiles」ページから、次のことができます。

- IMM へのアクセスを制御するために、ログイン・プロファイルを設定する
- ログインの試みが失敗した後のロックアウト期間など、グローバル・ログイン設定を構成する
- アカウント・セキュリティー・レベルを構成する

「Alerts」ページから、次のことができます。

- リモート・アラート受信者を構成する
- リモート・アラート試行回数を設定する
- アラート間の遅延を選択する
- 送信するアラートおよびその転送方法を選択する

「Serial Port」ページから、次のことができます。

- シリアル・リダイレクト用のシリアル・ポート 2 (COM2) のボー・レートを構成する
- シリアル・リダイレクトとコマンド・ライン・インターフェース (CLI) を切り替えるのに使用するキー・ストローク・シーケンスを指定する

「Port Assignments」ページから、IMM サービスのポート番号を変更できます。

「Network Interfaces」ページから、IMM のイーサネット接続をセットアップすることができます。

「Network Protocols」ページから、以下を構成できます。

- SNMP セットアップ
- DNS セットアップ
- Telnet プロトコル
- SMTP セットアップ
- LDAP セットアップ
- Service Location Protocol

「Security」ページから、Secure Sockets Layer (SSL) の設定のインストールと構成を行うことができます。

「Configuration File」ページから、IMM の構成のバックアップ、変更、およびリストアを行うことができます。

「Restore Defaults」ページから、IMM の構成を出荷時のデフォルト値にリセットできます。

「Restart IMM」ページから、IMM を再始動できます。

システム情報の設定

IMM システム情報を設定するには、以下のステップを実行します。

1. システム情報を設定したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「System Settings」をクリックします。次の図のようなページが表示されます。

注: 「System Settings」ページで使用可能なフィールドは、アクセス先のリモート・サーバーによって決まります。

The screenshot displays the IBM Integrated Management Module (IMM) web interface. The top header shows the IBM logo, 'Integrated Management Module', and 'System X'. The left sidebar contains a navigation menu with options like System, Monitors, System Status, Tasks, Power/Restart, Remote Control, IMM Control, and System Settings (which is highlighted). The main content area is titled 'System Settings' and includes sections for IMM Information, Server Timeouts, IMM Date and Time, and Miscellaneous. The IMM Information section has input fields for Name, Contact, and Location. The Server Timeouts section has dropdown menus for OS watchdog and Loader watchdog, both set to 0.0 minutes. The IMM Date and Time section shows the current date and time, with a link to 'Set IMM Date and Time'. The Miscellaneous section has a checkbox for 'Do not allow commands on USB interface'.

3. 「IMM Information」エリアの「Name」フィールドに、IMM の名前を入力します。「Name」フィールドを使用して、このサーバー内の IMM の名前を指定します。この名前は、アラートの送信元を識別するために E メールおよび SNMP アラート通知に含まれます。

注: ご使用の IMM 名 (「Name」フィールド) と IMM の IP ホスト名 (「Network Interfaces」ページの「Hostname」フィールド) は、自動的に同じ名前を共用するわけではありません。「Name」フィールドは 16 文字以内に限定されているからです。「Hostname」フィールドには、最大 63 文字を格納できます。混乱を最小限に抑えるために、「Name」フィールドを IP ホスト名の非修飾部分に設定してください。非修飾 IP ホスト名は、完全修飾 IP ホスト名の最初のピリオドまでで構成されます。例えば、完全修飾 IP ホスト名

imm1.us.company.com の場合、非修飾 IP ホスト名は imm1 です。ホスト名については、41 ページの『ネットワーク・インターフェースの構成』を参照してください。

4. 「**Contact**」フィールドに連絡先情報を入力します。例えば、このサーバーに問題がある場合に、連絡を取る人の名前と電話番号を指定することができます。このフィールドには、47 文字以内で入力できます。
5. 「**Location**」フィールドに、サーバーの位置を入力します。このフィールドには、保守またはその他の目的でサーバーの場所を迅速に見付けるのに十分な詳細を記入します。このフィールドには、47 文字以内で入力できます。
6. そのページの下部までスクロールして、「**Save**」をクリックします。

サーバー・タイムアウトの設定

注: サーバー・タイムアウトは、インバンド USB インターフェース (または LAN over USB) が使用可能に設定され、コマンドを許可する必要があります。USB インターフェースのコマンドの使用可能化および使用不可化について詳しくは、26 ページの『USB インバンド・インターフェースの使用不可化』を参照してください。必要なデバイス・ドライバのインストールに関する情報は、142 ページの『デバイス・ドライバのインストール』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 IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**System Settings**」をクリックし、「**Server Timeouts**」エリアまでスクロールダウンします。

以下のイベントに自動的に応答するように、IMM 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. IMM 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。

OS ウォッチドッグ

「**OS watchdog**」フィールドを使用して、IMM によるオペレーティング・システムのチェック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 つに応答しないと、IMM 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、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、メニューから「**0.0**」を選択します。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、「**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。

Loader watchdog

「**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、IMM が待つ分数を指定します。この間隔を超えると、IMM 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 IMM 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「**0.0**」を選択します。

電源オフ遅延

「**Power off delay**」フィールドを使用して、(オペレーティング・システムによってサーバーの電源がオフにされない場合に) IMM がサーバーの電源をオフにする前にオペレーティング・システムのシャットダウンを待つ分数を指定します。電源オフ遅延を設定した場合、サーバー電源がオフにされる前にオペレーティング・システムが正常シャットダウンを行うための十分な時間を確保することができます。ご使用のサーバーの電源オフ遅延を判別するには、サーバーをシャットダウンして、シャットダウンにかかる時間を監視してください。その値に時間バッファを加算して、その結果の数値を電源オフ遅延の設定値として使用します。

電源オフ遅延の値を設定するには、メニューから目的の時間値を選択します。値 **X'0'** は、IMM ではなくオペレーティング・システムがサーバー電源をオフにすることを意味します。

4. そのページの下部までスクロールして、「**Save**」をクリックします。

IMM の日付と時刻の設定

IMM 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。

注: IMM 日時設定は、IMM 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。IMM 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。IMM クロックとサーバー・クロックを同期するには、ページの「**Network Time Protocol**」エリアに進み、サーバー・クロックを設定するのに使用したのと同じ NTP サーバーのホスト名または IP アドレスを設定します。詳しくは、25 ページの『ネットワーク内のクロックの同期』を参照してください。

電子メールおよび SNMP によって送信されるアラートは、リアルタイム・クロックの設定を使用して、アラートにタイム・スタンプを付けます。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 (DST) 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。

IMM の日時設定を確認するには、以下のステップを実行してください。

1. IMM の日付と時刻の値を設定したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで「**System Settings**」をクリックし、「**IMM Date and Time**」エリアまでスクロールダウンします。このセクションには、Web ページが生成された日時が示されています。
3. 日時の設定を変更し、夏時間 (DST) およびグリニッジ標準時 (GMT) オフセットを使用可能にするには、「**Set IMM Date and Time**」をクリックします。次の図のようなページが表示されます。



4. 「**Date**」フィールドに、現在の月、日、および年を表す数値を入力します。
5. 「**Time**」フィールドで、現在の時、分、秒に対応する数値をそれぞれの該当する入力フィールドに入力します。時 (hh) は、24 時間クロックで表される 00 から 23 までの数値であることが必要です。分 (mm) および秒 (ss) は、00 から 59 までの数値であることが必要です。
6. 「**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、グリニッジ標準時 (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。
7. 「**Automatically adjust for daylight saving changes**」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、IMM クロックを自動的に調整するかどうかを指定します。
8. 「**Save**」をクリックします。

ネットワーク内のクロックの同期

Network Time Protocol (NTP) は、コンピューター・ネットワーク全体のクロックを同期する手段を提供し、すべての NTP クライアントが NTP サーバーから正確な時刻を取得することを可能にします。

IMM の NTP 機能は、IMM リアルタイム・クロックを NTP サーバーが提供する時刻と同期する手段を提供します。使用する NTP サーバー、および IMM を同期する頻度を指定したり、NTP 機能を使用可能あるいは使用不可に設定したり、即時の時刻同期を要求することができます。

NTP 機能は、拡張セキュリティーや、NTP バージョン 3 および NTP バージョン 4 での暗号化アルゴリズムによって提供される認証を備えていません。IMM の NTP 機能は、認証を行わない Simple Network Time Protocol (SNTP) のみをサポートします。

IMM の NTP 機能設定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. ネットワーク内でクロックを同期する IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**System Settings**」をクリックし、「**IMM Date and Time**」エリアまでスクロールダウンします。
3. 「**Set IMM Date and Time**」をクリックします。次の図のようなページが表示されます。



4. 「**Network Time Protocol (NTP)**」の下で、以下の設定から選択することができます。

NTP auto-synchronization service

この選択を使用して、IMM クロックと NTP サーバーの自動同期を使用可能あるいは使用不可にします。

NTP server host name or IP address

このフィールドを使用して、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。

NTP update frequency

このフィールドを使用して、同期要求のおおよその間隔 (分) を指定します。3 から 1440 分の間の値を入力します。

Synchronize Clock Now

このボタンをクリックすると、間隔に指定した時間が経過するのを待たずに、即時同期を要求します。

5. 「**Save**」をクリックします。

USB インバンド・インターフェースの使用不可化

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 IMM 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、IMM Web インターフェースの「Firmware Update」オプションを使用して、ファームウェアを更新します。詳しくは、136 ページの『ファームウェアの更新』を参照してください。

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。詳しくは、23 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。

USB インバンド・インターフェース、あるいは LAN over USB は、IMM へのインバンド通信に使用されます。サーバー上で稼働しているアプリケーションが IMM にタスクの実行を要求することを防ぐには、USB インバンド・インターフェースを使用不可にする必要があります。LAN over USB について詳しくは、141 ページの『第 6 章 LAN over USB』を参照してください。

USB インバンド・インターフェースを使用不可にするには、以下のステップを実行します。

1. USB インバンド・インターフェースを使用不可にする IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**System Settings**」をクリックし、「**Miscellaneous**」エリアまでスクロールダウンします。次の図のようなページが表示されます。



3. USB インバンド・インターフェースを使用不可にするには、「**Allow commands on the USB interface**」リストから「**Disabled**」を選択します。このオプションを選択しても、USB リモート・プレゼンス機能（例えば、キーボード、マウス、および大容量ストレージ）には影響を与えません。USB インバンド・インターフェースを使用不可にすると、Advanced Settings ユーティリティ（ASU）やファームウェア更新パッケージ・ユーティリティなどのインバンド・システム管理アプリケーションが動作しない場合があります。

注: IPMI デバイス・ドライバがインストールされていると、ASU は 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状態で動作します。

インバンド・インターフェースが使用不可にされている状態では、システム管理アプリケーションは使用できない場合があります。

4. 「**Save**」をクリックします。

USB インバンド・インターフェースが使用不可にされた後、使用可能に戻すには、「**Do not allow commands on USB interface**」チェック・ボックスをクリアして「**Save**」をクリックします。

注:

1. USB インバンド・インターフェースは「LAN over USB」とも呼ばれます。詳しくは、141 ページの『第 6 章 LAN over USB』で説明されています。
2. 一部の Linux ディストリビューションのネットワーク・インストールを試行する場合、IMM の USB インバンド・インターフェースが使用可能にされているとインストールが失敗する可能性があります。詳しくは、<http://rhn.redhat.com/errata/RHBA-2009-0127.html> を参照してください。

3. 前述の注 2 (27 ページ) で示された Red Hat Web サイトにある更新を含まないネットワーク・インストールを実行する場合、インストールを実行する前に USB インバンド・インターフェースを使用不可にし、インストールが完了した後で使用可能に戻す必要があります。
4. LAN over USB インターフェースの構成については、142 ページの『LAN over USB インターフェースの手動構成』を参照してください。

ログイン・プロファイルの作成

「Login Profiles」のテーブルを使用して、個々のログイン・プロファイルを表示、構成、または変更します。「Login ID」列のリンクを使用して、個々のログイン・プロファイルを構成してください。最大 12 個までの固有なプロファイルを定義できます。「Login ID」列のそれぞれのリンクには、関連プロファイルの構成済みログイン ID がラベルとして付いています。

特定のログイン・プロファイルは IPMI ユーザー ID と共有され、IPMI を含むすべての IMM ユーザー・インターフェースと連動する単一セットのローカル・ユーザー・アカウント (ユーザー名/パスワード) を提供します。これらの共有ログイン・プロファイルに関連する規則は、以下のリストに記載されています。

- IPMI ユーザー ID 1 は、常に NULL ユーザーです。
- IPMI ユーザー ID 2 は、ログイン ID 1 にマップされ、IPMI ユーザー ID 3 は、ログイン ID 2 にマップされ、以降も同様に続きます。
- IMM デフォルト・ユーザーは、IPMI ユーザー ID 2 およびログイン ID 1 について、USERID および PASSWORD (英字の O でなくゼロ) に設定されます。

例えば、IPMI コマンドを使用してユーザーが追加されると、そのユーザー情報も Web、Telnet、SSH、およびその他のインターフェースを介する認証に使用可能です。反対に、Web あるいはその他のインターフェースを介してユーザーが追加されると、そのユーザー情報は IPMI セッションの開始に使用可能です。

ユーザー・アカウントが IPMI と共有されるため、一部の制約事項が、これらのアカウントを使用するインターフェース間で共通の制約事項になる場合があります。以下のリストは、IMM および IPMI のログイン・プロファイルの制限について説明しています。

- IPMI は、最大 64 個のユーザー ID を許可します。IMM IPMI 実装環境では、12 個のユーザー・アカウントのみが許可されます。
- IPMI は匿名ログイン (NULL ユーザー名と NULL パスワード) を許可しますが、IMM は許可しません。
- IPMI は同一のユーザー名に対して複数のユーザー ID を許可しますが、IMM は許可しません。
- ユーザー名を現行の名前から現行の名前と同じ名前に変更する IPMI 要求は、invalid parameter 完了コードを返します。これは、要求されたユーザー名が既に使用中であるためです。
- IMM の IPMI パスワードの最大長は 16 バイトです。
- 以下のワードは制限されており、ローカル IMM ユーザー名として使用することはできません。

– immroot

- nobody
- ldap
- lighttpd
- sshd
- daemon
- immftp

ログイン・プロファイルを構成するには、以下のステップを実行します。

1. ログイン・プロファイルを作成したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Login Profiles**」をクリックします。

注: プロファイルを構成していない場合は、「Login Profiles」テーブルには表示されません。

「Login Profiles」ページには、次の図に示すように、各ログイン ID、ログイン・アクセス・レベル、およびパスワードの有効期限の情報が表示されます。

The screenshot shows the IBM Integrated Management Module (IMM) web interface. The left navigation pane lists various system management options. The main content area is titled 'Login Profiles' and includes a table of existing profiles. Below the table, there are 'Global Login Settings' for configuring authentication and session parameters.

Slot No.	Login ID	Access	Password Expires
1	USERID	Supervisor	No expiration
2	ed_k	Supervisor	No expiration
3	LONGUYEN	Supervisor	No expiration
4	ANDREW	Supervisor	No expiration
5	jeffat	Supervisor	No expiration

Global Login Settings

These settings apply to all login profiles.

User authentication method: Local only

Lockout period after 5 login failures: 2 minutes

Web inactivity session timeout: User picks timeout

重要: デフォルトでは、IMM は USERID というログイン・ユーザー ID と、PASSWORD (0 は英字の O でなく数字のゼロ) というパスワードを使用してリモート・アクセスを可能にする 1 つのログイン・プロファイルで構成されます。機密漏れの可能性を回避するために、このデフォルトのログイン・プロファイルを IMM の初期セットアップ時に変更してください。

3. 「**Add User**」をクリックします。次の図に示すような個別のプロファイル・ページが表示されます。

Login Profile 1

Login ID:

Password:

Confirm password:

Authority Level

☒ Supervisor

☐ Read-Only

☐ Custom

- ☐ User Account Management
- ☐ Remote Console Access
- ☐ Remote Console and Remote Disk Access
- ☐ Remote Server Power/Restart Access
- ☐ Ability to Clear Event Logs
- ☐ Adapter Configuration - Basic
- ☐ Adapter Configuration - Networking & Security
- ☐ Adapter Configuration - Advanced (Firmware Update, Restart IMM, Restore Configuration)

4. 「**Login ID**」フィールドにプロファイルの名前を入力します。「**Login ID**」フィールドに 16 文字以内で入力できます。有効な文字は、英大文字および英小文字、数字、ピリオド、および下線です。

注: このログイン ID は、IMM へのリモート・アクセスを認可するために使用されます。

5. 「**Password**」フィールドで、ログイン ID にパスワードを割り当てます。パスワードは 5 文字以上で、そのうち 1 文字は英字以外の文字であることが必要です。NULL または空のパスワードも受け入れられます。

注: このパスワードは、IMM へのリモート・アクセスを認可するために、ログイン ID と一緒に使用されます。

6. 「**Confirm password**」フィールドに、再度パスワードを入力します。
7. 「**Authority Level**」エリアで、次のいずれかのオプションを選択して、そのログイン ID のアクセス権を設定します。

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

「Custom」オプションを選択した場合は、次のカスタム権限レベルを 1 つ以上選択する必要があります。

- **User Account Management:** ユーザーは、ユーザーの追加、変更、または削除ができ、「Login Profiles」ページのグローバル・ログイン設定を変更できます。
- **Remote Console Access:** ユーザーはリモート・コンソールにアクセスできます。
- **Remote Console and Virtual Media Access:** ユーザーはリモート・コンソールと仮想メディア機能の両方にアクセスできます。

- **Remote Server Power/Restart Access:** ユーザーは、リモート・サーバーのパワーオン機能と再始動機能にアクセスできます。これらの機能は、「Power/Restart」ページで使用できます。
- **Ability to Clear Event Logs:** ユーザーはイベント・ログを消去できます。イベント・ログは、誰でも見ることはできますが、ログを消去するには、この特定の許可が必要です。
- **Adapter Configuration - Basic:** ユーザーは、「System Settings」および「Alerts」ページで構成パラメーターを変更できます。
- **Adapter Configuration - Networking & Security:** ユーザーは、「Security」、「Network Protocols」、「Network Interface」、「Port Assignments」、「Serial Port」の各ページで構成パラメーターを変更できます。
- **Adapter Configuration - Advanced:** ユーザーは、IMM を構成するときに何も制約を受けません。また、ユーザーは「IMM に対する管理アクセス権を持つ」と見なされます。これは、そのユーザーが、ファームウェアの更新、PXE ネットワーク・ブート、IMM 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 IMM 構成の変更とリストア、および IMM の再始動とリセットなどの拡張機能も実行できることを意味します。

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

- ユーザーが IMM ログイン ID の権限レベルを Supervisor に設定すると、IPMI 特権レベルは Administrator に設定されます。
- ユーザーが IMM ログイン ID の権限レベルを Read Only に設定すると、IPMI 特権レベルは User に設定されます。
- ユーザーが IMM ログイン ID の権限レベルを以下のいずれかのタイプのアクセス権限に設定すると、IPMI 特権レベルは Administrator に設定されます。
 - User Account Management Access
 - Remote Console Access
 - Remote Console and Remote Disk Access
 - Adapter Configuration - Networking & Security
 - Adapter Configuration - Advanced
- ユーザーが IMM ログイン ID の権限レベルを Remote Server Power/Restart Access または Ability to Clear Event Logs に設定すると、IPMI 特権レベルは Operator に設定されます。
- ユーザーが IMM ログイン ID の権限レベルを Adapter Configuration (Basic) に設定すると、IPMI 特権レベルは User に設定されます。

注: ログイン・プロファイルを出荷時のデフォルト値に戻すには、「Clear Login Profiles」をクリックします。

8. SNMPv3 プロトコルを使用して IMM にアクセスする権限をユーザーに付与する場合、「Configure SNMPv3 User」エリアでチェック・ボックスを選択します。チェック・ボックスをクリックした後、次の図のようなページのエリアが表

示されます。



以下のフィールドを使用して、ユーザー・プロファイルの SNMPv3 設定を構成します。

Authentication Protocol

このフィールドを使用して、「**HMAC-MD5**」または「**HMAC-SHA**」のいずれかを認証プロトコルとして指定します。これらは、SNMPv3 セキュリティー・モデルが認証に使用するハッシュ・アルゴリズムです。Linux アカウント用のパスワードが認証に使用されます。「**None**」を選択すると、認証プロトコルは使用されません。

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

このフィールドを使用して、暗号化パスワードを指定します。

Confirm Privacy Password

このフィールドを使用して、暗号化パスワードを確認します。

Access Type

このフィールドを使用して、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、照会操作のみを実行することができます。アクセス・タイプが「**Set**」の SNMPv3 ユーザーは、照会操作および設定変更 (例えば、ユーザーのパスワードの設定) の両方を実行することができます。

Hostname/IP address for traps

このフィールドを使用して、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)。

9. 「**Save**」をクリックして、ログイン ID の設定を保管します。

ログイン・プロファイルの削除

ログイン・プロファイルを削除するには、次の手順に従ってください。

1. ログイン・プロファイルを作成したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Login Profiles**」をクリックします。「Login Profiles」ページには、各ログイン ID、ログイン・アクセス・レベル、およびパスワードの有効期限の情報が表示されます。
3. 削除するログイン・プロファイルをクリックします。そのユーザーの「Login Profile」ページが表示されます。
4. 「**Clear Login Profile**」をクリックします。

グローバル・ログイン設定の構成

IMM のすべてのログイン・プロファイルに適用する条件を設定するには、以下のステップを実行します。

1. グローバル・ログイン設定を設定する IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Login Profiles**」をクリックします。
3. 「**Global Login Settings**」エリアまでスクロールダウンします。次の図のようなページが表示されます。

Global Login Settings	
These settings apply to all login profiles.	
User authentication method	Local only
Lockout period after 5 login failures	2 minutes
Web inactivity session timeout	User picks timeout
Account security level:	
☒ Legacy security settings	No password required No password expiration No password re-use restrictions
☐ High security settings	Password required Passwords expire in 90 days Password reuse checking enabled (last 5 passwords kept in history)
☐ Custom security settings	User login password required: Disabled Number of previous passwords that cannot be used: 0 Maximum Password Age: 0 days
<button>Save</button>	

4. 「**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します。次のいずれかの認証方式を選択してください。
 - **Local only:** ユーザーは、IMM にローカルなテーブル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。正常に認証されたユーザーには、28 ページの『ログイン・プロファイルの作成』で構成された権限レベルが割り当てられます。
 - **LDAP only:** IMM 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、IMM 上のローカル・ユーザー・テーブルは検索されません。
 - **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:

- IPMI は LDAP 認証をサポートしないため、ローカルで管理されているアカウントのみが IPMI インターフェースと共有されます。
 - 「**User authentication method**」フィールドが「**LDAP only**」に設定されている場合でも、ユーザーはローカルで管理されているアカウントを使用して IPMI インターフェースにログインすることができます。
- 「**Lockout period after 5 login failures**」フィールドで、連続 5 回を超えてリモート側からのログインに失敗したことが検出された場合に、IMM がリモート・ログインの試行を禁止する時間の長さを分単位で指定します。特定のユーザーのロックアウトは、他のユーザーのログインを妨げるものではありません。
 - 「**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 IMM の待ち時間を分単位で指定します。この機能を使用不可にするには、「**No timeout**」を選択します。ユーザーがログイン・プロセスでタイムアウト期間を選択する場合は、「**User picks timeout**」を選択します。
 - (オプション) 「**Account security level**」エリアで、パスワード・セキュリティ・レベルを選択します。「**Legacy security settings**」および「**High security settings**」は、要件リストで示されているデフォルト値を設定します。
 - セキュリティ設定をカスタマイズするには、「**Custom security settings**」を選択し、アカウント・セキュリティ管理の構成を表示して変更します。

User login password required

このフィールドを使用して、パスワードを持たないログイン ID を許可するかどうかを指定します。

Number of previous passwords that cannot be used

このフィールドを使用して、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します。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。

Maximum Password Age

このフィールドを使用して、パスワードを変更せずに使用することができる最大日数を指定します。0 から 365 日の間の値がサポートされます。0 を選択すると、パスワードの期限切れ検査が無効になります。

- 「**Save**」をクリックします。

リモート・アラート設定の構成

ナビゲーション・ペインの「**Alerts**」リンクから、リモート・アラート受信者、アラートの試行回数、リモート・アラートをトリガーする出来事、およびローカル・アラートを構成できます。

リモート・アラート受信者を構成した後に、「**Monitored Alerts**」グループで選択したイベントが発生すると、IMM はネットワーク接続を介して受信者にアラートを送信します。このアラートには、イベントの性質、イベントの日付と時刻、アラートを生成したシステムの名前に関する情報が含まれます。

注: 「SNMP Agent」または「SNMP Traps」フィールドが「Enabled」に設定されていない場合、SNMP トラップは送信されません。これらのフィールドについては、48 ページの『SNMP の構成』を参照してください。

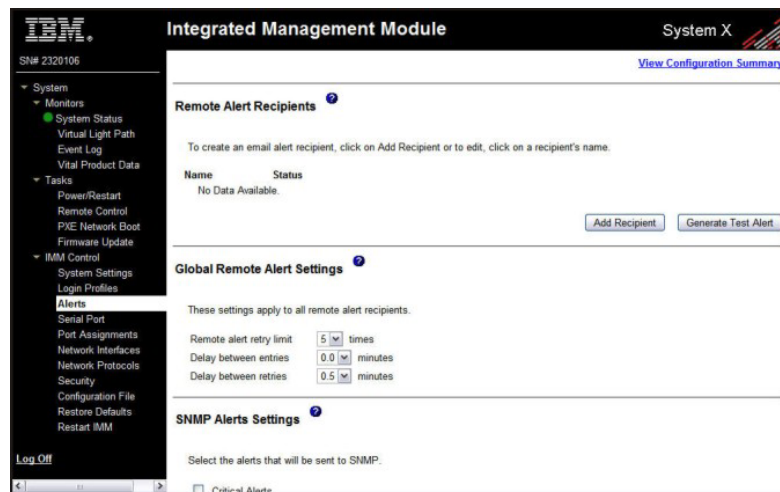
リモート・アラート受信者の構成

最大 12 件の固有なリモート・アラート受信者を定義できます。アラート受信者用の各リンクには、受信者名およびアラート状況がラベルとして付きます。

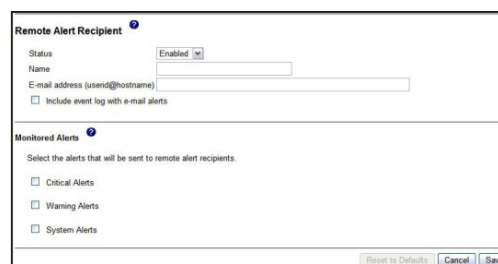
注: アラート受信者プロファイルを構成していない場合、リモート・アラートの受信者リストにプロファイルが表示されません。

リモート・アラート受信者を構成するには、以下のステップを実行します。

1. リモート・アラート設定を構成したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「Alerts」をクリックします。「Remote Alert Recipients」ページが表示されます。それぞれの受信者の通知方式とアラート状況が設定されていれば、それらを表示できます。



3. リモート・アラート受信者リンクのいずれか 1 つ、あるいは「Add Recipient」をクリックします。次の図に示すような個々の受信者のウィンドウが開かれます。



4. 「Status」フィールドで、「Enabled」をクリックしてリモート・アラート受信者をアクティブにします。

5. 「Name」フィールドに受信者の名前またはその他の ID を入力します。入力した名前は、その受信者用のリンクとして「Alerts」ページに表示されます。
6. 「E-mail address」フィールドで、アラート受信者の E-mail アドレスを入力します。
7. チェック・ボックスを使用すると、イベント・ログが E-mail アラートに含まれます。
8. 「Monitored Alerts」フィールドで、アラート受信者に送信するアラートのタイプを選択します。リモート・アラートは、次の重大度レベルによって分類されます。

Critical alerts

クリティカル・アラートは、サーバー・コンポーネントがもはや機能していないことを知らせるイベントについて生成されます。

Warning alerts

警告アラートは、クリティカル・レベルまで進む可能性があるイベントについて生成されます。

System alerts

システム・アラートは、システム・エラーの結果として発生したイベント、あるいは構成変更の結果として発生したイベントについて生成されます。

すべてのアラートは、イベント・ログに格納され、構成済みのすべてのリモート・アラート受信者へ送信されます。

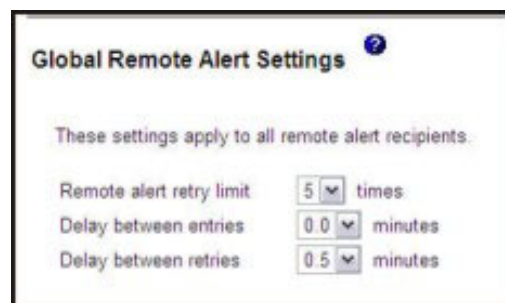
9. 「Save」をクリックします。

グローバル・リモート・アラート設定の構成

グローバルなリモート・アラートの設定は、転送されるアラートにのみ適用されます。

IMM がアラートの送信を試みる回数を設定するには、以下のステップを実行します。

1. リモート・アラート試行を設定したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「Alerts」をクリックし、「Global Remote Alert Settings」エリアまでスクロールダウンします。



次の設定を使用して、リモート・アラート試行回数および試行間の時間間隔を定義します。この設定は、構成済みのすべてのリモート・アラート受信者に適用されます。

Remote alert retry limit

「**Remote alert retry limit**」フィールドを使用して、IMM が受信者へアラートの送信を試みる追加の回数を指定します。IMM は、複数のアラートを送信しません。追加アラートを試行するのは、IMM が最初のアラートの送信に失敗した場合のみです。

注: このアラート設定は、SNMP アラートには適用されません。

Delay between entries

「**Delay between entries**」フィールドを使用して、IMM がリスト内の次の受信者へアラートを送信する前に待つ時間間隔 (分単位) を指定します。

Delay between retries

「**Delay between retries**」フィールドを使用して、IMM が受信者へのアラートの送信を再試行してから次に再試行するまで待つ時間間隔 (分単位) を指定します。

3. そのページの下部までスクロールして、「**Save**」をクリックします。

SNMP アラート設定の構成

SNMP エージェントは、SNMP トラップを介して IMM にイベントを通知します。イベント・タイプに基づいてイベントをフィルタリングするように SNMP を構成することができます。フィルタリングに使用可能なイベント・カテゴリーは、Critical、Warning および System です。SNMP アラート設定は、すべての SNMP トラップに対して包括的です。

注:

1. IMM は、SNMP アプリケーションで使用する 2 つの管理情報ベース (MIB) ファイルを提供します。MIB ファイルは、IMM ファームウェア更新パッケージに含まれています。
2. IMM は、SNMPv1 および SNMPv3 規格をサポートします。

以下のステップを実行して、SNMP に送信されるアラートのタイプ (複数可) を選択してください。

1. リモート・アラート試行を設定したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Alerts**」をクリックし、「**SNMP Alerts Settings**」エリアまでスクロールダウンします。
3. アラートのタイプ (複数可) を選択します。リモート・アラートは、次の重大度レベルによって分類されます。
 - Critical
 - Warning
 - System

4. そのページの下部までスクロールして、「**Save**」をクリックします。

シリアル・ポート設定の構成

IMM 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。

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。

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 サーバーでは、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。

両方のシリアル・ポートが 8 データ・ビット、NULL パリティ、および 1 ストップ・ビットを使用します。ボー・レートは、9600、19200、38400、57600、115200、および 230400 が選択可能です。

IMM の COM2 ポートのシリアル・リダイレクトおよびコマンド・ライン・インターフェースを構成することができます。

シリアル・データ転送速度およびシリアル・リダイレクトを構成するには、以下のステップを実行します。

1. シリアル・ポートを構成する IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Serial Port**」をクリックします。次の図のようなページが表示されます。

The screenshot shows a web form for configuring Serial Port 2 (COM2). The form has two main sections. The first section, titled 'Serial Port 2 (COM2)', contains a 'Baud rate' dropdown menu set to '115200'. The second section, titled 'Serial Redirect / CLI Settings', contains a 'Port 2 (COM2)' label, a 'CLI mode' dropdown menu set to 'CLI with user defined keystroke sequences', and a 'User Defined Keystroke Sequences' section with a text input field for 'Exit CLI key sequence' containing '^[Q'. A 'Save' button is located at the bottom right of the form.

3. 「**Baud rate**」フィールドで、シリアル・リダイレクトに使用するサーバーの COM ポートの速度に一致するデータ転送速度を選択します。「**Baud rate**」フィールドを使用して、シリアル・ポート接続のデータ転送速度を指定してください。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データ転送速度をビット/秒単位で選択します。
4. 「**Serial Redirect/CLI Settings**」エリアの「**CLI mode**」フィールドで、Microsoft Windows Server 2003 Emergency Management Services (EMS) 互換のキー・シー

ケンスを使用してシリアル・リダイレクト操作を終了する場合は「**CLI with EMS compatible keystroke sequences**」を、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、それぞれ選択します。

注: 「**CLI with user defined keystroke sequences**」を選択する場合は、キー・シーケンスを定義する必要があります。

シリアル・リダイレクトが開始されると、ユーザーが終了キー・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 あるいは SSH セッションのコマンド・モードに戻ります。この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。

5. 「**Save**」をクリックします。

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 IMM 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. IMM 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. コマンド・ライン・インターフェースの **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 Q

終了キー・シーケンスを入力して、コマンド・ライン・インターフェースに戻ります。この例では、Esc を押してから q を入力します。

Back to LegacyCLI console....

ポート割り当ての構成

IMM サービスのポート番号を変更するには、以下のステップを実行します。

1. ポート割り当てを構成する IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「Port Assignments」をクリックします。次の図のようなページが表示されます。

Service	Port
HTTP	80
HTTPS	443
Telnet Legacy CLI	23
SSH Legacy CLI	22
SNMP Agent	161
SNMP Traps	162
Remote Presence	3900
IBM Systems Director over HTTP	5988
IBM Systems Director over HTTPS	5989

3. 次の情報を使用して、各フィールドに値を割り当てます。

HTTP これは、IMM の HTTP サーバーのポート番号です。デフォルトのポート番号は 80 です。それ以外の有効な値は、1 から 65535 までの範囲です。このポート番号を変更する場合は、このポート番号の前にコロンを付け、それを Web アドレスの末尾に追加する必要があります。例えば、HTTP ポートが 8500 に変更された場合、IMM Web インターフェースを開くには、`http://hostname:8500/` と入力します。IP アドレスおよびポート番号の前に、接頭部の `http://` を入力する必要があることに注意してください。

HTTPS

これは、Web インターフェース HTTPS (SSL) トラフィックに使用されるポート番号です。デフォルト値は 443 です。それ以外の有効な値は、1 から 65535 までの範囲です。

Telnet Legacy CLI

これは、Legacy 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です。デフォルト値は 23 です。それ以外の有効な値は、1 から 65535 までの範囲です。

SSH Legacy CLI

これは、Legacy CLI が SSH を介してログインするために構成されたポート番号です。デフォルトは 22 です。

SNMP Agent

これは、IMM 上で稼働する SNMP エージェントのポート番号です。デフォルト値は 161 です。それ以外の有効な値は、1 から 65535 までの範囲です。

SNMP Traps

これは、SNMP トラップに使用されるポート番号です。デフォルト値は 162 です。それ以外の有効な値は、1 から 65535 までの範囲です。

Remote Presence

これは、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です。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は 3900 です。

注: BladeCenter の並行キーボード、ビデオ、マウス (cKVM) 機能では、ポート番号が 2068 であることが必要です。ブレード・サーバー上でこのポート番号を変更しないでください。

IBM Systems Director over HTTP

これは、IBM Systems Director がサーバー・コンソールとの対話に使用するポート番号です。デフォルトは 5988 です。

IBM Systems Director over HTTPS

これは、IBM Systems Director が SSL を使用してサーバー・コンソールと対話するためのポート番号です。デフォルトは 5989 です。

次に示すポート番号は予約済みであり、それぞれに対応するサービスにのみ使用できます。

表 3. 予約済みポート番号

ポート番号	使用対象のサービス
427	SLP
7070 から 7077	パーティション管理

4. 「Save」をクリックします。

ネットワーク・インターフェースの構成

「Network Interfaces」ページで、IMM へのイーサネット接続を構成することで、IMM へのアクセス権限を設定することができます。IMM のイーサネット・セットアップを構成するには、「Network Interfaces」ページの「Ethernet」、「IPv4」、または「IPv6」エリアの設定を必要に応じて変更します。各エリアの設定については、以下のセクションで説明しています。

注: 次の図は、値の例を示しています。お客様の設定は、これとは異なります。

Ethernet

Interface:

☒ IPv6 Enabled

Hostname: IMM-001A64E604D5

Domain name: -

DDNS Status:

Domain Name Used: DHCP

[Advanced Ethernet Setup](#)

IPv4

DHCP:

*** The IP configuration for this interface is assigned by a DHCP server. Follow the link
*** "IP Configuration Assigned by DHCP Server" to see the assigned configuration.

Static IP Configuration

IP address: 192.168.70.125

Subnet mask: 255.255.255.0

Gateway address: 0.0.0.0

[IP Configuration Assigned by DHCP Server](#)

IPv6

Link local address: fe80::21a:64ff:fe6:4d5

IPv6 static IP configuration:

DHCPv6:

Stateless Auto-configuration:

[View Automatic Configuration](#)

現行構成のすべての設定の要約を参照するには、「Network Interfaces」ページの「**View Configuration Summary**」をクリックします。「Network Interfaces」ページの設定を構成する前に、次のセクションの情報を確認してください。

注: Setup ユーティリティから IMM ネットワーク接続を構成することもできます。詳しくは、13 ページの『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 IMM ネットワーク接続のセットアップ』を参照してください。

イーサネット設定の構成

以下の設定は、「Network Interfaces」ページの「Ethernet」エリアで変更することができます。

Interface

このフィールドを使用して、このネットワーク・インターフェースを使用可能または使用不可に設定します。このネットワーク・インターフェースを使用したネットワーク接続を許可するには、「**Enabled**」を選択します。

IPv6 Enabled

このチェック・ボックスを使用して、IMM での IPv6 サポートを使用可能または使用不可に設定します。

注: 「**IPv6 Enabled**」チェック・ボックスをクリアすると、「**Hide all IPv6 configuration fields when IPv6 is disabled**」チェック・ボックスが表示されます。新規チェック・ボックスを選択すると、「Network Interfaces」ページの IPv6 エリアは Web インターフェース上で非表示になります。

Hostname

このフィールドを使用して、IMM サブシステムに固有のホスト名を定義します。このフィールドには、63 文字以内で入力できます。ホスト名に使用できるのは、英数字、ハイフン、および下線のみです。

注: デフォルトのホスト名は、IMM- の後に組み込み MAC アドレスが続きます。

Domain name

このフィールドを使用して、DNS ドメイン・ネームを定義します。

DDNS Status

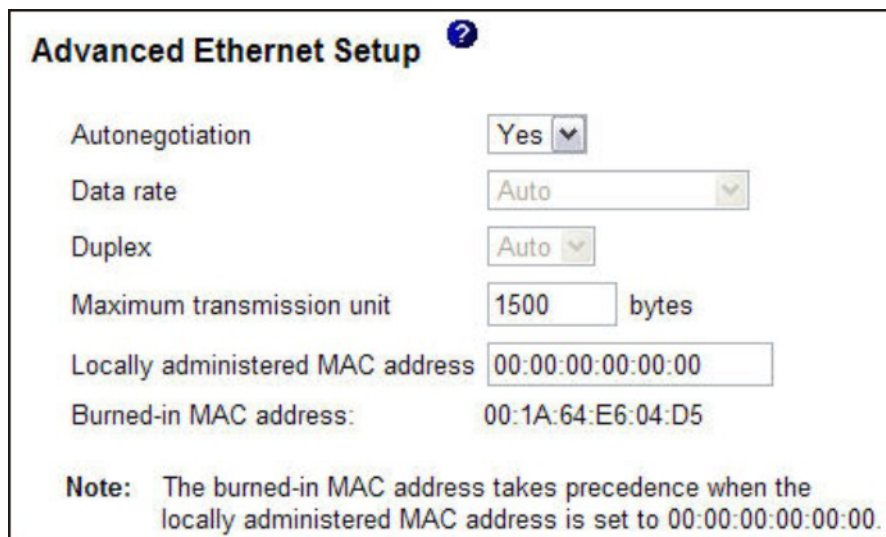
このフィールドを使用して、動的 DNS (DDNS) を使用可能または使用不可に設定します。DDNS を使用すると、IMM が DNS サーバーに対して、構成済みのホスト名、アドレス、あるいは DNS に保管されているその他の情報について、現行の DNS 構成を変更するように、リアルタイムに通知することが可能になります。DDNS が使用可能に設定されている場合、IMM は、DHCP サーバーから受け取った IP アドレスまたは自己構成した IP アドレスを DNS サーバーに通知します。

Domain Name Used

このフィールドを使用して、DDNS が使用可能に設定された場合に、DHCP によって割り当てられたドメイン・ネームと手動で割り当てたドメイン・ネームのどちらを DNS に送信するかを選択します。この値には、DHCP または Manual のいずれかを設定します。

Advanced Interface Setup

このリンクをクリックすると、次のイメージのような「Advanced Interface Setup」ページが開きます。



The screenshot shows the 'Advanced Ethernet Setup' configuration page. It includes the following settings:

- Autonegotiation:** Set to 'Yes' via a dropdown menu.
- Data rate:** Set to 'Auto' via a dropdown menu.
- Duplex:** Set to 'Auto' via a dropdown menu.
- Maximum transmission unit:** Set to '1500' bytes.
- Locally administered MAC address:** Set to '00:00:00:00:00:00'.
- Burned-in MAC address:** Displayed as '00:1A:64:E6:04:D5'.

A note at the bottom states: 'Note: The burned-in MAC address takes precedence when the locally administered MAC address is set to 00:00:00:00:00:00.'

このページから、インターフェースに関する追加設定を表示したり変更したりできます。次の表は、「Advanced Ethernet Setup」ページの設定を説明したものです。

表 4. 「Advanced Ethernet Setup」 ページの設定

設定	機能
Autonegotiate	この設定を使用して、データ転送速度および二重ネットワーク設定を構成可能にするかどうかを選択します。 Autonegotiate が Yes に設定されている場合、データ転送速度および二重設定は Auto に設定され、構成することはできません。 Autonegotiate が No に設定されている場合、ユーザーがデータ転送速度および二重設定を構成することができます。
Data rate	このフィールドを使用して、LAN 接続上で転送される 1 秒当たりのデータ量を指定します。データ転送速度を設定するには、ご使用のネットワーク性能に対応するデータ転送速度をメガビット (Mb) 単位で選択します。データ転送速度を自動的に検出するには、 Auto を選択します。
Duplex	このフィールドを使用して、ネットワーク内で使用される通信チャネルのタイプを指定します。二重モードを設定するには、 Full または Half を選択します。全二重 (Full) では、データを両方向に同時に転送することができます。半二重通信路 (Half) では、データをいずれか 1 つの方向に転送することはできませんが、同時に両方向に転送することはできません。二重タイプを自動的に検出するには、 Auto を選択します。
Maximum transmission unit (MTU)	このフィールドを使用して、ネットワーク・インターフェースでのパケットの最大サイズ (バイト単位) を指定します。 MTU 値を設定するには、テキスト・フィールドに目的の数値を入力します。イーサネットの場合、有効な MTU の範囲は、68 から 1,500 です。
Locally administered MAC address	このフィールドを使用して、この IMM サブシステムの物理アドレスを指定します。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 の間の 16 進値でなければなりません。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 の間の数値および A から F です。 IMM では、マルチキャスト・アドレスの使用は許可されません。マルチキャスト・アドレスは、最初のバイトの最下位ビットが 1 に設定されます。したがって、最初のバイトは偶数でなければなりません。

表 4. 「Advanced Ethernet Setup」 ページの設定 (続き)

設定	機能
Burned-in MAC address	組み込み MAC アドレスは、製造元によって IMM に割り当てられている固有な物理アドレスです。

IPv4 設定の構成

以下の設定は、「Network Interfaces」ページの「IPv4」エリアで変更することができます。

DHCP このフィールドを使用して、IMM サブシステムのイーサネット・ポート TCP/IP 設定を、ネットワーク上の動的ホスト構成プロトコル (DHCP) サーバーを使用して設定するかどうかを指定します。DHCP 構成を使用するには、「**Enabled - Obtain IP config. from DHCP server**」を選択します。TCP/IP 設定を手動で構成するには、「**Disabled - Use static IP configuration**」を選択します。DHCP サーバーを試行し、DHCP サーバーにアクセスできない場合には固定 IP 構成に戻るようにしたい場合は、「**Try DHCP server. If it fails, use static IP config**」を選択します。

IP 構成が DHCP サーバーによって割り当てられている場合は、リンク「**IP Configuration Assigned by DHCP server**」をクリックすると構成の詳細が表示されます。

注:

1. 「**Enabled - Obtain IP config. from DHCP server**」オプションを選択する場合、ネットワーク上にアクセス可能でアクティブな構成済み DHCP サーバーがなければなりません。
2. DHCP サーバーによって割り当てられた構成は、すべての固定 IP 設定をオーバーライドします。
3. 「**Try DHCP server. If it fails, use static IP config.**」オプションは、すべての IMM でサポートされているわけではありません。

Static IP Configuration

以下のフィールドには、このインターフェースの固定 IP 構成が含まれます。これらの設定は、DHCP が使用不可にされている場合にのみ使用されます。DHCP が使用可能にされている場合、DHCP サーバーによって割り当てられた動的 IP 構成がこれらの固定構成をオーバーライドします。

- **IP address:** このフィールドを使用して、このネットワーク・インターフェースを介してアクセスする IMM サブシステムの IP アドレスを定義します。IP アドレスを設定するには、テキスト・ボックスにアドレスを入力します。IP アドレスは、4 つの整数 (0 から 255) をピリオドで区切って指定し、スペースを含めてはなりません。

注: このフィールドのデフォルト値は 192.168.70.125 です。

- **Subnet mask:** このフィールドを使用して、IMM サブシステムが使用するサブネット・マスクを定義します。サブネット・マスクを設定するには、テキスト・ボックスにビット・マスクを入力します。サブネット・マスクは、4 つの整数 (0 から 255) をピリオドで区切って指定し、スパー

スを含めてはなりません。ビットは、左端のビットから順に連続して設定されます。例えば、0.255.0.0 は、無効なサブネット・マスクです。このフィールドは、0.0.0.0 および 255.255.255.255 に設定することはできません。

注: このフィールドのデフォルトは 255.255.255.0 です。

- **Gateway address:** このフィールドを使用して、デフォルト・ゲートウェイの IP アドレスを識別します。ゲートウェイ・アドレスを設定するには、テキスト・ボックスにアドレスを入力します。ゲートウェイ・アドレスは、4 つの整数 (0 から 255) をピリオドで区切って指定し、スペースや連続したピリオドを含めてはなりません。

注: このフィールドのデフォルトは 0.0.0.0 です。

IP Configuration Assigned by DHCP Server

このリンクをクリックすると、DHCP サーバーによって割り当てられた IP 構成が表示されます。次のイメージのような「IP Configuration Assigned by DHCP Server」ページが表示されます。

注: このオプションは、DHCP が使用可能に設定されている場合にのみ選択可能です。

IP Configuration Assigned by DHCP Server ?	
Host name	IMM-001A64E604D5
IP address	9.44.146.191
Gateway address	9.44.146.129
Subnet mask	255.255.255.128
Domain name	raleigh.ibm.com
DNS Server IP Addresses	
Primary	9.0.6.1
Secondary	9.0.7.1
Tertiary	N/A

IPv6 設定の構成

以下の設定は、「Network Interfaces」ページの「IPv6」エリアで変更することができます。

注: このセクションで記載されている IPv6 構成オプション (IPv6 固定構成、DHCPv6、またはステートレス自動構成) の少なくとも 1 つが使用可能に設定されている必要があります。

Link local address

リンク・ローカル・アドレスは、IMM に割り当てられた IPv6 アドレスです。リンク・ローカル・アドレスは、次の例のような形式で指定されます。

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

IPv6 Static Configuration

このフィールドを使用して、IPv6 の固定構成設定を使用可能または使用不可に設定します。「**IPv6 Static Configuration**」チェック・ボックスを選択すると、以下の項目が選択可能になります。

- **IP address:** このフィールドを使用して、このネットワーク・インターフェースを介してアクセスする IMM サブシステムの IPv6 アドレスを定義します。IP アドレスを設定するには、テキスト・ボックスに IPv6 アドレスを入力します。このフィールドの値は、有効な IPv6 アドレスでなければなりません。

注: このフィールドのデフォルトは 0::0 です。

- **Address prefix length (1 - 128):** このフィールドを使用して、固定 IPv6 アドレスの接頭部の長さを設定します。
- **Default route:** このフィールドを使用して、デフォルト経路の IPv6 アドレスを設定します。デフォルト経路を設定するには、対応するボックスに IPv6 アドレスを入力します。このフィールドの値は、有効な IPv6 アドレスでなければなりません。

注: このフィールドのデフォルト値は 0::0 です。

DHCPv6

このフィールドを使用して、DHCPv6 による IMM 構成の割り当てを使用可能または使用不可に設定します。

Stateless Auto-configuration

このフィールドを使用して、IMM のステートレス自動構成を使用可能または使用不可に設定します。

View Automatic Configuration (link)

DHCP サーバーによって割り当てられた IPv6 構成を表示するには、このリンクをクリックします。「IPv6 Automatic Configuration」ページが表示されます。

ネットワーク・プロトコルの構成

「Network Protocols」ページでは、以下の機能を実行できます。

- Simple Network Management Protocol (SNMP) を構成する
- ドメイン・ネーム・システム (DNS) を構成する
- Telnet プロトコルを構成する
- Simple Mail Transfer Protocol (SMTP) を構成する
- Lightweight Directory Access Protocol (LDAP) を構成する
- Service Location Protocol (SLP) を構成する

ネットワーク・プロトコル設定の変更を有効にするには、IMM を再始動する必要があります。複数のプロトコルを変更する場合は、すべてのプロトコル変更が行われて保存されてから、IMM を再始動してください。

SNMP の構成

SNMP エージェントを使用して情報の収集およびサーバーの制御を行うことができます。構成済みのホスト名または IP アドレスに SNMP アラートを送信するように IMM を構成することもできます。

注:

1. IMM は、SNMP アプリケーションで使用する 2 つの管理情報ベース (MIB) ファイルを提供します。MIB ファイルは、IMM ファームウェア更新パッケージに含まれています。
2. IMM は、SNMPv1 および SNMPv3 規格をサポートします。

SNMP を構成するには、次のステップを実行します。

1. SNMP を構成したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Network Protocols**」をクリックします。次の図のようなページが表示されます。

The screenshot shows the IBM Integrated Management Module (IMM) web interface. The left sidebar contains a navigation menu with the following items: System, Monitors, System Status, Virtual Light Path, Event Log, Vital Product Data, Tasks, Power/Restart, Remote Control, PXE Network Boot, Firmware Update, IMM Control, System Settings, Login Profiles, Alerts, Serial Port, Port Assignments, Network Interfaces, **Network Protocols** (selected), Security, Configuration File, Restore Defaults, and Restart IMM. The main content area is titled 'Simple Network Management Protocol (SNMP)'. It contains the following settings:

- SNMPv1 agent: Disabled
- SNMPv3 agent: Enabled
- SNMP traps: Disabled

Below these settings are two sections for configuring communities and users:

SNMPv1 Communities

Community Name	Access Type	Host Name or IP Address
	Get	1.
		2.
		3.
	Get	1.
		2.
		3.
	Get	1.
		2.
		3.

SNMPv3 Users

3. 「SNMPv1 agent」あるいは「SNMPv3 agent」フィールドで、「Enabled」を選択します。

注: SNMPv3 エージェントを使用可能にした場合、SNMPv3 マネージャーと SNMPv3 エージェントの間の対話が正常に機能するように、アクティブ・ログイン・プロファイルの SNMPv3 設定を構成する必要があります。これらの設定は、「Login Profiles」ページの各ログイン・プロファイル設定の下部で構成することができます (詳しくは、28 ページの『ログイン・プロファイルの作成』を参照)。構成するログイン・プロファイルのリンクをクリックし、ページの下部までスクロールして「**Configure SNMPv3 User**」チェック・ボックスをクリックします。

4. 「SNMP traps」フィールドで「Enabled」を選択して、ご使用のネットワーク上の SNMP コミュニティーにアラートを転送します。SNMP 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。

- システム連絡先が「System Settings」ページで指定されている必要があります。「System Settings」ページの設定については、22 ページの『システム情報の設定』を参照してください。
- システム・ロケーションが「System Settings」ページで指定されている必要があります。
- 少なくとも 1 つのコミュニティ名が指定されている必要があります。
- そのコミュニティについて少なくとも 1 つの有効な IP アドレスまたはホスト名 (DNS が使用可能な場合) が指定されている必要があります。

注: 通知方式が SNMP であるアラート受信者は、「SNMPv1 agent」あるいは「SNMPv3 agent」と、「SNMP traps」フィールドの両方が「Enabled」に設定されていない場合、アラートを受信しません。

5. 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、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。各コミュニティの定義は、以下のパラメーターで構成されます。

- Community Name
- Access Type
- IP address

これらのパラメーターが 1 つでも正しくないと、SNMP 管理アクセスは認可されません。

注: エラー・メッセージ・ウィンドウが開く場合は、エラー・ウィンドウにリストされるフィールドに必要な調整を行ってください。その後、ページの下部までスクロールし、「Save」をクリックして、訂正した情報を保管します。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。

6. 「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。
7. 「Access Type」フィールドで、アクセス・タイプを選択します。コミュニティ内のすべてのホストにトラップの受信を許可するには、「Trap」を選択します。コミュニティ内のすべてのホストにトラップの受信と MIB オブジェクトの照会を許可するには、「Get」を選択します。コミュニティ内のすべてのホストにトラップの受信、MIB オブジェクトの照会、および MIB オブジェクトの設定を許可するには、「Set」を選択します。
8. 対応する「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。
9. そのページの下部までスクロールして、「Save」をクリックします。
10. ナビゲーション・ペインで、「Restart IMM」をクリックして変更をアクティブにします。

DNS の構成

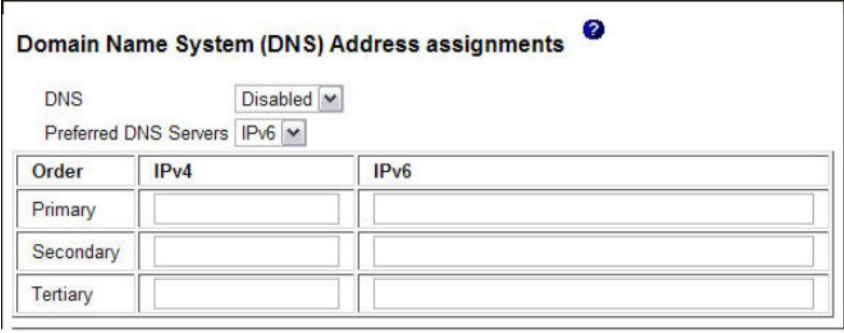
ドメイン・ネーム・システム (DNS) 設定を構成し、ホスト名から IP アドレスへの解決に使用する検索順序に追加の DNS サーバー・アドレスを組み込むかどうかを

指定します。DNS 検索は、常に使用可能に設定されており、DHCP 機能が有効にされている場合は、DHCP サーバーによって別の DNS アドレスが自動的に割り当てられます。

追加の DNS アドレスを使用可能にするには、そのうちの少なくとも 1 つがゼロ以外の値でなければなりません。追加の DNS サーバーは検索リストの最上部に追加されるため、ホスト名検索は、DHCP サーバーによって自動的に割り当てられた DNS サーバー上で行われる前に、追加されたこれらのサーバー上で行われます。

DNS を構成するには、以下のステップを実行します。

1. DNS を構成したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Network Protocols**」をクリックし、ページの「**Domain Name System (DNS) Address assignments**」エリアまでスクロールダウンします。次の図に示すようなページのセクションが表示されます。



Order	IPv4	IPv6
Primary		
Secondary		
Tertiary		

3. ご使用のネットワークで DNS サーバー（複数の場合あり）が利用可能な場合、「**DNS**」フィールドで「**Enabled**」を選択します。「**DNS**」フィールドでは、ご使用のネットワーク上で DNS サーバーを使用してホスト名を IP アドレスに変換するかどうかを指定します。
4. IPv4 および IPv6 DNS サーバー・アドレスがある場合は、「**Preferred DNS Servers**」リストで「**IPv4**」または「**IPv6**」を選択し、どのサーバー・アドレスを優先するかを指定します。
5. DNS を使用可能にした場合、「Primary, Secondary, and Tertiary」テキスト・フィールドを使用して、ネットワーク上にある最大 6 個の DNS サーバーの IP アドレスを指定します。3 つの IPv4 DNS サーバー・アドレスまたは 3 つの IPv6 DNS サーバー・アドレスを設定するには、該当するテキスト・フィールドにアドレスを入力します。IPv4 または IPv6 アドレスが有効な形式で指定されていることを確認します。
6. そのページの下部までスクロールして、「**Save**」をクリックします。
7. ナビゲーション・ペインで、「**Restart IMM**」をクリックして変更をアクティブにします。

Telnet の構成

Telnet を構成するには、次のステップを実行します。

1. Telnet を構成したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。

2. ナビゲーション・ペインで、「**Network Protocols**」をクリックし、このページの「**Telnet Protocol**」エリアまでスクロールダウンします。最大数の同時 Telnet ユーザーを設定することができます。あるいは、Telnet アクセスを使用不可にすることもできます。
3. そのページの下部までスクロールして、「**Save**」をクリックします。
4. ナビゲーション・ペインで、「**Restart IMM**」をクリックして変更をアクティブにします。

SMTP の構成

Simple Mail Transfer Protocol (SMTP) サーバーの IP アドレスまたはホスト名を指定するには、以下のステップを実行します。

1. SMTP を構成したい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Network Protocols**」をクリックし、このページの「**SMTP**」エリアまでスクロールダウンします。
3. 「**SMTP server host name or IP address**」フィールドに、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。
4. そのページの下部までスクロールして、「**Save**」をクリックします。
5. ナビゲーション・ペインで、「**Restart IMM**」をクリックして変更をアクティブにします。

LDAP の構成

Lightweight Directory Access Protocol (LDAP) サーバーを使用すると、IMM 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。その後、IMM 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。そのためには、IMM が LDAP クライアントをサポートしている必要があります。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 IMM 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、IMM 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 IMM に関連付けられている少なくとも 1 つのグループに属している場合にのみ、グループ認証にパスします。

以下の 2 つの LDAP サーバーの構成については、このセクションで説明しています。

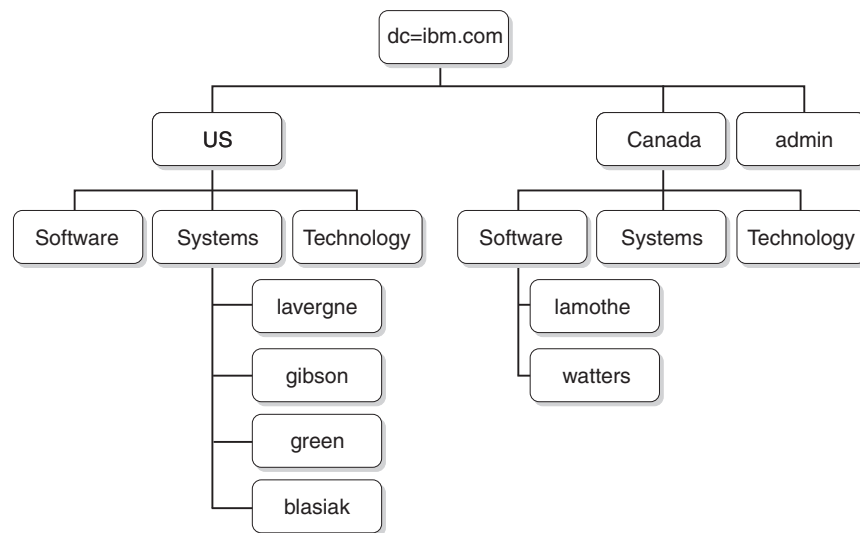
- Novell eDirectory バージョン 8.7.1
- Microsoft Windows Server 2003 Active Directory

ユーザー・スキーマの例

このセクションでは、単純なユーザー・スキーマの例について説明しています。このスキーマ例は、LDAP クライアントと LDAP サーバーの両方の構成を説明するために、本書全体で使用されます。

このユーザー・スキーマの例は、ibm.com と呼ばれるドメイン・コンポーネントがルートになっています。つまり、このツリー内のすべてのオブジェクトが、dc=ibm,dc=com というルート識別名を持っています。ここでは、このツリーは、ユーザーとユーザー・グループを国および組織に基づいて分類したい会社を表していると仮定します。階層は、ルート → 国 → 組織 → 人です。

次の図は、本書で使用されるスキーマを単純化したビューを示しています。ルートの直下にあるユーザー・アカウント (userid=admin) の用途に注目してください。このユーザー・アカウントは、管理者です。



次の図は、ユーザー・グループの追加を示しています。6 個のユーザー・グループが定義されており、最初のレベルに追加されています。また、別のユーザー・グループが国「Canada」の「Software」組織に追加されています。

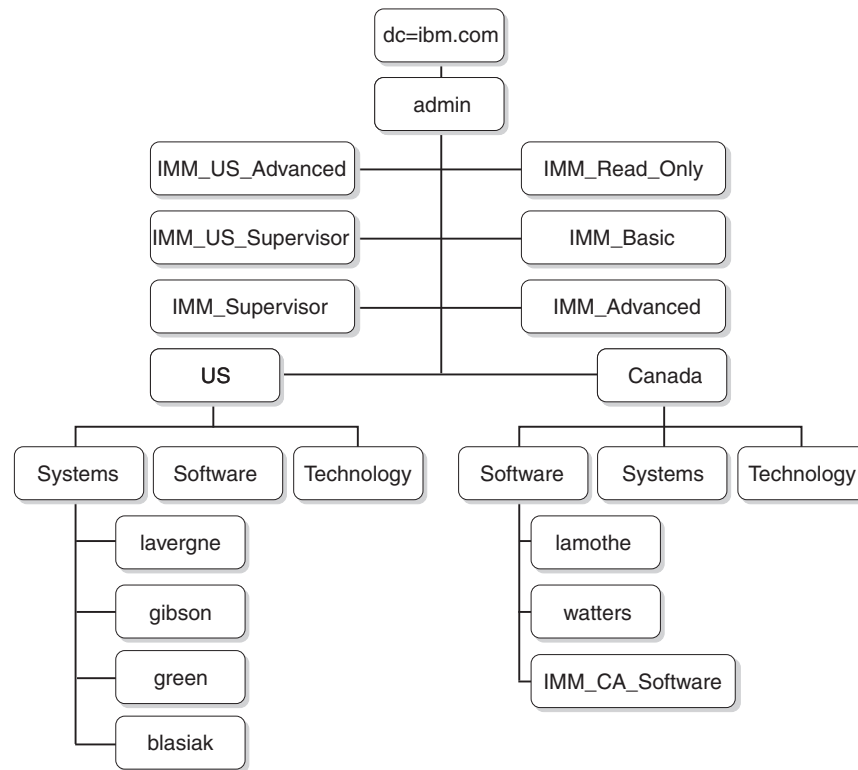


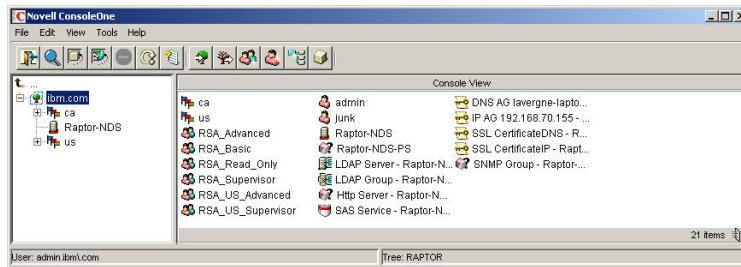
表 5 のユーザーおよび関連するユーザー・グループは、スキーマを完成するために使用されます。

表 5. ユーザーからグループへのマッピング

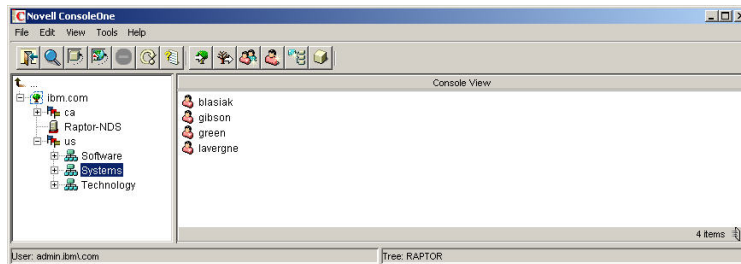
ユーザー識別名	グループ・メンバーシップ
cn=lavergne, o=Systems, c=us, dc=ibm.com	cn=IMM_Supervisor, dc=ibm.com cn=IMM_US_Supervisor, dc=ibm.com
cn=blasiak, o=Systems, c=us, dc=ibm.com	cn=IMM_US_Advanced, dc=ibm.com
cn=gibson, o=Systems, c=us, dc=ibm.com	cn=IMM_Basic, dc=ibm.com
cn=green, o=Systems, c=us, dc=ibm.com	cn=IMM_Read_Only, dc=ibm.com
cn=watters, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com
cn=lamothe, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com

Novell eDirectory スキーマ・ビュー

Novell ConsoleOne ツールを使用すると、52 ページの『ユーザー・スキーマの例』で示されているスキーマが Novell eDirectory に取り込まれます。次の図は、ConsoleOne ツールで表示されるスキーマの最上位ビューを示しています。



次の図は、o=Systems、c=us、dc=ibm.com のユーザーを示しています。



グループ・メンバーシップ

Novell eDirectory は、**GroupMembership** と呼ばれる属性を使用して、ユーザーがメンバーとして属するグループを識別します。ユーザー・オブジェクト・クラスは、特にこの属性を使用します。LDAP クライアントは、ユーザーがメンバーとして属するグループを照会する場合、LDAP サーバーに対する検索要求で **memberOf** のデフォルト値を使用します。

以下のいずれかの方法を使用して、メンバーシップ照会を行うために LDAP クライアントを構成することができます。

- LDAP クライアント上で、「**Group Search Attribute**」フィールドの値 **GroupMembership** を構成する。
- Novell eDirectory LDAP サーバー上で、**GroupMembership** と **memberOf** の間の属性マッピングを作成する。

LDAP クライアント上のデフォルト属性を構成するには、以下のステップを実行します。

1. IMM Web インターフェースの左側のナビゲーション・ペインで、「**Network Protocols**」をクリックします。
2. 「**LDAP Search Attributes**」エリアまでスクロールします。
3. 「**Group Search Attribute**」フィールドで、目的のデフォルト属性を入力します。

「**Group Search Attribute**」フィールドがブランクの場合、デフォルトの **memberOf** に設定されます。その場合、Novell eDirectory サーバーを構成して、属性 **GroupMembership** を **memberOf** にマップする必要があります。Novell eDirectory サーバーを構成して、属性 **GroupMembership** を **memberOf** にマップするには、以下のステップを実行します。

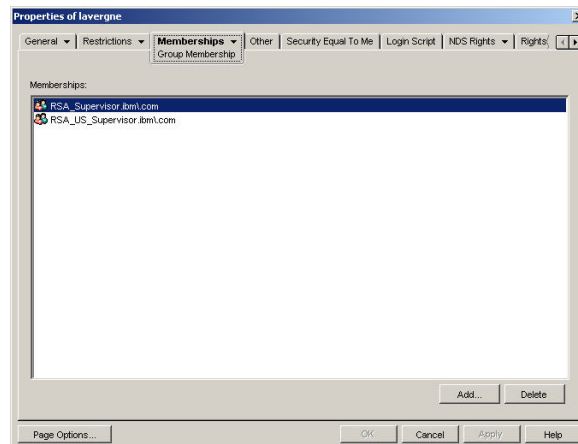
1. ConsoleOne ツールを使用して、「**LDAP Group**」アイコンを右クリックし、「**Properties**」をクリックします。「Properties of LDAP Group」ウィンドウが開きます。
2. 「**Attribute Mappings**」タブをクリックします。
3. 「**Add**」をクリックし、**Group Membership** と **memberOf** の間のマッピングを作成します。
4. 「**OK**」をクリックします。LDAP グループのプロパティを示すページが開きます。

ユーザー・グループへのユーザーの追加

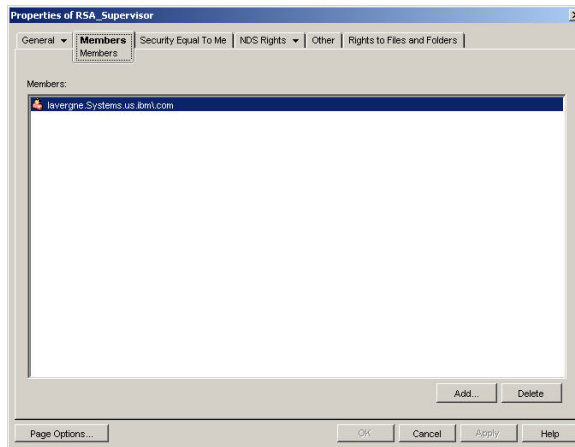
グループをユーザーのプロファイルに追加するか、あるいはユーザーをグループのプロファイルに追加することで、ユーザーを適切なユーザー・グループに追加することができます。最終的な結果は同じです。

例えば、上記のユーザー・スキーマの例では、ユーザー **lavergne** は、**IMM_US_Supervisor** と **IMM_Supervisor** の両方のメンバーです。Novell ConsoleOne などのブラウザー・ツールを使用して、スキーマを確認することができます (ユーザー **lavergne** をダブルクリックして「**メンバーシップ**」タブを選択)。

次の図のようなページが開きます。



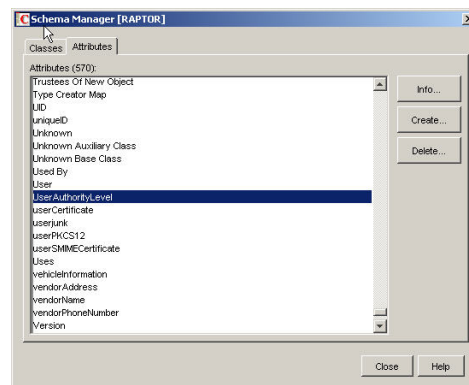
同様に、**IMM_Supervisor** グループのプロパティが表示され、「**メンバー**」タブをクリックすると、次の図のいずれかと同様のページが開きます。



権限レベル

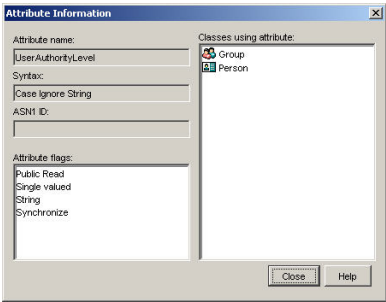
権限レベル機能を使用するには、ConsoleOne を使用して Novell eDirectory 上で **UserAuthorityLevel** とラベル付けした新規属性を作成します。この新規属性は、権限レベルをサポートするために使用されます。

1. Novell ConsoleOne ツールで、「ツール」 > 「スキーママネージャ」をクリックします。
2. 「属性」タブをクリックし、「作成」をクリックします。
3. 属性に **UserAuthorityLevel** とラベル付けします。「ASN1 ID」をブランクのまま残すか、LDAP 管理者に確認し、使用する値を判別します。「次へ」をクリックします。
4. 構文を「Case Ignore String」に設定します。「次へ」をクリックします。
5. フラグを適用可能として設定します。LDAP 管理者に、これらの設定が正しいことを確認します。「公開読み込み」チェック・ボックスをクリックし、「次へ」をクリックします。
6. 「完了」をクリックします。次の図のようなページが開きます。



7. 「スキーママネージャ」ウィンドウに戻り、「クラス」タブをクリックします。
8. 「個人」クラスをクリックし、「追加」をクリックします。代わりに、ユーザー・オブジェクト・クラスを使用することもできます。

- 9. 「**UserAuthorityLevel**」属性までスクロールダウンして選択し、このクラスの属性に追加します。「**OK**」をクリックします。
- 10. 「**グループ**」クラスをクリックし、「**追加**」をクリックします。
- 11. 「**UserAuthorityLevel**」属性までスクロールダウンして選択し、このクラスの属性に追加します。「**OK**」をクリックします。
- 12. 属性が正常にクラスに追加されたことを確認するには、「スキーママネージャ」ウィンドウで「**属性**」クラスを選択します。
- 13. 「**UserAuthorityLevel**」属性までスクロールし、「**情報**」をクリックします。次の図のようなページが開きます。



権限レベルの設定

このセクションでは、UserAuthorityLevel 属性をどのように解釈および使用するかを説明します。 UserAuthorityLevel 属性に割り当てられた値によって、正常に認証されたユーザーに割り当てられる権限 (または権限レベル) が決定されます。

UserAuthorityLevel 属性は、ビット・ストリング (0 と 1 から構成) として読み取られます。ビットは、左から順に番号付けされています。最初のビットは、ビット位置 0 です。2 番目のビットは、ビット位置 1 です (以下同様)。

次の表は、各ビット位置について説明しています。

表 6. 許可ビット

ビット位置	機能	説明
0	常に拒否	これが設定されている場合、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	これが設定されている場合、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 6. 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	これが設定されている場合、ユーザーは読み取り専用アクセス権を持ち、保守手順 (再始動、リモート・アクション、ファームウェア更新など) を実行することはできません。保存、消去、あるいは復元機能を使用して変更することはできません。ビット位置 2 と他のすべてのビットは相互に排他的で、ビット位置 2 の優先順位が最下位です。他のいずれかのビットが設定されている場合、このビットは無視されます。
3	ネットワーキングおよびセキュリティ	これが設定されている場合、ユーザーは、「Security」、「Network Protocols」、「Network Interface」、「Port Assignments」、「Serial Port」の各パネルで構成を変更できます。
4	ユーザー・アカウント管理	これが設定されている場合、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」パネルで「Global Login Settings」を変更できます。
5	リモート・コンソール・アクセス権	これが設定されている場合、ユーザーは、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、「Serial Port」パネルで構成を変更できます。
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	これが設定されている場合、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。また、ユーザーは、「Serial Port」パネルで構成を変更できます。
7	リモート・サーバーの電源/再始動アクセス権	これが設定されている場合、ユーザーは、リモート・サーバーの電源オン、再始動、およびサーバー・タイムアウト機能にアクセスできます。
8	アダプターの基本構成	これが設定されている場合、ユーザーは、「System Settings」および「Alerts」ページで構成パラメーター (Contact、Location、および Server Timeout を除く) を変更できます。

表 6. 許可ビット (続き)

ビット位置	機能	説明
9	イベント・ログを消去する権限	これが設定されている場合、ユーザーはイベント・ログを消去できます。 注: すべてのユーザーがイベント・ログを表示できますが、ログを消去するには、ユーザーにこのレベルの権限が必要です。
10	アダプターの拡張構成	これが設定されている場合、ユーザーは、アダプターの構成時に制限はなく、IMM に対する管理アクセス権限を持っています。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、アダプター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、およびアダプター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。サーバーの電源/再始動の制御およびタイムアウト機能は除きます。
11	予約済み	このビット位置は、将来の使用のために予約済みです (現行では無視されます)。
注: - ビットが使用されない場合、デフォルトでは、ユーザーに対して「読み取り専用」を設定します。 - 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。ユーザー・レコードの「Login Permission Attribute」フィールドに名前が含まれていない場合、ユーザーが属しており、グループ・フィルターに一致するグループから権限の取得が試行されます。この場合、ユーザーには、すべてのグループのすべてのビットの包含 OR が割り当てられます。 - いずれかのグループに「常に拒否」(ビット位置 0) ビットが設定されている場合、ユーザーはアクセスを拒否されます。「常に拒否」ビットは、すべてのビットに対して優先されます。 - ユーザーに基本、ネットワーキング、またはセキュリティ関連のアダプター構成パラメーターを変更する権限がある場合、そのユーザーに IMM を再始動する権限 (ビット位置 10) を付与することを検討してください。この権限がない場合、ユーザーはパラメーターの変更はできる場合がありますが、そのパラメーターは有効になりません。		

次の表には、例およびその説明が示されています。

表 7. UserLevelAuthority 属性の例と説明

UserLevelAuthority 属性の例	説明
IBMRBSPermissions=010000000000	スーパーバイザー・アクセス権 (ビット位置 1 を設定)

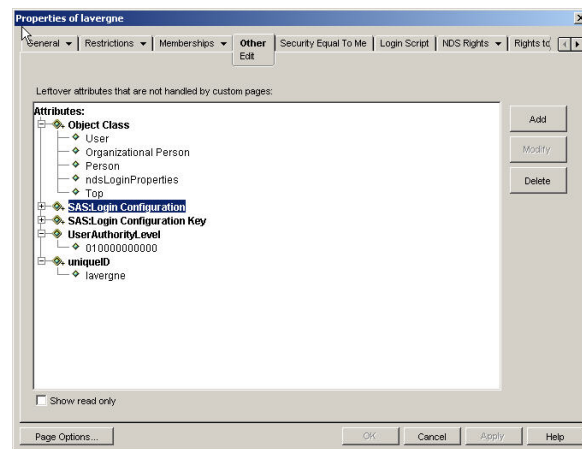
表 7. UserLevelAuthority 属性の例と説明 (続き)

UserLevelAuthority 属性の例	説明
IBMRBSPermissions=001000000000	読み取り専用アクセス権 (ビット位置 2 を設定)
IBMRBSPermissions=100000000000	アクセス権なし (ビット位置 0 を設定)
IBMRBSPermissions=000011111100	アダプターの拡張構成を除くすべての権限
IBMRBSPermissions=000011011110	仮想メディアへのアクセスを除くすべての権限

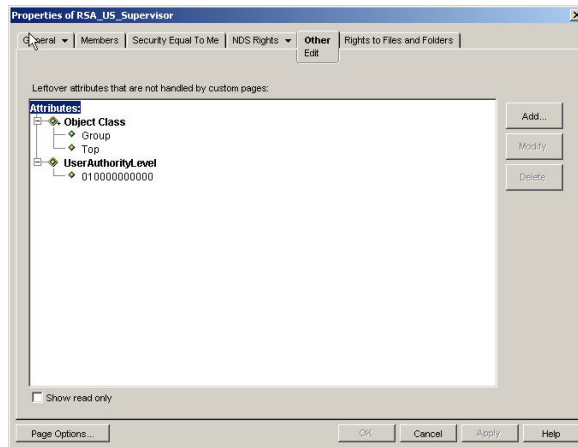
ユーザー *lavergne* および各ユーザー・グループに UserAuthorityLevel 属性を追加するには、以下のステップを実行します。

1. **lavergne** を右クリックし、「プロパティ」をクリックします。
2. 「その他」タブをクリックします。「追加」をクリックします。
3. 「UserAuthorityAttribute」までスクロールダウンし、「OK」をクリックします。
4. 属性に指定したい値を入力します。例えば、スーパーバイザー・アクセス権を割り当てたい場合は、属性に **IBMRBSPermissions=010000000000** を設定します。「OK」をクリックします。
5. 各ユーザー・グループに対してステップ 1 から 4 を繰り返し、適切に **UserAuthorityLevel** を設定します。

次の図は、ユーザー *lavergne* のプロパティを示しています。



次の図は、IMM_US_Supervisor のプロパティを示しています。



次の表は、ユーザー・スキーマの例の各ユーザー・グループに割り当てられた **UserAuthorityLevel** を示しています。

表 8. ユーザー・グループに割り当てられた *UserAuthorityLevel*

ユーザー・グループ	UserAuthorityLevel	変換
IMM_Basic	IBMRBSPermissions=000100000000	ネットワーキングおよびセキュリティ
IMM_CA_Software	IBMRBSPermissions=000101111010	ネットワーキングおよびセキュリティ リモート・コンソールおよび仮想メディアのアクセス権 リモート・サーバーの電源および再始動のアクセス権 アダプターの基本構成 アダプターの拡張構成
IMM_Advanced	IBMRBSPermissions=000110111100	ネットワーキングおよびセキュリティ リモート・コンソールおよび仮想メディアのアクセス権 リモート・サーバーの電源および再始動のアクセス権 アダプターの基本構成 アダプターの拡張構成 イベント・ログを消去する権限
IMM_Supervisor	IBMRBSPermissions=010000000000	スーパーバイザー・アクセス権
IMM_Read_Only	IBMRBSPermissions=001000000000	読み取り専用アクセス権

表 8. ユーザー・グループに割り当てられた *UserAuthorityLevel* (続き)

ユーザー・グループ	UserAuthorityLevel	変換
IMM_US_Advanced	IBMRBSPermissions=000110111100	ネットワーキングおよびセキュリティ ユーザー・アカウント管理 リモート・コンソールおよび 仮想メディアのアクセス権 リモート・サーバーの電源お よび再始動のアクセス権 アダプターの基本構成 イベント・ログを消去する権 限
IMM_US_Supervisor	IBMRBSPermissions=010000000000	スーパーバイザー・アクセス 権

LDAP サーバーの参照

IMM 上の LDAP クライアントから LDAP サーバーへの接続を試行する前に、任意のサード・パーティー LDAP ブラウザーを使用して、LDAP サーバーに接続します。例えば、<http://www.ldapbrowser.com> からディレクトリー参照ツールを入手することができます。

IMM の LDAP クライアントを使用する前に LDAP ブラウザーを使用することで、以下の利点があります。

- さまざまな資格情報を使用してサーバーにバインドすることが可能。これにより、LDAP サーバー上のユーザー・アカウントが正しくセットアップされているかを確認できます。ブラウザーを使用してサーバーにバインドできるにも関わらず、IMM の LDAP クライアントを使用してサーバーにバインドできない場合は、LDAP クライアントが誤って構成されています。ブラウザーを使用してバインドできない場合は、IMM 上の LDAP クライアントを使用してバインドすることもできません。
- サーバーへのバインドが正常に完了すると、LDAP サーバー・データベースにナビゲートすることができ、検索照会を迅速に発行することが可能になります。これにより、さまざまなオブジェクトへのアクセスに対して、LDAP サーバーが意図したように構成されているかを確認できます。例えば、特定の属性を表示することができない、あるいは特定の検索要求で表示されると予期していたオブジェクトがすべて表示されない場合があります。これは、オブジェクトに割り当てられた権限 (例えば、一般に表示されるか非表示か) が正しく構成されていないことを示します。LDAP サーバーの管理者に連絡して、問題を修正します。バインドに使用する資格情報によって、サーバー上でユーザーが持つ特権が決定されることに注意することが重要です。
- すべてのユーザーのグループ・メンバーシップを検証します。ユーザーおよびユーザー・グループに割り当てられた **UserAuthorityLevel** 属性を検証します。

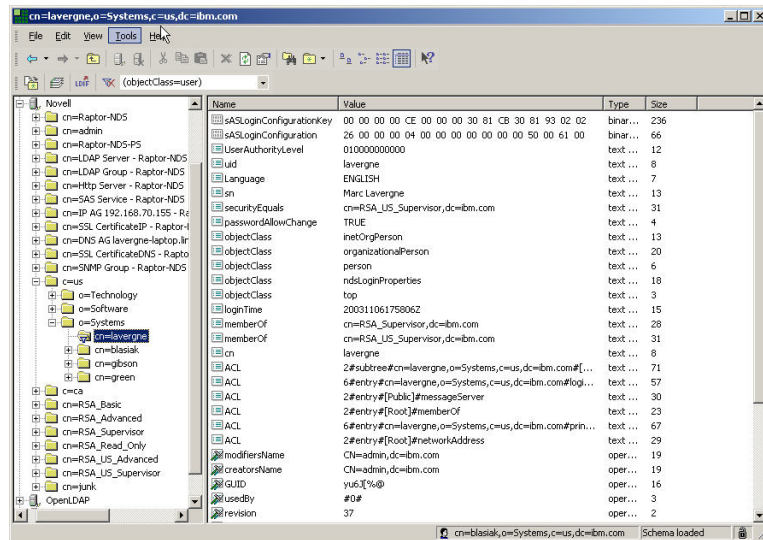
次の図は、52 ページの『ユーザー・スキーマの例』を使用して構成された Novell eDirectory サーバーに対して行われた、さまざまな照会と検索結果を示しています。このケースでは、Softerra LDAP ブラウザー・ツールが使用されました。サーバーへの初回バインドは、図に示されているプロパティおよび資格情報を使用して行

われました。

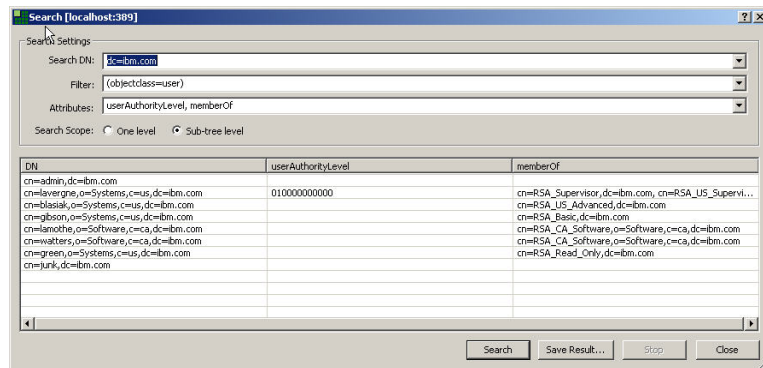
The 'Server Properties' dialog box is shown with the 'General' tab selected. The 'Server Monitor' section is active, and the 'Novell' icon is displayed. The 'Host' field contains 'localhost', the 'Port' is '389', and the 'Protocol version' is set to '3'. The 'Base' field contains 'dc=ibm.com'. The 'Type' is 'Novell NDS' and the 'URL' is 'ldap://localhost:389/dc=ibm.com??base?(objectClass=)'. The 'Entry Properties' section is also visible, showing 'LDAP Settings'.

The 'Server Properties' dialog box is shown with the 'Credentials' tab selected. The 'User DN' field contains 'cn=blasiak,o=Systems,c=us,dc=ibm.com'. The 'Password' and 'Confirm' fields are masked with 'xxxxxxx'. The 'Save password' checkbox is checked, and the 'Anonymous bind' checkbox is unchecked. The 'Server Monitor' section is also visible, showing 'LDAP Settings'.

初回バインドが成功した後、Novell eDirectory 上のスキーマが次のように表示されます。



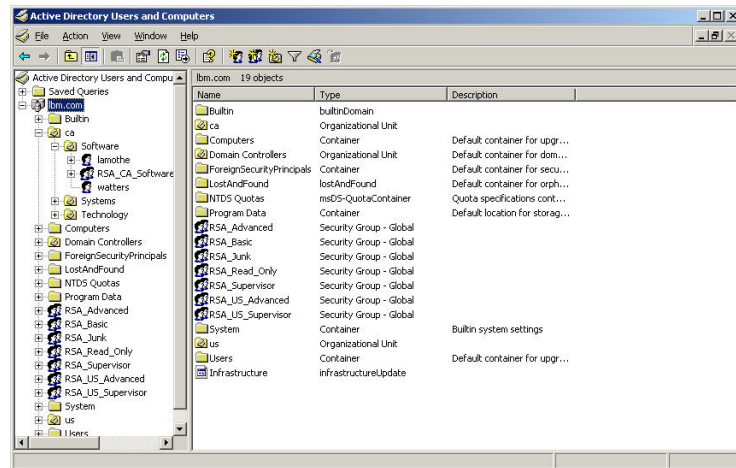
次の図は、**userAuthorityLevel** および **memberOf** 属性を検索する要求を使用した場合の、すべてのユーザーの照会を示しています。



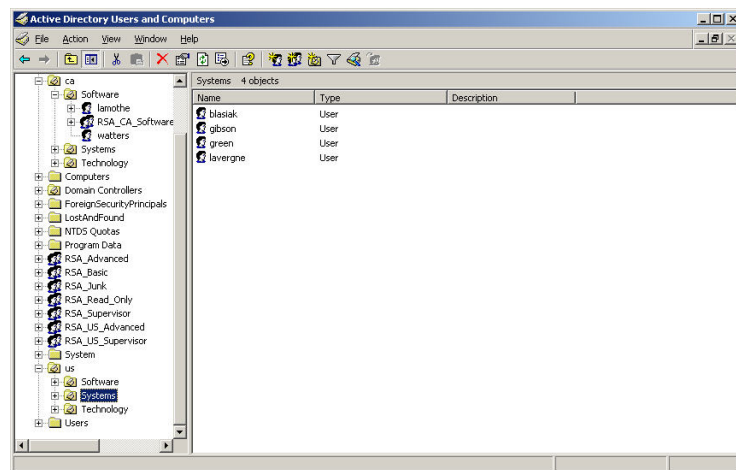
Microsoft Windows Server 2003 Active Directory スキーマ・ビュー

このセクションでは、Microsoft Windows Server 2003 Active Directory 上での、52 ページの『ユーザー・スキーマの例』の情報の収集に関連する構成の状況をいくつか説明します。

次の図は、「Active Directory ユーザーとコンピュータ」管理ツールで表示されるスキーマの最上位ビューを示しています。



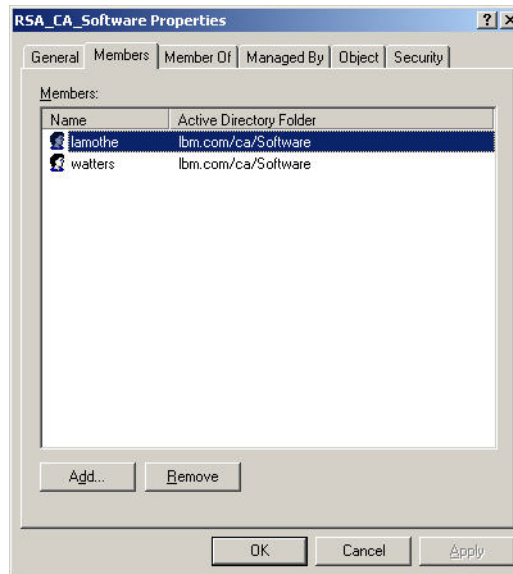
次の図は、ou=Systems、ou=us、dc=ibm、dc=com でのユーザーを示しています。



ユーザー・グループへのユーザーの追加

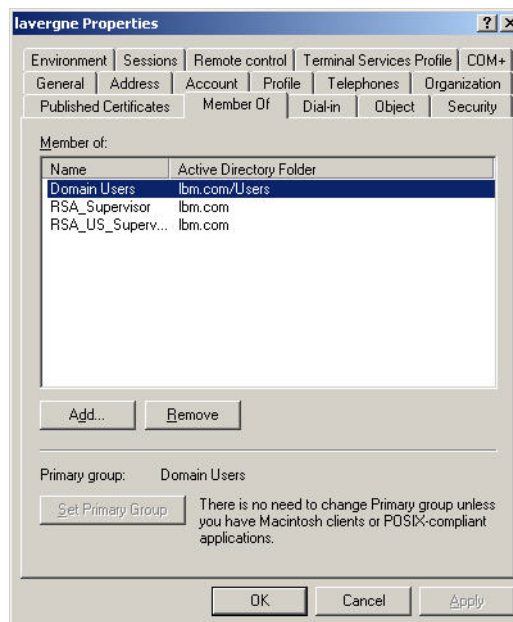
Active Directory では、特定のユーザーにグループを追加したり、特定のグループにユーザーを追加したりすることができます。ユーザーまたはユーザー・グループ・オブジェクトを右クリックし、「**Properties**」をクリックします。

ユーザー・グループを選択して「メンバ」タブをクリックすると、次の図のいずれかと同様のページが開きます。



ユーザー・グループのユーザーを追加あるいは削除するには、「追加」あるいは「削除」をクリックします。

ユーザーを選択して「所属するグループ」タブをクリックすると、次の図のいずれかと同様のページが開きます。

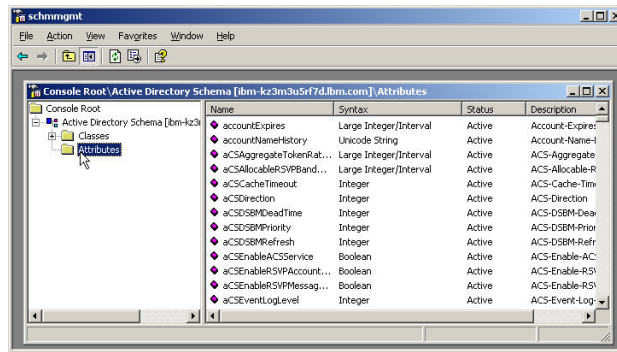


ユーザー・グループのユーザーを追加あるいは削除するには、「追加」あるいは「削除」をクリックします。

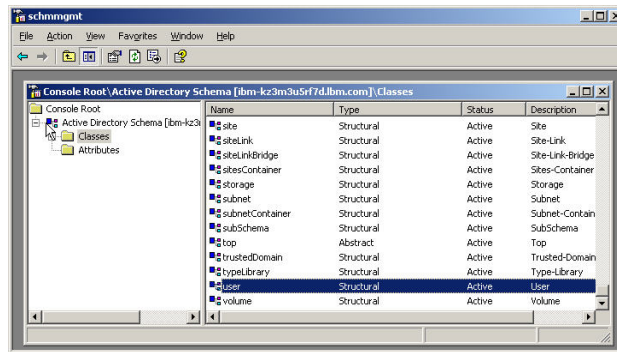
権限レベル

セクション 56 ページの『権限レベル』では、Novell eDirectory サーバーを使用して、権限レベルの概念をサポートするための新規属性を作成する方法、および IMM から LDAP サーバーに対して認証するユーザーにその属性を割り当てる方法を説明しています。作成された属性は、**UserAuthorityLevel** と呼ばれていました。このセクションでは、この属性を Active Directory 上で作成します。

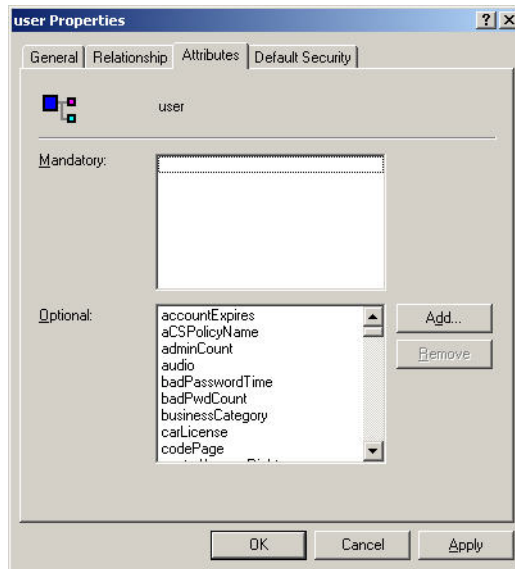
1. Active Directory スキーマのスナップイン・ツールをインストールします。詳しくは、Active Directory に付属の資料を参照してください。
2. Active Directory スキーマを開始します。
3. 「アクション」 > 「属性の作成」をクリックします。以下のフィールドに入力します。
 - a. 共通名を **UserAuthorityLevel** に設定します
 - b. 構文を **Case Insensitive String** に設定します
 - c. 最小および最大を **12** に設定します
4. 新規の X.500 OID を割り当てる場合は、システム管理者に連絡してください。
新規の X.500 OID を定義しない場合は、権限レベルに対して新規属性を作成する代わりに既存の属性を使用します。



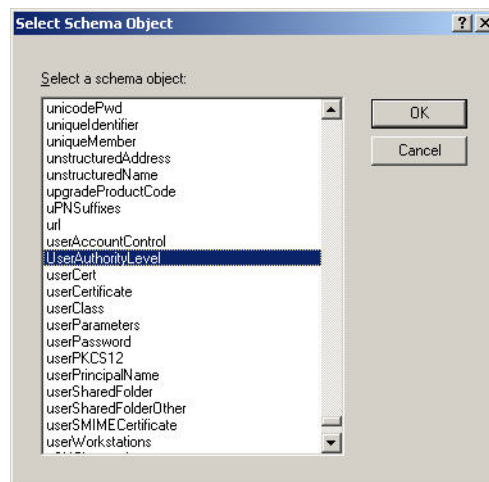
5. 属性を保存した後、「Classes」フォルダーを選択します。



6. クラス **user** をダブルクリックします。ユーザーの「プロパティ」ウィンドウが開きます。

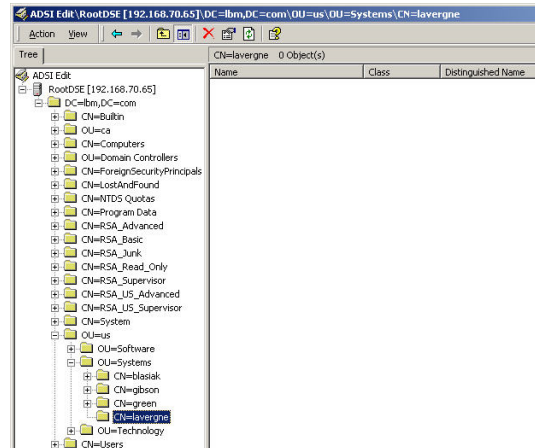


7. 「属性」タブを選択し、「追加」をクリックします。「スキーマ オブジェクトの選択」ウィンドウが開きます。

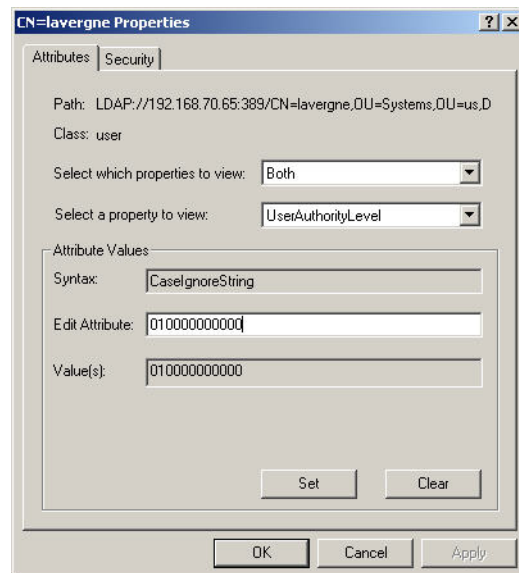


8. 「**UserAuthorityLevel**」までスクロールダウンし、「**OK**」をクリックします。この属性は、ユーザー・オブジェクト・クラスのオプションの属性のリストに表示されます。
9. クラス groups に対して、ステップ 6 (67 ページ) からステップ 8 を繰り返します。これにより、**UserAuthorityLevel** 属性をユーザーあるいはユーザー・グループに割り当てることが可能になります。この新規属性を使用する必要があるのは、この 2 つのオブジェクト・クラスのみです。
10. **UserAuthorityLevel** 属性を適切なユーザーおよびユーザー・グループに割り当てます。Novell eDirectory サーバーで定義されたスキーマと一致させるには、57 ページの『権限レベルの設定』と同じ値を使用します。ADSI Edit ツールを使用して、これを行うことができます。Microsoft ADSI Edit サポート・ツールは、ディレクトリー内のすべてのオブジェクト (スキーマおよび構成情報など) の表示、オブジェクトの変更、オブジェクト上のアクセス制御リストの設定を行うために使用する Microsoft 管理コンソール (MMC) スナップインです。

11. この例では、**UserAuthorityLevel** 属性をユーザー **lavergne** に追加すると仮定します。ADSI Edit を使用して、これを行います。Active Directory に接続するには、適切な資格情報を提供する必要があります。そうしない場合、サーバー上のオブジェクトを変更するための適切なユーザー特権が付与されない可能性があります。次の図は、サーバーに接続した後に ADSI によって表示されるスキーマを示しています。



12. **lavergne** を右クリックし、「プロパティ」をクリックします。次の図のようなウィンドウが開きます。



13. 「表示するプロパティのセットを選択」フィールドで、「**UserAuthorityLevel**」を選択します。
14. 「属性の編集」フィールドで、**IBMRBSPermissions=010000000000** を入力します。これにより、スーパーバイザー・アクセス権に変換されます。「設定」をクリックします。
15. 「**OK**」をクリックします。
16. 変更したいユーザー・グループ・オブジェクトに対して同じステップを実行することで、この属性をユーザー・グループに追加することができます。

Active Directory 構成の検査

LDAP クライアントを (ユーザーの認証のために) Active Directory に接続する前に、LDAP ブラウザーを使用して Active Directory スキーマを参照します。少なくとも以下の表にリストされた照会を発行し、権限レベルとグループ・メンバーシップを検査します。

表 9. 権限レベルとグループ・メンバーシップの検査

検索識別名	フィルター	属性
DC=ibm、DC=com	(objectclass=user)	memberOf、userAuthorityLevel
DC=ibm、DC=com	(objectclass=group)	member、userAuthorityLevel

LDAP クライアントの構成

LDAP を構成して、マネージメント・モジュールのユーザーを認証することができます。IMM は、ローカルおよびリモート両方のユーザー認証をサポートします。ローカル認証では、「Login Profiles」ページで提供される情報を使用してユーザーを認証します。LDAP サーバーを使用すると、マネージメント・モジュールはローカルのユーザー・データベースではなく、リモート LDAP サーバー上の LDAP ディレクトリーを照会あるいは検索してユーザーを認証することができます。

不特定型リモート認証が使用されている場合、ローカルで、あるいはリモート認証に使用される LDAP サーバー上に保管されている情報に基づいて正常に認証されたユーザーごとに、権限を持つことを選択できます。ユーザーに許可された権限により、各ユーザーが IMM にログインしている間に実行することができるアクションを指定します。リモート認証方式については、以下のトピックで説明しています。

- ローカル権限付きの Active Directory 認証
- Active Directory の役割ベースの認証および許可
- 従来の LDAP 認証および許可

ローカル権限付きの Active Directory 認証

Active Directory を使用して、ユーザーのリモート LDAP 認証 (ローカル・ユーザー権限付き) をセットアップすることができます。

注: ローカル権限付きの Active Directory 認証は、Active Directory 環境内で使用されるサーバーにのみ適用されます。

ローカル権限付きの Active Directory 認証を使用する場合、Active Directory サーバーはユーザーの認証、ユーザーの資格情報の検証にのみ使用されます。任意のユーザーの権限情報は、Active Directory サーバーには保管されていません。IMM に保管されるグループ・プロファイルは、権限情報を持つように構成される必要があります。グループ・プロファイルの構成に使用される権限情報は、Active Directory サーバーからユーザーのメンバーシップ情報を取得することで入手可能です。このメンバーシップ情報は、ユーザーが属しているグループのリストを提供します (ネスト・グループがサポートされます)。次に、Active Directory サーバーで指定されたグループが、IMM 上のローカルで構成されたグループ名と比較されます。ユーザーがメンバーとして属している各グループごとに、ユーザーはそのグループから権限を割り当てられます。IMM 上でローカルに構成された各グループ名ごとに、そのグループ用に構成された対応する権限プロファイルがあります。

IMM は、ローカルで構成されたグループ名を最大 16 個サポートします。各グループ名の長さは、63 文字が上限です。Active Directory サーバーから取得したグループ・メンバーシップ情報と一致させるため、以下の属性のうち 1 つをグループ名として構成する必要があります。

- 識別名 (DN)
- 「cn」属性
- 「名前」属性
- 「sAMAccountName」属性

IMM にローカル権限付きの Active Directory 認証を構成するには、次のステップを実行してください。

1. ナビゲーション・ペインで、「**Network Protocols**」をクリックします。
2. 「**Lightweight Directory Access Protocol (LDAP) Client**」セクションまでスクロールダウンします。
3. 「**Use LDAP Servers for Authentication Only (with local authorization)**」を選択します。
4. ドメイン・コントローラーを手動で構成したり動的に検出するには、以下の選択項目から 1 つを選択します。
 - 「**Use DNS to find LDAP Servers**」を選択し、DNS SVR レコードに基づいてドメイン・コントローラーを動的に検出します。
 - 「**Use Pre-Configured LDAP Servers**」(デフォルトの選択)を選択し、ドメイン・コントローラーを手動で構成します。
5. DNS を使用してドメイン・コントローラーを動的に検出する場合は、以下の設定を構成してから、ステップ 7 (72 ページ) に進んでください。

注: DNS を使用してドメイン・コントローラーを動的に検出している場合は、ドメイン・コントローラーの完全修飾ドメイン・ネームを指定する必要があります。

- Search Domain
 - 「**Search Domain**」フィールドにドメイン・コントローラーのドメイン・ネームを入力します。
- Active Directory Forest Name
 - このオプション・フィールドは、グローバル・カタログの検出に使用されます。グローバル・カタログは、ドメイン間で共通のグループに所属しているユーザーに必要です。ドメイン間グループ・メンバーシップが適用されない環境では、このフィールドはブランクのままにしておきます。

次の図は、DNS を使用してドメイン・コントローラーを動的に検出している場合の「LDAP Client」ウィンドウを示しています。

Lightweight Directory Access Protocol (LDAP) Client ?

☐ Use LDAP Servers for Authentication and Authorization

☒ Use LDAP Servers for Authentication Only (with local authorization)

☒ Use DNS to Find LDAP Servers

Active Directory Forest Name

Search Domain

☐ Use Pre-configured LDAP Servers

Active Directory Settings

View or set up authorization: [Group Profiles](#)

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method

Client DN

Password

Confirm password

- ドメイン・コントローラーおよびグローバル・カタログを手動で構成する場合は、「**Use Pre-Configured LDAP Servers**」(デフォルト)を選択し、「**LDAP Server Host Name or IP Address**」および「**Port**」フィールドを構成します。

IP アドレスまたは完全修飾ホスト名を使用して、最大 4 個のドメイン・コントローラーを構成することができます。グローバル・カタログ・サーバーは、ポート番号 3268 または 3269 を使用していることで識別されます。その他のポート番号を使用している場合、ドメイン・コントローラーが構成中であることを示します。

- グループ権限プロファイルを使用している場合、「Active Directory Settings」セクションで「**Group Profiles**」をクリックして、そのプロファイルを表示あるいは構成します (詳しくは、75 ページの『Active Directory ユーザーのグループ・プロファイル』を参照)。
- 「Network Protocols」ページに戻ります。「Group Profiles for Active Directory Users」ページにある「**LDAP Client section of the Network Protocols page**」リンクをクリックし、「**Lightweight Directory Access Protocol (LDAP) Client**」セクションまでスクロールします。
- IMM の各種パラメーターを構成します。パラメーターについては、次の表を参照してください。

表 10. 各種パラメーター

フィールド	説明	オプション
Root DN	IMM は、DN 形式の「 Root DN 」フィールドをディレクトリー・ツリーのルート・エントリーとして使用します。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。例えば、 <code>dc=mycompany,dc=com</code> のように示されます。	

表 10. 各種パラメーター (続き)

フィールド	説明	オプション
Binding method	「 Binding Method 」フィールドは、ドメイン・コントローラー・サーバーへの初回バインドに使用され、オプションの 1 つを選択します。	• With configured credentials: 初回バインドに使用するクライアント DN およびパスワードを入力します。このバインドが失敗すると、認証プロセスも失敗します。バインドが成功すると、「Client DN」フィールドに入力されたクライアント DN に一致するユーザー・レコードの検索が試行されます。一般的に、検索はログイン・プロセス中に提示されたユーザー ID に一致する共通属性を探します。これらの属性には、「>displayName」、「sAMAccountName」、および「userPrincipalName」が含まれます。「UID search attribute」フィールドが構成されている場合は、この属性も検索に含まれます。 検索が成功すると、2 回目のバインドが試行されます。2 回目は、検索で取得されたユーザー DN およびログイン・プロセス中に提示されたパスワードが使用されます。2 回目のバインドの試行が成功すると、認証部分が成功し、ユーザーのグループ・メンバーシップ情報が取得されて、IMM のローカルで構成されているグループとマッチングされます。一致したグループが、ユーザーに割り当てられた許可権限を定義します。 • With login credentials: ドメイン・コントローラー・サーバーへの初回バインドは、ログイン・プロセス中に提示された資格情報を使用して行われます。このバインドが失敗すると、認証プロセスも失敗します。バインドが成功すると、ユーザー・レコードの検索が試行されます。ユーザー・レコードが見つかったら、ユーザーのグループ・メンバーシップ情報が取得されて、IMM のローカルで構成されているグループとマッチングされます。一致したグループが、ユーザーに割り当てられた許可権限を定義します。 • Anonymously: ドメイン・コントローラー・サーバーへの初回バインドは、DN およびパスワードを使用せずに行われます。ほとんどのサーバーが特定のユーザー・レコードでの検索要求を許可しないように構成されているため、このオプションの使用は推奨されません。

Active Directory ユーザーのグループ・プロファイル

グループ・プロファイルは、ユーザーのグループに対するローカル権限の指定を提供するために構成されます。各グループ・プロファイルには、権限レベル（役割）として表される権限（ログイン・プロファイルと同一）が含まれます。グループ・プロファイルを構成するには、ユーザーがユーザー・アカウント管理権限を持っている必要があります。ユーザーとグループ・プロファイルに関連付けるには、LDAP 認証サーバーが必要です。

グループ・プロファイル・リスト

グループ・プロファイル・リストには、「**IMM Control**」>「**Login Profiles**」をクリックすることでアクセスできます。各グループ・プロファイルごとに、グループ ID と役割の要約が表示されます（ログイン・プロファイルとして）。このリストから、新規グループを追加したり、既存のグループを選択して編集あるいは削除したりすることができます。

次の図は、「Active Directory Users」ウィンドウのグループ・プロファイルを示しています。



グループ・プロファイルを編集するには、「**Edit**」をクリックします。そのグループの「Group Profile」ページが開きます。グループ・プロファイルを削除するには、「**Delete**」をクリックします。グループ・プロファイルの削除の確認が要求されます。新規のグループ・プロファイルを追加するには、「**Add a group**」リンクをクリックします。「Group Profile」ページが開き、新規グループ・プロファイルの情報を入力することができます。最大 16 個のグループ・プロファイルを追加することができます。グループ・プロファイル名は、固有である必要はありません。

次の表は、「Group Profile」ページのフィールドについて説明しています。

表 11. グループ・プロファイル情報

フィールド	オプション	説明
Group ID		このフィールドは、グループ・プロファイルのグループ ID を指定するために使用します。最大 63 文字を入力することができます。グループ ID は、LDAP サーバー上の対応する ID と同一でなければなりません。グループ名の例には、IMM Admin Group や IMM/Robert などがあります。

表 11. グループ・プロフィール情報 (続き)

フィールド	オプション	説明
Role		このログイン ID に関連付ける役割 (権限レベル) を選択し、それらを「 Assigned roles 」ボックスに転送します。 Enter キーまたはマウス・クリックを使用して、選択した項目をボックス間で転送することができます。
	Supervisor	このユーザーには、割り当てられた有効範囲を除き、制限はありません。
	Operator	このユーザーには、読み取り専用アクセス権のみがあり、変更 (保存、変更、消去など) を実行することはできません。これには、操作に影響する状態 (IMM の再始動、デフォルトのリストア、ファームウェアのアップグレードなど) も含まれます。
Role	Custom	ユーザーの制限は、ユーザーに割り当てられたカスタム権限レベルによって異なります。「Custom」オプションを選択した場合は、次のカスタム権限レベルを 1 つ以上選択する必要があります。 • Networking and Security – このユーザーは、「Security」、「Network Protocols」、「Network Interface」、「Port Assignments」、「Serial Port」の各パネルで構成を変更できます。 • User account management – 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」パネルで「Global Login」設定を変更できます。 • Remote Console Access – 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。 • Remote Console and Remote Disk Access – 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。 • Remote Server Power/Restart Access – このユーザーは、リモート・サーバーの電源オン、再始動、およびサーバー・タイムアウト機能にアクセスできます。 • Basic Adapter Configuration – このユーザーは、「System Settings」パネル (Contact、Location、および Server Timeouts を除く) および「Alerts」パネルで構成パラメーターを変更できます。

表 11. グループ・プロファイル情報 (続き)

フィールド	オプション	説明
		• Ability to Clear Event Logs – このユーザーはイベント・ログを消去することができます。 - 注: イベント・ログはすべてのユーザーが表示できますが、ログを消去するにはこの権限が必要です。 • Advanced Adapter Configuration – このユーザーは、アダプターの構成時に制限はなく、IMM に対する管理アクセス権限を持っています。ユーザーは、ファームウェア・アップグレード、プリブート実行環境 (PXE) ネットワーク・ブート、アダプター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、およびアダプター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。 - 注: この権限レベルからは、サーバーの電源/再始動の制御およびタイムアウト機能は除外されます。
注: 読み取り/書き込みアクセス権を持つユーザーがいない状態を避けるために、ログイン・プロファイル番号 1 は、少なくともログイン・プロファイルを変更する権限を持つように設定する必要があります。このユーザーには、スーパーバイザー・アクセス権またはユーザー・アカウント管理アクセス権を付与する必要があります。これにより、少なくとも 1 つのユーザーが、アクションの実行、構成の変更、およびログイン・プロファイルへのユーザー (アクションの実行や構成の変更を行えるユーザー) の追加を行えることが保証されます。		

次の図は、「Group Profile」ウィンドウを示しています。

Group Profile (new)

Group ID

Role

☒ Supervisor

☐ Operator (readonly)

☐ Custom (requires Roles)

To move an item from one column to another, click the item or use the enter key when the item has focus.

Unassigned roles

- User Account Management
- Remote Console Access
- Remote Console and Remote Disk Access
- Remote Server Power/Restart Access
- Ability to clear Event Logs
- Basic Adapter Configuration
- Networking & Security
- Advanced Adapter Configuration

Assigned roles

Cancel Save

Active Directory の役割ベースの認証および許可

Active Directory を使用して、ユーザーのリモート LDAP 認証および許可をセットアップすることができます。

注:

- Active Directory の役割ベースの認証および権限は、Active Directory 環境内で使用されるサーバーにのみ適用されます。
- Active Directory の役割ベースの認証および許可には、「拡張役割ベース・セキュリティ・スナップイン」ツールが必要です。

Active Directory の役割ベースの認証および許可は、Active Directory サーバーに保管されている構成情報を使用してユーザーを認証し、権限をユーザーに関連付けます。Active Directory の役割ベースの認証および許可を使用可能にするには、「拡張役割ベース・セキュリティ・スナップイン」ツールを使用して、権限をユーザーに関連付けるための構成情報を Active Directory サーバーに保管しておく必要があります。このツールは、すべての Microsoft Windows クライアントで実行することができます。このツールは、<http://www.ibm.com/support/jp/ja/> からダウンロードすることができます。

「拡張役割ベース・セキュリティ・スナップイン」ツールにより、Active Directory サーバー上で役割を構成し、IMM、ユーザー、およびグループをこれらの役割に関連付けることができます。情報および手順については、「拡張役割ベース・セキュリティ・スナップイン」ツールの資料を参照してください。役割は、ユーザーおよびグループに割り当てられた権限を識別し、役割が付与されるコマンド・ターゲット (IMM あるいはブレード・サーバーなど) を識別します。Active Directory の役割ベースの認証および許可を使用可能にするには、Active Directory サーバー上で役割が構成されている必要があります。

「Server Target Name」フィールドで構成されているオプションの名前によって、特定の IMM を識別し、「役割ベース・セキュリティ・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ます。これは、管理対象ターゲットを作成し、そのターゲットに固有の名前をつけて適切な役割に関連付けることで実現されます。「Server Target Name」が構成されている場合、ユーザーおよび同じ役割のメンバーである IMM ターゲットに特定の役割を定義することができます。ユーザーが IMM にログインし、Active Directory 経由で認証されると、このユーザーの役割をディレクトリーから取得します。ユーザーに割り当てられる権限は、その IMM と名前が一致するメンバーがターゲットである役割、あるいは任意の IMM に一致しているターゲットの役割から取り出されます。IMM には固有の名前をつけることも、複数の IMM で同じターゲット名を共有することもできます。複数の IMM を同じターゲット名に割り当てることで、それらをグループ化し、同じ役割に割り当てることができます。

IMM に Active Directory の役割ベースの認証および許可を構成するには、次のステップを実行してください。

1. ナビゲーション・ペインで、「**Network Protocols**」をクリックします。
2. 「**Lightweight Directory Access Protocol (LDAP) Client**」セクションまでスクロールダウンします。
3. 「**Use LDAP Servers for Authentication and Authorization**」を選択します。

4. 「Enhanced role-based security for Active Directory Users」フィールドで「Enabled」を選択します。
5. ドメイン・コントローラーを動的に検出したり手動で構成するには、以下の選択項目から 1 つを選択します。
 - 「Use DNS to find LDAP Servers」を選択し、DNS SVR レコードに基づいてドメイン・コントローラーを動的に検出します。
 - 「Use Pre-Configured LDAP Servers」(デフォルトの選択) を選択し、ドメイン・コントローラーを手動で構成します。
6. DNS を使用してドメイン・コントローラーを動的に検出する場合は、ドメイン・コントローラーのドメイン・ネームを構成してから、ステップ 8 (80 ページ) に進んでください。ドメイン・コントローラーの完全修飾ドメイン・ネームを指定する必要があります。「Search Domain」フィールドにドメイン・コントローラーのドメイン・ネームを入力します。

次のウィンドウは、DNS を使用してドメイン・コントローラーを動的に検出している場合の「LDAP Client」ウィンドウを表示しています。

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization
☐ Use LDAP Servers for Authentication Only (with local authorization)

☒ Use DNS to Find LDAP Servers

Search Domain

☐ Use Pre-configured LDAP Servers

Active Directory Settings

Enhanced role-based security for Active Directory Users

Server Target Name

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method

Client DN

Password

Confirm password

7. ドメイン・コントローラーを手動で構成する場合は、「LDAP Server Host Name or IP Address」および「Port」フィールドを構成します。

注: IP アドレスまたは完全修飾ホスト名を使用して、最大 4 個のドメイン・コントローラーを構成することができます。

次の図は、ドメイン・コントローラーを手動で構成している場合の「LDAP Client」ウィンドウを示しています。

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization
☐ Use LDAP Servers for Authentication Only (with local authorization)

☐ Use DNS to Find LDAP Servers
☒ Use Pre-configured LDAP Servers

	LDAP Server Fully Qualified Host Name or IP Address	Port
1.		
2.		
3.		
4.		

Active Directory Settings

Enhanced role-based security for Active Directory Users ▾

Server Target Name

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method ▾

Client DN

Password

Confirm password

8. 「Enhanced role-based security for Active Directory Users」メニューから「Enabled」を選択し、「Active Directory Settings」を構成します。
9. 「Miscellaneous Parameters」を構成します。パラメーターについては、次の表を参照してください。

表 12. 各種パラメーター

フィールド	説明	オプション
Root DN	IMM は、DN 形式の「 Root DN 」フィールドをディレクトリー・ツリーのルート・エントリーとして使用します。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。例えば、 <code>dc=mycompany,dc=com</code> のように示されます。	
バインド方式	「 Binding Method 」フィールドは、ドメイン・コントローラー・サーバーへの初回バインドに使用され、オプションの 1 つを選択します。	• Anonymously: ドメイン・コントローラー・サーバーへの初回バインドは、DN およびパスワードを使用せずに行われます。ほとんどのサーバーが特定のユーザー・レコードでの検索要求を許可しないように構成されているため、このオプションの使用は推奨されません。 • With configured credentials: 初回バインドに使用するクライアント DN およびパスワードを入力します。 • With login credentials: ドメイン・コントローラー・サーバーへの初回バインドは、ログイン・プロセス中に提示された資格情報を使用して行われます。ユーザー ID は、DN、部分 DN、完全修飾ドメイン・ネームを使用して、あるいは IMM 上で構成された「UID Search Attribute」フィールドに一致するユーザー ID から提供することができます。 資格情報が部分 DN (例えば、<code>cn=joe</code>) と同様の場合、この部分 DN は、ユーザーの記録に一致する DN の作成を試行するときに、構成済みのルート DN の接頭部として付けられます。バインド試行が失敗した場合、最後のバインドは、接頭部 <code>cn=</code> をログイン資格情報に追加することで試行されます。その後、その結果のストリングを構成済みのルート DN に追加します。

従来の LDAP 認証および許可

従来の LDAP 認証および許可は、IMM で使用されているオリジナル・モデルです。従来の LDAP 認証および許可は、Active Directory、Novell eDirectory、および OpenLDAP 環境をサポートし、LDAP サーバーに保管されている構成情報に依存して権限とユーザーを関連付けます。従来の LDAP 認証および許可は、LDAP サーバ

ーを介したユーザーの認証および許可に使用されます。Active Directory ユーザーの拡張役割ベース・セキュリティーが IMM 上で無効にされている場合、IMM の LDAP 検索属性を構成することができます。

IMM に従来の LDAP 認証および許可を構成するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**Network Protocols**」をクリックします。
2. 「**Lightweight Directory Access Protocol (LDAP) Client**」セクションまでスクロールダウンします。
3. 「**Use LDAP Servers for Authentication and Authorization**」を選択します。
4. 「**Enhanced role-based security for Active Directory Users**」フィールドで「**Disabled**」を選択します。
5. 認証に使用する LDAP サーバーを動的に検出したり手動で構成するには、以下の選択項目から 1 つを選択します。
 - 「**Use DNS to find LDAP Servers**」を選択し、DNS SVR レコードに基づいて LDAP サーバーを動的に検出します。
 - 「**Use Pre-Configured LDAP Servers**」(デフォルトの選択)を選択し、LDAP サーバーを手動で構成します。
6. DNS を使用して LDAP サーバーを動的に検出する場合は、LDAP サーバーのドメイン・ネームを構成してから、ステップ 8 (84 ページ) に進んでください。LDAP サーバーの完全修飾ドメイン・ネームを指定する必要があります。「**Search Domain**」フィールドに LDAP サーバーのドメイン・ネームを入力します。

次のウィンドウは、DNS を使用して LDAP サーバーを動的に検出している場合の「LDAP Client」ウィンドウを表示しています。

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization

☐ Use LDAP Servers for Authentication Only (with local authorization)

☒ Use DNS to Find LDAP Servers

Search Domain

☐ Use Pre-configured LDAP Servers

Active Directory Settings

Enhanced role-based security for Active Directory Users

Disabled ▼

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method

With configured credentials ▼

Client DN

Password

Confirm password

Group Filter

Group Search Attribute

Login Permission Attribute

7. LDAP サーバーを手動で構成する場合は、「**LDAP Server Host Name or IP Address**」フィールドと「**Port**」フィールドを構成し、ステップ 8 (84 ページ) に進みます。

注: IP アドレスまたは完全修飾ホスト名を使用して、最大 4 個の LDAP サーバーを構成することができます。

次のウィンドウは、LDAP サーバーを手動で構成している場合の「LDAP Client」ウィンドウを表示しています。

Lightweight Directory Access Protocol (LDAP) Client

☒ Use LDAP Servers for Authentication and Authorization
☐ Use LDAP Servers for Authentication Only (with local authorization)

☐ Use DNS to Find LDAP Servers
☒ Use Pre-configured LDAP Servers

	LDAP Server Fully Qualified Host Name or IP Address	Port
1.		
2.		
3.		
4.		

Active Directory Settings
Enhanced role-based security for Active Directory Users

Miscellaneous Parameters

Root DN	
UID Search Attribute	
Binding Method	With configured credentials
Client DN	
Password	
Confirm password	
Group Filter	
Group Search Attribute	
Login Permission Attribute	

8. 「Enhanced role-based security for Active Directory Users」メニューから「Disabled」を選択し、「Active Directory Settings」を構成します。
9. 「Miscellaneous Parameters」を構成します。必須パラメーター・フィールドの説明については、以下のリストを参照してください。
 - IMM は、DN 形式の「Root DN」フィールドをディレクトリー・ツリーのルート・エントリーとして使用します。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。例えば、dc=mycompany,dc=com のように示されます。
 - 「Binding Method」フィールドは、ドメイン・コントローラー・サーバーへの初回バインドに使用されます。次のバインディング・オプションのいずれかを使用します。
 - Anonymously:

ドメイン・コントローラー・サーバーへの初回バインドは、DN およびパスワードを使用せずに行われます。ほとんどのサーバーが特定のユーザー・レコードでの検索要求を許可しないように構成されているため、このオプションの使用は推奨されません。

- With configured credentials:

初回バインドに使用するクライアント DN およびパスワードを入力します。

- With login credentials:

ログイン・プロセス時に提供される資格情報を使用してバインドします。ユーザー ID は、DN、部分 DN、完全修飾ドメイン・ネームを使用して、あるいは IMM 上で構成された「**UID Search Attribute**」フィールドの情報に一致するユーザー ID から提供することができます。資格情報が部分 DN (例えば、cn=joe) と同様の場合、この部分 DN は、ユーザーの記録に一致する DN の作成を試行するときに、構成済みのルート DN の接頭部として付けられます。バインド試行が失敗した場合、最後のバインドは、接頭部 cn= をログイン資格情報に追加することで試行されます。その後、その結果のストリングを構成済みのルート DN に追加します。

- 「**Group Filter**」フィールドは、グループ認証に使用されます。これは、IMM が属するグループを指定します。グループ・フィルター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。グループ認証は、ユーザー認証の後に実行されます (有効にされている場合)。グループ・フィルター内の少なくとも 1 つのグループと、ユーザーが所属しているグループの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。一致するグループが少なくとも 1 つある場合は、グループ認証はパスします。この比較は大/小文字を区別します。

グループ認証が無効にされている場合、ユーザー自身の記録に権限属性が含まれている必要があります。含まれていない場合、アクセスは拒否されます。フィルターに一致する各グループについては、そのグループに関連付けられている権限がユーザーに割り当てられます。グループに関連付けられた権限は、**ログイン権限属性情報**を取り出すことで確認できます。

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されます。複数のグループ名を指定するには、コロン (:) 文字を使用する必要があります。先行スペースおよび後続スペースは無視されます。その他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。

注: 以前に使用されていたアスタリスク (*) 記号は、ワイルドカード記号として処理されなくなりました。セキュリティ上の理由から、ワイルドカードの概念は除去されました。

- 「**Group Search Attribute**」フィールドは、特定ユーザーのグループ・メンバーシップ情報を検索するために検索アルゴリズムで使用されます。グループのフィルター名が構成されると、ユーザーが属しているグループのリストが LDAP サーバーから検索される必要があります。このリストは、グループ認証

を行うために必要です。このリストを検索するには、LDAP サーバーに送信される検索フィルターでグループと関連付けられる属性名を指定する必要があります。「**Group Search Attribute**」フィールドは、属性名を指定します。

Active Directory あるいは Novell eDirectory 環境では、「**Group Search Attribute**」フィールドは、ユーザーが所属するグループを識別するための属性名を指定します。Active Directory では属性 **memberOf** が使用され、Novell eDirectory では属性 **groupMembership** が使用されます。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。このコンテキストでは、「Group Search Attribute」パラメーターは特定の PosixGroup のメンバーを識別するための属性名を指定し、通常これは「**memberUid**」です。「**Group Search Attribute**」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**」フィールドは、ユーザーのログイン権限に関連付けられる属性名を指定します。ユーザーが LDAP サーバーを使用して正常に認証された場合は、このユーザーのログイン権限を取得する必要があります。

注: この「**Login Permission Attribute**」フィールドは、ブランクにしてはなりません。ブランクにすると、ユーザーの権限を取得することができません。検証済みの権限がない場合、ログイン試行は失敗します。

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。このキーワードの直後には、(0 と 1 から構成される最大 12 桁の) ビット・ストリングが続きます。各ビットは、各機能の特定の設定を表します。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。特定の位置の値を 1 に設定すると、特定の機能が使用可能になります。値が 0 である場合、その機能は使用不可になります。ストリング **IBMRBSPermissions=010000000000** は例です。

IBMRBSPermissions= キーワードは、「**Login Permission Attribute**」フィールドの任意の位置に配置することができます。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 スキーマの拡張が防止され、属性を元の目的で使用できるようになります。これで、ユーザーはキーワード・ストリングを、このフィールドの先頭、末尾、あるいは任意の位置に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。

次の表は、各ビット位置について説明しています。

表 13. 許可ビット

ビット位置	機能	説明
0	常に拒否	これが設定されている場合、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	これが設定されている場合、ユーザーに管理者特権が付与されます。ユーザーは、すべての機能に対して読み取り/書き込みアクセス権を持ちます。このビットを設定した場合、他のビットを個別に設定する必要はありません。
2	読み取り専用アクセス権	これが設定されている場合、ユーザーは読み取り専用アクセス権を持ち、保守手順（再始動、リモート・アクション、ファームウェア更新など）を実行することはできません。保存、消去、あるいは復元機能を使用して変更することはできません。ビット位置 2 と他のすべてのビットは相互に排他的で、ビット位置 2 の優先順位が最下位です。他のいずれかのビットが設定されている場合、このビットは無視されます。
3	ネットワーキングおよびセキュリティ	これが設定されている場合、ユーザーは、「Security」、「Network Protocols」、「Network Interface」、「Port Assignments」、「Serial Port」の各パネルで構成を変更できます。
4	ユーザー・アカウント管理	これが設定されている場合、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」パネルで「Global Login Settings」を変更できます。
5	Remote Console Access	これが設定されている場合、ユーザーは、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、「Serial Port」パネルで構成を変更できます。
6	Remote Console and Remote Disk Access	これが設定されている場合、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。また、ユーザーは、「Serial Port」パネルで構成を変更できます。

表 13. 許可ビット (続き)

ビット位置	機能	説明
7	リモート・サーバーの電源/再始動アクセス権	これが設定されている場合、ユーザーは、リモート・サーバーの電源オン、再始動、およびサーバー・タイムアウト機能にアクセスできます。
8	アダプターの基本構成	これが設定されている場合、ユーザーは、「System Settings」および「Alerts」ページで構成パラメーター (Contact、Location、および Server Timeout を除く) を変更できます。
9	イベント・ログを消去する権限	これが設定されている場合、ユーザーはイベント・ログを消去できます。 注: すべてのユーザーがイベント・ログを表示できますが、ログを消去するには、ユーザーにこのレベルの権限が必要です。
10	アダプターの拡張構成	これが設定されている場合、ユーザーは、アダプターの構成時に制限はなく、IMM に対する管理アクセス権限を持っています。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、アダプター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、およびアダプター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。サーバーの電源/再始動の制御およびタイムアウト機能は除きます。
11	予約済み	このビット位置は、将来の使用のために予約済みです (現行では無視されます)。

注:

- ビットが使用されない場合、デフォルトでは、ユーザーに対して「読み取り専用」を設定します。
- 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。ユーザー・レコードの「**Login Permission Attribute**」フィールドに名前が含まれていない場合、ユーザーが属しており、グループ・フィルターに一致するグループから権限の取得が試行されます。この場合、ユーザーには、すべてのグループのすべてのビットの包含 **OR** が割り当てられます。
- いずれかのグループに「常に拒否」(ビット位置 0) ビットが設定されている場合、ユーザーはアクセスを拒否されます。「常に拒否」ビットは、すべてのビットに対して優先されます。
- ユーザーに基本、ネットワーキング、またはセキュリティ関連のアダプター構成パラメーターを変更する権限がある場合、そのユーザーに IMM を再始動する権限 (ビット位置 10) を付与することを確認してください。この権限がない場合、ユーザーはパラメーターの変更はできる場合がありますが、そのパラメーターは有効になりません。

セキュリティの構成

このセクションの一般手順を使用して、IMM Web サーバー、IMM と IBM Systems Director の間の接続、および IMM と LDAP サーバーの間の接続のセキュリティを構成します。SSL 証明書の使用に慣れていない場合は、90 ページの『SSL 証明書の概要』の情報を参照してください。

IMM のセキュリティを構成するには、次の汎用タスク・リストを使用します。

1. 次のようにして、セキュアな Web サーバーを構成します。
 - a. SSL サーバーを使用不可に設定します。「Security」ページの「**HTTPS Server Configuration for Web Server**」エリアを使用してください。
 - b. 証明書を生成またはインポートします。「Security」ページの「**HTTPS Server Certificate Management**」エリアを使用してください (91 ページの『SSL サーバー証明書管理』を参照)。
 - c. SSL サーバーを使用可能に設定します。「Security」ページの「**HTTPS Server Configuration for Web Server**」エリアを使用してください (96 ページの『HTTPS 上でセキュア Web サーバーまたは IBM Systems Director を使用するための SSL の使用可能化』を参照)。
2. 次のように、IBM Systems Director 接続を構成します。
 - a. Systems Director over HTTPS 設定を使用不可にします。「Security」ページの「**IBM Systems Director over HTTPS Server Configuration**」エリアを使用します。
 - b. 証明書を生成またはインポートします。「Security」ページの「**IBM Systems Director over HTTPS Server Certificate Management**」エリアを使用します (91 ページの『SSL サーバー証明書管理』を参照)。
 - c. SSL サーバーを使用可能に設定します。「Security」ページの「**IBM Systems Director over HTTPS Server Configuration**」エリアを使用します (96 ページの『HTTPS 上でセキュア Web サーバーまたは IBM Systems Director を使用するための SSL の使用可能化』を参照)。
3. 次のようにして、LDAP 接続の SSL セキュリティを構成します。
 - a. SSL クライアントを使用不可に設定します。「Security」ページの「**SSL Client Configuration for LDAP Client**」エリアを使用してください。
 - b. 証明書を生成またはインポートします。「Security」ページの「**SSL Client Certificate Management**」エリアを使用してください (91 ページの『SSL サーバー証明書管理』を参照)。
 - c. 1 つ以上のトラステッド証明書をインポートします。「Security」ページの「**SSL Client Trusted Certificate Management**」エリアを使用してください (96 ページの『SSL クライアントのトラステッド証明書管理』を参照)。
 - d. SSL クライアントを使用可能に設定します。「Security」ページの「**SSL Client Configuration for LDAP Client**」エリアを使用してください (96 ページの『HTTPS 上でセキュア Web サーバーまたは IBM Systems Director を使用するための SSL の使用可能化』を参照)。

4. IMM を再始動して、SSL サーバーの構成変更を有効にします。詳しくは、102 ページの『IMM の再始動』を参照してください。

注: SSL クライアント構成に対する変更は即時に有効になるため、IMM を再始動する必要はありません。

セキュア Web サーバー、IBM Systems Director、およびセキュア LDAP

セキュア・ソケット・レイヤー (SSL) は、通信プライバシーを提供するセキュリティ・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。

IMM は、SSL サポートをセキュア・サーバー (HTTPS) およびセキュア LDAP (LDAPS) の 2 つのタイプの接続に使用するように構成できます。IMM は、接続のタイプに応じて SSL クライアントまたは SSL サーバーの役割を果たします。次の表は、IMM がセキュア Web サーバー接続用の SSL サーバーとして機能することを示しています。セキュア LDAP 接続では、IMM は SSL クライアントとして機能します。

表 14. IMM の SSL 接続サポート

接続タイプ	SSL クライアント	SSL サーバー
セキュア Web サーバー (HTTPS)	ユーザーの Web ブラウザー (例えば Microsoft Internet Explorer)	IMM の Web サーバー
セキュア IBM Systems Director 接続	IBM Systems Director	IMM Systems Director サーバー
セキュア LDAP 接続 (LDAPS)	IMM LDAP クライアント	LDAP サーバー

SSL の設定は、「Security」ページから表示または変更できます。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ができます。

SSL 証明書の概要

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・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。第三者がサーバーの偽名を使用し、IMM と 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 IMM 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を実現するには、認証局が署名する証明書を使用できます。署名された証明書を入手するには、「SSL Certificate Management」ページを使

用して、証明書署名要求を生成します。次に、証明書署名要求を認証局に送信して、証明書を手配します。証明書が受信されると、証明書は「**Import a Signed Certificate**」リンクを使用して IMM にインポートされ、SSL を使用可能にできます。

認証局の機能は、IMM の ID を検査することです。証明書には、認証局および IMM のデジタル署名が含まれます。既知の認証局が証明書を発行する場合、または認証局の証明書が既に 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 IMM の Web サーバーを識別できます。

IMM では、セキュア Web サーバーとセキュア LDAP クライアントのそれぞれに証明書が必要です。また、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が必要です。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認証局の証明書です。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。

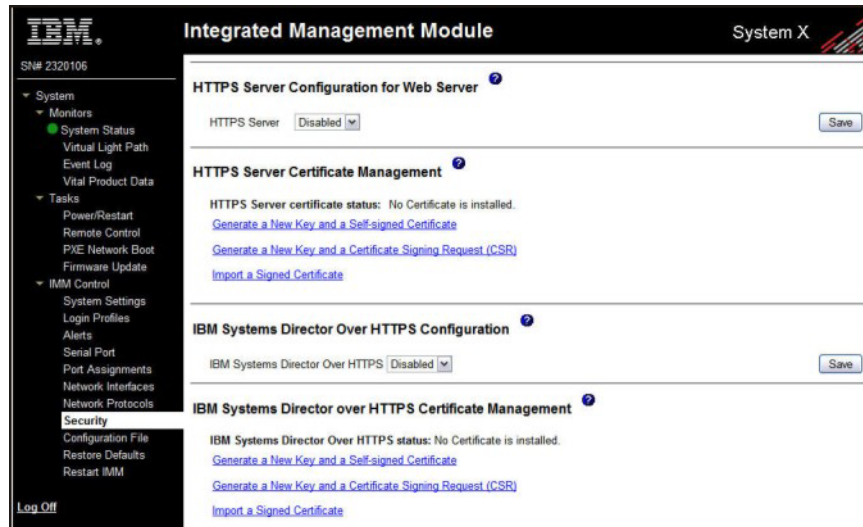
SSL サーバー証明書管理

SSL サーバーでは、SSL が使用可能にされる前に、有効な証明書および対応する秘密暗号鍵がインストールされている必要があります。秘密鍵と必要な証明書を生成する方法には、自己署名証明書を使用する方法と、認証局により署名された証明書を使用する方法の 2 通りがあります。自己署名証明書を SSL サーバーに使用する場合は、『自己署名証明書の生成』を参照してください。認証局により署名される証明書を SSL サーバーに使用する場合は、93 ページの『証明書署名要求の生成』を参照してください。

自己署名証明書の生成

新規の秘密暗号鍵と自己署名証明書を生成するには、次のステップを実行します。

1. ナビゲーション・ペインで、「**Security**」をクリックします。次の図のようなページが表示されます。



2. 「SSL Server Configuration for Web Server」エリアまたは「IBM Systems Director Over HTTPS Configuration」エリアで、「Disabled」に設定されていることを確認します。使用不可になっていない場合、「Disabled」を選択してから、「Save」をクリックします。

注:

- a. 選択した値 (Enabled または Disabled) を有効にするには、IMM を再始動する必要があります。
 - b. SSL を使用可能にするには、有効な SSL 証明書が所定の位置になければなりません。
 - c. SSL を使用するには、クライアントの Web ブラウザーを、SSL3 または TLS を使用するように構成する必要があります。SSL2 サポートしかない古いエクスポート・グレードのブラウザーはサポートされません。
3. 「SSL Server Certificate Management」エリアで、「Generate a New Key and a Self-signed Certificate」を選択します。次の図のようなページが表示されます。

4. 必須フィールドおよびご使用の構成に適用されるオプションのフィールドに情報を入力します。各フィールドの説明については、93 ページの『必要な証明書データ』を参照してください。情報の入力が終わった後、「**Generate Certificate**」をクリックします。これで、新規の暗号鍵および証明書が生成されました。この処理には数分間かかる場合があります。自己署名証明書がインストールされると、確認が表示されます。

証明書署名要求の生成

新規の秘密暗号鍵と証明書署名要求を生成するには、次のステップを実行します。

1. ナビゲーション・ペインで、「**Security**」をクリックします。
2. 「**SSL Server Configuration for Web Server**」エリアで、SSL サーバーが使用不可になっていることを確認します。使用不可になっていない場合、「**SSL Server**」フィールドで「**Disabled**」を選択してから、「**Save**」をクリックします。
3. 「**SSL Server Certificate Management**」エリアで、「**Generate a New Key and a Certificate-Signing Request**」を選択します。次の図のようなページが表示されます。



4. 必須フィールドおよびご使用の構成に適用されるオプションのフィールドに情報を入力します。これらのフィールドは自己署名証明書の場合と同じものですが、いくつか追加フィールドがあります。

共通する各フィールドの説明については、以下のセクションの情報をお読みください。

Required certificate data 以下のユーザー入力フィールドは、自己署名証明書または証明書署名要求の生成に必須です。

Country

このフィールドを使用して、IMM を物理的に配置する国を示します。このフィールドには、2 文字の国別コードを入力する必要があります。

State or Province

このフィールドを使用して、IMM を物理的に配置する都道府県を示します。このフィールドには、最大 30 文字を入力できます。

City or Locality

このフィールドを使用して、IMM を物理的に配置する市区町村を示します。このフィールドには、最大 50 文字を入力できます。

Organization Name

このフィールドは、IMM を所有している企業または組織を示すために使用されます。これを使用して証明書署名要求を生成する場合、発行側の認証局は、証明書を要求している組織が所定の会社名または組織名の所有権を主張する法的な資格があるかどうかを検証できます。このフィールドには、最大 60 文字を入力できます。

IMM Host Name

このフィールドは、ブラウザの Web アドレス・バーに現在表示されている IMM のホスト名を示すために使用されます。

このフィールドに入力した値が、Web ブラウザーで使用されているホスト名と完全に一致することを確認してください。ブラウザは、解決された Web アドレスのホスト名を、証明書に現在表示されている名前と比較します。ブラウザから証明書の警告を出されないようにするには、このフィールドに使用された値は、IMM への接続にブラウザに使用されたホスト名と一致している必要があります。例えば、Web アドレス・バーに入っているアドレスが `http://mm11.xyz.com/private/main.ssi` の場合、「IMM Host Name」フィールドに使用する値は `mm11.xyz.com` であることが必要です。Web アドレスが `http://mm11/private/main.ssi` である場合、使用される値は `mm11` です。Web アドレスが `http://192.168.70.2/private/main.ssi` である場合、使用される値は `192.168.70.2` です。

この証明書属性は通常、共通名と呼ばれます。

このフィールドには、最大 60 文字を入力できます。

Contact Person

このフィールドは、IMM の担当者の名前を示すために使用されます。このフィールドには、最大 60 文字を入力できます。

Email Address

このフィールドは、IMM の担当者の E メール・アドレスを示すために使用されます。このフィールドには、最大 60 文字を入力できます。

Optional certificate data 以下のユーザー入力フィールドは、自己署名証明書または証明書署名要求の生成でオプションです。

Organizational Unit

このフィールドは、IMM を所有する企業または組織内の単位を示すために使用します。このフィールドには、最大 60 文字を入力できます。

姓 このフィールドは、IMM の責任者の姓などの追加情報を示すために使用します。このフィールドには、最大 60 文字を入力できます。

Given Name

このフィールドは、IMM の責任者の名前などの追加情報を示すために使用します。このフィールドには、最大 60 文字を入力できます。

イニシャル

このフィールドは、IMM 担当者のイニシャルなどの追加情報を示すために使用します。このフィールドには、最大 20 文字を入力できます。

DN Qualifier

このフィールドは、IMM の識別名修飾子などの追加情報を示すために使用します。このフィールドには、最大 60 文字を入力できます。

Certificate-Signing request attributes 以下のフィールドは、選択した認証局から要求されない限り、オプションです。

Challenge Password

このフィールドは、証明書署名要求にパスワードを割り当てるために使用します。このフィールドには、最大 30 文字を入力できます。

Unstructured Name

このフィールドは、IMM に割り当てられた非構造化された名前などの追加情報を示すために使用します。このフィールドには、最大 60 文字を入力できます。

5. 情報を入力した後、「**Generate CSR**」をクリックします。これで、新規の暗号鍵および証明書が生成されました。この処理には数分間かかる場合があります。
6. 「**Download CSR**」をクリックしてから「**Save**」をクリックし、ファイルをワークステーションに保管します。証明書署名要求の作成時に作成されたファイルは DER 形式です。認証局が、PEM などのその他の形式でデータを要求する場合は、ファイルを OpenSSL (<http://www.openssl.org>) などのツールを使用して変換できます。認証局が証明書署名要求ファイルの内容を Web ブラウザーのウィンドウにコピーするよう求めてくる場合、通常では PEM 形式が期待されています。

OpenSSL を使用して証明書署名要求を DER 形式から PEM 形式に変換するためのコマンドの例を次に示します。

```
openssl req -in csr.der -inform DER -out csr.pem -outform PEM
```

7. 証明書署名要求を認証局へ送信します。認証局が署名された証明書を戻すと、その証明書を DER 形式に変換する必要がある場合があります。(証明書を E メールまたは Web ページでテキストとして受信した場合は、恐らく PEM 形式になっています。) 形式を変更するには、認証局が提供するツールを使用するか、OpenSSL (<http://www.openssl.org>) などのツールを使用します。証明書を PEM 形式から DER 形式に変換するためのコマンドの例を次に示します。

```
openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
```

署名された証明書が認証局から戻されたら、ステップ 8 に進みます。

8. ナビゲーション・ペインで、「**Security**」をクリックします。「**SSL Server Certificate Management**」エリア、または「**IBM Systems Director Over HTTPS Certificate Management**」エリアまでスクロールします。
9. 「**Import a Signed Certificate**」をクリックします。
10. 「**Browse**」をクリックします。
11. 該当する証明書ファイルをクリックしてから、「**Open**」をクリックします。ファイル名 (絶対パスを含む) が「**Browse**」ボタンの隣のフィールドに表示されます。
12. 「**Import Server Certificate**」をクリックして、処理を開始します。ファイルが IMM 上のストレージに転送されると進行標識が表示されます。転送が完了するまで、このページの表示を続けてください。

HTTPS 上でセキュア Web サーバーまたは IBM Systems Director を使用するための SSL の使用可能化

セキュアな Web サーバーを使用可能にするには、以下のステップを実行します。

注: SSL を使用可能にするには、有効な SSL 証明書がインストールされている必要があります。

1. ナビゲーション・ペインで、「**Security**」をクリックします。表示されるページには、有効な SSL サーバー証明書がインストールされていることが示されます。SSL サーバー証明書状況に、有効な SSL 証明書がインストールされていると表示されない場合は、91 ページの『SSL サーバー証明書管理』を参照してください。
2. 「**SSL Server Configuration for web Server**」エリア、または「**IBM Systems Director Over HTTPS Configuration**」エリアまでスクロールし、「**SSL Client**」フィールドで「**Enabled**」を選択して「**Save**」をクリックします。選択された値は、次回 IMM が再始動された時点で有効になります。

SSL クライアント証明書管理

SSL クライアントでは、SSL が使用可能にされる前に、有効な証明書および対応する秘密暗号鍵がインストールされている必要があります。秘密鍵と必要な証明書を生成するためには、2 つの方法があります。自己署名証明書を使用する方法と、認証局によって署名された証明書を使用する方法です。

SSL クライアント用の秘密暗号鍵と証明書を生成する手順は、SSL サーバーの場合の手順と同じですが、「**Security**」Web ページの「**SSL Server Certificate Management**」エリアの代わりに、「**SSL Client Certificate Management**」エリアを使用する点が異なります。自己署名証明書を SSL クライアントに使用する場合は、91 ページの『自己署名証明書の生成』を参照してください。SSL クライアントに認証局の署名が付いた証明書を使用したい場合は、93 ページの『証明書署名要求の生成』を参照してください。

SSL クライアントのトラステッド証明書管理

セキュア SSL クライアント (LDAP クライアント) は、確実に LDAP サーバーを識別するためにトラステッド証明書を使用します。トラステッド証明書として使用できるのは、LDAP サーバーの証明書に署名した認証局の証明書か、あるいは LDAP サーバーの実際の証明書です。SSL クライアントが使用可能にされる前に、少なくともいずれかの証明書が IMM にインポートされる必要があります。最大 3 つのトラステッド証明書をインポートできます。

トラステッド証明書をインポートするには、次のステップを実行します。

1. ナビゲーション・ペインで、「**Security**」を選択します。
2. 「**SSL Client Configuration for LDAP Client**」エリアで、SSL クライアントが使用不可になっていることを確認します。使用不可になっていない場合、「**SSL Client**」フィールドで「**Disabled**」を選択してから、「**Save**」をクリックします。
3. 「**SSL Client Trusted Certificate Management**」エリアまでスクロールします。

4. 「**Trusted CA Certificate 1**」フィールドの隣にある「**Import**」をクリックします。
5. 「**Browse**」をクリックします。
6. 該当する証明書ファイルを選択して、「**Open**」をクリックします。ファイル名 (絶対パスを含む) が「**Browse**」ボタンの隣のボックスに表示されます。
7. インポート・プロセスを開始するには、「**Import Certificate**」をクリックします。ファイルが IMM 上のストレージに転送されると進行標識が表示されます。転送が完了するまで、このページを表示しつづけます。

これで、「Trusted CA Certificate 1」のオプションとして「**Remove**」ボタンが使用できるようになりました。トラステッド証明書を除去する場合は、対応する「**Remove**」ボタンをクリックします。

その他のトラステッド証明書をインポートするには、「Trusted CA Certificate 2」および「Trusted CA Certificate 3」の「**Import**」ボタンを使用します。

LDAP クライアント用の SSL を使用可能にする

LDAP クライアント用の SSL を使用可能または使用不可にするには、「Security」ページの「**SSL Client Configuration for LDAP Client**」エリアを使用します。SSL を使用可能にするには、有効な SSL クライアント証明書と、少なくとも 1 つのトラステッド証明書を最初にインストールする必要があります。

クライアント用の SSL を使用可能にするには、次のステップを実行します。

1. ナビゲーション・ペインで、「**Security**」をクリックします。

「Security」ページに、インストールされている SSL クライアント証明書と「Trusted CA Certificate 1」が表示されます。

2. 「SSL Client Configuration for LDAP Client」ページの「**SSL Client**」フィールドで、「**Enabled**」を選択します。

注:

- a. 選択された値 (使用可能または使用不可) は即時に有効になります。
 - b. SSL を使用可能にするには、有効な SSL 証明書が所定の位置になければなりません。
 - c. ご使用の LDAP サーバーが、LDAP クライアントが使用する SSL 実装環境と互換性を持つには、SSL3 または TLS をサポートしている必要があります。
3. 「**Save**」をクリックします。選択された値は即時に有効になります。

セキュア・シェル・サーバーの構成

セキュア・シェル (SSH) 機能は IMM のコマンド・ライン・インターフェースとシリアル (テキスト・コンソール) リダイレクト機能へのセキュアなアクセスを提供します。

セキュア・シェル・ユーザーは、ユーザー ID とパスワードを交換することにより認証されます。パスワードとユーザー ID は、暗号化チャネルが確立された後に送信されます。ユーザー ID とパスワードのペアは、ローカルに保管されている 12

のユーザー ID とパスワードのいずれかを使用することも、LDAP サーバーに保管することもできます。公開鍵認証はサポートされません。

セキュア・シェル・サーバー鍵の生成

セキュア・シェル・サーバー鍵は、セキュア・シェル・サーバーの ID をクライアントに認証するために使用されます。新しいセキュア・シェル・サーバー秘密鍵を作成する前に、セキュア・シェルを使用不可にしておく必要があります。セキュア・シェル・サーバーを使用可能にする前に、サーバー鍵を作成する必要があります。

新しいサーバー鍵を要求すると、SSH バージョン 2 のクライアントから IMM にアクセスできるよう、Rivest、Shamir、および Adelman 鍵と DSA 鍵の両方が作成されます。セキュリティの点から、セキュア・シェル・サーバー秘密鍵は構成の保管およびリストア操作時にはバックアップされません。

新規のセキュア・シェル・サーバー鍵を作成するには、次のステップを実行します。

1. ナビゲーション・ペインで、「**Security**」をクリックします。
2. 「**Secure Shell (SSH) Server**」エリアまでスクロールして、セキュア・シェル・サーバーが使用不可になっていることを確認します。使用不可になっていない場合、「**SSH Server**」フィールドで「**Disabled**」を選択してから、「**Save**」をクリックします。
3. 「**SSH Server Key Management**」エリアまでスクロールします。
4. 「**Generate SSH Server Private Key**」をクリックします。進行状況を示すウィンドウが開きます。操作が完了するまで待ってください。

セキュア・シェル・サーバーの使用可能化

「Security」ページから、セキュア・シェル・サーバーを使用可能または使用不可にすることができます。選択する項目は、IMM が再始動してからでないとは有効になりません。画面に表示される値 (Enabled または Disabled) は最後に選択された値であり、IMM が再始動されると使用されます。

注: セキュア・シェル・サーバーを使用可能にできるのは、有効なセキュア・シェル・サーバー秘密鍵がインストールされている場合に限られます。

セキュア・シェル・サーバーを使用可能にするには、次のステップを実行します。

1. ナビゲーション・ペインで、「**Security**」をクリックします。
2. 「**Secure Shell (SSH) Server**」エリアまでスクロールします。
3. 「**SSH Server**」フィールドで「**Enabled**」をクリックします。
4. ナビゲーション・ペインで、「**Restart IMM**」をクリックして IMM を再始動します。

セキュア・シェル・サーバーの使用

Red Hat Linux バージョン 7.3 に組み込まれているセキュア・シェル・クライアントを使用している場合、IMM でネットワーク・アドレス 192.168.70.132 を使用してセキュア・シェル・セッションを開始するには、次の例のようにコマンドを入力します。

```
ssh -x -l userid 192.168.70.132
```

ここで、-x は X Window システム転送なしを示し、-l はセッションでユーザー ID *userid* を使用することを示します。

IMM の構成の復元と変更

保管された構成を完全にリストアすることができます。あるいは、IMM に構成をリストアする前に、保管された構成のキー・フィールドを変更することもできます。構成ファイルをリストアする前に変更することにより、構成がよく似た複数の IMM をセットアップできます。共通する共用情報を再入力することなしに、名前や IP アドレスなどの固有値を必要とするパラメーターを素早く指定することができます。

現行の構成を復元または変更するには、次のステップを実行します。

1. 構成をリストアする IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Configuration File**」をクリックします。
3. 「**Restore IMM Configuration**」エリアで、「**Browse**」をクリックします。
4. 該当する構成ファイルをクリックしてから、「**Open**」をクリックします。ファイル (絶対パスを含む) が「**Browse**」の隣のボックスに表示されます。
5. 構成ファイルに変更を加えない場合は、「**Restore**」をクリックします。新しいウィンドウが開き、IMM 構成情報が表示されます。それがリストアしたい構成であることを確認してください。それが正しい構成ではない場合は、「**Cancel**」をクリックします。

構成をリストアする前に構成ファイルを変更する場合は、「**Modify and Restore**」をクリックして編集可能な構成要約ウィンドウを開きます。初めは、変更できるフィールドのみが表示されます。このビューと完全な構成要約ウィンドウを切り替えるには、ウィンドウの上部または下部にある「**Toggle View**」ボタンをクリックします。フィールドの内容を変更するには、対応するテキスト・ボックスをクリックして、データを入力します。

注: 「**Restore**」または「**Modify and Restore**」をクリックすると、リストアしようとしている構成ファイルが別のタイプのサービス・プロセッサによって作成された場合や、同じタイプでも古いファームウェアの (したがって機能性の低い) サービス・プロセッサによって作成された場合は、アラート・ウィンドウが開かれることがあります。このアラート・メッセージには、リストアが完了した後に構成する必要があるシステム管理機能のリストが表示されます。一部の機能は、複数のウィンドウで構成する必要があります。

6. IMM へのこのファイルのリストアを続行するには、「**Restore Configuration**」をクリックします。IMM 上のファームウェアが更新されると進行標識が表示されます。更新が正常に行われたかどうかを確認するための確認ウィンドウが開きます。

注: 「Security」ページのセキュリティ設定は、リストア操作では復元されません。セキュリティ設定の変更については、90 ページの『セキュア Web サーバー、IBM Systems Director、およびセキュア LDAP』を参照してください。

7. リストア・プロセスが完了した旨の確認を受け取った後、ナビゲーション・ペインで「**Restart IMM**」をクリックし、「**Restart**」をクリックします。
8. 「**OK**」をクリックして、IMM を再始動することを確認します。
9. 「**OK**」をクリックして、現行のブラウザー・ウィンドウを閉じます。
10. IMM に再度ログインするには、ブラウザーを始動して、通常のログイン・プロセスに従います。

構成ファイルの使用

IMM 構成のバックアップとリストアを行うには、ナビゲーション・ペインで「**Configuration File**」を選択します。

重要: 「Security」ページの設定値は、バックアップ操作で保管されず、リストア操作でリストアすることができません。

現行構成のバックアップ

現行の IMM の構成のコピーを、IMM Web インターフェースを実行しているクライアント・コンピューターにダウンロードできます。IMM の構成が誤って変更または損傷された場合に、このバックアップ・コピーを使用して復元することができます。このコピーは、変更を加えて、構成が似ている複数の IMM を構成するための基本としても使用できます。

この手順で保管された構成情報には、System x[®] サーバー・ファームウェアの構成設定、非 IPMI ユーザー・インターフェースと共通ではないすべての IPMI 設定は、いずれも含まれません。

現行の構成をバックアップするには、次のステップを実行します。

1. 現行の構成をバックアップしたい IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Configuration File**」をクリックします。
3. 「**Backup IMM Configuration**」エリアで、「**view the current configuration summary**」をクリックします。
4. 設定を確認してから、「**Close**」をクリックします。
5. この構成をバックアップするには、「**Backup**」をクリックします。
6. バックアップの名前を入力し、ファイルを保管する場所を選択してから、「**Save**」をクリックします。

Mozilla Firefox の場合、「**Save File**」をクリックして、「**OK**」をクリックします。

Microsoft Internet Explorer では、「**Save this file to disk**」をクリックしてから、「**OK**」をクリックします。

IMM の構成の復元と変更

保管された構成を完全にリストアすることができます。あるいは、IMM に構成をリストアする前に、保管された構成のキー・フィールドを変更することもできます。構成ファイルをリストアする前に変更することにより、構成がよく似た複数の IMM をセットアップできます。共通する共用情報を再入力することなしに、名前や IP アドレスなどの固有値を必要とするパラメーターを素早く指定することができます。

現行の構成を復元または変更するには、次のステップを実行します。

1. 構成をリストアする IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Configuration File**」をクリックします。
3. 「**Restore IMM Configuration**」エリアで、「**Browse**」をクリックします。
4. 該当する構成ファイルをクリックしてから、「**Open**」をクリックします。ファイル（絶対パスを含む）が「**Browse**」の隣のボックスに表示されます。
5. 構成ファイルに変更を加えない場合は、「**Restore**」をクリックします。新しいウィンドウが開き、IMM 構成情報が表示されます。それがリストアしたい構成であることを確認してください。それが正しい構成ではない場合は、「**Cancel**」をクリックします。

構成をリストアする前に構成ファイルを変更する場合は、「**Modify and Restore**」をクリックして編集可能な構成要約ウィンドウを開きます。初めは、変更できるフィールドのみが表示されます。このビューと完全な構成要約ウィンドウを切り替えるには、ウィンドウの上部または下部にある「**Toggle View**」ボタンをクリックします。フィールドの内容を変更するには、対応するテキスト・ボックスをクリックして、データを入力します。

注: 「**Restore**」または「**Modify and Restore**」をクリックすると、リストアしようとしている構成ファイルが別のタイプのサービス・プロセッサによって作成された場合や、同じタイプでも古いファームウェアの（したがって機能性の低い）サービス・プロセッサによって作成された場合は、アラート・ウィンドウが開かれることがあります。このアラート・メッセージには、リストアが完了した後に構成する必要があるシステム管理機能のリストが表示されます。一部の機能は、複数のウィンドウで構成する必要があります。

6. IMM へのこのファイルのリストアを続行するには、「**Restore Configuration**」をクリックします。IMM 上のファームウェアが更新されると進行標識が表示されます。更新が正常に行われたかどうかを確認するための確認ウィンドウが開きます。

注: 「**Security**」ページのセキュリティー設定は、リストア操作では復元されません。セキュリティー設定の変更については、90 ページの『セキュア Web サーバー、IBM Systems Director、およびセキュア LDAP』を参照してください。

7. リストア・プロセスが完了した旨の確認を受け取った後、ナビゲーション・ペインで「**Restart IMM**」をクリックし、「**Restart**」をクリックします。
8. 「**OK**」をクリックして、IMM を再始動することを確認します。
9. 「**OK**」をクリックして、現行のブラウザ・ウィンドウを閉じます。
10. IMM に再度ログインするには、ブラウザを始動して、通常のログイン・プロセスに従います。

デフォルトのリストア

Supervisor アクセス権を持っている場合、「**Restore Defaults**」リンクを使用して、IMM のデフォルト構成をリストアします。

重要: 「**Restore Defaults**」をクリックすると、IMM に加えたすべての変更が失われます。

IMM デフォルトをリストアするには、以下のステップを実行します。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Restore Defaults**」をクリックして IMM のデフォルト設定をリストアします。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。
3. IMM Web インターフェースを使用するために、再びログインします。
4. 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。ネットワーク・インターフェースについては、41 ページの『ネットワーク・インターフェースの構成』を参照してください。

IMM の再始動

「**Restart IMM**」リンクを使用して、IMM を再始動します。この機能を実行できるのは、Supervisor アクセス権を持っている場合だけです。すべてのイーサネット接続は、一時的に停止します。IMM Web インターフェースを使用するには、再度ログインする必要があります。

IMM を再始動するには、次の手順に従ってください。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Restart IMM**」をクリックして IMM を再始動します。TCP/IP 接続またはモデム接続は、破壊されます。
3. IMM Web インターフェースを使用するために、再びログインします。

スケーラブル・パーティショニング

IMM を使用して、スケーラブル・マルチノード・システム内のシステムを構成および制御することができます。

IMM を使用して、スケーラブル・マルチノード・システム内のシステムを構成および制御することができます。サーバーにエラーが存在する場合、IMM がイベント・ログにイベント・コードを返します (114 ページの『イベント・ログの表示』を参照)。

1. 構成をリストアする IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Scalable Partitioning**」をクリックし、次に「**Manage Partitions**」をクリックします。

Service Advisor 機能

Service Advisor 機能は、システム・ハードウェアのエラー・イベントを検出および収集し、問題判別のためにそのデータを自動的に IBM サポートに転送します。また、Service Advisor 機能は、システム・エラーに関するデータを収集して、そのデータを IBM サポートに転送することもできます。ご使用のサーバーがこの機能をサポートしているかを確認するには、サーバーの資料を参照してください。Service Advisor のセットアップ、テスト、および保守の手順は、以下のトピックで説明しています。

- Service Advisor の構成
- Service Advisor の使用

Service Advisor の構成

Service Advisor を構成するには、次のステップを実行してください。

1. Service Advisor をアクティブにする IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Service Advisor**」をクリックします。
3. このオプションを初めて使用する場合、あるいは IMM がデフォルト値にリセットされた場合は、使用許諾契約書を確認して受諾する必要があります。
 - a. 「**View Terms and Conditions**」をクリックし、Service Advisor の使用許諾契約書を表示します。
 - b. 契約条件ページで「**I accept the agreement**」をクリックし、Service Advisor をアクティブ化します。
4. 「**Service Advisor Settings**」タブをクリックします。

次の図のようなページが表示されます。

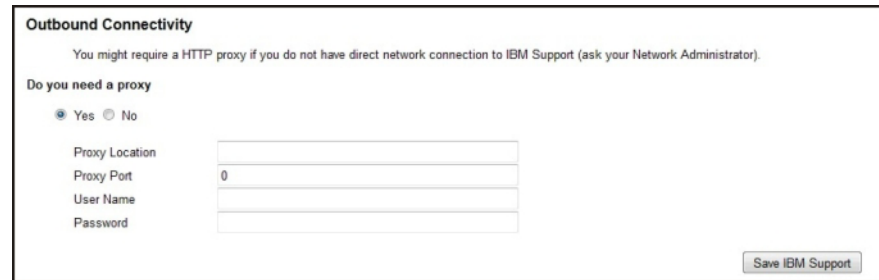
5. サーバー管理者の連絡先情報を入力します。「**Contact Information**」フィールドの説明については、以下の表を参照してください。

表 15. 連絡先情報

フィールド	説明
IBM Service Support Center	このフィールドでは、IBM Service Support Center の国別コードを指定します。これは、2 文字の ISO 国別コードで、IBM Service Support Center にアクセスできる国にのみ適用されます。
Company Name	このフィールドでは、連絡先担当者の組織名または会社名を指定します。このフィールドには、1 から 30 文字を入力できます。
Contact Name	このフィールドでは、連絡先担当者の組織名または会社名を指定します。このフィールドには、1 から 30 文字を入力できます。
Phone	このフィールドでは、連絡先担当者の電話番号を指定します。このフィールドには、5 から 30 文字を入力できます。
Email	このフィールドでは、連絡先担当者の E メール・アドレスを指定します。このフィールドの最大長は 30 文字です。
Address	このフィールドでは、IMM が物理的に配置されている住所を指定します。このフィールドには、1 から 30 文字を入力できます。
City	このフィールドでは、IMM が物理的に配置されている市町村名または地域を指定します。
State/Province	このフィールドでは、IMM が物理的に配置されている都道府県を指定します。このフィールドには、2 から 3 文字を入力できます。
Postal Code	このフィールドでは、サーバーの設置場所の郵便番号を指定します。このフィールドには、1 から 9 文字を入力できます (英数字のみが有効)。

6. IMM が IBM サポートに直接ネットワーク接続されていない場合は、HTTP プロキシを作成します。アウトバウンド接続情報を構成するには、以下のステップを実行します。
 - a. 「**Do you need a proxy**」フィールドで「**Yes**」をクリックします。上記の図を参照してください。

次の図のようなページが表示されます。

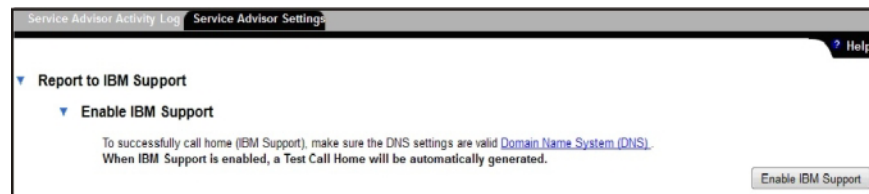


- b. 「**Proxy Location**」、「**Proxy Port**」、「**User Name**」、および「**Password**」を入力します。
7. 「**Save IBM Support**」をクリックし、変更を保存します。
8. 「**Enable IBM Support**」(ページの上部付近にあります)をクリックし、保守可能イベント・コードが生成されたときに Service Advisor が IBM サポートに連絡できるようにします。

注: IBM サポートを使用可能にすると、IBM サポート・サイトにテスト・コードが送信されます。

9. 「**Service Advisor Activity Log**」タブをクリックし、テスト・コードの状況を表示します。

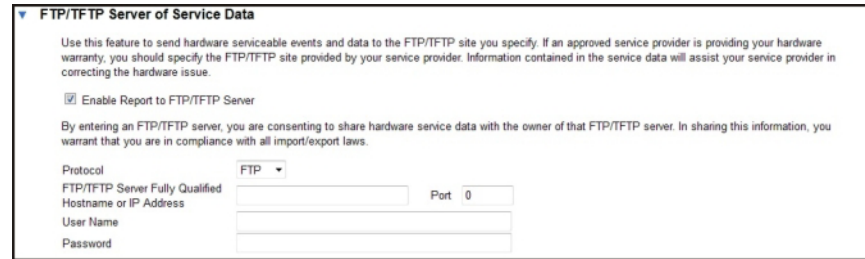
次の図のようなページが表示されます。



10. IBM サポートに連絡する前に別のサービス・プロバイダーがイベント・コードを受信することを許可する場合は、「**Enable Report to FTP/TFTP Server**」をクリックします。

重要: FTP/TFTP サーバーを入力することで、FTP/TFTP サーバーの所有者とハードウェア・サービス・データを共有することを承諾したことになります。この情報を共有することで、すべてのインポート/エクスポートの法律に準拠することを保証します。

次の図のようなページが表示されます。



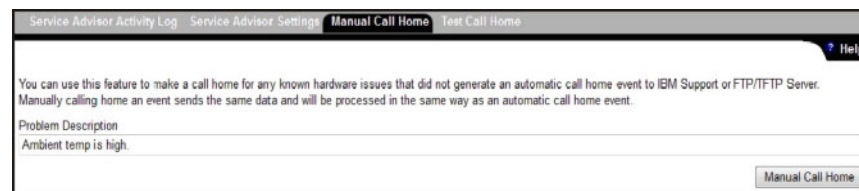
Service Advisor の使用

Service Advisor がセットアップされると、アクティビティー・ログの表示あるいはテスト・メッセージの生成が可能になります。

ご使用のサーバーに関するハードウェア障害レポートを作成するには、以下のステップを実行します。

1. Service Advisor を使用する IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Service Advisor**」をクリックします。
3. 「**Manual Call Home**」タブをクリックします。

次の図のようなページが表示されます。



4. イベントを手動でコール・ホームするには、以下のステップを実行します。
 - a. 「**Problem Description**」フィールドに問題の説明を入力します。
 - b. 「**Manual Call Home**」ボタンをクリックします。
5. テスト・メッセージを生成するには、「**Test Call Home**」タブをクリックし、「**Test Call Home**」ボタンを選択します。

注:

- テスト・コール・ホーム・メニューは、現行設定を使用して、IMM と IBM または FTP/TFTP サーバーとの間の通信パスを検査します。
 - テストが成功しない場合、ネットワーク・セットアップを確認してください。
 - IBM サポートにレポートを送信するには、Service Advisor は、IMM で DNS サーバー・アドレスが適切にセットアップされていることを必要とします。
 - コールが成功した場合は、「Assigned Service Number」あるいはチケット番号が割り当てられます。IBM サポートでオープンされるチケットは、テスト・チケットとして識別されます。テスト・チケットの場合、IBM から要求されるアクションはありません。また、コールはクローズされます。
6. 「**Service Advisor Activity Log**」タブをクリックし、アクティビティー・ログの状況を表示します。

次の図のようなページが表示されます。

Service Advisor Activity Log

Service Advisor Settings

Manual Call Home

Test Call Home

Help

Refresh

Display For Both IBM Support and FTP/TFTP Server

Corrected	IBM Support		FTP/TFTP Server	Event ID	Event Severity	Date/Time	Message	
	Send	Assigned Num						
☐	NO	Pending	N/A	Pending	0x400000ca00000000	Info	08/07/2012; 18:58:41	Manual Call Home by USERID: Ambient temp is high.
☐	NO	Pending	N/A	Pending	0x400000c900000000	Info	08/07/2012; 18:31:56	Test Call Home Generated by USERID
☐	NO	Success	672P492FG3	Disabled	0x400000c900000000	Info	08/07/2012; 18:29:25	Test Call Home Generated by USERID
☐	NO	Disabled	N/A	Pending	0x400000c900000000	Info	08/07/2012; 17:47:14	Test Call Home Generated by USERID
End Of Log								

Save

You can use the [Call Home Exclusion List](#) to specify specific call home events not to be reported

注:

- アクティビティー・ログは、「Test Call Home」および「Manual Call Home」イベントを含む最新のコール・ホーム・イベントを 5 個表示します。
- 「Send」フィールドに、以下のいずれかの結果が示されます。

Success

コールは正常に IBM または FTP/TFTP で受信されました。

「Assigned Service Number」フィールドに、問題チケット番号が表示されます。

Pending

コール・ホーム・イベントは進行中です。

Failed

コール・ホーム・イベントは失敗しました。コール・ホーム・イベントが失敗した場合、IBM サポートに連絡し、ハードウェア・サービス・イベントを報告してください。失敗したコール・ホーム・イベントは、再試行されません。

7. イベントを解決した後、そのイベントの「Corrected」チェック・ボックスをクリックし、未解決のイベントを見つけやすいようにします。

注: イベントの「Corrected」チェック・ボックスが選択されていないと、同じイベントが次に発生した場合に、そのイベントが最初に発生してから 5 日間経過するまでコール・ホーム されません。

8. 「Refresh」をクリックし、最新情報を表示します。

注: 「Assigned Service Number」を使用して、IBM サポートとの通信時にコール・ホーム・イベントを参照することができます。

9. 指定されたイベントを IBM サポートへのレポートから削除するには、以下のステップを実行します。
 - a. 「Call Home Exclusion List」リンクをクリックします。次の図のようなページが表示されます。

Call Home Exclusion List 

This table below shows the list of event IDs that will not be reported by call home. You can add events to this table by entering an event ID in the text box and clicking the add button. Event IDs can be obtained from the [Event Log](#) and [Service Advisor Activity Log](#) and entered into the textbox using the copy-and-paste function.

 A maximum of 20 events can be added to this exclusion list, currently 20 more events can be added.

Event ID:

Selected	Index	Event ID
No entries		

- b. 16 進数のイベント ID を「**Event ID**」フィールドに入力します。
- c. 「**追加**」をクリックします。

ログオフ

IMM あるいは他のリモート・サーバーからログオフするには、ナビゲーション・ペインで「**Log Off**」をクリックします。

第 4 章 サーバー状況のモニター

アクセス先のサーバーの状況を表示するには、ナビゲーション・ペインの「**Monitors**」という見出しの下にあるリンクを使用します。

「**System Status**」ページから、次のことができます。

- サーバーの電源状況をモニターし、オペレーティング・システムの状態を表示する
- サーバーの温度測定値、電圧しきい値、およびファン速度を表示する
- 最新のサーバー・オペレーティング・システム障害画面取りを表示する
- IMM にログインしたユーザーのリストを表示する

「**Virtual Light Path**」ページから、サーバー上で点灯しているすべての LED の名前、色、および状況を表示することができます。

「**Event Log**」ページから、次のことができます。

- IMM のイベント・ログに記録された特定のイベントを表示する
- イベントの重大度を表示する

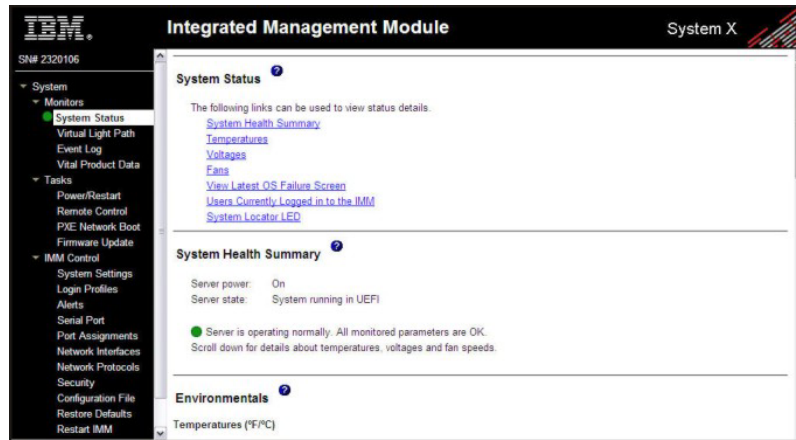
「**Vital Product Data (VPD)**」ページから、重要プロダクト・データを表示することができます。

システム状況の表示

「**System Status**」ページでは、サーバーの温度測定値、電圧しきい値、ファン状況をモニターできます。最新のオペレーティング・システム障害画面、IMM にログインしたユーザー、およびシステム・ロケーター LED を表示することもできます。

サーバーのシステム・ヘルスおよび環境情報を表示するには、以下のステップを実行します。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**System Status**」をクリックして、サーバーの全般的なヘルスに関する動的に生成された更新を表示します。次の図のようなページが表示されます。



サーバーの状況に応じて、「System Health Summary」ページの上部に示されるメッセージが決まります。次のいずれかのシンボルが表示されます。

- ・ 緑色で塗りつぶした円と「Server is operating normally」の語句
- ・ 中に X が入っている赤色の円、または中に感嘆符が入っている黄色の三角形と、「One or more monitored parameters are abnormal」の語句

モニター対象のパラメーターが通常範囲外で作動している場合は、「System Health Summary」ページに特定の異常パラメーターのリストが表示されます。

3. このページの「**Environmentals**」セクションで「**Temperature**」エリアまでスクロールダウンします。ここには、温度、電圧、およびファン速度情報が表示されます。

IMM は、マイクロプロセッサ、システム・ボード、およびハード・ディスク・バックプレーンなどのシステム・コンポーネントについて、現行の温度測定値としきい値レベルを追跡します。温度測定値をクリックすると、新しいウィンドウが開きます。

Ambient Temp Thresholds (°C)			
Sensors	Non - Critical	Critical	Fatal
Upper Threshold	34.000000	37.000000	41.000000
Lower Threshold	N/A	N/A	N/A

「Temperature Thresholds」ページには、IMM が反応する温度レベルが表示されます。これらの温度しきい値はリモート・サーバー上で事前設定されており、変更することはできません。

報告される温度は、以下のしきい値範囲に対して測定されています。

Non-Critical

温度が指定された値に達すると、構成済みのリモート・アラート受信者

へ温度アラートが送信されます。アラートを送信するには、「Alerts」ページの「SNMP Alerts Settings」エリアで「Warning Alerts」チェック・ボックスを選択するか、あるいは「Remote Alert Recipient」ページで「Warning Alerts」チェック・ボックスを選択する必要があります。

アラート・オプションの詳しい選択方法については、37 ページの『SNMP アラート設定の構成』 または 35 ページの『リモート・アラート受信者の構成』 を参照してください。

Critical

温度が警告値より高い指定値 (ソフト・シャットダウンしきい値) に達すると、構成済みのリモート・アラート受信者へ 2 番目の温度アラートが送信され、サーバーはオペレーティング・システムの通常のシャットダウンによるシャットダウン・プロセスを開始します。その後、サーバーは自身の電源をオフにします。アラートを送信するには、「Alerts」ページの「SNMP Alerts Settings」エリアで「Critical Alerts」チェック・ボックスを選択するか、あるいは「Remote Alert Recipient」ページで「Critical Alerts」チェック・ボックスを選択する必要があります。

アラート・オプションの詳しい選択方法については、37 ページの『SNMP アラート設定の構成』 または 35 ページの『リモート・アラート受信者の構成』 を参照してください。

Fatal

温度がソフト・シャットダウン値より高い指定値 (ハード・シャットダウンしきい値) に達すると、サーバーはただちにシャットダウンを実行し、構成済みのリモート・アラート受信者にアラートを送信します。アラートを送信するには、「Alerts」ページの「SNMP Alerts Settings」エリアで「Fatal Alerts」チェック・ボックスを選択するか、あるいは「Remote Alert Recipient」ページで「Fatal Alerts」チェック・ボックスを選択する必要があります。

アラート・オプションの詳しい選択方法については、37 ページの『SNMP アラート設定の構成』 または 35 ページの『リモート・アラート受信者の構成』 を参照してください。

IMM は、しきい値に到達すると非クリティカル (non-critical) あるいはクリティカル (critical) イベントを生成し、必要に応じてシャットダウン処理を開始します。

4. 「Voltages」エリアまでスクロールダウンします。IMM は、モニター対象の給電部電圧が指定された作動範囲を外れると、アラートを送信します。

電圧測定値をクリックすると、新しいウィンドウが開きます。

Planar 3.3V Thresholds (Volt)			
Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	3.560000	N/A
Lower Threshold	N/A	3.040000	N/A

「Voltage Thresholds」ページには、IMM が反応する電圧範囲が表示されます。これらの電圧しきい値はリモート・サーバー上で事前設定されており、変更することはできません。

IMM Web インターフェースは、システム・ボードおよび電圧調節モジュール (VRM) の電圧測定値を表示します。システムは、次のアクションが取られる電圧範囲を設定します。

Non-Critical

電圧が指定された電圧範囲を下回るか上回った場合、構成済みのリモート・アラート受信者へ電圧アラートが送信されます。アラートを送信するには、「Alerts」ページの「**SNMP Alerts Settings**」エリアで

「**Warning Alerts**」チェック・ボックスを選択する必要があります。

アラート・オプションの詳しい選択方法については、37 ページの『SNMP アラート設定の構成』を参照してください。

Critical

電圧が指定された電圧範囲を下回るか上回った場合、構成済みのリモート・アラート受信者へ電圧アラートが送信され、サーバーはオペレーティング・システムの通常のシャットダウンによるシャットダウン・プロセスを開始します。その後、サーバーは自身の電源をオフにします。アラートを送信するには、「Alerts」ページの「**SNMP Alerts Settings**」エリアで「**Critical Alerts**」チェック・ボックスを選択する必要があります。

アラート・オプションの詳しい選択方法については、37 ページの『SNMP アラート設定の構成』を参照してください。

Fatal 電圧が指定された電圧範囲を下回るか上回った場合、サーバーはただちにシャットダウンを実行し、構成済みのリモート・アラート受信者にアラートを送信します。アラートを送信するには、「Alerts」ページの「**SNMP Alerts Settings**」エリアで「**Critical Alerts**」チェック・ボックスを選択する必要があります。

注: ハード・シャットダウン・アラートが送信されるのは、ソフト・シャットダウン・アラートがまだ送信されていない場合だけです。

アラート・オプションの詳しい選択方法については、37 ページの『SNMP アラート設定の構成』を参照してください。

IMM は、しきい値に到達すると非クリティカル (non-critical) あるいはクリティカル (critical) イベントを生成し、必要に応じてシャットダウン処理を生成します。

Non-critical

このしきい値に到達したことを IMM が示すと、警告イベントが生成されます。

Critical

このしきい値に到達したことを IMM が示すと、クリティカル・イベントが生成されます。

5. 「Fan Speeds (% of max)」エリアまでスクロールダウンします。IMM Web インターフェースは、サーバー・ファンの稼働速度 (最大ファン速度のパーセントとして表されます) を表示します。ファン測定値をクリックすると、新しいウィンドウが開きます。

Fan 1A Tach Thresholds (RPM)			
Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	N/A	N/A
Lower Threshold	N/A	290 000000	N/A

ファン速度が許容不可レベルまで低下するか、ファンが停止すると、ファン・アラートを受信します。アラートを送信するには、「Alerts」ページの「**SNMP Alerts Settings**」エリアで「**Critical Alerts**」チェック・ボックスを選択する必要があります。

アラート・オプションの詳しい選択方法については、37 ページの『SNMP アラート設定の構成』を参照してください。

6. 「View Latest OS Failure Screen」エリアまでスクロールします。「View OS Failure Screen」ボタンをクリックして、サーバーが機能を停止したときにキャプチャーされたオペレーティング・システム障害画面のイメージにアクセスします。

注:

オペレーティング・システム障害スクリーン・キャプチャー機能は、IMM 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は、5 ページの『IMM Standard から IMM Premium へのアップグレード』を参照してください。

オペレーティング・システムの稼働停止を引き起こすイベントが発生すると、オペレーティング・システム・ウォッチドッグが起動し、これによって IMM はオペレーティング・システム障害画面データをキャプチャーして保管します。IMM 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、古いオペレーティング・システム障害画面データは上書きされます。

サーバーのオペレーティング・システム障害画面イメージ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。

- IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
- ナビゲーション・ペインで、「System Health」をクリックした後、「View Latest OS Failure Screen」エリアまでスクロールダウンします。
- 「View OS Failure Screen」をクリックします。画面にオペレーティング・システム障害画面イメージが表示されます。

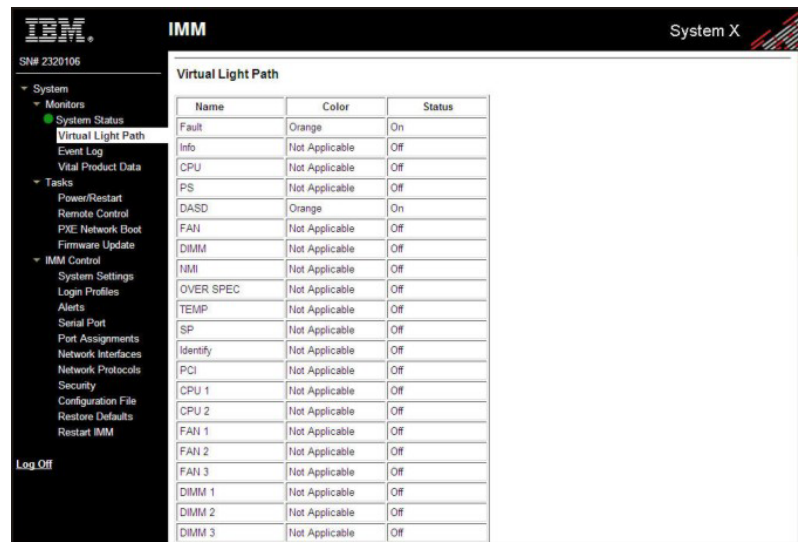
7. 「**Users Currently Logged in**」エリアまでスクロールします。 IMM Web インターフェイスは、IMM にログインしている各ユーザーのログイン ID とアクセス方式を表示します。
8. 「**System Locator LED**」エリアまでスクロールダウンします。 IMM Web インターフェイスは、システム・ロケータ LED の状況を表示します。また、LED の状況を変更するためのボタンも提供します。このエリアで表示される図について詳しくは、オンライン・ヘルプを参照してください。

Virtual Light Path の表示

「Virtual Light Path」画面では、サーバー上で点灯しているすべての LED の名前、色、状況が表示されます。

「Virtual Light Path」にアクセスして表示するには、以下のステップを実行します。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェイスの開始および使用』を参照してください。
2. ナビゲーション・ペインで「**Virtual Light Path**」をクリックし、サーバーの最近のイベント・ヒストリーを表示します。次の図のようなページが表示されます。



The screenshot shows the IMM Web interface. On the left is a navigation pane with a tree view containing 'System', 'Monitors', 'System Status', 'Virtual Light Path', 'Event Log', 'Vital Product Data', 'Tasks', 'Power/Restart', 'Remote Control', 'PXE Network Boot', 'Firmware Update', 'IMM Control', 'System Settings', 'Login Profiles', 'Alerts', 'Serial Port', 'Port Assignments', 'Network Interfaces', 'Network Protocols', 'Security', 'Configuration File', 'Restore Defaults', 'Restart IMM', and 'Log Off'. The main content area is titled 'Virtual Light Path' and contains a table with three columns: 'Name', 'Color', and 'Status'.

Name	Color	Status
Fault	Orange	On
Info	Not Applicable	Off
CPU	Not Applicable	Off
PS	Not Applicable	Off
DASD	Orange	On
FAH	Not Applicable	Off
DIMM	Not Applicable	Off
NMI	Not Applicable	Off
OVER SPEC	Not Applicable	Off
TEMP	Not Applicable	Off
SP	Not Applicable	Off
Identify	Not Applicable	Off
PCI	Not Applicable	Off
CPU 1	Not Applicable	Off
CPU 2	Not Applicable	Off
FAH 1	Not Applicable	Off
FAH 2	Not Applicable	Off
FAH 3	Not Applicable	Off
DIMM 1	Not Applicable	Off
DIMM 2	Not Applicable	Off
DIMM 3	Not Applicable	Off

3. スクロールダウンして、「Virtual Light Path」の完全なコンテンツを表示します。

注: サーバー上で LED が点灯していない場合、「Virtual Light Path」テーブルの「Color」列は LED Color が「Not Applicable」であると示します。

イベント・ログの表示

注: 特定のイベントあるいはメッセージの説明については、ご使用のサーバーの資料を参照してください。

エラー・コードおよびメッセージは、以下のタイプのイベント・ログに表示されます。

- **システム・イベント・ログ:** このログには、POST およびシステム管理割り込み (SMI) のイベントと、IMM に組み込まれている BMC が生成したすべてのイベントが含まれます。システム・イベント・ログは、Setup ユーティリティーおよび Dynamic System Analysis (DSA) プログラム (IPMI イベント・ログとして) から表示することができます。

システム・イベント・ログのサイズには制限があります。サイズがフルになっても、新規のエントリーは既存のエントリーを上書きしません。そのため、Setup ユーティリティーから定期的にシステム・イベント・ログを保存してクリアする必要があります。トラブルシューティングを行う場合は、最新のイベントを分析に使用できるように、システム・イベント・ログを保存してからクリアする必要があります。

画面の左側にメッセージがリストされ、選択したメッセージの詳細が画面の右側に表示されます。任意のエントリーから次のエントリーに移動するには、上矢印 (↑) キーおよび下矢印 (↓) キーを使用します。

イベントが発生すると、システム・イベント・ログに表明イベントが示されます。イベントが発生なくなると、システム・イベント・ログに表明解除イベントが示されます。

一部の IMM センサーは、表明イベントがその設定値に達すると、ログに記録されます。設定値に到達した状態ではなくなると、対応する表明解除イベントがログに記録されます。ただし、すべてのイベントのタイプが表明イベントというわけではありません。

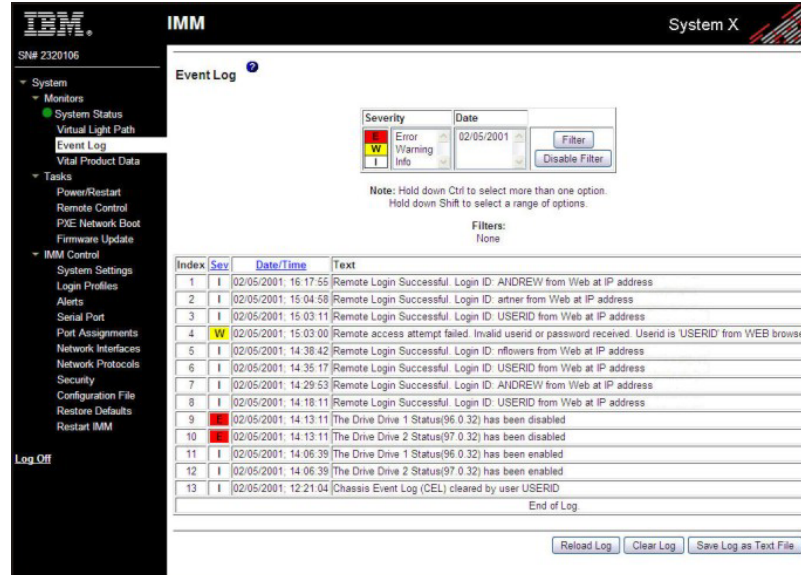
- **統合管理モジュール (IMM) イベント・ログ:** このログには、すべての IMM イベント、POST イベント、およびシステム管理割り込み (SMI) イベントのフィルタリングされたサブセットが含まれます。IMM イベント・ログは、IMM Web インターフェースおよび DSA プログラム (ASM イベント・ログとして) から表示することができます。
- **DSA ログ:** このログは、DSA プログラムによって生成され、システム・イベント・ログ (IPMI イベント・ログとして)、IMM シャーシ・イベント・ログ (ASM イベント・ログとして)、およびオペレーティング・システム・イベント・ログを時系列でまとめたものです。DSA ログは、DSA プログラムから表示することができます。
- **シャーシ・イベント・ログ:** IMM は、IPMI の表明イベントおよび表明解除イベントのテキスト・メッセージを生成し、それらのエントリーをシャーシ・イベント・ログに作成します。このテキストは、Distributed Management Task Force (DMTF) 仕様 DSP0244 から DSP8007 までのイベントについて生成されます。このログには、IPMI センサーの表明イベントおよび表明解除イベント以外のイベントのエントリーも含まれます。例えば、シャーシ・イベント・ログには、ユーザーがネットワーク設定を変更したり、Web インターフェースにログインしたことを示すエントリーも含まれます。このログは、IMM Web インターフェースから表示することができます。

Web インターフェースからのシステム・イベント・ログの表示

注: システム・イベント・ログは、限定された容量をもっています。限度に達すると、古いイベントが先入れ先出しの順に削除されます。

イベント・ログにアクセスして表示するには、次の手順に従ってください。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで「Event Log」をクリックし、サーバーの最近のイベント・ヒストリーを表示します。次の図のようなページが表示されます。



3. スクロールダウンして、イベント・ログの完全な目次を表示します。イベントに指定される重大度のレベルは、次のとおりです。

Informational

この重大度レベルは、注意する必要があるイベントに割り当てられます。

Warning

この重大度レベルは、サーバーのパフォーマンスに影響を及ぼす可能性があるイベントに割り当てられます。

エラー この重大度レベルは、ただちに注目する必要があるイベントに割り当てられます。

IMM Web インターフェースは、「Severity」列の中で警告イベント (黄色を背景とする英字 W) とエラー・イベント (赤色を背景とする英字 E) を区別します。

4. イベント・ログの内容をテキスト・ファイルとして保管するには、「Save Log as Text File」をクリックします。イベント・ログの表示をリフレッシュするには、「Reload Log」をクリックします。イベント・ログの内容を削除するには、「Clear Log」をクリックします。

Setup ユーティリティからのイベント・ログの表示

Setup ユーティリティの使用について詳しくは、ご使用のサーバーに付属の資料を参照してください。

POST イベント・ログあるいはシステム・イベント・ログを表示するには、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。

注: サーバーを AC 電源に接続してから約 2 分後に、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、イベント・ログを表示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. 「**System Event Logs**」を選択し、以下のいずれかの手順を実行します。
 - POST イベント・ログを表示するには、「**POST Event Viewer**」を選択します。
 - システム・イベント・ログを表示するには、「**System Event Log**」を選択します。

サーバーを再始動しないイベント・ログの表示

サーバーが停止していない場合に、サーバーを再始動することなく 1 つ以上のイベント・ログを表示する方法がいくつかあります。

Portable または Installable バージョンの Dynamic System Analysis (DSA) がインストールされている場合、それを使用してシステム・イベント・ログ (IPMI イベント・ログとして)、IMM イベント・ログ (ASM イベント・ログとして)、オペレーティング・システム・イベント・ログ、あるいはそれらをまとめた DSA ログを表示することができます。DSA Preboot を使用してこれらのログを表示することもできますが、DSA Preboot を使用するにはサーバーを再始動する必要があります。Portable DSA、Installable DSA、または DSA Preboot のインストール、あるいは DSA Preboot CD イメージのダウンロードを行うには、<http://www.ibm.com/support/jp/ja/supportsite.wss/docdisplay?lnocid=SERV-DSA&brandind=5000008> にアクセスするか、以下のステップを実行します。

注: IBM Web サイトは、定期的に変更されます。実際の手順は、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/jp/ja/> にアクセスします。
2. 「**Product support**」の下で「**System x**」をクリックします。
3. 「**Popular links**」の下で「**Software and device drivers**」をクリックします。
4. 「**Related downloads**」の下で、「**Dynamic System Analysis (DSA)**」をクリックし、ダウンロード可能な DSA ファイルのマトリックスを表示します。

サーバーに IPMItool がインストールされている場合は、それを使用してシステム・イベント・ログを表示することができます。最新バージョンの Linux オペレーティング・システムには、現行バージョンの IPMItool が付属しています。IPMItool については、<http://sourceforge.net/> にアクセスしてください。

注: IBM Web サイトは、定期的に変更されます。実際の手順は、本書の記載とは若干異なる場合があります。

1. <http://publib.boulder.ibm.com/infocenter/toolctr/v1r0/index.jsp> にアクセスします。
2. ナビゲーション・ペインで「**IBM System x and BladeCenter Tools Center**」をクリックします。

3. 「**Tools reference**」、「**Configuration tools**」、「**IPMI tools**」の順に展開し、「**IPMItool**」をクリックします。

IPMI の概要については、<http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/liaai/ipmi/liaaiipmi.htm> にアクセスするか、以下のステップを実行してください。

1. <http://publib.boulder.ibm.com/infocenter/systems/index.jsp> にアクセスします。
2. ナビゲーション・ペインで、「**IBM Systems Information Center**」をクリックします。
3. 「**Operating systems**」、「**Linux information**」、「**Blueprints for Linux on IBM systems**」の順に展開し、「**Using Intelligent Platform Management Interface (IPMI) on IBM Linux platforms**」をクリックします。

IMM イベント・ログは、IMM Web インターフェースの「**Event Log**」リンクから表示することができます。

次の表は、サーバーの状態に応じてイベント・ログを表示するのに使用できる方法を説明しています。最初の 2 つの状態では、通常、サーバーを再始動する必要はありません。

表 16. イベント・ログを表示する方法

状態	Action
サーバーは停止しておらず、ネットワークに接続されている。	以下のいずれかの方法を使用します。 • Portable バージョンまたは Installable バージョンの DSA を実行してイベント・ログを表示するか、あるいは IBM サービスおよびサポートに送信可能な出力ファイルを作成します。 • IMM の IP アドレスを入力し、「Event Log」ページに進みます。 • IPMItool を使用してシステム・イベント・ログを表示します。
サーバーは停止しておらず、ネットワークに接続されていない。	ローカルで IPMItool を使用してシステム・イベント・ログを使用します。

表 16. イベント・ログを表示する方法 (続き)

状態	Action
サーバーは停止している。	• DSA Preboot がインストールされている場合は、サーバーを再始動し、F2 を押して DSA Preboot を開始し、イベント・ログを表示します。 • DSA Preboot がインストールされていない場合は、DSA Preboot CD を挿入してサーバーを再始動し、DSA Preboot を開始してイベント・ログを表示します。 • あるいは、サーバーを再始動して F1 を押し、Setup ユーティリティーを開始して POST イベント・ログあるいはシステム・イベント・ログを表示します。詳しくは、116 ページの『Setup ユーティリティーからのイベント・ログの表示』を参照してください。

重要プロダクト・データの表示

サーバーの始動時に、IMM はサーバー情報、サーバー・ファームウェア情報、およびサーバー・コンポーネントの重要プロダクト・データ (VPD) を収集して、不揮発性メモリーに保管します。この情報には、ほとんどのコンピューターから随時アクセスできます。「Vital Product Data」ページには、IMM がモニターしているリモート管理対象サーバーに関する重要な情報が入っています。

サーバー・コンポーネントの重要プロダクト・データを表示するには、以下のステップを実行します。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「Vital Product Data」をクリックしてサーバー上のハードウェア・コンポーネントとソフトウェア・コンポーネントの状況を表示します。
3. スクロールダウンして、次の VPD 読み取り事項を表示します。

Machine level VPD

サーバーの重要プロダクト・データは、このエリアに表示されます。VPD の表示用に、マシン・レベル VPD には汎用固有 ID (UUID) が組み込まれています。

注: マシン・レベル VPD、コンポーネント・レベル VPD、およびコンポーネント・アクティビティー・ログはサーバーの電源がオンのときにのみ情報を提供します。

表 17. マシン・レベルの重要プロダクト・データ

フィールド	機能
マシン・タイプとモデル	IMM がモニターしているサーバーのタイプと型式番号を識別します。

表 17. マシン・レベルの重要プロダクト・データ (続き)

フィールド	機能
シリアル番号	IMM がモニターしているサーバーのシリアル番号を識別します。
UUID	IMM がモニターしているサーバーの汎用固有 ID (UUID) である 32 桁の 16 進数を識別します。

Component Level VPD

リモート管理対象サーバーのコンポーネントに関する重要プロダクト・データは、このエリアに表示されます。

表 18. コンポーネント・レベルの重要プロダクト・データ

フィールド	機能
FRU 名	各コンポーネントの FRU (現場交換可能ユニット) を識別します。
シリアル番号	各コンポーネントのシリアル番号を識別します。
Mfg ID	各コンポーネントの製造元 ID を識別します。

Component Activity Log

コンポーネント・アクティビティの記録をこのエリアに表示できます。

表 19. コンポーネントのアクティビティ・ログ

フィールド	機能
FRU 名	コンポーネントの FRU (現場交換可能ユニット) 名を識別します。
シリアル番号	コンポーネントのシリアル番号を識別します。
Mfg ID	コンポーネントの製造元を識別します。
Action	各コンポーネントに対して行われる処置を識別します。
Timestamp	コンポーネント・アクションの日付と時刻を識別します。日付は、 <i>mm/dd/yy</i> の形式で表示されます。時刻は、 <i>hh:mm:ss</i> の形式で表示されます。

IMM VPD

リモート管理対象サーバーの IMM ファームウェア、System x サーバー・ファームウェア、および Dynamic System Analysis ファームウェア VPD を、このエリアで表示することができます。

表 20. IMM、UEFI、および DSA ファームウェア重要プロダクト・データ

フィールド	機能
Firmware type	ファームウェア・コードのタイプを示します。
Version string	ファームウェア・コードのバージョンを示します。
Release date	ファームウェアがいつリリースされたかを示します。

第 5 章 IMM タスクの実行

IMM とサーバーのアクションを直接制御するには、ナビゲーション・ペインの「Tasks」という見出しの下にある機能を使用します。実行できるタスクは、IMM が取り付けられているサーバーによって異なります。

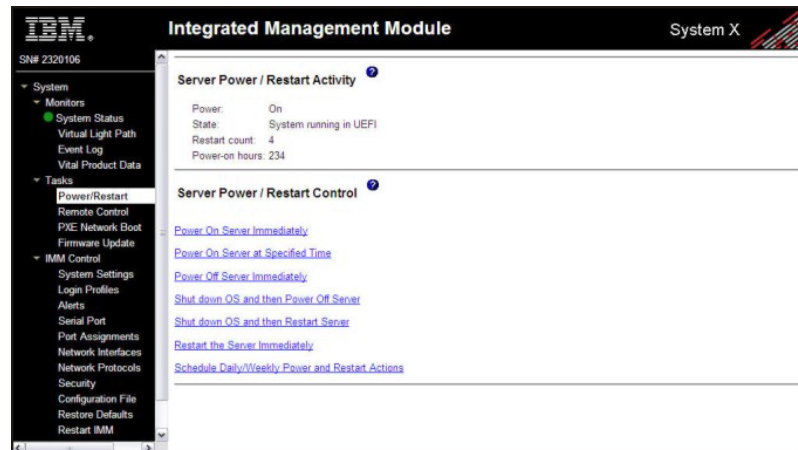
次のタスクを実行できます。

- 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
- IMM ファームウェアを更新する

注: 一部の機能は、サポートされている Microsoft Windows オペレーティング・システムを実行しているサーバー上でのみ使用可能です。

サーバーの電源および再始動アクティビティの表示

「Server Power/Restart Activity」エリアに、Web ページが生成された時点でのサーバーの電源状況が表示されます。



電源 このフィールドは、現在の Web ページが生成された時点でのサーバーの電源状況を示します。

State このフィールドは、現在の Web ページが生成された時点でのサーバーの状態を示します。考えられる状態は、次のとおりです。

- System power off/State unknown
- System on/starting UEFI
- System stopped in UEFI (Error detected)
- System running in UEFI

- Booting OS or in unsupported OS (might be in the operating system if the operating system is not configured to support the in-band interface to the IMM)
- OS booted

Restart count

このフィールドは、サーバーが再始動した回数を示します。

注: カウンターは、IMM サブシステムが出荷時のデフォルト値へクリアされるたびに、ゼロにリセットされます。

Power-on hours

このフィールドは、サーバーの電源がオンにされていた合計時間数を示します。

サーバーの電源状況の制御

IMM は、ご使用のサーバーを通じての完全な電源制御を提供し、パワーオン、パワーオフ、および再始動のアクションがあります。そのほかに、パワーオンおよび再始動の統計がキャプチャーされて表示され、ハードウェアの可用性を示します。

「**Server Power/Restart Control**」エリアにあるアクションを実行するには、IMM への Supervisor アクセス権限を持っている必要があります。

サーバーの電源および再始動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。

注: 以下のオプションを選択するのは、緊急時の場合、またはオフサイトにいてサーバーが反応しない場合だけにしてください。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Power/Restart**」をクリックします。「**Server Power/Restart Control**」エリアまでスクロールダウンします。
3. 次のいずれかのオプションをクリックします。

Power on server immediately

サーバーの電源をオンにしてオペレーティング・システムを始動します。

Power on server at specified time

指定した時刻にサーバーの電源をオンにしてオペレーティング・システムを始動します。

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します。

Shut down OS and then power off server

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。

注: 「Shut down OS and then power off server」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・セーバーまたはロック・モードの場合、IMM は正常シャットダウンを開始できない可能性があります。

IMM は、ハード・リセットを実行するか、あるいは電源オフ遅延間隔が経過した後に、OS がまだ稼働中であってもシャットダウンします。

Shut down OS and then restart server

オペレーティング・システムを再始動します。

注: 「Shut down OS and then restart server」 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・セーバーまたはロック・モードの場合、IMM は正常シャットダウンを開始できない可能性があります。
IMM は、ハード・リセットを実行するか、あるいは電源オフ遅延間隔が経過した後に、OS がまだ稼働中であってもシャットダウンします。

Restart the server immediately

オペレーティング・システムのシャットダウンを行わずに、即時にサーバーの電源をオフにしてからオンにします。

Schedule daily/weekly power and restart actions

オペレーティング・システムをシャットダウンし、毎日または毎週、指定した時刻にサーバーの電源をオフにし (サーバーを再始動する場合としない場合があります)、毎日または毎週、指定した時刻にサーバーの電源をオンにします。

これらのオプションのいずれかを選択すると確認メッセージが表示され、選択を誤った場合は操作を取り消すことができます。

リモート・プレゼンス

注:

1. IMM リモート・プレゼンス機能は、IMM 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、5 ページの『IMM Standard から IMM Premium へのアップグレード』を参照してください。
2. Remote Control 機能は、IMM Web インターフェースからのみ使用可能です。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 IMM にログインする必要があります。

IMM Web インターフェースでリモート・プレゼンス機能あるいは Remote Control 機能を使用することで、サーバー・コンソールの表示および対話を行うことができます。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ett・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。

Remote Control 機能は、以下の機能を提供します。

- サーバーの状態に関わらず、75 Hz で最大 1280 x 1024 のグラフィックス解像度のビデオをリモートで表示します。
- リモート・クライアントのキーボードおよびマウスを使用して、サーバーにリモート側からアクセスします。

- リモート・クライアントの 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 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 IMM メモリーにアップロードし、仮想ドライブとしてサーバーにマッピングします。

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

重要: IMM 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。IMM 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)。IMM 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、以下のステップを実行します。

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、IMM 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。

IMM ファームウェアの更新について詳しくは、136 ページの『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

注: IMM リモート・プレゼンス機能は、IMM 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、5 ページの『IMM Standard から IMM Premium へのアップグレード』を参照してください。

リモート・プレゼンス機能を使用可能にするには、次のステップを実行します。

1. 電源コードを抜いてサーバーから電源を切り離します。
2. 仮想メディア・キーをシステム・ボード上の専用スロットに取り付けます。
3. 電源をサーバーに再接続します。

注: サーバーを AC 電源に接続してから約 2 分後に、電源制御ボタンがアクティブになります。

4. サーバーの電源を入れます。

Remote Control

IMM の Remote Control 機能は、次の 2 つの個別のウィンドウで表示される 2 つの Java アプリケーションから構成されています。

Video Viewer

「Video Viewer」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。サーバー・コンソールに表示されるとおりのものがお客様のモニター上に表示され、お客様はコンソールのキーボードとマウスを制御できます。

Virtual Media Session

「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。これにより、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。

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. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Remote Control**」をクリックします。次の図のようなページが表示されます。

Remote Control

Status: No currently active sessions

To control the server remotely, use one of the links at the bottom of the page. If you want exclusive remote access during your session, click "Start Remote Control in Single User Mode." If you want to allow other users remote console (KVM) access during your session, click "Start Remote Control in Multi-user Mode." A new window will appear that provides access to the Remote Disk and Remote Console functionality. The Remote Disk functionality is launched from the Remote Console window, "Tools" drop-down menu. (Note that the Remote Disk function does not support multiple users).

To protect sensitive disk and KVM data during your session, click the "Encrypt disk and KVM data during transmission" check box before starting Remote Control. For complete security, this should be used in conjunction with SSL (SSL can be configured on the Security page under IMM Control).

☒ Use the Java Client
☐ Use the ActiveX Client with Microsoft Internet Explorer

Note: An Internet connection is required to download the Java Runtime Environment (JRE) if the Java Plug-in is not already installed. Remote Control is supported for Sun JRE 6.0 update 10 or later versions.

[Get Java Web Start and the latest Java Runtime here](#)

☐ Encrypt disk and KVM data during transmission
☐ Disable USB high speed performance (Change takes effect after an IMM Restart)

[Start Remote Control in Single User Mode](#)
[Start Remote Control in Multi-User Mode](#)

3. 次のオプションのいずれかを選択してください。
 - Java アプレットを使用してリモート・プレゼンスを実行するには、「**Use the Java Client**」をクリックします。

- Windows オペレーティング・システムで Internet Explorer を使用し、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するには、「**Use the ActiveX Client with Microsoft Internet Explorer**」をクリックします。

注: 32 ビット ActiveX リモート・プレゼンス・クライアントは、IMM ファームウェア・バージョン 1.28 以降で使用可能です。64 ビット ActiveX クライアントは、IMM ファームウェア・バージョン 1.30 以降で使用可能です。

4. サーバーをリモート側で制御するには、「Remote Control」ページの下部にあるリンクの 1 つを使用します。セッションで排他的なリモート・アクセスが必要な場合は、「**Start Remote Control in Single User Mode**」をクリックします。セッションで他のユーザーにもリモート・コンソール (KVM) アクセスを許可したい場合は、「**Start Remote Control in Multi-user Mode**」をクリックします。新しいウィンドウが開き、リモート・ディスクおよびリモート・コンソール機能にアクセスできます。

「Remote Control」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。

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

注:

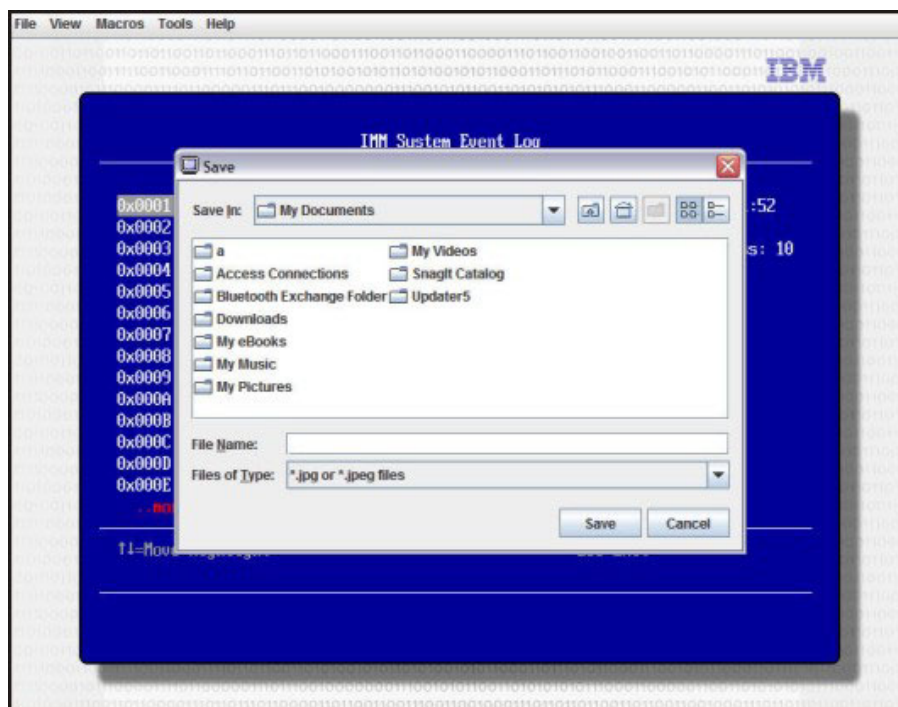
1. リモート・ディスクがマップされている状態で「Virtual Media Session」ウィンドウを閉じないでください。リモート・ディスクのクローズおよびマップ解除の手順については、132 ページの『リモート・ディスク』を参照してください。
2. Remote Control を使用してマウスまたはキーボードの問題が生じた場合は、Web インターフェースの「Remote Control」ページから使用できるヘルプを参照してください。
3. リモート・コンソールを使用して、Setup ユーティリティー・プログラムで IMM の設定を変更すると、サーバーが IMM を再始動する場合があります。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 IMM 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。

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・ファイルの名前を付け、ローカル・クライアント上で選択した場所にそのファイルを保存します。

注: スクリーン・キャプチャー・イメージは、JPG または JPEG ファイル・タイプで保管されます。



Remote Control の Video Viewer の表示モード

「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。

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。

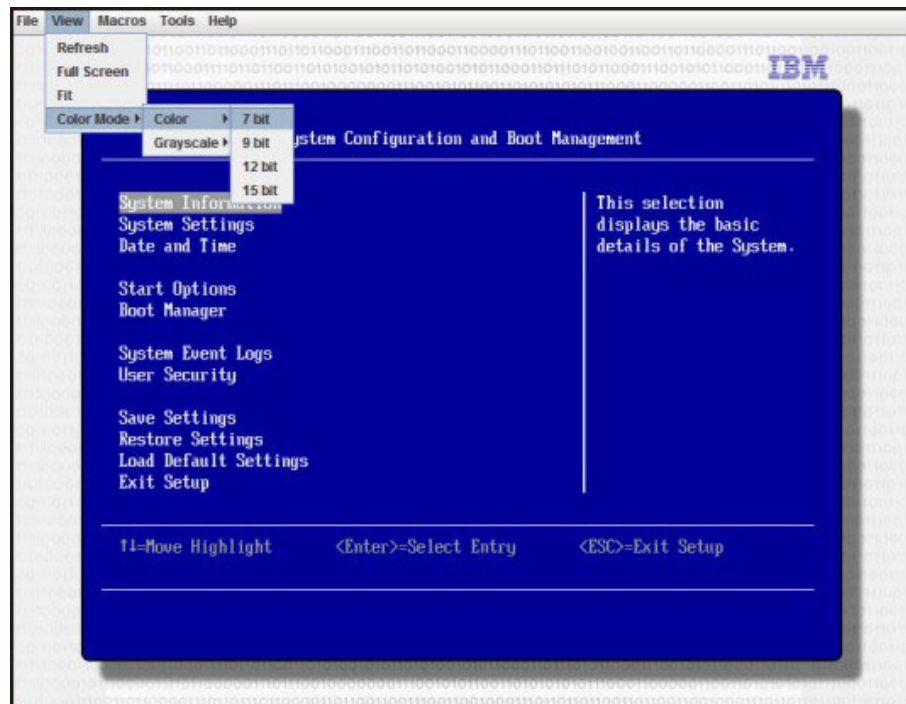
Remote Control のビデオ・カラー・モード

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: リモート管理アダプター II インターフェースの帯域幅スライダーに代わり、IMM にはカラー階調調整によって低帯域幅状態で送信されるデータを削減することができるメニュー項目があります。

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. メニューの「**Color Mode**」の上にマウス・ポインターを移動すると、次の 2 つのカラー・モード選択項目が表示されます。
 - Color: 7、9、12、および 15 bit
 - Grayscale: 16、32、64、128 shade

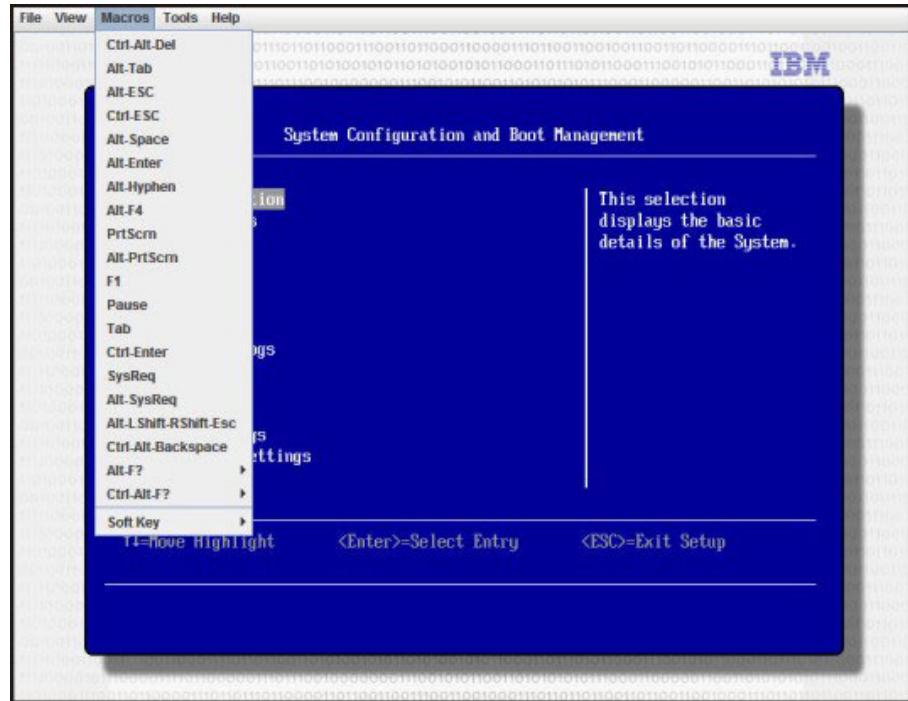


3. カラーあるいはグレースケールの設定を選択します。

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（例えば、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、例えば 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。



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. 新規のキーの組み合わせを追加する場合は、ポップアップ・ウィンドウに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・パススルー機能は、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」ウィンドウが表示されたら、「**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、機能を使用可能あるい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。

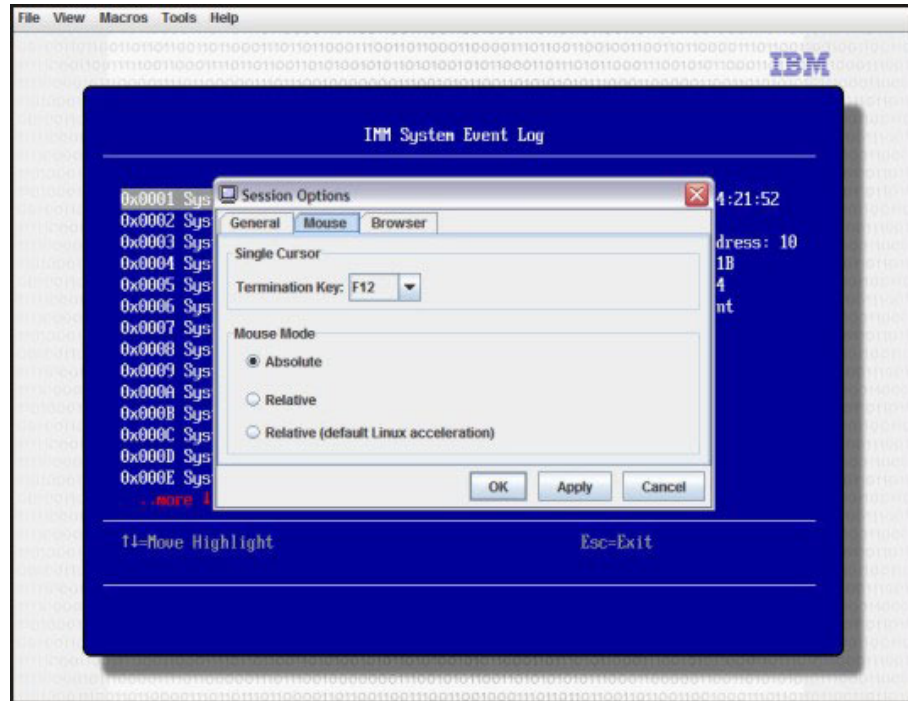
Remote Control のマウス・サポート

「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。



4. 以下のマウス・モードから 1 つを選択します。

Absolute

クライアントは、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。これは常に表示エリアの原点 (左上) との相対位置です。

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、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. 「**Single Cursor**」を選択します。

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、定義した終了キーを押します。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. メニューの「**Power**」の上にマウス・ポインターを移動すると、以下の選択項目が表示されます。

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 のパフォーマンス統計を表示するには、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. 「**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ように切り替えることができます。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。

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、あるいは 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

ディスク・イメージをサーバーで使用するように指定することもできます。そのドライブを使用して、サーバーの再始動 (ブート)、コードの更新、サーバーへの新規ソフトウェアのインストール、サーバー上のオペレーティング・システムのインストールまたは更新などの機能を実行できます。Remote Control 機能を使用して、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:

1. 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・ディスク機能に必要な USB サポートがあります。
 - Microsoft Windows Server 2008
 - Microsoft Windows Server 2003
 - Red Hat 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
2. 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。
3. 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. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**Remote Control**」をクリックします。
3. 「Remote Control」ページで、「**Start Remote Control**」オプションのいずれかををクリックします。
 - セッションで排他的なリモート・アクセスが必要な場合は、「**Start Remote Control in Single User Mode**」をクリックします。
 - ユーザーのセッション中に他のユーザーがリモート・コンソール (KVM) にアクセスすることを許可するには、「**Start Remote Control in Multi-user Mode**」をクリックします。

「Video Viewer」ウィンドウが開きます。
4. 「Virtual Media Session」ウィンドウを開くには、「Video Viewer」ウィンドウで「**Tools**」 > 「**Launch Virtual Media**」をクリックします。

注: 「Remote Control」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。

IMM ファームウェア・バージョン 1.03 以降での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。

ディスク・イメージ・ファイルを選択して、ディスク・イメージを IMM メモリーに保管することができます。これにより、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、IMM Web インターフェース・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。IMM カード上に格納できるドライブ・イメージは、最大で 1 つです。そのドライブまたはイメージの内容は、1.44 MB 以下でなければなりません。ディスク・イメージ・ファイルをアップロードするには、以下のステップを実行します。

1. 「**RDOC**」をクリックします。
2. 新規ウィンドウが開いたら、「**Upload**」をクリックします。
3. 「**Browse**」をクリックして、使用するイメージ・ファイルを選択します。
4. 「**Name**」フィールドでイメージの名前を入力し、「**OK**」をクリックしてファイルをアップロードします。

注: 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。

IMM ファームウェア・バージョン 1.02 以前での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「**Mapped**」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。

「**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、そのドライブの「**Mapped**」チェック・ボックスをクリアします。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。

ディスク・イメージ・ファイルを選択して、ディスク・イメージを IMM メモリーに保管することができます。これにより、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、IMM Web インターフェース・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。IMM カード上に格納できるドライブ・イメージは、最大で 1 つです。そのドライブまたはイメージの内容は、1.44 MB 以下でなければなりません。ディスク・イメージ・ファイルをアップロードするには、以下のステップを実行します。

1. 「**RDOC**」をクリックします。
2. 新規ウィンドウが開いたら、「**Upload**」をクリックします。
3. 「**Browse**」をクリックして、使用するイメージ・ファイルを選択します。
4. 「**Name**」フィールドでイメージの名前を入力し、「**OK**」をクリックしてファイルをアップロードします。

注: 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**」ウィンドウを両方とも閉じます。

PXE ネットワーク・ブートのセットアップ

次のサーバー再始動時に Preboot Execution Environment (PXE) ネットワーク・ブートを試行するようにサーバーをセットアップするには、以下のステップを実行します。

1. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
2. ナビゲーション・ペインで、「**PXE Network Boot**」をクリックします。
3. 「**Attempt PXE network boot at next server restart**」チェック・ボックスを選択します。
4. 「**Save**」をクリックします。

ファームウェアの更新

ナビゲーション・ペインで「Firmware Update」オプションを使用して、IMM ファームウェア、System x サーバー・ファームウェア、および Dynamic System Analysis (DSA) ファームウェアを更新します。

ファームウェアを更新するには、以下の手順を実行してください。

注: IBM Web サイトは、定期的に変更されます。実際の手順は、本書の記載とは若干異なる場合があります。

1. IMM が取り付けられているサーバーに適用可能な最新のファームウェア更新をダウンロードします。
 - a. <http://www.ibm.com/support/jp/ja/> にアクセスします。
 - b. 「**Product support**」の下で「**System x**」あるいは「**BladeCenter**」をクリックします。
 - c. 「**Popular links**」の下で「**Software and device drivers**」をクリックします。
 - d. ご使用のサーバーに適用可能なリンクをクリックし、ダウンロード可能なファイルのマトリックスを表示します。
 - e. IMM、サーバー・ファームウェア、あるいは DSA のエリアまでスクロールし、ファームウェア更新のリンクを選択して更新ファイルを保存します。
2. IMM にログインします。詳しくは、13 ページの『第 2 章 IMM Web インターフェースの開始および使用』を参照してください。
3. ナビゲーション・ペインで、「**Firmware Update**」をクリックします。
4. 「**Browse**」をクリックします。
5. 更新する更新パッケージにナビゲートします。

注:

- a. サーバーの電源がオフの間、あるいはサーバーの始動中に、System x サーバー・ファームウェアを更新することはできません。
 - b. 使用するファームウェア・ファイルのタイプを判別するには、更新パッケージの README ファイルを参照してください。ほとんどの場合、IMM は EXE ファイルあるいは BIN ファイルのいずれかを使用して更新を実行することができます。
6. 「**Open**」をクリックします。ファイル (絶対パスを含む) が「**Browse**」の隣のボックスに表示されます。
 7. 更新プロセスを開始するには、「**Update**」をクリックします。ファイルが IMM 上の一時ストレージに転送されるときに、進行標識が表示されます。ファイルの転送が完了すると、確認ウィンドウが開きます。
 8. 「**Confirm Firmware Update**」ウィンドウに表示されるファイルが、更新しようとしているファイルであることを確認します。そうでない場合は、「**Cancel**」をクリックします。
 9. 更新プロセスを実行するために、「**Continue**」をクリックします。ファームウェアの更新時に進行標識が表示されます。更新が正常に行われたかどうかを確認するための確認ウィンドウが開きます。

10. IMM ファームウェアを更新する場合は、ナビゲーション・ペインで「**Restart IMM**」をクリックし、次に「**Restart**」をクリックします。System x サーバー・ファームウェアおよび DSA 更新では、IMM を再始動する必要はありません。これらの更新は、次にサーバーが始動したときに有効になります。
11. 「**OK**」をクリックして、IMM を再始動することを確認します。
12. 「**OK**」をクリックして、現行のブラウザー・ウィンドウを閉じます。
13. IMM が再始動した後、IMM の再度ログインして Web インターフェースにアクセスします。

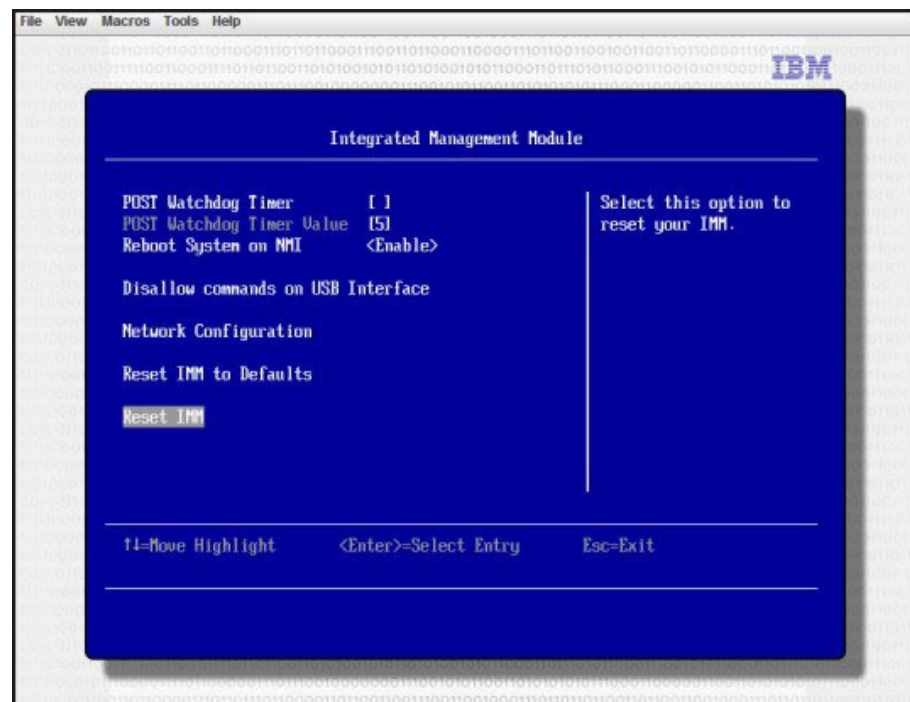
Setup ユーティリティを使用した IMM のリセット

Setup ユーティリティから IMM をリセットするには、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。

注: サーバーを AC 電源に接続してから約 2 分後に、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 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. 「**Reset IMM**」を選択します。



注: IMM をリセットした直後に、次の確認メッセージが表示されます。

IMM reset command has been sent successfully!! Press ENTER to continue.

IMM リセット・プロセスはまだ完了していません。IMM が再度機能するようになるまで、IMM がリセットするのを約 4 分間待つ必要があります。サーバーのリセット中にサーバー・ファームウェア情報へのアクセスを試行すると、フィールドに「Unknown」と表示され、説明は「Error retrieving information from IMM」と表示されます。

IMM および IBM System x サーバー・ファームウェア対応の管理ツール およびユーティリティー

このセクションでは、IMM および IBM System x サーバー・ファームウェアがサポートするツールおよびユーティリティーについて説明しています。IMM インバンドを管理するために使用する IBM ツールは、デバイス・ドライバーをインストールする必要がありません。ただし、IPMITool インバンドなどの特定のツールを使用する場合は、OpenIPMI ドライバーをインストールする必要があります。

IBM システム管理ツールおよびユーティリティーの更新およびダウンロードは、IBM Web サイトで可能です。ツールおよびユーティリティーの更新を確認するには、以下のステップを実行します。

注: 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/jp/ja/> にアクセスします。
2. 「Product support」の下で「System x」をクリックします。
3. 「Popular links」の下で「Utilities」をクリックします。

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、IMM 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。

OSA システム管理ブリッジの使用

OSA システム管理ブリッジ (SMBridge) は、サーバーをリモートで管理するのに使用できるツールです。このツールを使用すると、IPMI 1.5 および Serial over LAN (SOL) プロトコルを使用してサーバーを管理することができます。

SMBridge について詳しくは、<http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lnocid=MIGR-62198&brandind=5000008> を参照するか、以下のステップを実行します。

1. <http://www.ibm.com/support/jp/ja/> にアクセスします。
2. 「System x」をクリックします。
3. 「Support & downloads」の下で、「Search」をクリックします。
4. 検索フィールドで「smbridge」と入力し、「Search」をクリックします。

5. その結果として表示されたリストから、「**SMBridge Tool Help - Servers**」のリンクをクリックします。

IBM Advanced Settings ユーティリティの使用

IMM を管理するには、IBM Advanced Settings ユーティリティ (ASU) バージョン 3.0.0 以降が必要です。ASU は、複数のオペレーティング・システム・プラットフォーム上でコマンド・ライン・インターフェースからファームウェア設定を変更するのに使用できるツールです。また、選択した IMM にセットアップ・コマンドを発行することができます。ASU インバンドまたはアウト・オブ・バンドを使用して、IMM を管理および構成することができます。

注: USB インバンド・インターフェース (LAN over USB) が使用不可にされている場合、ASU を使用するには IPMI デバイス・ドライバがインストールされている必要があります。

ASU について詳しくは、<http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lnocid=MIGR-55021&brandind=5000008> を参照するか、以下のステップを実行します。

1. <http://www.ibm.com/support/jp/ja/> にアクセスします。
2. 「**System x**」をクリックし、「**Product family**」メニューからご使用のサーバーを選択して、「**Go**」をクリックします。
3. 「**Refine results**」メニューから「**Advanced Settings Utility**」を選択し、「**Go**」をクリックします。
4. 最新バージョンの ASU へのリンクをクリックします。

IBM フラッシュ・ユーティリティの使用

フラッシュ・ユーティリティを使用すると、ハードウェアおよびサーバーのファームウェアの更新が可能になり、物理ディスクあるいは他のメディアから新規ファームウェアのインストールまたはファームウェア更新を手動で行う必要がなくなります。IMM、サーバー・ファームウェア、および DSA について、インバンドまたはアウト・オブ・バンドで IBM フラッシュ・ユーティリティを使用することができます。フラッシュ・ユーティリティを見つけるには、以下のステップを実行します。

1. <http://www.ibm.com/support/jp/ja/> にアクセスします。
2. 「**Product support**」の下で「**System x**」をクリックします。
3. 検索フィールドで「flash utility」と入力し、「**Search**」をクリックします。
4. 適用可能なフラッシュ・ユーティリティへのリンクをクリックします。

IMM を管理する他の方法

以下のユーザー・インターフェースを使用して、IMM を管理および構成することができます。

- IMM Web インターフェース
- SNMPv1
- SNMPv3
- Telnet CLI

- SSH CLI

第 6 章 LAN over USB

BMC およびリモート管理アダプター II と異なり、IMM は IMM インバンド通信に IPMI デバイス・ドライバーや USB デーモンを必要としません。代わりに、LAN over USB インターフェースによって IMM へのインバンド通信が可能になります。システム・ボード上の IMM ハードウェアは、IMM からオペレーティング・システムへの内部イーサネット NIC を提供します。

注: LAN over USB は、IMM Web インターフェースで「USB インバンド・インターフェース」とも呼ばれます。

IMM の LAN over USB インターフェース用の IP アドレスは、静的アドレス 169.254.95.118 サブネット・マスク 255.255.0.0 に設定されます。唯一の例外はマルチノード・システム (例えば、x3850 X5 または x3950 X5) の 2 次ノード内にある IMM で、この場合は LAN over USB インターフェースの IMM 側の IP アドレスは 169.254.96.118 です。

LAN over USB インターフェースとの競合の可能性

状況によっては、IMM の LAN over USB インターフェースが特定のネットワーク構成、アプリケーション、またはその両方と競合を起こす可能性があります。例えば、Open MPI はサーバー上の使用可能なすべてのネットワーク・インターフェースの使用を試みます。Open MPI は、IMM の LAN over USB インターフェースを検出し、クラスター環境のその他のシステムとの通信にそのインターフェースを使用しようとします。LAN over USB インターフェースは内部インターフェースのため、このインターフェースをクラスター内の他のシステムとの外部通信に使用することはできません。

IMM LAN over USB インターフェースとの競合の解決

LAN over USB とネットワーク構成およびアプリケーションとの競合を解決するために、以下のようないくつかのアクションがあります。

- Open MPI との競合の場合、アプリケーションがこのインターフェースを使用しないように構成します。
- インターフェースをダウンさせます (Linux で `ifdown` を実行します)。
- デバイス・ドライバーを削除します (Linux で `rmmmod` を実行します)。
- 以下のいずれかの方法を使用して、IMM 上の USB インバンド・インターフェースを使用不可にします。

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 のフラッシュ・ユーティリティを使用する IMM ファームウェアのインバンド更新を実行できません。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、IMM Web インターフェースの「Firmware Update」オプションを使用して、ファームウェアを更新します。詳しくは、136 ページの『ファームウェアの更新』を参照してください。

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。ウォッチドッグを使用不可にする方法については、23 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。

- IMM Web インターフェースから LAN over USB インターフェースを使用不可にするには、26 ページの『USB インバンド・インターフェースの使用不可化』を参照してください。
- アドバンスド・マネージメント・モジュール Web インターフェースから LAN over USB インターフェースを使用不可にするには、以下のを実行します。
 1. アドバンスド・マネージメント・モジュール Web インターフェースにログインします。
 2. ナビゲーション・ペインで、「**Blade Tasks**」見出しの下で「**Blade Configuration**」をクリックします。
 3. 「Blade Configuration」Web ページで「service processor LAN over USB interface」までスクロールダウンします。このセクションには、LAN over USB インターフェースを使用可能および使用不可にすることが可能なシャーシ内のすべてのブレード・サーバーがリストされます。
 4. 使用可能あるいは使用不可にするブレード・サーバーの横にあるチェック・ボックスを選択します。
 5. 選択したブレード・サーバーの LAN over USB インターフェースを使用不可にするには、「**Disable**」をクリックします。

LAN over USB インターフェースの手動構成

IMM で LAN over USB インターフェースを使用するには、自動セットアップが失敗した場合、あるいは LAN over USB を手動でセットアップする場合は、他の構成タスクを完了することをお勧めします。ファームウェア更新パッケージあるいは Advanced Settings ユーティリティ (ASU) は、セットアップを自動的に実行しようとしています。別のオペレーティング・システムでの LAN over USB 構成については、IBM Web サイトで IBM ホワイト・ペーパー「*Transitioning to UEFI and IMM*」を参照してください。

デバイス・ドライバーのインストール

IMM で LAN over USB インターフェースを使用するには、オペレーティング・システム・ドライバーをインストールすることをお勧めします。自動セットアップが失敗した場合、あるいは LAN over USB を手動でセットアップする場合は、以下のいずれかの手順を使用します。別のオペレーティング・システムでの LAN over USB 構成については、IBM Web サイトで IBM ホワイト・ペーパー「*Transitioning to UEFI and IMM*」を参照してください。

Windows IPMI デバイス・ドライバーのインストール

Microsoft IPMI デバイス・ドライバーは、Microsoft Windows Server 2003 R2 オペレーティング・システムではデフォルトでインストールされていません。Microsoft IPMI デバイス・ドライバーをインストールするには、以下のステップを実行します。

1. Windows デスクトップから「スタート」>「コントロール パネル」>「プログラムの追加と削除」をクリックします。
2. 「Windows コンポーネントの追加と削除」をクリックします。
3. コンポーネント・リストから、「管理とモニタ ツール」を選択して、「詳細」をクリックします。
4. 「ハードウェアの管理」を選択します。
5. 「次へ」をクリックします。インストール・ウィザードが開き、インストール手順をガイドします。

注: Windows インストール CD が必要になる場合があります。

LAN over USB の Windows デバイス・ドライバのインストール

Windows をインストールする場合、「デバイス マネージャ」に不明な RNDIS デバイスが表示されます。このデバイスを識別する Windows INF ファイルをインストールする必要があります。また、Windows INF ファイルは、Windows オペレーティング・システムが LAN over USB 機能を検出して使用するために必要です。署名されたバージョンの INF ファイルは、すべての Windows 版の IMM、UEFI、および DSA 更新パッケージに含まれています。このファイルをインストールする必要があるのは一度のみです。Windows INF ファイルをインストールするには、以下のステップを実行します。

1. Windows 版の IMM、サーバー・ファームウェア、あるいは DSA 更新パッケージを入手します (詳しくは、136 ページの『ファームウェアの更新』を参照)。
2. ファームウェア更新パッケージから `ibm_rndis_server_os.inf` と `device.cat` ファイルを抽出し、それらのファイルを `%WINDOWS%\inf` サブディレクトリーにコピーします。
3. **Windows 2003 の場合**、`ibm_rndis_server_os.inf` ファイルで右クリックして「インストール」を選択してインストールします。これにより、`%WINDOWS%\inf` に同じ名前の PNF ファイルが生成されます。**Windows 2008 の場合**、「コンピュータの管理」に進んで「デバイス マネージャ」で RNDIS デバイスを見つけてみます。「プロパティ」>「ドライバ」>「ドライバの再インストール」を選択します。`%Windows%\inf` ディレクトリー (`ibm_rndis_server_os.inf` ファイルが置かれているディレクトリー) を指定して、デバイスをインストールします。
4. 「コンピュータの管理」に進んで「デバイス マネージャ」で「ネットワークアダプタ」を右クリックし、「ハードウェア変更のスキャン」を選択します。イーサネット・デバイスが検出されインストールされていることを確認するメッセージが表示されます。「新しいハードウェアの検出ウィザード」が自動的に開始します。
5. 「ソフトウェア検索のため、Windows Update に接続しますか」というプロンプトが表示されたら、「いいえ、今回は接続しません」をクリックします。「次へ」をクリックして続行します。
6. 「インストール方法を選んでください」というプロンプトが表示されたら、「一覧または特定の場所からインストールする (詳細)」を選択します。「次へ」をクリックして続行します。

7. 「検索とインストールのオプションを選んでください」というプロンプトが表示されたら、「**検索しないで、インストールするドライバを選択する**」をクリックします。「**次へ**」をクリックして続行します。
8. 「ハードウェアの種類を選択して「次へ」をクリックしてください」というプロンプトが表示されたら、「**ネットワーク アダプタ**」をクリックします。「**次へ**」をクリックして続行します。
9. 「新しいハードウェアの検索ウィザードの完了」をいうプロンプトが表示されたら、「**完了**」をクリックします。

注: 新規のローカル・エリア接続が表示され、「この接続は、限られているか利用不可能です」という状態である可能性があります。このメッセージは無視してください。

10. 「デバイス マネージャ」に戻ります。「**ネットワーク アダプタ**」の下に「**IBM USB Remote NDIS Network Device**」が表示されていることを確認します。
11. コマンド・プロンプトを開く、`ipconfig` と入力して `Enter` を押します。IBM USB RNDIS のローカル・エリア接続が表示されます。この IP アドレスは `169.254.xxx.xxx` の範囲で、サブネット・マスクは `255.255.0.0` に設定されています。

LAN over USB の Linux デバイス・ドライバのインストール

Linux の現行バージョンである RHEL5 Update 2 および SLES10 Service Pack 2 などは、LAN over USB インターフェースをデフォルトでサポートしています。このインターフェースは、これらのオペレーティング・システムのインストール時に検出され、表示されます。デバイスの構成する場合、固定 IP アドレス `169.254.95.130`、サブネット・マスク `255.255.0.0` を使用してください。

注: 古い Linux ディストリビューションでは、LAN over USB インターフェースが検出されず、手動構成が必要になる場合があります。特定の Linux ディストリビューションでの LAN over USB の構成については、IBM Web サイトで IBM ホワイト・ペーパー「*Transitioning to UEFI and IMM*」を参照してください。

IMM の LAN over USB インターフェースを使用するには、`usbnet` および `cdc_ether` デバイス・ドライバがロードされている必要があります。デバイス・ドライバがインストールされていない場合は、`modprobe` コマンドを使用してデバイス・ドライバをインストールしてください。これらのデバイス・ドライバがインストールされている場合は、オペレーティング・システム上で IMM USB ネットワーク・インターフェースがネットワーク・デバイスとして表示されます。オペレーティング・システムが IMM USB ネットワーク・インターフェースに割り当てた名前を検出するには、次のコマンドを入力します。

```
dmesg | grep -i cdc ether
```

`ifconfig` コマンドを使用して、インターフェースの IP アドレスを `169.254.xxx.xxx` の範囲で構成します。以下に例を示します。

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

このインターフェースは、オペレーティング・システムを始動するたびに、IP アドレスを `169.254.xxx.xxx` の範囲で構成します。

第 7 章 コマンド・ライン・インターフェース

IMM 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 IMM 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、IMM に認証されている必要があります。

IPMI を使用した IMM の管理

IMM は、標準でユーザー ID 2 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、初期構成時にこのデフォルト・パスワードを変更してください。

また、IMM 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

コマンド・ライン・インターフェースでは、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。SMBridge または 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。SMBridge を使用すると、テキスト・ファイルに 1 つ以上のコマンドを保管して、そのファイルをスクリプトとして実行することもできます。IPMITool について詳しくは、138 ページの『IPMITool の使用』を参照してください。SMBridge について詳しくは、138 ページの『OSA システム管理ブリッジの使用』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、SMBridge または 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、138 ページの『IPMITool の使用』を参照してください。SMBridge について詳しくは、138 ページの『OSA システム管理ブリッジの使用』を参照してください。

コマンド・ラインへのアクセス

コマンド・ラインにアクセスするには、IMM 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、39 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. IMM 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、IMM 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。その後、ログオフされ、セッションは終了します。

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 IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

- コマンド・ライン・インターフェースでは、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。例えば、`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、使用できない場合があります。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> ?
```

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
- ヘルプ
- history

exit コマンド

exit コマンドは、コマンド・ライン・インターフェース・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 IMMA00096B9E003A
-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
- fans
- readlog
- syshealth
- temps
- volts

- vpd

clearlog コマンド

clearlog コマンドを使用すると、IMM 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>
```

readlog コマンド

readlog コマンドは、IMM 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 -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。

構文:

```
readlog [options]
option:
-f
```

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>
```

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 IMM 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  9/320
DASD1 66/19  73/23  82/28  88/31  9/332
Amb   59/15  70/21  83/28  90/32  9/355
system>
```

注:

1. 出力には、次の列見出しがあります。

WR: 警告リセット

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

2. 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 コマンドを使用すると、システム (sys)、IMM、サーバー・ファームウェア (bios)、および Dynamic System Analysis Preboot (dsa) の重要プロダクト・データを表示します。Web インターフェースの場合と同じ情報が表示されます。

構文:

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

例:

```
system> vpd dsa
Type      Version      ReleaseDate
-----
dsa       D6YT19AUS      02/27/2009
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。

- 電源
- reset

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]
```

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` 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 IMM のシリアル・ポートに対するシリアル・リダイレクト・コンソール・セッションが開始されます。

構文:

```
console 1
```

構成コマンド

構成コマンドは、以下のとおりです。

- `dhcpinfo`
- `dns`
- `gprofile`
- `ifconfig`
- `ldap`
- `ntp`
- `passwordcfg`
- `portcfg`
- `slp`
- `srcfg`
- `ssl`
- `tcpcmdmode`
- `timeouts`
- `usbeth`
- `users`

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      : IMMA-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、IMM の DNS 構成を表示するために使用します。

構文:

dns

注: 以下の例では、DNS が使用可能にされた場合の IMM 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
-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 (enabled または disabled)
-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)
-p	優先される DNS サーバー (ipv4 または ipv6)

gprofile コマンド

gprofile コマンドは、IMM 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 <i>group_name</i> は、固有でなければなりません。
-a	役割ベースのセキュリティ (権限) レベル	Supervisor、operator、rbs <role list>: nsluamlrcalrcrdalrprlbacelaac 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	コマンドの使用方法およびオプションの表示	

構文:

```
gprofile [1 - 16] [options]
options:
-clear state
-n group_name
-a security level:
    -ns network and security
    -uam user account management
    -rca remote console access
    -rcrda remote console and remote disk access
    -rpr remote server power/restart access
    -bac basic adapter configuration
    -ce ability to clear event logs
    -aac advanced adapter configuration
-h
```

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 try dhcp server, if it fails use static config オプションに対応します。)
-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。
-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
-ipv6	IPv6 の状態	disabled、enabled
-lla	リンク・ローカル・アドレス 注: リンク・ローカル・アドレスが表示されるのは、IPv6 が使用可能な場合のみです。	リンク・ローカル・アドレスは、IMM によって決定されます。この値は読み取り専用であり、構成できません。
-ipv6static	固定 IPv6 の状態	disabled、enabled
-i6	固定 IP アドレス	イーサネット・チャネル 0 の固定 IP アドレス (IPv6 フォーマット)

オプション	説明	値
-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
-address_table	自動生成された IPv6 アドレスと、そのプレフィックスの長さの表 注: このオプションは、IPv6 およびステートレス自動構成が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。
-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
-r	Data rate	10、100、auto
-d	二重モード	full、half、auto
-m	MTU	60 から 1500 までの数値
-l	LAA	MAC アドレス・フォーマット。マルチキャスト・アドレスは許容されません (最初のバイトは偶数であることが必要です)。

構文:

```

ifconfig eth0 [options]
options:
-state interface_state
-c config_method
-i static_ip_address
-g gateway_address
-s subnet_mask
-n hostname
-r data_rate
-d duplex_mode
-m max_transmission_unit
-l locally_administered_MAC

```

例:

```

system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-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 IMM.
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。

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
-aom	認証専用モード	enabled、disabled
-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
-b	バインド方式	匿名でのバインド、ClientDN とパスワードを使用したバインド、および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 63 文字のSTRING
-fn	フォレスト名	Active Directory 環境の <i>forest_name</i> に対する最大 127 文字のSTRING
-d	検索ドメイン	<i>search_domain</i> の最大 31 文字のSTRING
-f	グループ・フィルター	<i>group_filter</i> の最大 63 文字のSTRING
-g	グループ検索属性	<i>group_search_attr</i> の最大 63 文字のSTRING
-l	ログイン許可属性	<i>string</i> の最大 63 文字のSTRING
-p	クライアント・パスワード	<i>client_pw</i> の最大 15 文字のSTRING
-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STRING コマンドの使用法: <code>ldap -p <i>client_pw</i> -pc <i>confirm_pw</i></code> 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、それらが一致しない場合、コマンドは失敗します。
-r	root エントリ識別名 (DN)	<i>root_dn</i> の最大 63 文字のSTRING
-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 63 文字のSTRING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 63 文字のSTRINGまたは IP アドレス

オプション	説明	値
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 63 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 63 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
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 オプションが有効にされている場合、このフィールドは、役割ベース・セキュリティのスナップインを使用して Active Directory サーバー上の 1 つ以上の役割に関連付けることができ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 23 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:
  -aom enabled|disabled|
  -a loc|ldap|locId|ldloc
  -b anon|client|login
  -c client_dn
  -d search_domain
  -fn forest_name
  -f group_filter
  -g group_search_attr
  -l string
  -p client_pw
  -pc confirm_pw
  -r root_dn
  -rbs enabled|disabled
  -s1ip host_name/ip_addr
  -s2ip host_name/ip_addr
  -s3ip host_name/ip_addr
  -s4ip host_name/ip_addr
  -s1pn port_number
  -s2pn port_number
  -s3pn port_number
  -s4pn port_number
  -t name
  -u search_attrib
  -v 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	Network Time Protocol サーバーの名前または IP アドレス	クロック同期には NTP サーバーの名前を使用します。
-f	IMM クロックを Network Time Protocol サーバーと同期する頻度 (分単位)	3 から 1440 分
-synch	Network Time Protocol サーバーとの即時同期の要求	このパラメーターには値を使用しません。

構文:

```
ntp [options]
options:
-en state
-i hostname
-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 legacy 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 high 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
```

portcfg コマンド

portcfg コマンドは、シリアル・ポートを構成するために使用します。シリアル・ポート構成を変更するには、オプションと、それに続けて値を入力します。シリアル・ポート構成を変更するには、少なくとも「アダプター・ネットワーキングおよびセキュリティー構成 (Adapter Networking and Security Configuration authority)」権限を持っている必要があります。

次のパラメーターはハードウェアに設定されているため、変更できません。

- 8 データ・ビット
- パリティなし
- 1 ストップ・ビット

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	ボー・レート	9600, 19200, 38400, 57600, 115200, 230400
-climode	CLI モード	none、cliems、cliuser • none: コマンド・ライン・インターフェースは使用不可になります。 • cliems: コマンド・ライン・インターフェースは 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。 • cliuser: コマンド・ライン・インターフェースは、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。

構文:

```
portcfg [options]
portcfg [options]
options:
-b baud_rate
-climode cli_mode
-cliauth cli_auth
```

例:

```
system> portcfg
-b : 115200
-climode : 2 (CLI with user defined keystroke sequences) system>
system>
```

srcfg コマンド

srcfg コマンドは、シリアル・リダイレクトを構成するために使用します。現行の構成を表示するには、**srcfg** と入力します。シリアル・リダイレクト構成を変更するには、オプションと、それに続けて値を入力します。シリアル・リダイレクト構成を変更するには、少なくとも「アダプター・ネットワーキングおよびセキュリティ構成 (Adapter Networking and Security Configuration authority)」権限を持っている必要があります。

次の表は、**-exitcliseq** オプションの引数を示しています。

オプション	説明	値
-exitcliseq	コマンド・ライン・インターフェース・キー・ストローク・シーケンスから出ます。	CLI から出するためのユーザー定義キー・ストローク・シーケンス。詳細については、この表の -entercliseq オプションの値を参照してください。

構文:

```
srcfg [options]
options:
-exitcliseq exitcli_keyseq
```

例:

```
system> srcfg
-exitcliseq ^[Q
system>
```

ssl コマンド

ssl コマンドは、Secure Sockets Layer (SSL) パラメーターの表示と構成を行うために使用します。

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	説明
-ce	SSL クライアントの使用可能化または使用不可化

オプション	説明
-se	SSL サーバーの使用可能化または使用不可化
-h	使用方法およびオプションのリスト

構文:

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

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、コマンド・ライン・インターフェース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

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

オプション	タイムアウト	単位	値
-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
-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

構文:

```
timeouts [options]  
options:  
-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 インターフェースを使用可能または使用不可にすることができます。このインターフェースの使用可能化または使用不可化について詳しくは、26 ページの『USB インバンド・インターフェースの使用不可化』を参照してください。

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へのアクセス、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使用します。

以下の **users** コマンドに関するガイドラインをお読みください。

- ユーザー番号は、1 以上 12 以下である必要があります。
- ユーザー名は 16 文字未満で、数字、英字、ピリオド、およびアンダースコアのみを含むことができます。
- パスワードは、長さが 6 文字以上 15 文字以下で、少なくとも 1 つの英字と 1 つの非英字を含んでいる必要があります。
- 権限レベルは、以下のいずれかのレベルにすることができます。
 - super (スーパーバイザー)
 - ro (読み取り専用)
 - 以下の値を | で区切って任意に組み合わせたもの
 - am (ユーザー・アカウント管理アクセス)
 - rca (リモート・コンソール・アクセス)
 - rcvma (リモート・コンソールおよび仮想メディア・アクセス)
 - pr (リモート・サーバー電源/再始動アクセス)
 - cel (イベント・ログを消去する能力)
 - bc (アダプター構成 [基本])
 - nsc (アダプター構成 [ネットワークおよびセキュリティー])
 - ac (アダプター構成 [拡張])

構文:

```
users [options]  
options:  
-user number  
-n username  
-p password  
-a authority level
```

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. jacobyaackenovic 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. jacobyaackenovic 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>

```

IMM 制御コマンド

IMM 制御コマンドは、以下のとおりです。

- clearcfg
- clock
- identify
- resetsp
- update

clearcfg コマンド

clearcfg コマンドは、IMM 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。IMM の構成がクリアされた後、IMM は再始動されます。

clock コマンド

clock コマンドは、IMM 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 または +10 の GMT オフセットでは、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)、gtb (グレートブリテン島)、egt (エジプト)、fle (フィンランド) があります。
- +10 の場合、夏時間の設定には、off、ea (東部オーストラリア)、tas (タスマニア)、vlad (ウラジオストック) があります。

- 年は、2000 以上 2089 以下である必要があります。
- 月、日、時、分、秒は、1 桁の値 (例えば、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
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 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>
```

resetsp コマンド

resetsp コマンドは、IMM 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。

update コマンド

update コマンドを使用すると、IMM のファームウェアを更新します。このコマンドを使用するには、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。 *filename* で指定したファームウ

エア・ファイルは、最初に (IP アドレスで指定された) TFTP サーバーから IMM に転送され、その後、フラッシュされます。 **-v** オプションは詳細モードを指定します。

注: TFTP サーバーが、ファイルのダウンロード元であるサーバー上で稼働していることを確認してください。

オプション	説明
-i	TFTP サーバーの IP アドレス
-l	ファイル名 (フラッシュされるもの)
-v	詳細モード

構文:

```
update -i TFTP_server_IP_address -l filename
```

例: 詳細モードでは、フラッシュの進行状況は完了のパーセンテージでリアルタイムに表示されます。

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Downloading image - 66%
```

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
```

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flashing image - 45%
```

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flash operation completed.
system>
```

フラッシュが冗長モードで行われていない場合、進行状況は連続する # 文字で表示されます。

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Firmware update is in progress. Please wait..
Downloading image: #####
Flashing image: #####
Flash operation completed.
```

Service Advisor コマンド

Service Advisor コマンドには、次のものがあります。

- autoftp
- chconfig
- chlog
- chmanual
- events
- sdemail

autoftp コマンド

autoftp コマンドは、Service Advisor の FTP/TFTP サーバー設定を表示および構成するために使用します。

注: このコマンドを使用する前に、Service Advisor 契約条件を受諾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
-m	自動問題報告モード	<i>ftp</i> 、 <i>tftp</i> 、 <i>disabled</i>
-i	自動問題報告で使用する FTP/TFTP サーバーの IP アドレスまたはホスト名	IP アドレスまたはホスト名
-p	FTP/TFTP 送信ポート	<i>port_number</i> の 1 から 65535 の間の数値
-u	問題報告で使用する引用符区切りの FTP ユーザー名	<i>user_name</i> の最大 63 文字のストリング
-pw	問題報告で使用する引用符区切りの FTP パスワード	<i>password</i> の最大 63 文字のストリング
注: <i>ftp</i> の値には、すべてのオプション (フィールド -i、-p、-u、および -pw) を設定する必要があります。 <i>tftp</i> の値には、オプション -i および -p のみが必須です。		

構文:

```
autoftp [options]
options:
-m ftp|tftp|disable
-i host name|ip_addr
-p port_number
-u user_name
-pw password
```

chconfig コマンド

chconfig コマンドは、IMM の Service Advisor 設定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
-li	Service Advisor 契約条件を表示あるいは受諾します。他のオプションを設定する前に、このオプションを使用して Service Advisor 契約条件を受諾する必要があります。	view、accept
-sa	Service Advisor の IBM サポート状況	enabled、disabled
-sc	IBM Service Support Center の国別コード	2 文字の ISO 国別コード

オプション	説明	値
-ca	引用符区切りのマシン設置場所のアドレス	<i>address</i> の最大 30 文字のスト リング
-cci	引用符区切りのマシン設置場所の市町村	<i>city</i> の最大 30 文字のスト リング
-ce	連絡先担当者の E メール・アドレス (形式 <i>userid@hostname</i>)	<i>email_addr</i> の最大 30 文字の ストリング
-cn	引用符区切りの連絡先担当者名	<i>contact_name</i> の最大 30 文字 のストリング
-co	引用符区切りの連絡先担当者の組織/会社名	<i>company_name</i> の最大 30 文 字のストリング
-cph	引用符区切りの連絡先担当者の電話番号	<i>phone_number</i> の 5 から 30 文字のストリング
-cs	マシン設置場所の都道府県	<i>state/province</i> の 2 から 3 文字 のストリング
-cz	引用符区切りのマシン設置場所の郵便番号	<i>postal_code</i> の最大 9 文字の ストリング
-loc	HTTP プロキシの完全修飾ホスト名または IP アドレス	<i>host_name/ip_addr</i> の最大 63 文字のストリングまたは IP アドレス
-po	HTTP プロキシ・ポート	<i>port_number</i> の 1 から 65535 の間の数値ポート番号
-ps	HTTP プロキシ状況	enabled、disabled
-pw	引用符区切りの HTTP プロキシ・パスワ ード	<i>password</i> の最大 15 文字のス トリング
-u	引用符区切りの HTTP プロキシ・ユーザ ー名	<i>user_name</i> の最大 30 文字のス トリング
1. 他のオプションを設定する前に、オプション -li を使用して Service Advisor 契約条件を 受諾する必要があります。 2. Service Advisor の IBM サポートを使用可能にするには、事前に IBM Service Support Center フィールドと、すべての連絡先情報フィールドが入力されている必要があります。 プロキシが必要な場合、HTTP プロキシ・フィールドを設定する必要があります。		

構文:

```

chconfig [options]
options:
-li view|accept
-sa service_advisor state
-sc country_code
-ca address
-cci city
-ce email_addr
-cn contact_name
-co company_name
-cph phone_number
-cs state/province
-cz postal_code
-loc host_name/ip_addr

```

```
-po port_number
-ps status
-pw password
-u user_name
```

chlog コマンド

chlog コマンドは、システムまたはユーザーによって生成されたコール・ホーム・イベントの最新の 5 個を表示します。最新のコール・ホーム・エントリーが最初にリストされます。

次の表は、オプションの引数を示しています。

注: このコマンドを使用する前に、Service Advisor 契約条件を受諾する必要があります。

オプション	説明	値
-event_index	アクティビティー・ログからの索引を使用して、コール・ホーム・エントリーを指定します。	1 から 5 までの数値
-ack	修正されたコール・ホーム・イベントに対して応答を返すか応答しないかを指定します。	yes、no
-s	IBM サポートの結果のみを表示します。	
-f	FTP/TFTP サーバーの結果のみを表示します。	

構文:

```
chlog [options]
options:
-event_index
-ack yes|no
-s
-f
```

chmanual コマンド

chmanual コマンドは、手動コール・ホーム・イベントまたはテスト・コール・ホーム・イベントを生成するために使用します。

注: このコマンドを使用する前に、Service Advisor 契約条件を受諾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
-test	テスト・コール・ホーム・イベントを生成します。	
-desc	引用符区切りの問題記述	<i>description</i> の最大 100 文字のストリング

構文:

```
chmanual [options]
options:
-test
-desc description
```

events コマンド

events コマンドは、除外イベントを表示および編集するために使用します。

注: このコマンドを使用する前に、Service Advisor 契約条件を受諾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
-che	除外イベントを表示および編集します。	
-add	コール・ホーム除外リストにコール・ホーム・イベントを追加します。	<i>event_id</i> (形式 0xxxxxxxxxxxxxxxxxx)
-rm	コール・ホーム除外リストからコール・ホーム・イベントを削除します。	<i>event_id</i> (形式 0xxxxxxxxxxxxxxxxxx または all)

構文:

```
events [options]
options: -che {-add} | {-rm}
-add event_id
-rm event_id|all
```

sdemail コマンド

sdemail コマンドは、指定された受信者に対する E メール・サービス情報を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
-subj	引用符区切りの E メール件名	<i>email_subject</i> の最大 119 文字のストリング
-to	受信者の E メール・アドレス。このオプションは、コンマで区切った複数のアドレスから構成することができます。	<i>email_addrs</i> の最大 119 文字のストリング

構文:

```
sdemail [options]
options:
-subj email_subject
-to email_addrs
```

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 製品用に更新されたソフトウェア、ファームウェア、およびオペレーティング・システム・デバイス・ドライバがないか確認してください。
IBM の保証条件では、製品に関わるすべて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は、IBM 製品の所有者であるお客様の責任で行っていただくとしています (ただし、追加の保守契約で保証される場合を除きます)。ソフトウェアを更新することで、お客様の問題に文書化された解決方法が示される場合、IBM サービス技術員は、お客様によるソフトウェアおよびファームウェアの更新を要求する場合があります。
- 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 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/systems/jp/x/intellistation/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
- 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
- セキュア・アップロード: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

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・ラインについて詳しくは、<http://www.ibm.com/services/supline/products> をご覧ください。

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/copytrade.shtml> をご覧ください。

Adobe および PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

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・ドライブ・ベイに取り付けることを想定しています。

最大メモリーは、標準メモリーをオプション・メモリー・モジュールと取り替える必要がある場合があります。

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[®] 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[®] 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るため、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 21. 微粒子およびガスの制限

汚染物質	制限
微粒子	- 室内の空気は、ASHRAE Standard 52.2 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)¹。 - データ・センターに取り入れる空気は、MIL-STD-282 に準拠する HEPA フィルターを使用し、99.97% 以上の粒子捕集率効果のあるフィルタリングが実施されなければならない。 - 粒子汚染の潮解相対湿度は、60% を超えていなければならない²。 - 室内には、亜鉛ウィスカーのような導電性汚染があってはならない。
ガス	- 銅: ANSI/ISA 71.04-1985 準拠の Class G1³ - 銀: 腐食率は 30 日間で 300 Å 未満

¹ ASHRAE 52.2-2008 - 一般的な換気および空気清浄機器について、微粒子の大きさごとの除去効率をテストする方法。Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

² 粒子汚染の潮解相対湿度とは、水分を吸収した塵埃が、十分に濡れてイオン導電性を持つようになる湿度のことです。

³ ANSI/ISA-71.04-1985。プロセス計測およびシステム制御のための環境条件: 気中浮遊汚染物質。Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

通信規制の注記

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 목
적으로 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】

アドバンスト・マネージメント・モジュール 1, 10, 13, 141
アプレット
 ActiveX 124
 Java 124
アラート 34
 グローバル設定 36
 受信者の構成 35
 送信するための選択
 警告 35
 システム 35
 critical 35
 リモート試行の設定 36, 37
 SNMP 設定 37
暗号鍵、生成 93
イーサネット接続の構成 41
イベント・ログ
 重大度レベル 115
 説明 114
 リモート・アクセス 24
 Setup ユーティリティからの表示 116
 Web インターフェースからの表示 115
イベント・ログの表示 117
インフォメーション・センター 174
ウォッチドッグ (サーバー・タイムアウト)
 オペレーティング・システム (OS) 23
 ローダー 23
汚染、粒子およびガス 180
オペレーティング・システム (OS) ウォッチドッグ (サーバー・タイムアウト) 23
オペレーティング・システムのスクリーン・キャプチャー 6, 126
オペレーティング・システム要件 11
温度のモニター 109
オンライン資料
 エラー・コード情報 1
 資料更新情報 1
 ファームウェア更新情報 1

【力行】

ガス汚染 180
カスタム権限レベル、ログイン・プロフィール 28
カスタム・サポート Web ページ 175
許可ビット
 説明 81
クリティカル・アラート 35
グローバル・リモート・アラート試行、設定 36
グローバル・ログイン設定 (Web インターフェース) 33
クロック、ネットワーク内の同期 25
警告アラート 35
権限レベル、ログイン・プロフィールでの設定 28
更新、ファームウェアの 136
構成
 イーサネット接続 41
 グローバル・リモート・アラート設定 36
 グローバル・ログイン設定 33
 シリアル・ポート 38
 セキュリティ 89
 ネットワーク・インターフェース 41
 ネットワーク・プロトコル 47
 ポート割り当て 39
 リモート・アラート 34, 35
 DNS 49
 LDAP 51
 Serial-to-SSH リダイレクト 39
 Serial-to-Telnet リダイレクト 39
 SMTP 51
 SNMP 37, 48
 SSH 97
 Telnet 50
構成コマンド 152
構成サマリー、表示 17
構成ファイル 100
固定 IP アドレス、デフォルト 13
個別設定したサポート Web ページの作成 175
コマンド、タイプ
 構成 152
 サーバーの電源および再始動 151
 シリアル・リダイレクト 152
 モニター 148
 ユーティリティ 148
IMM 制御 165
Service Advisor 167

コマンド・ライン・インターフェース (CLI)

 アクセス 145
 機能および制限 146
 コマンド構文 146
 説明 145
 ログイン 146
コンポーネント・アクティビティ・ログ
 重要プロダクト・データの表示 119
コンポーネント・レベル VPD 119

【サ行】

サーバーの電源および再始動
 活動 121
 コマンド 151
 Remote Control 122
サーバー・イベント・ログ
 重大度レベル 115
サーバー・コンソール 123, 125
サーバー・タイムアウト
 電源オフ遅延 23
 Loader watchdog 23
 OS ウォッチドッグ 23
サーバー・タイムアウト、設定 23
サービスおよびサポート
 依頼する前に 173
 ソフトウェア 175
 ハードウェア 175
サポート Web ページ、カスタム 175
支援、入手 173
事項、重要 178
時刻設定内の GMT オフセット 24
自己署名証明書、生成 91
システム状況 109
システム情報、設定 22
システム・アラート 35
システム・イベント・ログ 114
システム・ヘルスのモニター
 温度しきい値 109
 システム・ロケーター LED 109
 電圧しきい値 109
 ファン速度 109
 要約ページ 109
システム・ロケーター LED 109
始動シーケンスの変更 17
シャーシ・イベント・ログ 114
「重要」の注記 178
重要プロダクト・データ (VPD) 119
 コンポーネント・アクティビティ・ログの表示 119

重要プロダクト・データ (VPD) (続き)
コンポーネント・レベル VPD 119
マシン・レベル VPD の表示 119
IMM VPD の表示 119
従来の LDAP
許可 81
認証 81
出荷時のデフォルトのリストア 102
商標 178
証明書署名要求の生成 93
シリアル・ポート、構成 38
シリアル・リダイレクト・コマンド 152
資料
使用 174
スケーラブル・パーティションの構成 103
セキュア web サーバーおよびセキュア LDAP
セキュア Web サーバー用の SSL の使用可能化 96
説明 90
LDAP クライアント用の SSL の使用可能化 97
SSL クライアント証明書管理 96
SSL クライアントのトラステッド証明書管理 96
SSL サーバー証明書管理 91
SSL 証明書の説明 90
セキュア・シェル・サーバー
使用 99
使用可能化 98
生成、秘密鍵の 98
セキュア・シェル・サーバー (SSH) 97
セキュリティ 89
絶対マウス制御 130
設定
イーサネット 42
グローバル・ログイン、構成 33
システム情報 22
日時 24
リモート・アラート 34
IPv4 45
IPv6 46
Secure Sockets Layer (SSL) 90
相対マウス制御 130
ソフトウェアのサービスおよびサポートの電話番号 175

[タ行]

タイムアウト、サーバー・タイムアウトを参照 23
単一カーソル・モード 131
注記 11
ツール 138
その他の IMM 管理ツール 139

ツール (続き)
フラッシュ・ユーティリティ 139
Advanced Settings ユーティリティ (ASU) 139
IPMITool 138
SMBridge 138, 145
通信規制の注記 180
粒子汚染 180
ディスク、リモート 3, 132
デフォルトの構成のリストア 102
デフォルトの固定 IP アドレス 13
電圧のモニター 109
電源オフ遅延 (サーバー・タイムアウト) 23
電源および再始動、サーバーの活動 121
Remote Control 122
電話番号 175
統合管理モジュール・イベント・ログ 114
ドライブのマッピング 134

[ナ行]

夏時間調整時刻、調整 24
日時、確認 24
認証方式、ログインでのユーザーの 33
ネットワーク接続 13, 42, 45, 46
固定 IP アドレス、デフォルト 13
デフォルトの固定 IP アドレス 13
IP アドレス、デフォルトの固定 13
ネットワーク内のクロックの同期 25
ネットワーク・インターフェース
イーサネット接続の構成 41
ネットワーク・プロトコル
構成、SMTP の 51
構成、SSL の 90
説明 47
DNS の構成 49
LDAP の構成 51
SNMP の構成 48

[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 175
表明イベント、システム・イベント・ログ 114
表明解除イベント、システム・イベント・ログ 114
ファームウェアの更新 136
ファン速度のモニター 109
ブラウザーの要件 11
フラッシュ・ユーティリティ 139
ブルー・スクリーン・キャプチャー 126

ブレード・サーバー 1, 10, 13, 39
プロトコル
DNS 49
LDAP 51
SMTP 51
SNMP 48
SSL 90
Telnet 50
プロファイル、ログイン
アクセス権の設定 28
削除 32
作成 28
ベースボード管理コントローラー (BMC) 1, 6
ヘルプ
ソース 173
IBM への診断データの送信 174
WWW から 174
ポート番号、予約済み 39
ポート割り当ての構成 39
ホスト・サーバーの始動シーケンスの変更 17

[マ行]

マウス制御
絶対 130
相対 130
デフォルト Linux 加速を使用する相対 130
マシン・レベル VPD 119
モニター・コマンド 148

[ヤ行]

役割ベースの認証
アクティブ・ディレクトリー 78
セキュリティ・スナップイン・ツール 78
ユーザー ID
IMM 28
IPMI 28
ユーザー認証、ログインでの 33
ユーザー・スキーマの例、LDAP 52
ユーティリティ 138
ユーティリティ・コマンド 148
要件
オペレーティング・システム 11
Web ブラウザー 11

[ラ行]

リアルタイム・クロック、NTP サーバーを使用した同期 25
リモート管理アダプター II 1, 3, 6

リモート電源制御 132

リモート・アラート

試行の設定 37

受信者の構成 35

設定の構成 34

タイプ

警告 35

システム 35

critical 35

リモート・サーバーのモニター

温度しきい値 109

電圧しきい値 109

ファン速度 109

リモート・ディスク 3, 132, 134

リモート・デスクトップ・プロトコル

(RDP)、起動 132

リモート・ブート 132

リモート・プレゼンス

使用可能化 124

説明 123

ローカル許可

Active Directory 認証 70

ローダー・ウォッチドッグ (サーバー・タ

イムアウト) 23

ログ、タイプ

システム・イベント・ログ 114

シャーシ・イベント・ログ 114

DSA ログ 114

IMM イベント・ログ 114

ログイン設定、グローバル (Web インタ

ーフェース) 33

ログイン・プロファイル

アクセス権の設定 28

カスタム権限レベル 28

削除 32

作成 28

ユーザー ID の制限 28

ログイン・プロファイルの作成 28

A

Active Directory 認証

ローカル許可 70

ActiveX 124

Advanced Settings ユーティリティ

(ASU) 1, 6, 139

ASM イベント・ログ 114

Australia Class A statement 181

B

BIOS (基本入出力システム) 1

BladeCenter 1, 10, 13, 39

C

Canada Class A electronic emission

statement 181

China Class A electronic emission

statement 184

Class A electronic emission notice 181

D

DNS、構成 49

DSA ログ 114

DSA、IBM へのデータの送信 174

Dynamic System Analysis (DSA) 119

E

electronic emission Class A notice 181

European Union EMC Directive

conformance statement 182

F

FCC Class A notice 181

feature

Service Advisor 106

G

Germany Class A statement 182

I

IBM BladeCenter 1, 10, 13, 39

IBM System x サーバー・ファームウェア

更新、ファームウェアの 136

説明 1

ツールおよびユーティリティ 138

Setup ユーティリティ 13, 116, 137

VPD 119

IBM プレード・サーバー 1, 10, 13, 39

IBM への診断データの送信 174

IMM

アクションの説明 17

アラート 34

イベント・ログ 114

機能 3, 6

更新、ファームウェアの 136

構成 21, 100

再始動 102

システム情報 22

シリアル・リダイレクト 39

新機能 1

説明 1

タスク 121

IMM (続き)

ツールおよびユーティリティの管理

138

デフォルト 102

ネットワーク接続 13

ネットワーク・インターフェース 41

ネットワーク・プロトコル 47

ポート割り当て 39

モニター 109

ユーザー ID 28

リモート・プレゼンス 123

ログイン・プロファイル 28

ログオフ 108

IMM Premium 3

IMM Premium、へアップグレード 5

IMM Standard 3

IMM Standard、からアップグレード

5

LAN over USB 141

Remote Control 125

RSA 付きの BMC との比較 6

Virtual Light Path 114

Web インターフェース 13

IMM Premium、へアップグレード 5

IMM Standard、からアップグレード 5

IMM イベント・ログ 114

表示 115

IMM 構成

スケーラブル・パーティション 103

ネットワーク接続 42, 45

バックアップ 100

変更およびリストア 99, 101

IMM

ネットワーク接続設定 42, 45, 46

IPv6 46

Service Advisor 機能の使用 106

Service Advisor の構成 103

IMM 構成のバックアップ 100

IMM 構成の変更 99, 101

IMM 構成のリストア 99, 101

IMM 制御コマンド 165

IMM デフォルト、リストア 102

IMM デフォルトのリストア 102

IMM の機能 3

IMM の再始動 102

IMM のリセット 137

IMM へのログイン 16

IP address

構成 13

IPv4 13

IPv6 13

IP アドレス、デフォルトの固定 13

IPMI

ユーザー ID 28

リモート・サーバー管理 145

IPMI イベント・ログ 114

IPMItool 138, 145
IPv6 13

J

Java 6, 11, 124, 125, 132

K

Korea Class A electronic emission
statement 183

L

LAN over USB
競合 141
手動構成 142
設定 141
説明 141
Linux ドライバー 144
Windows IPMI デバイス・ドライバー
142
Windows ドライバー 143
LAN over USB の Linux ドライバー
144
LAN over USB の Windows ドライバー
143
LDAP
セキュア 90
説明 51
認証順序の構成 33
LDAP、構成
従来の許可 81
従来の認証 81
ユーザー・スキーマの例 52
Active Directory 認証 70
Active Directory の役割ベース 78
LDAP クライアントの構成 70
LDAP サーバーの参照 62
Microsoft Windows Server 2003 Active
Directory
権限レベル 66
構成の検査 70
ユーザー・グループへのユーザーの
追加 65
Novell eDirectory
グループ・メンバーシップ 54
権限レベル 56
権限レベルの設定 57
ユーザー・グループへのユーザーの
追加 55
Novell eDirectory スキーマ・ビュー
53
Windows Server 2003 Active Directory
スキーマ・ビュー 64

Light Path 114
Linux (デフォルト Linux 加速) での相対
マウス制御 130

M

Microsoft Windows Server 2003 Active
Directory 64
権限レベル 66
構成の検査 70
ユーザー・グループへのユーザーの追
加 65

N

Network Time Protocol (NTP) 25
New Zealand Class A statement 181
notices 177
electronic emission 181
FCC, Class A 181
Novell eDirectory スキーマ・ビュー 53
Novell eDirectory スキーマ・ビュー、
LDAP
グループ・メンバーシップ 54
権限レベル 56
権限レベルの設定 57
ユーザー・グループへのユーザーの追
加 55

O

OSA システム管理ブリッジ 138

P

People's Republic of China Class A
electronic emission statement 184
PXE ネットワーク・ブート 135
PXE ブート・エージェント 17

R

Remote Control
キーボード・サポート 128
キーボード・パススルー・モード 130
機能 123
終了 135
スクリーン・キャプチャー 126
絶対マウス制御 130
説明 125
相対マウス制御 130
多国語キーボードのサポート 129
単一カーソル・モード 131
電源および再始動コマンド 132

Remote Control (続き)
パフォーマンス統計 132
マウス・サポート 130
ActiveX アプレット 124
Java アプレット 124, 125
Linux (デフォルト Linux 加速) での相
対マウス制御 130
Video Viewer 125, 127
Virtual Media Session 125, 132
Remote Control での多国語キーボードの
サポート 129
Remote Control のキーボード・サポート
128
Remote Control のキーボード・パススル
ー・モード 130
Remote Control のビデオ・カラー・モー
ド 127
Remote Control の表示モード 127
Remote Control のマウス・サポート 130
Remote Control、サーバーの電源の 122
Russia Class A electronic emission
statement 184

S

Secure Sockets Layer (SSL) 90
Serial over LAN 145
Serial-to-SSH リダイレクト 39
Serial-to-Telnet リダイレクト 39
Service Advisor
構成 103
Service Advisor 機能
説明 103
Service Advisor 機能の使用 106
Service Advisor コマンド 167
Service Advisor の構成 103
SMBridge 138, 145
SMTP の構成 51
SNMP 28, 34
アラート設定 37
構成 48
SSL クライアント証明書管理 96
SSL クライアントのトラステッド証明書
管理 96
SSL サーバー証明書管理 91
自己署名証明書 91
証明書署名要求 93
over HTTPS 96
SSL 証明書の説明 90
SSL セキュリティー・プロトコル 90
SSL の使用可能化
セキュア Web サーバー用 96
LDAP クライアント用 97

T

Taiwan Class A electronic emission
statement 184
Telnet 50

U

United States FCC Class A notice 181
USB インバンド・インターフェース、使
用不可化 26, 141
USB インバンド・インターフェースの使
用不可化 26
アドバンスド・マネージメント・モジ
ュールから 141
IMM から 141

V

Video Viewer 125
キーボード・パススルー・モード 130
終了 135
スクリーン・キャプチャー 126
絶対マウス制御 130
相対マウス制御 130
多国語キーボードのサポート 129
単一カーソル・モード 131
電源および再始動コマンド 132
パフォーマンス統計 132
ビデオ・カラー・モード 127, 128
表示モード 127
マウス・サポート 130
Linux (デフォルト Linux 加速) での相
対マウス制御 130
Virtual Light Path 17, 114
Virtual Media Session 125
終了 135
ドライブのマップ 134
ドライブのマップ解除 134
リモート・ディスク 132

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
16
Web インターフェースからのログオフ
108
Web インターフェースの開始および使用
13
Web サーバー、セキュア 90
Web ブラウザーの要件 11
Windows IPMI デバイス・ドライバ
142



部品番号: 47C9120

Printed in Japan

(1P) P/N: 47C9120



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