



統合管理モジュール ユーザ ガイド

2011 年 4 月 14 日

【注意】シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/)をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 準拠装置に関する記述: この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述: この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの制限は、住宅地で使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。干渉しているかどうかは、装置の電源のオン/オフによって判断できます。

- 受信アンテナの向きを変えるか、場所を移動します。
- 装置と受信機との距離を離します。
- 受信機と別の回路にあるコンセントに装置を接続します。
- 販売業者またはラジオやテレビに詳しい技術者に連絡します。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(0711R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

統合管理モジュール ユーザ ガイド

© 2011 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

概要 1-1

IMM の機能 1-1

Web ブラウザとオペレーティング システムの要件 1-2

このマニュアルで使用される注記 1-2

CHAPTER 2

IMM Web インターフェイスの開始および使用 2-1

IMM Web インターフェイスへのアクセス 2-1

IMM へのログイン 2-1

IMM アクションの説明 2-3

CHAPTER 3

IMM の設定 3-1

システム情報の設定 3-2

サーバ タイムアウトの設定 3-3

IMM の日付と時刻の設定 3-4

ネットワーク内のクロックの同期化 3-5

USB インバンド インターフェイスのディセーブル化 3-6

ログイン プロファイルの作成 3-7

ログイン プロファイルの削除 3-12

グローバル ログインの設定 3-13

リモート アラートの設定 3-14

リモート アラート受信者の設定 3-15

グローバル リモート アラートの設定 3-17

SNMP アラートの設定 3-18

ポートの割り当ての設定 3-18

ネットワーク インターフェイスの設定 3-20

ネットワーク プロトコルの設定 3-23

SNMP の設定 3-23

DNS の設定 3-25

Telnet の設定 3-26

SMTP の設定 3-26

LDAP の設定 3-27

LDAP サーバを使用するためのクライアントの設定 3-27

LDAP クライアント認証の設定 3-30

- LDAP 検索属性の設定 3-30
- サービス ロケーション プロトコル (SLP) 3-32
- セキュリティの設定 3-33
 - セキュア Web サーバおよびセキュア LDAP 3-33
 - SSL 証明書の概要 3-34
 - SSL サーバ証明書の管理 3-35
 - セキュア Web サーバに対する SSL のイネーブル化 3-39
 - SSL クライアント証明書の管理 3-39
 - SSL クライアントの信頼できる証明書の管理 3-39
 - LDAP クライアントに対する SSL のイネーブル化 3-40
- セキュア シェル サーバの設定 3-41
 - セキュア シェル サーバ キーの生成 3-41
 - セキュア シェル サーバのイネーブル化 3-41
 - セキュア シェル サーバの使用 3-42
- 設定ファイルの使用 3-42
 - 現在の設定のバックアップ 3-42
 - IMM の設定の復元と変更 3-43
- デフォルトの復元 3-44
 - IMM の復元 3-44
- ログオフ 3-44

CHAPTER 4

- サーバステータスのモニタ 4-1
 - システム ステータスの表示 4-1
 - 仮想ライト パスの表示 4-5
 - Web インターフェイスからのシステム イベント ログの表示 4-6
 - 重要な製品データの表示 4-7

CHAPTER 5

- IMM タスクの実行 5-1
 - サーバの電源および再起動アクティビティの表示 5-1
 - サーバの電源ステータスの制御 5-3
 - IMM を管理するその他の方法 5-4

CHAPTER 6

- コマンドライン インターフェイス 6-1
 - IPMI を使用した IMM の管理 6-1
 - コマンドラインへのアクセス 6-1
 - コマンドライン セッションへのログイン 6-1
 - コマンド構文 6-2
 - 機能および制限事項 6-2

ユーティリティ コマンド	6-3
exit コマンド	6-4
help コマンド	6-4
history コマンド	6-4
モニタ コマンド	6-4
clearlog コマンド	6-5
fans コマンド	6-5
readlog コマンド	6-5
syshealth コマンド	6-6
temps コマンド	6-6
volts コマンド	6-7
vpd コマンド	6-8
サーバの電源および再起動の制御コマンド	6-8
power コマンド	6-8
reset コマンド	6-9
コンフィギュレーション コマンド	6-9
dhcpinfo コマンド	6-9
ifconfig コマンド	6-10
ldap コマンド	6-12
ntp コマンド	6-13
passwordcfg コマンド	6-14
portcfg コマンド	6-15
srcfg コマンド	6-16
ssl コマンド	6-17
timeouts コマンド	6-18
usbeth コマンド	6-19
users コマンド	6-19
IMM 制御コマンド	6-20
clearcfg コマンド	6-21
clock コマンド	6-21
identify コマンド	6-22
resetsp コマンド	6-22



CHAPTER 1

概要

統合管理モジュール (IMM) は、サービス プロセッサとリモート管理の機能をサーバ システム ボード上の 1 つのチップに統合しています。

IMM には、さまざまなメリットがあります。

- 専用または共有イーサネット接続の選択。
- Intelligent Platform Management Interface (IPMI) とサービス プロセッサ インターフェイスの両方に 1 つの IP アドレスを使用。
- 更新処理を開始するためにサーバを再起動する必要がなく、他のエンティティをローカルまたはリモートで更新することが可能。
- アプリケーションおよびツールがインバンドまたはアウトオブバンドのいずれかで IMM にアクセス可能。

このマニュアルでは、IMM の機能の使用方法について説明します。

IMM の機能

IMM は、シスコ モビリティ サービス エンジン、Cisco Flex コントローラ、および Cisco Prime Network Control System の共通管理コンポーネントです。IMM で提供される機能は、3 つの製品すべてで同じです。マニュアル全体を通じて、必要に応じて製品固有の違いが示されています。

IMM は、次の機能を提供します。

- サーバの 24 時間リモート アクセスおよび管理
- 管理対象サーバのステータス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 コントロール
- 標準の Web ブラウザを使用した Web ベースの管理

IMM には、次の機能があります。

- 重要なサーバ設定へのアクセス
- 重要な製品データ (VPD) へのアクセス
- 自動通知およびアラート
- 継続的なヘルス モニタリングおよび制御
- 専用または共有イーサネット接続の選択
- ドメイン ネーム システム (DNS) サーバのサポート
- ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) のサポート

- 電子メール アラート
- 組み込み Dynamic System Analysis (DSA)
- 拡張されたユーザ権限レベル
- IMM とのインバンド通信用の LAN over USB
- タイム スタンプが付けられ、IMM に保存された、電子メールに添付できるイベント ログ
- 業界標準のインターフェイスおよびプロトコル
- OS ウォッチドッグ
- リモート ファームウェア更新
- リモート電源制御
- セキュアな Web サーバ ユーザ インターフェイス
- 簡易ネットワーク管理プロトコル (SNMP) のサポート
- Lightweight Directory Access Protocol (LDAP) サーバへのセキュア接続を使用したユーザ認証

Web ブラウザとオペレーティング システムの要件



警告

Cisco TAC からの適切な指示なしに、システムファームウェアを更新しないでください。シスコが認定およびリリースしたファームウェアを使用して、Cisco TAC から指示されたとおりにファームウェアを更新する必要があります。このガイドラインに従わない場合、システムが動作しなくなる可能性があります。

IMM Web インターフェイスには、Java™ Plug-in 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



(注)

IMM Web インターフェイスは 2 バイト文字セット (DBCS) 言語をサポートしていません。

このマニュアルで使用される注記

このマニュアルでは、次の注記が使用されています。

- **注**：これらの注記には、重要なヒント、ガイダンス、または助言が記載されています。
- **重要**：これらの注記には、不都合な状況や問題のある状況を避けるのに役立つ情報または助言が記載されています。
- **注意**：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があることを示します。「注意」の注記は、損傷を起こすおそれのある指示または状況の直前に書かれています。



CHAPTER 2

IMM Web インターフェイスの開始および使用

IMM は、サービス プロセッサの機能とビデオ コントローラを 1 つのチップに統合しています。IMM Web インターフェイスを使用してリモートから 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、ログイン手順と、IMM Web インターフェイスから実行できるアクションについて説明します。

IMM Web インターフェイスへのアクセス

IMM は、スタティックおよびダイナミック ホスト コンフィギュレーション プロトコル (DHCP) 両方の IP アドレッシングをサポートしています。IMM に割り当てられるデフォルトのスタティック IP アドレスは 192.168.70.125 です。IMM は、まず DHCP サーバからのアドレス取得を試行し、取得できない場合はスタティック IP アドレスを使用します。

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、サーバと共有のネットワーク接続を使用するかを選択できます。

IMM ネットワーク接続をセットアップする場合、その方法は製品によって異なります。たとえば、Cisco Flex 7500 シリーズ ワイヤレス コントローラでは、IMM アクセスを設定する CLI コマンドが提供されており、Cisco 3355 モビリティ サービス エンジンではスクリプト (immconfig.sh) が提供されています。詳細については、製品固有の設定マニュアルを参照してください。

IMM へのログイン

重要 : IMM は、ユーザ名 USERID とパスワード PASSWORD (文字の O ではなくゼロ) で初期設定されています。このデフォルト ユーザ設定には、スーパーバイザ アクセス権があります。セキュリティを高めるために、最初の設定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 インターフェイスで IMM にアクセスするには、次の手順を実行します。

-
- ステップ 1** Web ブラウザを開きます。アドレスまたは URL フィールドに、接続する IMM サーバの IP アドレスまたはホスト名を入力します。

ステップ 2 [IMM Login] ウィンドウにユーザ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、システム管理者からユーザ名とパスワードを入手できます。ログインの試行はすべてイベント ログに記録されます。システム管理者が行ったユーザ名の設定によっては、新しいパスワードの入力が必要となる場合があります。デフォルトのユーザ名は USERID で、デフォルトのパスワードは PASSWORD（ゼロを使用）です。

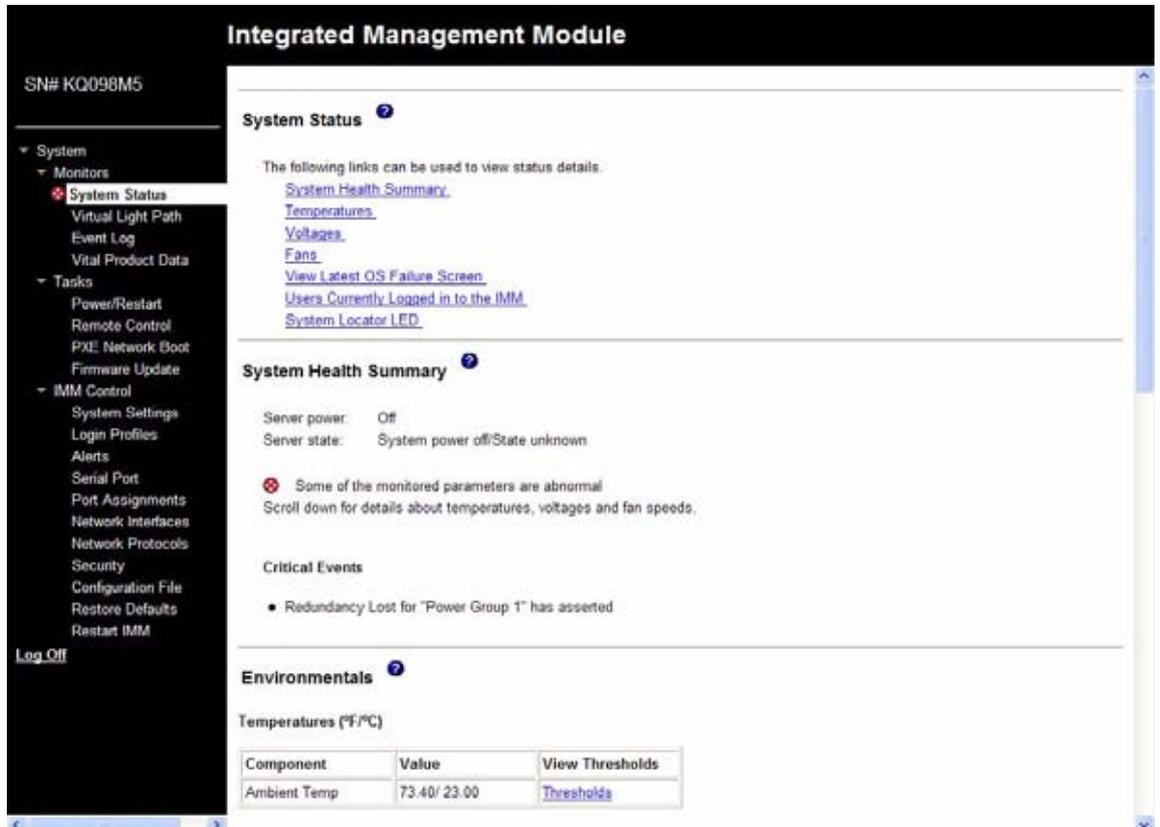
ステップ 3 [Welcome] Web ページで、提供されるフィールドのドロップダウン リストからタイムアウト値を選択します。ご使用のブラウザがその分数の間、非アクティブだった場合、IMM はユーザを Web インターフェイスからログオフさせます。



(注) システム管理者が設定したグローバル ログイン設定によっては、タイムアウト値が固定値である場合があります。

ステップ 4 [Continue] をクリックしてセッションを開始します。

ブラウザで [System Status] ページが開きます。ここではサーバステータスとサーバヘルスの要約をすばやく確認できます。



IMM Web インターフェイ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 アクションの説明」(P.2-3)を参照してください。その後、第 3 章「IMM の設定」に進みます。

IMM アクションの説明

表 2-1 に、IMM にログインしたときに使用できるアクションを示します。

表 2-1 IMM アクション

リンク	アクション	説明
System Status	サーバのシステムヘルスを表示し、オペレーティングシステム障害の画面キャプチャを表示し、IMM にログインしたユーザを表示する	[System Health] ページでは、サーバの電源およびヘルス状態、サーバの温度、電圧、およびファンのステータスをモニタできます。直近のオペレーティングシステム障害の画面キャプチャ、および IMM にログインしたユーザも表示できます。
Virtual Light Path	サーバライトパスのすべての LED の名前、色、およびステータスを表示する	[Virtual Light Path] ページには、サーバ上の LED の現在のステータスが表示されます。

表 2-1 IMM アクション (続き)

リンク	アクション	説明
Event Log	リモート サーバのイベント ログを表示する	[Event Log] ページには、現在シャーシ イベント ログに保存されているエントリが表示されます。ログには、BMC によって報告されたイベントのテキスト説明に加えて、すべてのリモート アクセス試行および設定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 の日時設定を使用してタイム スタンプが付けられます。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設定されている場合)。イベント ログ内のイベントをソートしたりフィルタリングしたりすることもできます。
Vital Product Data	サーバの重要な製品データ (VPD) を表示する	IMM は、サーバ情報、サーバファームウェア情報、およびサーバ 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。
Power/Restart	リモートからサーバの電源をオンにする、または再起動する	IMM は、サーバに対し、電源オン、電源オフ、および再起動アクションによる完全なリモート電源制御を提供します。さらに、電源オンおよび再起動の統計情報がキャプチャされて表示され、サーバハードウェアの可用性を示します。
Remote Control	サーバ 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のディスク ドライブまたはディスク イメージをサーバ上のドライブとして使用する	この機能はサポートされていません。
PXE Network Boot	次回の再起動で Preboot Execution Environment (PXE) / ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) ネットワーク起動を試行するために、ホストサーバの起動 (ブート) シーケンスを変更する	この操作はサポートされていません。
Firmware Update	IMM のファームウェアを更新する	Cisco TAC からの適切な指示なしに、システムのファームウェアを更新しないでください。シスコが認定およびリリースしたファームウェアを使用して、Cisco TAC から指示されたとおりにファームウェアを更新する必要があります。このガイドラインに従わない場合、システムが動作しなくなる可能性があります。
System Settings	IMM サーバ設定を表示および変更する	[System Settings] ページから、サーバの場所および一般情報 (IMM の名前、サーバのタイムアウト設定、IMM の連絡先情報など) を設定できます。
	IMM のクロックを設定する	イベント ログ内のエントリにタイム 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 インターフェイスを有効または無効にする	USB インバンド (または LAN over USB) インターフェイスを有効または無効にすることができます。  (注) Cisco Flex シリーズ 7500 ワイヤレス コントローラでは、この操作はサポートされていません。

表 2-1 IMM アクション (続き)

リンク	アクション	説明
Login Profiles	IMM ログイン プロファイルおよびグローバル ログイン設定を設定する	IMM へのアクセスを可能にするログイン プロファイルを最大 12 個まで定義できます。Lightweight Directory Access Protocol (LDAP) サーバ認証の有効化やアカウントセキュリティ レベルのカスタマイズなど、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 ログイン設定も定義できます。
Alerts	リモート アラートおよびリモートアラート受信者を設定する	さまざまなイベントに関するアラートを生成して転送するように IMM を設定できます。[Alerts] ページでは、モニタ対象にするアラートと、その通知先にする受信者を設定できます。  (注) Cisco Flex 7500 シリーズワイヤレス コントローラでは、この操作はサポートされていません。
	簡易ネットワーク管理プロトコル (SNMP) イベントを設定する	SNMP トラップが送信されるイベントのカテゴリを設定できます。
	アラート設定を設定する	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 ポート設定を設定する	シリアル ポートはシリアル コンソール リダイレクション機能専用になります。そのため、IMM には使用できません。
Port Assignments	IMM プロトコルのポート番号の変更	[Port Assignments] ページから、IMM プロトコル (たとえば、HTTP、HTTPS、Telnet、および SNMP) に割り当てられたポート番号を表示および変更できます。
Network Interfaces	IMM のネットワーク インターフェイスを設定する	[Network Interfaces] ページから、IMM のイーサネット接続に関するネットワーク アクセス設定を設定できます。
Network Protocols	IMM のネットワーク プロトコルを設定する	[Network Protocols] ページから、IMM で使用される簡易ネットワーク管理プロトコル (SNMP)、ドメインネームシステム (DNS)、および簡易メール転送プロトコル (SMTP) の設定を設定できます。LDAP パラメータも設定できます。
Security	Secure Sockets Layer (SSL) を設定する	SSL を有効または無効にし、使用される SSL 証明書を管理できます。LDAP サーバへの接続に SSL 接続を使用できるようにするかどうかも設定できます。
	セキュア シェル (SSH) アクセスを有効にする	IMM への SSH アクセスを有効にできます。
Configuration	IMM 設定をバックアップおよび復元する	[Configuration File] ページから、IMM の設定のバックアップ、変更、および復元ができるほか、設定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	注意: [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 の設定を工場出荷時のデフォルトにリセットできます。
Restart IMM	IMM を再起動する	IMM を再起動できます。
Log off	IMM をログオフする	IMM への接続をログオフできます。

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 の設定をすばやく表示できます。



CHAPTER 3

IMM の設定

IMM を設定するには、ナビゲーション ペインの [IMM Control] にあるリンクを使用します。

- [System Settings] ページからは、次の操作ができます。
 - サーバ情報を設定する。
 - サーバ タイムアウトを設定する。
 - IMM の日付と時刻を設定する。
 - USB インターフェイスに対してコマンドをイネーブルまたはディセーブルにする。
- [Login Profiles] ページからは、次の操作ができます。
 - ログイン プロファイルを設定して IMM へのアクセスを制御する。
 - ログイン試行に失敗した後のロックアウト期間など、グローバル ログインの設定を行う。
 - アカウント セキュリティ レベルを設定する。
- [Alerts] ページからは、次の操作ができます。
 - リモート アラートの受信者を設定する。
 - リモート アラートの試行回数を設定する。
 - アラート間の遅延を選択する。
 - 送信するアラートとその転送方法を選択する。
- [Port Assignments] ページからは、IMM サービスのポート番号を変更できます。
- [Network Interfaces] ページからは、IMM のイーサネット接続を設定できます。
- [Network Protocols] ページからは、次の設定を行えます。
 - SNMP の設定
 - DNS の設定
 - Telnet プロトコル
 - SMTP の設定
 - LDAP の設定
 - サービス ロケーション プロトコル
- [Security] ページからは、Secure Sockets Layer (SSL) 設定をインストールし、設定できます。
- [Configuration File] ページからは、IMM の設定のバックアップ、変更、および復元が可能です。
- [Restore Defaults] ページからは、IMM の設定を工場出荷時のデフォルトにリセットできます。
- [Restart IMM] ページからは、IMM を再起動できます。

システム情報の設定

IMM システム情報を設定する手順は、次のとおりです。

- ステップ 1** システム情報を設定する IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで [System Settings] をクリックします。次の図に示すようなページが表示されます。



(注) [System Settings] ページで使用できるフィールドは、アクセスするリモート サーバによって決まります。

- ステップ 3** [IMM Information] 領域の [Name] フィールドで、IMM の名前を入力します。
- [Name] フィールドを使用して、このサーバに IMM の名前を指定します。この名前が、アラートの送信元を識別するために電子メールおよび SNMP アラート通知に含まれます。



(注) [Name] フィールドが 16 文字に制限されているため、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有しません。[Hostname] フィールドには、最大で 63 文字まで含めることができます。わかりやすいように、[Name] フィールドには IP ホスト名の非修飾部分を設定します。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。たとえば、完全修飾 IP ホスト名が imm1.us.company.com の場合、非修飾 IP ホスト名は imm1 となります。ホスト名の詳細については、「ネットワーク インターフェイスの設定」(P.3-20) を参照してください。

- ステップ 4** [Contact] フィールドには、連絡先情報を入力します。たとえば、このサーバに関して問題が生じた場合に連絡先となる人物の名前と電話番号を指定できます。このフィールドには、最大 47 文字を入力できます。
- ステップ 5** [Location] フィールドには、サーバの場所を入力します。このフィールドには、メンテナンスやその他の目的でサーバをすばやく見つけるのに十分な詳細を入力します。このフィールドには、最大 47 文字を入力できます。
- ステップ 6** ページの一番下までスクロールし、[Save] をクリックします。

サーバ タイムアウトの設定



(注) サーバ タイムアウトを設定するには、インバンド USB インターフェイス（または LAN over USB）をイネーブルにしてコマンドを使用可能にする必要があります。USB インターフェイスに対するコマンドのイネーブル化とディセーブル化の詳細については、「USB インバンド インターフェイスのディセーブル化」(P.3-6) を参照してください。



(注) LAN over USB および OS ウォッチドッグ機能は、Cisco Flex 7500 シリーズ ワイヤレス コントローラではサポートされていません。

サーバ タイムアウト値を設定する手順は、次のとおりです。

- ステップ 1** サーバ タイムアウトを設定する IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで、[System Settings] をクリックし、[Server Timeouts] 領域までスクロールします。
- 次のイベントに自動的に応答するように、IMM を設定できます。
- オペレーティング システムの停止
 - オペレーティング システムのロード失敗
- ステップ 3** IMM に自動的に応答させるイベントに対応するサーバ タイムアウトをイネーブルにします。

[OS watchdog] : [OS watchdog] フィールドを使用して、IMM がオペレーティング システムをチェックする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いずれかに応答しなかった場合、IMM は OS タイムアウト アラートを生成し、サーバを再起動します。サーバの再起動後は、オペレーティング システムがシャットダウンされ、サーバの電源が再投入されるまで、OS ウォッチドッグはディセーブルになります。

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 システム障害の画面を取得するには、[OS watchdog] フィールドでウォッチドッグをイネーブルにする必要があります。

[Loader watchdog] : [Loader watchdog] フィールドを使用して、POST の実行からオペレーティング システムの起動まで IMM が待機する分数を指定します。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、自動的にサーバを再起動します。サーバの再起動後は、オペレーティング システムがシャットダウンされ、サーバの電源が再投入されるまで（または、オペレーティング システムが起動し、ソフトウェアが正常にロードされるまで）ローダー タイムアウトは自動的にディセーブルになります。

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 システムの起動が完了するまで IMM が待機する時間の制限を選択します。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。

ステップ 4 ページの一番下までスクロールし、[Save] をクリックします。

IMM の日付と時刻の設定

IMM では独自のリアルタイム クロックを使用して、イベント ログに記録されるすべてのイベントのタイム スタンプを付けます。



(注)

IMM の日付と時刻の設定は、サーバクロックではなく、IMM クロックだけに影響します。IMM リアルタイム クロックとサーバクロックは独立した別個のクロックであり、異なる時刻を設定できます。IMM クロックとサーバクロックを同期化するには、ページの [Network Time Protocol] 領域に移動し、NTP サーバ ホスト名または IP アドレスを、サーバクロックの設定に使用したサーバ ホスト名または IP アドレスと同じものに設定します。詳細については、「ネットワーク内のクロックの同期化」(P.3-5) 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。クロックの設定では、タイムゾーンの異なる遠隔地からシステムを管理している管理者が使いやすいように、グリニッジ標準時 (GMT) のオフセットと夏時間 (DST) がサポートされています。サーバがオフまたはディセーブルである場合でも、イベント ログにリモートからアクセスできます。

IMM の日付と時刻の設定を確認する手順は、次のとおりです。

- ステップ 1** IMM の日付と時刻の値を設定する IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで [System Settings] をクリックし、[IMM Date and Time] 領域までスクロールします。ここに、Web ページが生成されたときの日付と時刻が表示されます。
- ステップ 3** 日付と時刻の設定を無効にして、夏時間 (DST) およびグリニッジ標準時 (GMT) のオフセットをイネーブルにするには、[Set IMM Date and Time] をクリックします。次の図に示すようなページが表示されます。

Network Time Protocol (NTP)

NTP auto-synchronization service

NTP server host name or IP address

NTP update frequency (in minutes)

- ステップ 4** [Date] フィールドに、現在の月、日、および年を示す数字を入力します。
- ステップ 5** [Time] フィールドでは、適用可能なエントリ フィールドにある現在の時、分、秒に対応する数字を入力します。時間 (hh) は、24 時間クロックの表示に従って 00 ~ 23 の数字にする必要があります。分 (mm) と秒 (ss) は、00 ~ 59 の数字にする必要があります。
- ステップ 6** [GMT offset] フィールドで、サーバが配置されているタイムゾーンに対応する、グリニッジ標準時 (GMT) からのオフセット (時間単位) を指定する数字を選択します。
- ステップ 7** [Automatically adjust for daylight saving changes] チェックボックスをオンまたはオフにして、現地時間が標準時間と夏時間で切り替わったときに IMM クロックを自動的に調整するかどうかを指定します。
- ステップ 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化

ネットワーク タイム プロトコル (NTP) は、コンピュータ ネットワーク全体でのクロックの同期化を可能にし、NTP クライアントが NTP サーバから正確な時刻を取得できるようにします。

IMM NTP 機能は、IMM リアルタイム クロックと、NTP サーバが提供する時刻の同期化を可能にします。使用される NTP サーバの指定、IMM を同期化する頻度の指定、NTP 機能のイネーブル化またはディセーブル化、および即時時刻同期化の要求を行うことができます。

NTP 機能は、NTP バージョン 3 および NTP バージョン 4 の暗号化アルゴリズムによって提供される拡張セキュリティおよび認証は提供しません。IMM NTP 機能は、認証のない簡易ネットワーク タイム プロトコル (SNTP) のみをサポートします。

IMM NTP 機能を設定する手順は、次のとおりです。

- ステップ 1** ネットワーク内でクロックを同期化する IMM にログインします。詳細については、[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。
- ステップ 2** ナビゲーション ペインで [System Settings] をクリックし、[IMM Date and Time] 領域までスクロールします。
- ステップ 3** [Set IMM Date and Time] をクリックします。次の図に示すようなページが表示されます。

Network Time Protocol (NTP) 

NTP auto-synchronization service

NTP server host name or IP address

NTP update frequency (in minutes)

ステップ 4 [Network Time Protocol (NTP)] から、次の設定を選択できます。

[NTP auto-synchronization service] : この選択を使用して、IMM クロックと NTP サーバの自動同期化をイネーブルまたはディセーブルにします。

[NTP server host name or IP address] : このフィールドを使用して、クロックの同期化に使用する NTP サーバの名前を指定します。

[NTP update frequency] : このフィールドを使用して、同期化要求のおおよその間隔（分単位）を指定します。3 ~ 1440 分の値を入力してください。

[Synchronize Clock Now] : 間隔時間の経過を待たずにただちに同期化を要求するには、このボタンをクリックします。

ステップ 5 [Save] をクリックします。

USB インバンド インターフェイスのディセーブル化



(注) Cisco Flex 7500 シリーズ ワイヤレス コントローラでは、USB インバンド インターフェイスをイネーブルすることができません。この設定は変更しないでください。



(注) **重要** : USB インバンド インターフェイスをディセーブルにすると、Linux フラッシュ ユーティリティを使用した IMM ファームウェア、サーバ ファームウェア、および DSA ファームウェアのインバンド アップデートを実行できません。USB インバンド インターフェイスがディセーブルの場合は、IMM Web インターフェイスに対する [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。

USB インバンド インターフェイスをディセーブルにした場合は、サーバが予期せずに再起動しないよう、ウォッチドッグ タイムアウトもディセーブルにしてください。詳細については、「[サーバ タイムアウトの設定](#)」(P.3-3) を参照してください。

USB インバンド インターフェイス、または LAN over USB は、IMM へのインバンド通信に使用されます。サーバで実行中のアプリケーションが、IMM に対してタスクの実行を要求しないよう、USB インバンド インターフェイスをディセーブルにする必要があります。

USB インバンド インターフェイスをディセーブルにする手順は、次のとおりです。

ステップ 1 USB デバイス ドライバ インターフェイスをディセーブルにする IMM にログインします。詳細については、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。

ステップ 2 ナビゲーション ペインで [System Settings] をクリックし、[Miscellaneous] 領域までスクロールします。次の図に示すようなページが表示されます。



ステップ 3 [Do not allow commands on USB interface] チェックボックスをオンにして、USB インバンド インターフェイスをディセーブルにします。USB インバンド インターフェイスをディセーブルにすると、Advanced Settings Utility (ASU) やファームウェア アップデート 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機能しなくなる場合があります。



(注) IPMI デバイス ドライバがインストールされている場合、ASU は USB インバンド インターフェイスがディセーブルの状態でも機能します。

インバンド インターフェイスがディセーブルのときに、システム管理アプリケーションを使用しようとしても、機能しない場合があります。

ステップ 4 [Save] をクリックします。

ディセーブルにした USB デバイス ドライバ インターフェイスをイネーブルにするには、[Do not allow commands on USB interface] チェックボックスをオフにして、[Save] をクリックします。



(注) USB インバンド インターフェイスは、「LAN over USB」とも呼ばれています。

ログイン プロファイルの作成

[Login Profiles] 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、設定、または変更できます。個々のログイン プロファイルを設定するには、[Login ID] カラムのリンクを使用します。一意のプロファイルを 12 個まで定義できます。[Login ID] カラムの各リンクには、関連するプロファイルに設定されたログイン ID のラベルが付いています。

特定のログイン プロファイルは、IPMI ユーザ ID と共有され、IPMI を含むすべての IMM ユーザ インターフェイスで使用する 1 組のローカル ユーザ アカウント (ユーザ名/パスワード) を提供します。次のリストで、これらの共有ログイン プロファイルに関するルールについて説明します。

- IPMI ユーザ ID 1 は、常にヌル ユーザです。
- IPMI ユーザ ID 2 はログイン ID 1、IPMI ユーザ ID 3 はログイン ID 2 というようにマップされます。
- IMM デフォルト ユーザには、IPMI ユーザ ID 2 とログイン ID 1 の USERID と PASSWORD (英字の O ではなくゼロを使用) が設定されます。

たとえば、IPMI コマンドによってユーザが追加された場合、そのユーザの情報も Web、Telnet、SSH、およびその他のインターフェイスを介した認証に使用できます。これに対して、Web やその他のインターフェイスでユーザが追加されると、そのユーザの情報は IPMI セッションを開始するために使用できます。

ユーザアカウントは IPMI と共有されるので、それらのアカウントを使用するインターフェイス間に共通性をもたらすために一定の制約が課されます。次のリストで、IMM および IPMI ログイン プロファイルの制約について説明します。

- IPMI では、最大 64 個のユーザ ID が許可されます。IMM IPMI の実装で許可されるユーザアカウントは 12 個のみです。
- IPMI では、匿名ログイン（ヌル ユーザ名とヌル パスワード）が許可されますが、IMM では許可されません。
- IPMI では、複数のユーザ ID が同じユーザ名を持つことが許可されますが、IMM では許可されません。
- 現在名から同じ現在名にユーザ名を変更する IPMI 要求では、要求されたユーザ名がすでに使用されているため、無効なパラメータ実行コードが返されます。
- IMM に対する IPMI パスワードの最大長は 16 バイトです。
- 次の単語には制約があり、ローカル IMM ユーザ名としては使用できません。
 - immroot
 - nobody
 - ldap
 - lighttpd
 - sshd
 - daemon
 - immftp

ログイン プロファイルを設定する手順は、次のとおりです。

-
- ステップ 1** ログイン プロファイルを作成する IMM にログインします。詳細については、[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。
- ステップ 2** ナビゲーション ペインで [Login Profiles] をクリックします。



(注) プロファイルを設定していない場合は、[Login Profiles] テーブルに表示されません。

次の図に示すように、[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期限情報が表示されます。

The screenshot shows the IMM web interface for device SN# KQ098M5. The left sidebar contains a navigation menu with categories like System, Monitors, Tasks, and IMM Control. The main content area is titled 'Login Profiles' and includes a table with columns for Slot No, Login ID, Access, and Password Expires. Below the table is an 'Add User' button. The 'Global Login Settings' section includes options for user authentication method, lockout period, and account security level.

Slot No	Login ID	Access	Password Expires
1	USERID	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

Account security level:

- Legacy security settings
 - No password required
 - No complex password required
 - No minimum password length
 - No password expiration
 - No password re-use restrictions
- High security settings
 - Password required
 - Complex password required
 - Minimum password length is 4
 - Passwords expire in 90 days
 - Password reuse checking enabled (last 5 passwords kept in history)

重要 : IMM にはデフォルトで、ログイン ユーザ ID に USERID およびパスワードに PASSWORD (0 は英字の O ではなくゼロ) を使用したリモート アクセスをイネーブルにする 1 つのログイン プロファイルが設定されます。潜在的なセキュリティ上の弱点を回避するため、IMM の初期設定でこのデフォルト ログイン プロファイルを変更してください。

ステップ 3 [Add User] をクリックします。次の図のような個別のプロファイル ページが表示されます。

Login Profile 

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)

ステップ 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] フィールドには最大 16 文字を入力できます。有効な文字は大文字、小文字、数字、ピリオド、および下線です。



(注) このログイン ID を使用して、IMM にリモート アクセス権が付与されます。

ステップ 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 文字以上とし、そのうちの 1 文字は英字以外の文字にする必要があります。ヌルまたは空のパスワードも許可されます。



(注) このパスワードは、IMM にリモート アクセス権を付与するためのログイン ID と一緒に使用されます。

ステップ 6 [Confirm Password] フィールドに、パスワードを再入力します。

ステップ 7 [Authority Level] 領域で、次のいずれかのオプションを選択して、このログイン ID のアクセス権を設定します。

[Supervisor] : ユーザには制限はありません。

[Read Only] : ユーザは、読み取り専用アクセスのみが可能となり、ファイル転送などのアクション、電源投入と再起動のアクション、またはリモートプレゼンス機能は実行できません。

[Custom] : [Custom] オプションを選択した場合は、次に示す 1 つまたは複数のカスタム許可レベルを選択する必要があります。

- [User Account Management] : ユーザは、ユーザの追加、変更、または削除、および [Login Profiles] ページのグローバル ログイン設定の変更を行うことができます。
- [Remote Console Access] : ユーザはリモート コンソールにアクセスできます。

- [Remote Console and Virtual Media Access] : これはサポートされていません。
- [Remote Server Power/Restart Access] : ユーザは、リモートサーバに対する電源投入および再起動の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] : ユーザは、イベント ログをクリアできます。イベント ログは誰でも見ることはできますが、ログをクリアするにはこの特定の権限が必要です。
- [Adapter Configuration - Basic] : ユーザは、[System Settings and Alerts] ページで設定パラメータを変更できます。
- [Adapter Configuration - Networking & Security] : ユーザは、[Security]、[Network Protocols]、[Network Interface]、[Port Assignments]、および [Serial Port] の各ページで設定パラメータを変更できます。
- [Adapter Configuration - Advanced] : ユーザには、IMM を設定するときの制限はありません。また、ユーザは、IMM への管理上のアクセスが可能です。つまり、ユーザは、ファームウェアアップデート、PXE ネットワーク ブート、IMM の工場出荷時のデフォルトの復元、設定ファイルからの IMM 設定の変更と復元、および IMM の再起動とリセットなどの高度な機能も実行できます。

ユーザが IMM ログイン ID の許可レベルを設定すると、対応する IPMI ユーザ ID の IPMI 特権レベルが次の優先順位に従って設定されます。

- ユーザが IMM ログイン ID の許可レベルを [Supervisor] に設定すると、IPMI 特権レベルは [Administrator] に設定されます。
- ユーザが IMM ログイン ID の許可レベルを [Read Only] に設定すると、IPMI 特権レベルは [User] に設定されます。
- ユーザが IMM ログイン ID の許可レベルに対して次のアクセス タイプのいずれかを設定すると、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
- ユーザが IMM ログイン ID の許可レベルに対して [Remote Server Power/Restart Access] または [Ability to Clear Event Logs] を設定すると、IPMI 特権レベルは [Operator] に設定されます。
- ユーザが IMM ログイン ID の許可レベルに対して [Adapter Configuration (Basic)] を設定すると、IPMI 特権レベルは [User] に設定されます。



(注) ログイン プロファイルを工場出荷時のデフォルトに戻すには、[Clear Login Profiles] をクリックします。

ステップ 8 [Configure SNMPv3 User] 領域で、ユーザが SNMPv3 プロトコルを使用して IMM にアクセスできるかどうかをチェックボックスで選択します。チェックボックスをオンすると、次の図のようなページの領域が表示されます。

Configure SNMPv3 User

 Configure SNMPv3 UserSNMPv3 User Profile 

Authentication Protocol	<input type="text" value="HMAC-MD5"/>
Privacy Protocol	<input type="text" value="None"/>
Privacy Password	<input type="text"/>
Confirm Privacy Password	<input type="text"/>
Access Type	<input type="text" value="Get"/>
Hostname/IP address for traps	<input type="text"/>

次のフィールドを使用して、ユーザ プロファイルに対する SNMPv3 の設定を行います。

[Authentication Protocol] : このフィールドを使用して、[HMAC-MD5] または [HMAC-SHA] 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 モデルで認証に使用されるハッシュアルゴリズムです。Linux アカウントのパスワードは、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できます。サポートされる方法は、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、[Get] または [Set] をアクセス タイプとして指定します。アクセス タイプが Get の SNMPv3 ユーザは、照会操作のみを実行できます。アクセス タイプが Set の SNMPv3 ユーザは、照会操作の実行と設定の変更（ユーザに対するパスワードの設定など）の両方を行えます。

[Hostname/IP address for traps] : このフィールドを使用して、ユーザ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になります。SNMP エージェントは、トラップを使用して、管理ステーションにイベント（プロセッサの温度が制限を超えた場合など）を通知します。

ステップ 9 [Save] をクリックして、ログイン ID の設定を保存します。

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手順は、次のとおりです。

- ステップ 1** ログイン プロファイルを作成する IMM にログインします。詳細については、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。
- ステップ 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期限情報が表示されます。
- ステップ 3** 削除するログイン プロファイルをクリックします。そのユーザに関する [Login Profile] ページが表示されます。

ステップ 4 [Clear Login Profile] をクリックします。

グローバル ログインの設定

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手順は、次のとおりです。

- ステップ 1 グローバル ログインを設定する IMM にログインします。詳細については、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。
- ステップ 2 ナビゲーション ペインで [Login Profiles] をクリックします。
- ステップ 3 [Global Login Settings] 領域までスクロールします。次の図に示す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:

<input checked="" type="radio"/> Legacy security settings	No password required No complex password required No minimum password length No password expiration No password re-use restrictions
<input type="radio"/> High security settings	Password required Complex password required Minimum password length is 4 Passwords expire in 90 days Password reuse checking enabled (last 5 passwords kept in history)
<input type="radio"/> Custom security settings	User login password required: Disabled Complex password required: <input type="checkbox"/> Minimum password length: 1 Number of previous passwords that cannot be used: 0 Maximum Password Age: days

ステップ 4 [User authentication method] フィールドで、ログインを試みているユーザの認証方法を指定します。次の認証方法のいずれかを選択します。

- [Local only]: ユーザは、IMM のローカルであるテーブルの検索によって認証されます。ユーザ ID とパスワードに不一致があると、アクセスは拒否されます。正常に認証されたユーザには、「[ログイン プロファイルの作成](#)」(P.3-7) で設定した許可レベルが割り当てられます。
- [LDAP only]: IMM は、LDAP サーバを使用してユーザの認証を試みます。IMM 上のローカル ユーザ テーブルは、この認証方法では検索されません。
- [Local first, then LDAP]: ローカル認証が最初に試みられます。ローカル認証に失敗すると、LDAP 認証が試みられます。
- [LDAP first, then Local]: LDAP 認証が最初に試みられます。LDAP 認証が失敗した場合は、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ので、ローカルで管理されるアカウントだけが IPMI インターフェイスと共有されます。



(注) [User authentication method] フィールドが [LDAP only] に設定されている場合でも、ユーザはローカルで管理されるアカウントを使用して IPMI インターフェイスにログインできます。

- ステップ 5** [Lockout period after 5 login failures] フィールドに、連続して 5 回を超えるリモート ログインの失敗があっ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（分単位）を指定します。1 人のユーザがロックアウトされても、他のユーザがログインできなくなることはありません。
- ステップ 6** [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前に IMM が待機する時間（分単位）を指定します。[No timeout] を選択すると、この機能がディセーブルになります。ユーザがログイン 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。
- ステップ 7** (任意) [Account security level] 領域で、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] には、要件リストに示すとおりデフォルト値が設定されます。
- ステップ 8** セキュリティ設定をカスタマイズするには、[Custom security settings] を選択してアカウントセキュリティ管理の設定を表示し、変更します。
- [User login password required] : このフィールドを使用して、パスワードなしのログイン ID が許可されるかどうかを示します。
- [Number of previous passwords that cannot be used] : このフィールドを使用して、再使用できない以前のパスワードの数を示します。以前のパスワードは 5 つまで照合できます。[0] を選択すると、以前のパスワードをすべて再使用できます。
- [Maximum Password Age] : このフィールドを使用して、パスワードの最大経過時間を示します。この経過時間を越えると、パスワードの変更が必要になります。0 ~ 365 日の値がサポートされます。パスワードの期限チェックをディセーブルにするには、[0] を選択します。
- ステップ 9** [Save] をクリックします。

リモートアラートの設定

ナビゲーション ペインの [Alerts] リンクから、リモートアラートの受信者、アラートの試行回数、リモートアラートをトリガーする事象、およびローカルアラートを設定できます。

リモートアラートの受信者を設定すると、[Monitored Alerts] グループから選択したイベントが発生した場合に、IMM からその受信者にネットワーク接続を介してアラートが送信されます。このアラートには、イベントの性質、イベントの日時、およびアラートを生成したシステムの名前についての情報が含まれます。



(注) [SNMP Agent] フィールドまたは [SNMP Traps] フィールドが [Enabled] に設定されていないと、SNMP トラップは送信されません。これらのフィールドの詳細については、「[SNMP の設定](#)」(P.3-23) を参照してください。

リモート アラート受信者の設定

固有のリモート アラート受信者を 12 件まで定義できます。アラート受信者に対する各リンクには、受信者の名前とアラート ステータスのラベルが付きます。



(注)

アラート受信者のプロファイルを設定していない場合は、リモート アラート受信者のリストにプロファイルが表示されません。

リモート アラート受信者を設定する手順は、次のとおりです。

- ステップ 1** リモートアラートを設定する IMM にログインします。詳細については、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。
- ステップ 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。各受信者に通知方法とアラート ステータスが設定されている場合は、それらの情報を表示できます。

The screenshot displays the 'Remote Alert Recipients' configuration page in the IMM web interface. The page includes a navigation sidebar on the left with 'Alerts' highlighted. The main content area features a table with 12 rows, each representing a recipient with a 'Name' (a link labeled '~ not used ~') and a 'Status' column. Below the table, there are sections for 'Global Remote Alert Settings' (with fields for 'Remote alert retry limit', 'Delay between entries', and 'Delay between retries') and 'SNMP Alerts Settings' (with a checkbox for 'Critical Alerts').

- ステップ 3** リモートアラート受信者のリンクのいずれかをクリックするか、[Add Recipient] をクリックします。次の図のような個々の受信者ウィンドウが開きます。

Remote Alert Recipient 1 ?

Status Enabled ▾

Name

E-mail address (userid@hostname)

Include event log with e-mail alerts

Monitored Alerts ?

Select the alerts that will be sent to remote alert recipients.

Critical Alerts

- Critical-Other
- Critical-Temperature
- Critical-Voltage
- Critical-Power
- Critical-Hard Disk Drive
- Critical-Fan Failure
- Critical-CPU
- Critical-Memory
- Critical-Hardware Incomptability
- Critical-Redundant Power Supply

Warning Alerts

- Warning-Other
- Warning-Temperature
- Warning-Voltage
- Warning-Power
- Warning-Fan
- Warning-CPU
- Warning-Memory
- Warning-Redundant Power Supply

System Alerts

- System-Other
- System-Remote Login

ステップ 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。

ステップ 5 [Name] フィールドに、受信者の名前やその他の識別子を入力します。入力した名前が、[Alerts] ページで受信者に対するリンクとして表示されます。

ステップ 6 [E-mail address] フィールドに、アラートの受信者の電子メールアドレスを入力します。

ステップ 7 電子メールアラートにイベントログを組み込むには、チェックボックスを使用します。

ステップ 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分類されます。

[Critical alerts] : 重大アラートは、サーバコンポーネントが機能しなくなっていることを示すイベントに対して生成されます。

[Warning alerts] : 警告アラートは、重大レベルに進むおそれのあるイベントに対して生成されます。

[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するイベント、または設定変更の結果として発生するイベントに対して生成されます。すべてのアラートはイベント ログに保存され、設定されているすべてのリモート アラート受信者に送信されます。

ステップ 9 [Save] をクリックします。

グローバル リモート アラートの設定

グローバル 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 によるアラート送信の試行回数を設定する手順は、次のとおりです。

ステップ 1 リモート アラートの試行を設定する IMM にログインします。詳細については、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。

ステップ 2 ナビゲーション ペインで [Alerts] をクリックし、[Global Remote Alert Settings] 領域までスクロールします。

Global Remote Alert Settings

These settings apply to all remote alert recipients.

Remote alert retry limit	<input type="text" value="5"/>	times
Delay between entries	<input type="text" value="0.0"/>	minutes
Delay between retries	<input type="text" value="0.5"/>	minutes

これらの設定を使用して、リモートアラートの試行回数と、試行の時間間隔を定義します。設定されているすべてのリモートアラート受信者にこれらの設定が適用されます。

[Remote alert retry limit] : [Remote alert retry limit] フィールドを使用して、IMM が受信者へのアラートの送信を試行する追加回数を指定します。IMM は複数のアラートを送信しません。追加のアラートの試行は、IMM が最初のアラートの送信を試みたときに失敗した場合のみ行われます。



(注) このアラートの設定は、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にアラートを送信するまで待機する時間間隔（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 が受信者に対してアラートの送信を再試行する時間間隔（分単位）を指定します。

ステップ 3 ページの一番下までスクロールし、[Save] をクリックします。

SNMP アラートの設定

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 を設定できます。フィルタリングに使用できるイベントカテゴリは、Critical、Warning、および System です。SNMP アラートの設定は、すべての SNMP トラップに対してグローバルになります。



(注) IMM は、SNMP アプリケーションと併用するために 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 アップデート パッケージに含まれています。



(注) IMM は、SNMPv1 および SNMPv3 標準をサポートします。

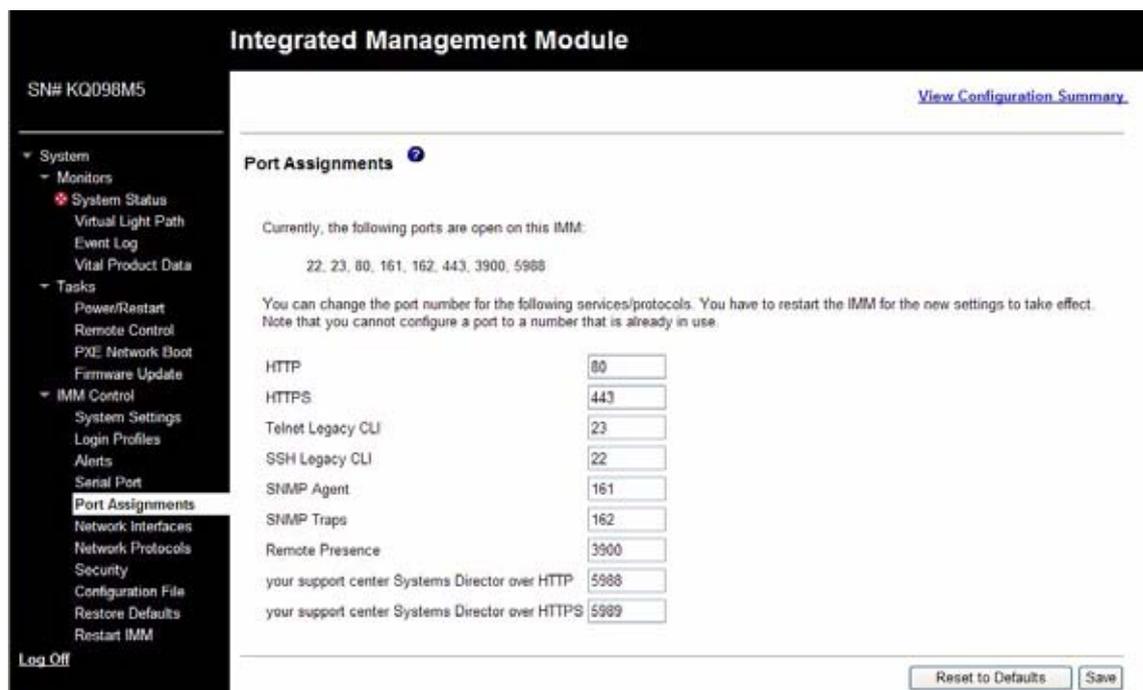
SNMP に送信するアラートのタイプを選択する手順は、次のとおりです。

- ステップ 1 リモートアラートの試行を設定する IMM にログインします。詳細については、[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。
- ステップ 2 ナビゲーション ペインで [Alerts] をクリックし、[SNMP Alert Settings] 領域までスクロールします。
- ステップ 3 1 つまたは複数のアラート 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分類されます。
 - Critical
 - Warning
 - System
- ステップ 4 ページの一番下までスクロールし、[Save] をクリックします。

ポートの割り当ての設定

IMM サービスのポート番号を変更する手順は、次のとおりです。

- ステップ 1 ポートの割り当てを設定する IMM にログインします。詳細については、[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。
- ステップ 2 ナビゲーション ペインで [Port Assignments] をクリックします。次の図に示すようなページが表示されます。



ステップ 3 次の情報を使用して、フィールドの値を割り当てます。

[HTTP] : これは、IMM の HTTP サーバのポート番号です。デフォルトのポート番号は 80 です。その他の有効な値の範囲は、1 ~ 65535 です。このポート番号を変更する場合は、Web アドレスの最後にコロンを付け、続けてこのポート番号を追加する必要があります。たとえば、HTTP ポートを 8500 に変更する場合は、<http://hostname:8500/> と入力して IMM Web インターフェイスを開きます。IP アドレスとポート番号の前に、プレフィックス `http://` を入力する必要がありますことに注意してください。

[HTTPS] : これは、Web インターフェイスの 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。その他の有効な値の範囲は、1 ~ 65535 です。

[Telnet Legacy CLI] : これは、Telnet サービスを介してログインするためのレガシー CLI 用のポート番号です。デフォルト値は 23 です。その他の有効な値の範囲は、1 ~ 65535 です。

[SSH Legacy CLI] : これは、SSH を介してログインするためにレガシー CLI に設定されているポート番号です。デフォルトは 22 です。

[SNMP Agent] : これは、IMM で実行する SNMP エージェント用のポート番号です。デフォルト値は 161 です。その他の有効な値の範囲は、1 ~ 65535 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。その他の有効な値の範囲は、1 ~ 65535 です。

[Remote Presence] : この機能は、3 つの製品すべてでサポートされているわけではありません。

次のポート番号は予約されており、対応するサービスにのみ使用できます。

表 3-1 予約済みポート番号

ポート番号	サービスの対象
427	SLP
7070 ~ 7077	パーティション管理

ステップ 4 [Save] をクリックします。

ネットワーク インターフェイスの設定

[Network Interfaces] ページでは、IMM へのイーサネット接続を設定することで、IMM へのアクセスを設定できます。IMM にイーサネットを設定する手順は、次のとおりです。

- ステップ 1** 設定を行う IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで [Network Interfaces] をクリックします。次の図に示すようなページが表示されます。



(注) 次の図に値の例を示します。実際の設定は異なります。

Ethernet ⓘ

Interface

IPv6 Enabled

Hostname

Domain name

DDNS Status

Domain Name Used

[Advanced Ethernet Setup](#)

▼ IPv4

DHCP

*** Currently the static IP configuration is active for this interface.
*** This static configuration is shown below.

Static IP Configuration

IP address

Subnet mask

Gateway address

▼ IPv6

Link local address:

IPv6 static IP configuration

DHCPv6

Stateless Auto-configuration

[View Automatic Configuration](#)

- ステップ 3** イーサネット接続を使用する場合は、[Interface] フィールドで [Enabled] を選択します。イーサネットはデフォルトで有効になっています。



(注) イーサネット インターフェイスをディセーブルにすると、外部ネットワークから IMM へのすべてのアクセスが防止されます。

ステップ 4 ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) サーバ接続を使用する場合は、[DHCP] フィールドで次のいずれかをクリックして、このサーバ接続をイネーブルにします。

- Enabled - Obtain IP config from DHCP server
- Try DHCP server.If it fails, use static IP config.

デフォルトの設定は、[Try DHCP server. If it fails, use static IP config.] です。



(注) ネットワーク上にアクセス可能でアクティブな設定済み DHCP サーバがない限り、DHCP をイネーブルにしないでください。DHCP を使用すると、自動設定によって手動設定が無効になります。

スタティック IP アドレスを IMM に割り当てる場合は、[Disabled - Use static IP configuration] を選択します。

DHCP がイネーブルの場合、ホスト名が次のとおりに割り当てられます。

- [Hostname] フィールドにエントリがある場合、IMM DHCP サポートによって、DHCP サーバがこのホスト名を使用することが要求されます。
- [Hostname] フィールドにエントリがない場合、IMM DHCP サポートによって、DHCP サーバが固有のホスト名を IMM に割り当てることが要求されます。

ステップ 5 [Hostname] フィールドに IMM の IP ホスト名を入力します。

このフィールドには、IMM の IP ホスト名を示す文字を 63 文字まで入力できます。ホスト名はデフォルトで IMM1 に設定され、その後に IMM Burned-in Media Access Control (MAC) Address が続きます。



(注) IMM の IP ホスト名 ([Hostname] フィールド) と IMM 名 ([System] ページの [Name] フィールド) は、自動的に同じ名前を共有しません。これは、[Name] フィールドは 15 文字に制限されていますが、[Hostname] フィールドには 63 文字まで入力できるためです。わかりやすいように、[Name] フィールドには IP ホスト名の非修飾部分を設定します。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。たとえば、完全修飾 IP ホスト名が imm1.us.company.com の場合、非修飾 IP ホスト名は imm1 となります。ホスト名の詳細については、「システム情報の設定」(P.3-2) を参照してください。

DHCP をイネーブルにした場合は、[ステップ 12](#)に進みます。

DHCP をイネーブルにしていない場合は、そのまま[ステップ 6](#)に進みます。

ステップ 6 [IP address] フィールドに、IMM の IP アドレスを入力します。IP アドレスは、0 ~ 255 の範囲の 4 つの整数で構成する必要があります。整数間はスペースを入れずに、ピリオドで区切ります。

ステップ 7 [Subnet mask] フィールドに、IMM で使用されるサブネット マスクを入力します。サブネット マスクは、0 ~ 255 の範囲の 4 つの整数で構成する必要があります。整数間はスペースや連続ピリオドを使用せず、ピリオドで区切ります。

デフォルトの設定は、255.255.255.0 です。

ステップ 8 [Gateway address] フィールドに、ネットワーク ゲートウェイ ルータを入力します。ゲートウェイ アドレスは、0 ~ 255 の範囲の 4 つの整数で構成する必要があります。整数間はスペースや連続ピリオドを使用せず、ピリオドで区切ります。

ステップ 9 ページの一番下までスクロールし、[Save] をクリックします。

ステップ 10 追加のイーサネット設定が必要である場合は、[Advanced Ethernet Setup] をクリックします。

Advanced Ethernet Setup ?

Autonegotiation: Yes ▾

Data rate: Auto ▾

Duplex: Auto ▾

Maximum transmission unit: 1500 bytes

Locally administered MAC address: 00:00:00:00:00:00

Burned-in MAC address: E4:1F:13:57:C1:DC

Note: The burned-in MAC address takes precedence when the locally administered MAC address is set to 00:00:00:00:00:00.

Cancel Save

次の表では、[Advanced Ethernet Setup] ページ上の機能について説明します。

表 3-2 [Advanced Ethernet Setup] ページ上の機能

フィールド	機能
Auto Negotiate	IMM は、スイッチ機能に応じてデータ レートとデュプレックス設定を自動的に決定します。
Data Rate	[Data Rate] フィールドを使用して、LAN 接続で毎秒転送されるデータ量を指定します。データ レートを設定するには、メニューをクリックし、ネットワークの機能に対応するデータ転送レート (Mb/s 単位) を選択します。データ転送レートを自動的に検出するには、[Auto Negotiate] フィールドを [Yes] に設定します。これは、デフォルト値になります。
Duplex	[Duplex] フィールドを使用して、ネットワークで使用する通信チャネルのタイプを指定します。 デュプレックス モードを設定するには、次のいずれかを選択します。 <ul style="list-style-type: none"> [Full] は、同時に双方向のデータ伝送を可能にします。 [Half] は、同時に双方向ではなく、いずれか一方のデータ伝送を可能にします。 デュプレックス タイプを自動的に検出するには、[Auto Negotiate] フィールドを [Yes] に設定します。これは、デフォルト値になります。
Maximum transmission unit	[Maximum transmission unit] フィールドを使用して、ネットワーク インターフェイスに対する最大パケット サイズ (バイト単位) を指定します。イーサネットの場合、有効な最大伝送単位 (MTU) の範囲は 60 ~ 1500 です。このフィールドのデフォルト値は 1500 です。
Locally administered MAC address	[Locally administered MAC address] フィールドに、IMM の物理アドレスを入力します。値が指定されていると、ローカルで管理されるアドレスによって Burned-In MAC Address が無効になります。ローカルで管理されるアドレスは、000000000000 ~ FFFFFFFF の 16 進数値であることが必要です。この値の形式は、xx:xx:xx:xx:xx:xx でなければならず、ここで x は数字の 0 ~ 9 となります。IMM は、マルチキャストアドレスの使用をサポートしません。マルチキャストアドレスの最初のバイトは、奇数です (最下位ビットは 1 に設定されます)。したがって、最初のバイトを偶数にする必要があります。

表 3-2 [Advanced Ethernet Setup] ページ上の機能 (続き)

フィールド	機能
Burned-in MAC address	Burned-In MAC Address は、製造業者によってこの IMM に割り当てられる一意の物理アドレスです。このアドレスは、読み取り専用フィールドになります。 ¹ Mb は、約 1,000,000 ビットです。

- ステップ 11** 必要に応じて詳細なイーサネット設定を変更します。
- ステップ 12** ページの一番下までスクロールし、[Save] をクリックします。
- ステップ 13** [Cancel] をクリックして、[Network Interfaces] ページに戻ります。DHCP がイネーブルの場合、サーバは自動的にホスト名、IP アドレス、ゲートウェイ アドレス、サブネット マスク、ドメイン名、DHCP サーバ IP アドレス、および最大 3 つの DNS サーバ IP アドレスを割り当てます。
- ステップ 14** DHCP がイネーブルの場合に DHCP サーバが割り当てる設定を表示するには、[IP Configuration Assigned by DHCP Server] をクリックします。
- ステップ 15** [Save] をクリックします。
- ステップ 16** [View Configuration Summary] をクリックして、現在のすべての設定の要約を表示します。
- ステップ 17** 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。

ネットワーク プロトコルの設定

[Network Protocols] ページで、次の機能を実行できます。

- 簡易ネットワーク管理プロトコル (SNMP) の設定
- ドメイン ネーム システム (DNS) の設定
- Telnet プロトコルの設定
- 簡易メール転送プロトコル (SMTP) の設定
- Lightweight Directory Access Protocol (LDAP) の設定
- サービス ロケーション プロトコル (SLP) の設定

ネットワーク プロトコルの設定に対する変更を有効にするには、IMM を再起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完了し、保存されるまで待機してから、IMM を再起動します。

SNMP の設定

SNMP エージェントを使用して、情報の収集とサーバの制御を行います。また、SNMP アラートが設定済みのホスト名または IP アドレスに送信されるように、IMM を設定できます。



- (注)** IMM は、SNMP アプリケーションと併用するために 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 アップデート パッケージに含まれています。



(注) IMM は、SNMPv1 および SNMPv3 標準をサポートします。

SNMP を設定する手順は、次のとおりです。

- ステップ 1** SNMP を設定する IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで [Network Protocols] をクリックします。次の図に示すようなページが表示されます。

Integrated Management Module

SNMPv1 agent: Disabled

SNMPv3 agent: Disabled

SNMP traps: Disabled

SNMPv1 Communities

Community Name	Access Type	Host Name or IP Address
	Get	1. <input type="text"/>
	Get	2. <input type="text"/>
	Get	3. <input type="text"/>

SNMPv3 Users

If you enabled the SNMPv3 agent, you must configure SNMPv3 settings for active login profiles in order for the interaction between the SNMPv3 manager and SNMPv3 agent to work properly. You can configure these settings at the bottom of the individual login profile pages which can be reached via the [Login Profiles](#) page. Click the link for the login profile to configure, scroll to the bottom of the page and then click the "Configure SNMPv3 User" check box.

- ステップ 3** [SNMPv1 agent] フィールドまたは [SNMPv3 agent] フィールドで、[Enabled] を選択します。



(注) SNMPv3 エージェントを有効にした場合、SNMPv3 マネージャと SNMPv3 エージェントが正常に相互作用するように、SNMPv3 にアクティブなログイン プロファイルを設定する必要があります。これらの設定は、[Login Profiles] ページにある個々のログイン プロファイル設定の一番下で行うことができます（詳細については、「ログイン プロファイルの作成」(P.3-7) を参照してください）。設定するログイン プロファイルのリンクをクリックし、ページの一番下までスクロールして、[Configure SNMPv3 User] チェックボックスをオンにします。

- ステップ 4** [SNMP traps] フィールドで [Enabled] を選択し、ネットワーク上の SNMP コミュニティにアラートを転送します。SNMP エージェントをイネーブルにするには、次の基準を満たす必要があります。

- システム接点が [System Settings] ページに指定されている。[System Settings] ページの詳細については、「システム情報の設定」(P.3-2) を参照してください。
- システム ロケーションが [System Settings] ページに指定されている。

- 少なくとも 1 つのコミュニティ名が指定されている。
- 少なくとも 1 つの有効な IP アドレスまたはホスト名 (DNS がイネーブルの場合) がそのコミュニティに指定されている。



(注) 通知方法が SNMP であるアラート受信者は、[SNMPv1 agent] フィールドまたは [SNMPv3 agent] フィールドと、[SNMP traps] フィールドが [Enabled] に設定されていない限り、アラートを受信できません。

ステップ 5 コミュニティを設定して、SNMP エージェントと SNMP マネージャ間の管理関係を定義します。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、次のパラメータで構成されます。

- Community Name
- Access Type
- IP address

これらのパラメータのいずれかに誤りがあると、SNMP 管理アクセス権は付与されません。



(注) エラー メッセージ ウィンドウが開いたら、エラー ウィンドウに表示されているフィールドに必要な調整を行ってください。次にページの一番下までスクロールし、[Save] をクリックして修正した情報を保存します。少なくとも 1 つのコミュニティでこの SNMP エージェントがイネーブルになるように設定する必要があります。

ステップ 6 [Community Name] フィールドに、名前または認証文字列を入力してコミュニティを指定します。

ステップ 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対して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対して、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。また、コミュニティ内のすべてのホストに対して、トラップの受信と MIB オブジェクトの照会および設定を許可するには、[Set] を選択します。

ステップ 8 対応する [Host Name or IP Address] フィールドに、各コミュニティ マネージャのホスト名または IP アドレスを入力します。

ステップ 9 ページの一番下までスクロールし、[Save] をクリックします。

ステップ 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 の設定

ドメイン ネーム システム (DNS) を設定する手順は、次のとおりです。

ステップ 1 DNS を設定する IMM にログインします。詳細については、[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。

ステップ 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)] 領域までスクロールします。次の図のようなページのセクションが表示されます。

Domain Name System (DNS) Address assignments ?

DNS ▾

Preferred DNS Servers ▾

Order	IPv4	IPv6
Primary	<input type="text"/>	<input type="text"/>
Secondary	<input type="text"/>	<input type="text"/>
Tertiary	<input type="text"/>	<input type="text"/>

- ステップ 3** ネットワークで 1 台または複数の DNS サーバを使用可能にする場合は、[DNS] フィールドで [Enabled] を選択します。[DNS] フィールドは、ホスト名を IP アドレスに変換するためにネットワーク上の DNS サーバを使用するかどうかを指定します。
- ステップ 4** DNS をイネーブルにした場合、[DNS server IP address] フィールドにネットワーク上の最大 3 台の DNS サーバの IP アドレスを指定します。各 IP アドレスは、ピリオドで区切られた 0 ~ 255 の整数で構成する必要があります。
- ステップ 5** ページの一番下までスクロールし、[Save] をクリックします。
- ステップ 6** 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 の設定

Telnet を設定する手順は、次のとおりです。

- ステップ 1** Telnet を設定する IMM にログインします。詳細については、[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。
- ステップ 2** ナビゲーション ペインで [Network Protocols] をクリックし、ページの [Telnet Protocol] 領域までスクロールします。同時 Telnet ユーザの最大数を設定するか、Telnet アクセスをディセーブルにすることができます。
- ステップ 3** ページの一番下までスクロールし、[Save] をクリックします。
- ステップ 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 の設定

簡易メール転送プロトコル (SMTP) サーバの IP アドレスまたはホスト名を指定する手順は、次のとおりです。

- ステップ 1** SMTP を設定する IMM にログインします。詳細については、[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。
- ステップ 2** ナビゲーション ペインで [Network Protocols] をクリックし、ページの [SMTP] 領域までスクロールします。

- ステップ 3** [SMTP Server Host Name or IP address] フィールドに、SMTP サーバのホスト名を入力します。このフィールドを使用して、IP アドレスか、DNS がイネーブルであり、設定されている場合は SMTP サーバのホスト名を指定します。
- ステップ 4** ページの一番下までスクロールし、[Save] をクリックします。
- ステップ 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 の設定

IMM は、ローカル ユーザ データベースを経由する代わりに、Lightweight Directory Access Protocol (LDAP) サーバを使用して、LDAP サーバ上の LDAP ディレクトリを照会または検索することにより、ユーザを認証できます。IMM はその後、中央の LDAP サーバを介してユーザ アクセスをリモートで認証できます。これには、IMM での LDAP クライアント サポートが必要です。LDAP サーバで検出された情報に従って、許可レベルを割り当てることもできます。

また、通常のユーザ (パスワードチェック) 認証に加え、LDAP を使用してユーザおよび IMM をグループに割り当て、グループ認証を実行することもできます。たとえば、IMM は 1 つまたは複数のグループに関連付けることができ、ユーザは、IMM に関連付けられている 1 つ以上のグループに属している場合のみグループ認証に合格します。

LDAP サーバを使用するためのクライアントの設定

LDAP サーバを使用するようにクライアントを設定する手順は、次のとおりです。

- ステップ 1** クライアントを設定する IMM にログインします。詳細については、[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。
- ステップ 2** ナビゲーション ペインで [Network protocols] をクリックし、ページの [Lightweight Directory Access Protocol (LDAP) Client] 領域までスクロールします。次の図に示すようなページが表示されます。

Lightweight Directory Access Protocol (LDAP) Client  Use DNS to Find LDAP Servers

Domain Source	<input type="text" value="Extract search domain from login ID"/>
Search Domain	<input type="text"/>
Service Name	<input type="text" value="ldap"/>

 Use Pre-configured LDAP Servers

	LDAP Server Fully Qualified Host Name or IP Address	Port
1.	<input type="text"/>	<input type="text"/>
2.	<input type="text"/>	<input type="text"/>
3.	<input type="text"/>	<input type="text"/>

Miscellaneous Parameters

Root DN	<input type="text" value="dc=us,dc=ibm,dc=com"/>
UID Search Attribute	<input type="text" value="sAMAccountName"/>
Binding Method	<input type="text" value="With configured credentials"/>
Client DN	<input type="text" value="cn=test,cn=Users,dc=us,dc=ibm,dc=com"/>
Password	<input type="text"/>
Confirm password	<input type="text"/>
Enhanced role-based security for Active Directory Users	<input type="text" value="Enabled"/>
Server Target Name	<input type="text"/>

IMM には、1 つまたは複数の LDAP サーバを介したユーザ認証を行うように設定できるバージョン 2.0 LDAP クライアントが含まれます。認証に使用される LDAP サーバは、動的に検出することも、手動で事前に設定することもできます。

ステップ 3 次のいずれかの方法を選択して、LDAP クライアントを設定します。

- LDAP サーバを動的に検出するには、[Use DNS to Find LDAP Servers] を選択します。

LDAP サーバを動的に検出することを選択した場合、サーバの検出には、RFC2782 に記述されているメカニズム（サービスの場所を指定するための DNS RR）が適用されます。これは、DNS SRV として知られています。次のリストで、各パラメータについて説明します。

[Domain Source] : DNS サーバに送信される DNS SRV 要求で、ドメイン名を指定する必要があります。LDAP クライアントは、選択されたオプションに応じてこのドメイン名を取得する場所を決定します。3 つのオプションがあります。

- [Extract search domain from login id]。LDAP クライアントでは、ログイン ID にドメイン名が使用されます。たとえば、ログイン ID が joesmith@mycompany.com である場合、ドメイン名は mycompany.com です。ドメイン名が抽出できない場合、DNS SRV が失敗し、それによってユーザ認証が自動的に失敗します。
- [Use only configured search domain below]。LDAP クライアントでは、[Search Domain] パラメータに設定されているドメイン名が使用されます。

- [Try login id first, then configured value]。LDAP クライアントは最初に、ログイン ID からのドメイン名の抽出を試みます。この抽出に成功すると、このドメイン名が DNS SRV 要求に使用されます。ドメイン名がログイン ID に存在しない場合、LDAP クライアントは設定されている [Search Domain] パラメータをドメイン名として DNS SRV 要求に使用します。何も設定されていない場合は、そこでユーザ認証が失敗します。

[Search Domain] : [Domain Source] パラメータの設定によっては、このパラメータをドメイン名として DNS SRV 要求で使用することもできます。

[Service Name] : DNS サーバに送信される DNS SRV 要求には、サービス名も指定する必要があります。設定されている値が使用されます。このフィールドを空白のままにした場合、デフォルト値は **ldap** です。DNS SRV 要求には、プロトコル名も指定する必要があります。デフォルトは **tcp** であり、設定することはできません。

- 事前に設定された LDAP サーバを使用するには、[Use Pre-Configured LDAP Server] を選択します。



(注) 各サーバのポート番号は任意です。フィールドを空白のままにした場合は、デフォルト値 389 が非セキュアな LDAP 接続用に使用されます。セキュアな接続用のデフォルト値は 636 です。少なくとも 1 つの LDAP サーバを設定する必要があります。

次のパラメータを設定できます。

[Root DN] : これは、LDAP サーバにあるディレクトリ ツリーのルート エントリの識別名 (DN) です (たとえば、dn=mycompany,dc=com)。この DN が、すべての検索のベース オブジェクトとして使用されます。

[UID Search Attribute] : 選択されたバインディング方法が [Anonymously] または [w/ Configured Credentials] の場合、LDAP サーバへの初期バインドの後に、ユーザの DN、ログイン権限、およびグループ メンバーシップなど、ユーザに関する特定の情報を取得することを目的とした検索要求が続けられます。この検索要求には、そのサーバ上でユーザ ID を示すために使用される属性名を指定する必要があります。この属性名は、ここで設定されます。

Active Directory サーバでは、この属性名は通常 **sAMAccountName** となります。Novell eDirectory および OpenLDAP サーバでは通常、**uid** となります。このフィールドを空白のままにすると、デフォルトで **uid** に設定されます。

[Group Filter] : このフィールドは、グループ認証に使用されます。グループ認証は、ユーザのクレデンシャルが正常に確認された後で試行されます。グループ認証に失敗すると、ユーザのログイン試行は拒否されます。グループ フィルタが設定されている場合、そのフィルタは、サービス プロセッサが属するグループを指定するために使用されます。つまり、ユーザがグループ認証に成功するためには、設定されている 1 つ以上のグループに属している必要があります。

[Group Filter] フィールドを空白のままにすると、グループ認証は自動的に成功します。グループ フィルタが設定されている場合は、リスト内の 1 つ以上のグループとユーザの属するグループの一致が試みられます。一致がない場合、ユーザは認証に失敗し、アクセスを拒否されます。1 つ以上の一致があると、グループ認証は成功します。これらの照合では、大文字と小文字が区別されます。

フィルタは 511 文字に制限されており、1 つまたは複数のグループ名で構成することができます。複数のグループ名を区切るために、コロン (:) 文字を使用する必要があります。先頭と末尾のスペースは無視されますが、その他のスペースはグループ名の一部として処理されます。グループ名内のワイルドカードの使用を許可するかどうかを選択できます。フィルタは、特定のグループ名 (IMMWest など)、すべてに一致するワイルドカード (*), またはプレフィックス付きのワイルドカード (IMM* など) にすることができます。デフォルトのフィルタは IMM* です。インストー

ルのセキュリティポリシーによってワイルドカードの使用が禁止されている場合、ワイルドカードの使用を許可しないことを選択でき、ワイルドカード文字(*)はワイルドカードではなく通常の文字として処理されます。

グループ名は、完全な DN として指定することも、cn 部分だけを使用することもできます。たとえば、DN が cn=adminGroup,dc=mycompany,dc=com のグループは、実際の DN または adminGroup を使用して指定できます。

Active Directory 環境の場合のみ、ネストされたグループメンバーシップがサポートされます。たとえば、ユーザが GroupA と GroupB のメンバーであり、GroupA が GroupC のメンバーである場合、ユーザは GroupC のメンバーでもあると言えます。128 個のグループが検索されると、ネストされた検索は停止します。1 つのレベルのグループが検索されてから、下位レベルのグループが検索されます。ループは検出されません。

[Binding Method] : LDAP サーバに対して検索または照会を行うには、まず、バインド要求を送信する必要があります。このパラメータは、LDAP サーバへのこの初期バインドの実行方法を制御します。次の 3 つのオプションから選択します。

- [Anonymously]。DN またはパスワードなしでバインドします。ほとんどのサーバは、特定のユーザレコードに対する検索要求を許可しないように設定されているので、このオプションは極力使用しないようにしてください。
- [w/ Configured Credentials]。設定されているクライアント DN とパスワードとともにバインドします。
- [w/ Login Credentials]。ログインプロセスで提供されるクレデンシャルとともにバインドします。ユーザ ID は、識別名、完全修飾ドメイン名、または IMM に設定されている [UID Search Attribute] に一致するユーザ ID を介して提供されます。

初期バインドが成功すると、ログインしているユーザに属する LDAP サーバ上のエントリを見つけるための検索が実行されます。必要に応じて 2 回目のバインドが試行され、この時点ではログインプロセスで入力されたユーザの LDAP レコードおよびパスワードから取得された DN が使用されます。このバインドに失敗すると、ユーザはアクセスを拒否されます。2 回目のバインドは、匿名または設定されたクレデンシャルによるバインディング方法を使用する場合のみ実行されます。

LDAP クライアント認証の設定

LDAP クライアント認証を設定する手順は、次のとおりです。

-
- ステップ 1** ナビゲーション ペインで [Network protocols] をクリックします。
 - ステップ 2** ページの [Lightweight Directory Access Protocol (LDAP) Client] 領域までスクロールし、[Set DN and password only if Binding Method used is w/ Configured Credentials] をクリックします。
 - ステップ 3** クライアントベースの認証を使用するには、[Client DN] フィールドにクライアントの識別名を入力します。[Password] フィールドにパスワードを入力するか、ブランクのままにします。
-

LDAP 検索属性の設定

LDAP 検索属性を設定する手順は、次のとおりです。

-
- ステップ 1** ナビゲーション ペインで [Network protocols] をクリックします。

ステップ 2 [Lightweight Directory Access Protocol (LDAP) Client] 領域までスクロールし、[Set attribute names for LDAP client search algorithm] をクリックします。

ステップ 3 検索属性を設定するには、次の情報を使用します。

[UID Search Attribute] : 選択されたバインディング方法が [Anonymously] または [w/ Configured Credentials] の場合、LDAP サーバへの初期バインドの後に、識別名、ログイン権限、およびグループメンバーシップなど、ユーザに関する特定の情報を取得することを目的とした検索要求が実行されません。この情報を取得するには、そのサーバ上のユーザ ID を示すために使用される属性名を検索要求で指定する必要があります。この名前は特に、ユーザが入力するログイン ID に対する検索フィルタとして使用されます。この属性名は、ここで設定されます。たとえば、Active Directory サーバでは、ユーザ ID に使用される属性名は通常 sAMAccountName となります。Novell eDirectory および OpenLDAP サーバでは通常、uid となります。このフィールドを空白のままにすると、ユーザ認証時にデフォルトの UID が使用されます。

[Group Search Attribute] : Active Directory または Novell eDirectory 環境では、このパラメータで、ユーザが属するグループの識別に使用される属性名を指定します。Active Directory では、これは通常 memberOf となり、eDirectory では通常 groupMembership となります。

OpenLDAP サーバ環境では、ユーザは一般に、objectClass が PosixGroup であるグループに割り当てられます。その環境では、このパラメータで、特定の PosixGroup のメンバーを識別するのに使用される属性名を指定します。これは通常、memberUid となります。

このフィールドを空白のままにすると、フィルタ内の属性名はデフォルトで memberOf に設定されます。

[Login Permission Attribute] : ユーザが LDAP サーバを介して正常に認証された場合、このユーザのログイン権限を取得する必要があります。これらの権限を取得するには、サーバに送信される検索フィルタで、ログイン権限に関連付けられた属性名を指定する必要があります。このフィールドは、この属性名を指定します。

このフィールドを空白のままにすると、ユーザにはデフォルトの読み取り専用権限が割り当てられ、ユーザおよびグループ認証に合格したものと見なされます。

キーワード文字列 IBMRBSPermissions= に対して、LDAP サーバから返される属性値が検索されます。このキーワードのすぐ後には必ず、12 個の連続する 0 または 1 で入力されるビット文字列が続きます。各ビットは、機能のセットを表します。ビットには、それぞれの位置に従って番号が割り当てられます。左端のビットはビット位置 0、右端のビットはビット位置 11 です。特定の位置の値が 1 である場合、その位置に関連付けられている機能がイネーブルになります。値 0 は、その機能をディセーブルにします。文字列 IBMRBSPermissions=010000000000 は、有効な例です。

IBMRBSPermissions= キーワードを使用すると、属性フィールドの任意の場所への配置が可能になります。これによって、LDAP 管理者は既存の属性を再使用することができるので、LDAP スキーマの拡張を防止できます。また、属性を本来の目的で使用することも可能になります。キーワード文字列は、属性フィールド内の任意の場所に追加できます。使用する属性は、自由形式の文字列に対応できる必要があります。

属性が正常に取得されると、LDAP サーバから返される値が、次の情報に基づいて解釈されます。

- **常に拒否 (ビット位置 0)** : このビットが設定されている場合、ユーザは常に認証に失敗します。この機能を使用して、特定のグループに関連付けられている 1 人または複数のユーザをブロックできます。
- **スーパーバイザ アクセス権 (ビット位置 1)** : このビットが設定されていると、ユーザには管理者特権が与えられます。ユーザは、すべての機能に対する読み取りおよび書き込みアクセス権を持ちます。このビットが設定されている場合、ビット 2 ~ 11 を個別に設定する必要はありません。
- **読み取り専用アクセス (ビット位置 2)** : このビットが設定されていると、ユーザには読み取り専用アクセスが割り当てられ、メンテナンス手順 (再起動、リモートアクション、ファームウェアアップデートなど) を実行したり、何らかのデータを (保存、クリア、または復元機能を使用し

て) 変更したりすることはできません。読み取り専用アクセス ビットとその他のすべてのビットは相互に排他的であり、読み取り専用アクセス ビットの優先順位が最も低くなります。その他のビットが設定されている場合、読み取り専用アクセス ビットは無視されます。

- **ネットワークおよびセキュリティ (ビット位置 3)** : このビットが設定されている場合、ユーザは [Security]、[Network Protocols]、[Network Interface]、[Port Assignments]、および [Serial Port] の各ページの設定を変更できます。
- **ユーザアカウント管理 (ビット位置 4)** : このビットが設定されている場合、ユーザは [Login Profiles] ページでユーザの追加、変更、または削除、および [Global Login Settings] の変更を行うことができます。
- **リモート コントロール アクセス (ビット位置 5)** : このビットが設定されている場合、ユーザはリモート サーバ コンソールにアクセスできます。
- **リモート コンソールおよびリモート ディスク (ビット位置 6)** : このビットが設定されている場合、ユーザはリモート サーバ コンソールと、リモート サーバに対するリモート ディスク機能にアクセスできます。
- **リモート サーバの電源投入/再起動アクセス (ビット位置 7)** : このビットが設定されていると、ユーザはリモート サーバに対する電源投入および再起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。
- **基本アダプタ設定 (ビット位置 8)** : このビットが設定されている場合、ユーザは、[System Settings] ページおよび [Alerts] ページの設定パラメータを変更できます。
- **イベント ログをクリアする機能 (ビット位置 9)** : このビットが設定されている場合、ユーザはイベント ログをクリアできます。イベント ログはすべてのユーザが表示できますが、ログをクリアするにはこの特定の権限が必要です。
- **高度なアダプタ設定 (ビット位置 10)** : このビットが設定されている場合、ユーザには IMM を設定するときの制約はありません。また、ユーザは、IMM への管理上のアクセスが可能です。つまり、ユーザはファームウェア アップデート、PXE ネットワーク ブート、IMM 工場出荷時のデフォルトの復元、設定ファイルからの IMM 設定の変更と復元、および IMM の再起動とリセットなどの高度な機能も実行できます。
- **予約済み (ビット位置 11)** : このビットは、将来のために予約されています。

いずれのビットも設定されていない場合、ユーザには読み取り専用許可が与えられます。

ユーザ レコードから直接取得されるログイン権限に、優先順位が割り当てられます。ログイン権限属性がユーザのレコードにない場合、ユーザが属するグループからの権限の取得が試みられます。この試みは、グループ認証フェーズの一環として行われます。ユーザには、すべてのグループに対するすべてのビットの包含的論理和が割り当てられます。読み取り専用ビットは、その他のビットがすべてゼロの場合のみ設定されます。常に拒否ビットがいずれかのグループに設定されている場合、ユーザはアクセスを拒否されます。常に拒否ビットは、その他のどのビットよりも優先されます。

重要 : ユーザに対して基本、ネットワーク、およびセキュリティ関連の IMM 設定パラメータを変更する権限を与える場合は、そのユーザに IMM を再起動する権限も与えることを検討してください (ビット位置 10)。そうしないと、ユーザはパラメータを変更できても (IMM の IP アドレスなど)、その変更を有効にすることができません。

サービス ロケーション プロトコル (SLP)

SLP の設定を表示する手順は、次のとおりです。

-
- ステップ 1** ナビゲーション ペインで [Network protocols] をクリックします。

- ステップ 2** [Service Location Protocol (SLP)] 領域までスクロールします。表示されるマルチキャスト アドレスは、IMM SLP サーバがリスンしている IP アドレスになります。

セキュリティの設定

この項の一般的な手順を使用して、IMM Web サーバと、IMM および LDAP サーバ間の接続に対するセキュリティを設定します。SSL 証明書の使用に慣れていない場合は、「[SSL 証明書の概要](#)」(P.3-34)の情報をお読みください。

次の一般的なタスク リストを使用して、IMM に対するセキュリティを設定します。

1. セキュア Web サーバを設定します。
 - a. SSL サーバをディセーブルにします。[Security] ページの [HTTPS Server Configuration for Web Server] 領域を使用します。
 - b. 証明書を生成またはインポートします。[Security] ページの [HTTPS Server Certificate Management] 領域を使用します（「[SSL サーバ証明書の管理](#)」(P.3-35)を参照）。
 - c. SSL サーバをイネーブルにします。[Security] ページの [HTTPS Server Configuration for Web Server] 領域を使用します（「[セキュア Web サーバに対する SSL のイネーブル化](#)」(P.3-39)を参照）。
2. LDAP 接続に対して SSL セキュリティを設定します。
 - a. SSL クライアントをディセーブルにします。[Security] ページの [SSL Client Configuration for LDAP Client] 領域を使用します。
 - b. 証明書を生成またはインポートします。[Security] ページの [SSL Client Certificate Management] 領域を使用します（「[SSL クライアント証明書の管理](#)」(P.3-39)を参照）。
 - c. 1 つまたは複数の信頼できる証明書をインポートします。[Security] ページの [SSL Client Trusted Certificate Management] 領域を使用します（「[SSL クライアントの信頼できる証明書の管理](#)」(P.3-39)を参照）。
 - d. SSL クライアントをイネーブルにします。[Security] ページの [SSL Client Configuration for LDAP Client] 領域を使用します（「[LDAP クライアントに対する SSL のイネーブル化](#)」(P.3-40)を参照）。
3. IMM を再起動して、SSL サーバの設定の変更を有効にします。詳細については、「[IMM の復元](#)」(P.3-44)を参照してください。



(注) SSL クライアントの設定の変更はただちに有効になり、IMM を再起動する必要はありません。

セキュア Web サーバおよびセキュア LDAP

Secure Sockets Layer (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 は、クライアント/サーバアプリケーションが、傍受、改ざん、およびメッセージの偽造を防止することを目的とした方法で通信できるようにします。

セキュアサーバ (HTTPS) とセキュア LDAP 接続 (LDAPS) の2つのタイプの接続に SSL サポートを使用するよう、IMM を設定できます。IMM は、接続タイプによって、SSL クライアントまたは SSL サーバの役割を果たします。次の表は、IMM がセキュア Web サーバ接続の場合に SSL サーバとして機能することを示しています。セキュア LDAP 接続の場合には、IMM は SSL クライアントとして機能します。

表 3-3 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
セキュア Web サーバ (HTTPS)	ユーザの Web ブラウザ (例: Microsoft Internet Explorer)	IMM Web サーバ
セキュア LDAP 接続 (LDAPS)	IMM LDAP クライアント	LDAP サーバ

SSL 設定は、[Security] ページから表示または変更できます。SSL をイネーブルまたはディセーブルにして、SSL に必要とされる証明書を管理できます。

SSL 証明書の概要

SSL は、自己署名証明書、または第三者の認証局が署名する証明書と一緒に使用できます。自己署名証明書の使用は、SSL の最も簡単な使用方法ですが、わずかなセキュリティリスクをもたらします。クライアントとサーバの間で試みられる最初の接続に対して、SSL サーバのアイデンティティを検証する手段が SSL クライアントにないために、リスクが生じます。第三者がサーバを装い、IMM と Web ブラウザ間に流れるデータを傍受するおそれがあります。ブラウザと IMM 間の初期接続時に、自己署名証明書がブラウザの証明書ストアにインポートされると、(初期接続で攻撃されなかったと仮定して) そのブラウザについてはそれ以降のすべての通信がセキュアになります。

さらにセキュリティを充実させるため、認証局によって署名された証明書を使用できます。署名付き証明書を取得するには、[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、その証明書署名要求を認証局に送信し、証明書を調達する手続きを行います。証明書を受信したら、[Import a Signed Certificate] リンクを介してその証明書を IMM にインポートし、SSL をイネーブルにすることができます。

認証局は、IMM のアイデンティティを確認する役割を果たします。証明書には、認証局と IMM に対するデジタル署名が含まれます。有名な認証局から証明書を発行されるか、認証局の証明書がすでに Web ブラウザにインポートされている場合、ブラウザはその証明書を検証し、IMM Web サーバを明確に識別します。

IMM は、セキュア Web サーバとセキュア LDAP クライアントのそれぞれの証明書を必要とします。また、セキュア LDAP クライアントは1つまたは複数の信頼できる証明書を必要とします。信頼できる証明書は、セキュア LDAP クライアントが LDAP サーバを明確に識別するために使用されます。信頼できる証明書とは、LDAP サーバの証明書に署名した認証局の証明書です。LDAP サーバが自己署名証明書を使用する場合、信頼できる証明書を LDAP サーバ自体の証明書にすることができます。複数の LDAP サーバを構成に使用する場合は、追加の信頼できる証明書をインポートする必要があります。

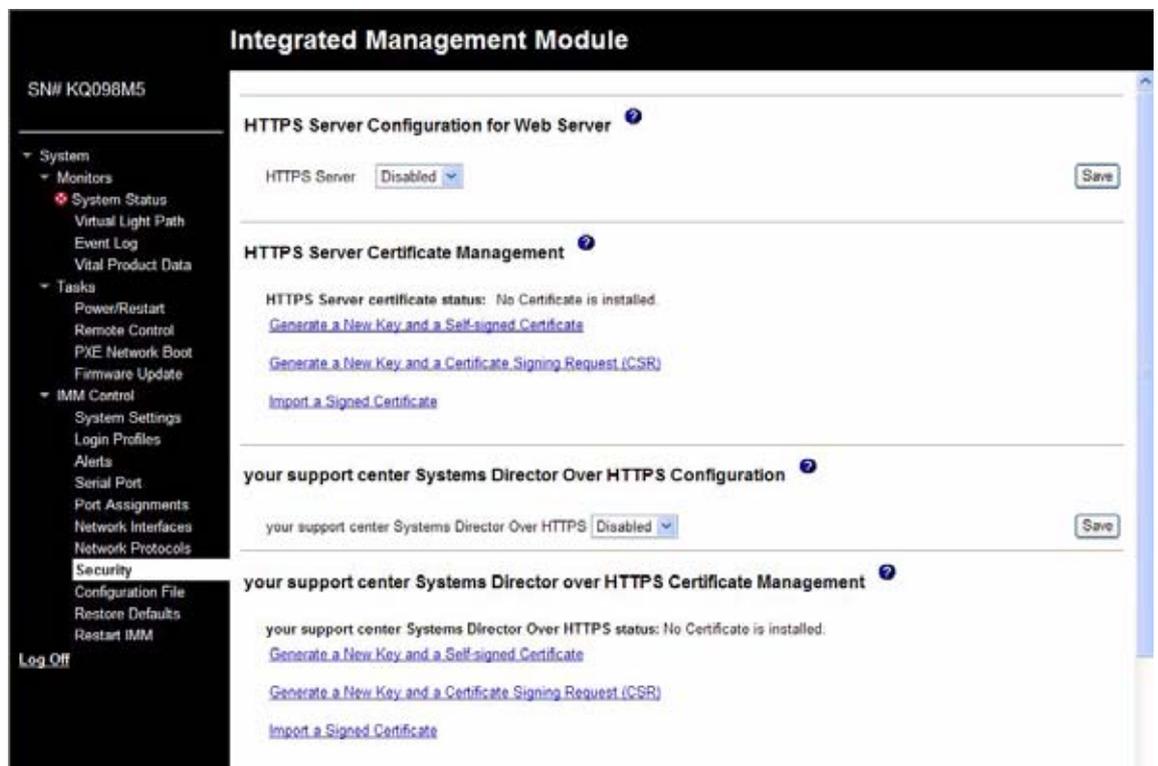
SSL サーバ証明書の管理

SSL サーバは、SSL をイネーブルにする前に、有効な証明書と対応する秘密暗号キーがインストールされていることを必要とします。秘密キーと必要な証明書を生成するには、自己署名証明書を使用する方法と、認証局が署名した証明書を使用する方法があります。SSL サーバの自己署名証明書の使用については、「自己署名証明書の生成」(P.3-35)を参照してください。SSL サーバの認証局署名証明書の使用については、「証明書署名要求の生成」(P.3-36)を参照してください。

自己署名証明書の生成

新規の秘密暗号キーと自己署名証明書を生成する手順は、次のとおりです。

ステップ 1 ナビゲーション ペインで [Security] をクリックします。次の図に示すようなページが表示されます。



ステップ 2 [SSL Server Configuration for Web Server] 領域で、設定が [Disabled] であることを確認します。ディセーブルでない場合は、[Disabled] を選択してから [Save] をクリックします。



(注) 選択した値 ([Enabled] または [Disabled]) を有効にするには、IMM を再起動する必要があります。



(注) SSL をイネーブルにするには、有効な SSL 証明書が所定の場所になければなりません。



(注) SSLを使用するには、SSL3 または TLS を使用するようにクライアントの Web ブラウザを設定する必要があります。SSL2 しかサポートしない以前のエクスポートグレードブラウザは使用できません。

ステップ 3 [SSL Server Certificate Management] 領域で、[Generate a New Key and a Self-signed Certificate] を選択します。次の図に示すようなページが表示されます。

SSL Self-signed Certificate

Certificate Data

Country (2 letter code)

State or Province

City or Locality

Organization Name

IMM Host Name

Optional Certificate Data

Contact Person

Email Address

Organizational Unit

Surname

Given Name

Initials

DN Qualifier

ステップ 4 設定に適用する必須のフィールドと任意のフィールドに情報を入力します。フィールドの説明については、「**必須の証明書データ**」(P.3-37) を参照してください。情報を入力し終わったら、[Generate Certificate] をクリックします。新規の暗号キーと証明書が生成されます。このプロセスには数分かかることがあります。自己署名証明書をインストールするかどうかの確認が表示されます。

証明書署名要求の生成

新規の秘密暗号キーと証明書署名要求を生成する手順は、次のとおりです。

- ステップ 1** ナビゲーション ペインで [Security] をクリックします。
- ステップ 2** [SSL Server Configuration for Web Server] 領域で、SSL サーバがディセーブルであることを確認します。ディセーブルでない場合は、[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。
- ステップ 3** [SSL Server Certificate Management] 領域で、[Generate a New Key and a Certificate-Signing Request] を選択します。次の図に示すようなページが表示されます。

SSL Certificate Signing Request (CSR) 

Certificate Request Data

Country (2 letter code)	<input type="text"/>
State or Province	<input type="text"/>
City or Locality	<input type="text"/>
Organization Name	<input type="text"/>
IMM Host Name	<input type="text"/>

Optional Certificate Data

Contact Person	<input type="text"/>
Email Address	<input type="text"/>
Organizational Unit	<input type="text"/>
Surname	<input type="text"/>
Given Name	<input type="text"/>
Initials	<input type="text"/>
DN Qualifier	<input type="text"/>

CSR Attributes and Extension Attributes

Challenge Password	<input type="text"/>
Unstructured Name	<input type="text"/>

ステップ 4 設定に適用する必須のフィールドと任意のフィールドに情報を入力します。フィールドは、一部の追加フィールドを除き、自己署名証明書のものと同じです。

各共通フィールドについては、次の項の情報をお読みください。

必須の証明書データ

自己署名証明書または証明書署名要求を生成するには、次のユーザ入力フィールドが必要です。

[Country] : このフィールドを使用して、IMM が物理的に配置されている国を示します。このフィールドには、2 文字の国番号を指定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 が物理的に配置されている州や地方を示します。このフィールドには、最大 30 文字を指定できます。

[City or Locality] : このフィールドを使用して、IMM が物理的に配置されている市や地域を示します。このフィールドには、最大 50 文字を指定できます。

[Organization Name] : このフィールドを使用して、IMM を所有する会社や組織を示します。証明書署名要求の生成にこのフィールドを使用すると、発行元の認証局は、証明書を要求している組織に所定の会社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確認できます。このフィールドには、最大 60 文字を指定できます。

[IMM Host Name] : このフィールドを使用して、現在、ブラウザの Web アドレス バーに表示されている IMM ホスト名を示します。

このフィールドに入力した値が、Web ブラウザで認識されているホスト名と正確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 アドレス内のホスト名と、証明書に表示される名前を照合します。ブラウザから証明書に関する警告が発せられないようにするには、このフィールドに使用する値が、IMM に接続するためにブラウザで使用されるホスト名と一致する必要があります。たとえ

ば、Web アドレス バー内のアドレスが `http://mm11.xyz.com/private/main.ssi` である場合、[IMM Host Name] フィールドに使用する値は `mm11.xyz.com` となります。Web アドレスが `http://mm11/private/main.ssi` である場合、使用する値は `mm11` となります。Web アドレスが `http://192.168.70.2/private/main.ssi` である場合、使用する値は `must be 192.168.70.2` となります。

この証明書属性は一般に、共通名と呼ばれます。

このフィールドには、最大 60 文字を指定できます。

[Contact Person] : このフィールドを使用して、IMM の担当者である連絡先の名前を示します。このフィールドには、最大 60 文字を指定できます。

[Email Address] : このフィールドを使用して、IMM の担当者である連絡先の電子メール アドレスを示します。このフィールドには、最大 60 文字を指定できます。

任意の証明書データ

自己署名証明書または証明書署名要求を生成する場合に、次のユーザ入力フィールドは任意となります。

[Organization Unit] : このフィールドを使用して、IMM を所有する会社や組織内の単位を示します。このフィールドには、最大 60 文字を指定できます。

[Surname] : このフィールドは、IMM の担当者の名字などの追加情報に使用します。このフィールドには、最大 60 文字を指定できます。

[Given Name] : このフィールドは、IMM の担当者の名前などの追加情報に使用します。このフィールドには、最大 60 文字を指定できます。

[Initials] : このフィールドは、IMM の担当者のイニシャルなどの追加情報に使用します。このフィールドには、最大 20 文字を指定できます。

[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に使用します。このフィールドには、最大 60 文字を指定できます。

証明書署名要求属性

選択した認証局から要求されない限り、次のフィールドは任意になります。

[Challenge Password] : このフィールドを使用して、証明書署名要求にパスワードを割り当てます。このフィールドには、最大 30 文字を指定できます。

[Unstructured Name] : このフィールドは、IMM に割り当てられている非構造化名などの追加情報に使用します。このフィールドには、最大 60 文字を指定できます。

ステップ 5 情報を入力し終えたら、[Generate CSR] をクリックします。新規の暗号キーと証明書が生成されます。このプロセスには数分かかることがあります。

ステップ 6 [Download CSR] をクリックし、[Save] をクリックしてファイルをワークステーションに保存します。証明書署名要求の作成時に生成されるファイルは、DER 形式になります。認証局が PEM など、その他の形式のデータを予期している場合は、OpenSSL (<http://www.openssl.org>) などのツールを使用してファイルを変換できます。認証局が、証明書署名要求ファイルのコンテンツを Web ブラウザ ウィンドウにコピーすることを求める場合は、通常、PEM 形式が予期されます。

OpenSSL を使用して DER から PEM 形式に証明書署名要求を変換するコマンドは、次の例のようになります。

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

ステップ 7 証明書署名要求を認証局に送信します。認証局から署名付きの証明書が返されたら、必要に応じて証明書を DER 形式に変換します（証明書を電子メールまたは Web ページでテキストとして受信した場合は、おそらく PEM 形式になっています）。形式は、認証局から提供され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て変更できます。PEM から DER 形式に証明書を変換するコマンドは、次の例のようになります。

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

認証局から署名付き証明書が返されたら、[ステップ 8](#)に進みます。

- ステップ 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] 領域までスクロールします。
- ステップ 9** [Import a Signed Certificate] をクリックします。
- ステップ 10** [Browse] をクリックします。
- ステップ 11** 必要な証明書ファイルをクリックし、[Open] をクリックします。ファイル名（フルパスを含む）は、[Browse] ボタンの横のフィールドに表示されます。
- ステップ 12** [Import Server Certificate] をクリックしてプロセスを開始します。ファイルが IMM 上のストレージに転送されるときに、進捗状況インジケータが表示されます。転送が完了するまで、このページを表示しておきます。

セキュア Web サーバに対する SSL のイネーブル化



(注) SSL をイネーブルにするには、有効な SSM 証明書をインストールする必要があります。

セキュア Web サーバをイネーブルにする手順は、次のとおりです。

- ステップ 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、有効な SSL サーバ証明書がインストールされていることが示されます。SSL サーバ証明書のステータスに、有効な SSL 証明書がインストールされていることが示されない場合は、「[SSL サーバ証明書の管理](#)」(P.3-35) を参照してください。
- ステップ 2** [SSL Server Configuration for Web Server] 領域までスクロールして、[SSL Client] フィールドで [Enabled] を選択してから、[Save] をクリックします。選択した値は、次に IMM を再起動するときに有効になります。

SSL クライアント証明書の管理

SSL クライアントは、SSL をイネーブルにする前に、有効な証明書と対応する秘密暗号キーがインストールされていることを必要とします。秘密キーと必要な証明書を生成するには、自己署名証明書を使用する方法、または認証局が署名した証明書を使用する方法があります。

SSL クライアントに対する秘密暗号キーと証明書を生成する手順は、[SSL Server Certificate Management] 領域の代わりに [Security Web] ページの [SSL Client Certificate Management] 領域を使用する点を除き、SSL サーバに関する手順と同じです。SSL クライアントの自己署名証明書の使用については、「[自己署名証明書の生成](#)」(P.3-35) を参照してください。SSL クライアントの認証局署名証明書の使用については、「[証明書署名要求の生成](#)」(P.3-36) を参照してください。

SSL クライアントの信頼できる証明書の管理

セキュア SSL クライアント (LDAP クライアント) は信頼できる証明書を使用して、LDAP サーバを明確に識別します。信頼できる証明書は、LDAP サーバの証明書に署名した認証局の証明書か、LDAP サーバの実際の証明書になります。SSL クライアントをイネーブルには、少なくとも 1 つの証明書を IMM にインポートする必要があります。信頼できる証明書は 3 つまでインポートできます。

信頼できる証明書をインポートする手順は、次のとおりです。

-
- ステップ 1** ナビゲーション ペインで [Security] を選択します。
- ステップ 2** [SSL Client Configuration for LDAP Client] 領域で、SSL クライアントがディセーブルであることを確認します。ディセーブルでない場合は、[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。
- ステップ 3** [SSL Client Trusted Certificate Management] 領域までスクロールします。
- ステップ 4** [Trusted CA Certificate 1] フィールドのいずれかの横にある [Import] をクリックします。
- ステップ 5** [Browse] をクリックします。
- ステップ 6** 必要な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（フルパスを含む）は、[Browse] ボタンの横のボックスに表示されます。
- ステップ 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きに、進捗状況インジケータが表示されます。転送が完了するまで、このページを表示しておきます。
- この時点で、[Trusted CA Certificate 1] オプションの [Remove] ボタンが使用可能になります。信頼できる証明書を削除する場合は、対応する [Remove] ボタンをクリックします。
- [Trusted CA Certificate 2] と [Trusted CA Certificate 3] の [Import] ボタンを使用して、その他の信頼できる証明書をインポートできます。

LDAP クライアントに対する SSL のイネーブル化

[Security] ページの [SSL Client Configuration for LDAP Client] 領域を使用し、LDAP クライアントに対して SSL をイネーブルまたはディセーブルにします。SSL をイネーブルにするには、まず、有効な SSL クライアント証明書と、1 つ以上の信頼できる証明書をインストールする必要があります。

クライアントに対して SSL をイネーブルにする手順は、次のとおりです。

-
- ステップ 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、インストールされた SSL クライアント証明書と [Trusted CA Certificate 1] が表示されます。
- ステップ 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)** 選択された値 ([Enabled] または [Disabled]) はただちに有効になります。
-  **(注)** SSL をイネーブルにするには、有効な SSL 証明書が所定の場所になければなりません。
-  **(注)** LDAP サーバは、LDAP クライアントが使用する SSL 実装との互換性を保つため、SSL3 または TLS をサポートする必要があります。
-
- ステップ 3** [Save] をクリックします。選択した値は、ただちに有効になります。

セキュア シェル サーバの設定

セキュア シェル (SSH) 機能は、IMM のコマンドライン インターフェイスおよびシリアル (テキスト コンソール) リダイレクト機能へのセキュア アクセスを提供します。

セキュア シェル ユーザは、ユーザ ID およびパスワードを交換することによって認証されます。パスワードとユーザ ID は、暗号化チャネルが確立された後で送信されます。ユーザ ID とパスワードのペアは、12 個のローカルに保存されたユーザ ID とパスワードのいずれかか、LDAP サーバに保存されたものになります。公開キー認証はサポートされていません。

セキュア シェル サーバ キーの生成

セキュア シェル サーバ キーは、クライアントに対してセキュア シェル サーバのアイデンティティを認証するために使用します。新規のセキュア シェル サーバ秘密キーを作成するには、セキュア シェル をディセーブルにする必要があります。セキュア シェル サーバをイネーブルにするには、サーバ キーを作成する必要があります。

新規のサーバ キーを要求すると、SSH バージョン 2 クライアントから IMM へのアクセスを可能にするために Rivest、Shamir、Adelman キー、および DSA キーの両方が作成されます。セキュリティ上の理由から、設定の保存および復元操作でセキュア シェル サーバ秘密キーがバックアップされることはありません。

新規のセキュア シェル サーバ キーを作成する手順は、次のとおりです。

-
- ステップ 1** ナビゲーション ペインで [Security] をクリックします。
 - ステップ 2** [Secure Shell (SSH) Server] 領域までスクロールして、セキュア シェル サーバがディセーブルかどうかを確認します。ディセーブルでない場合は、[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。
 - ステップ 3** [SSH Server Key Management] 領域までスクロールします。
 - ステップ 4** [Generate SSH Server Private Key] をクリックします。進捗状況ウィンドウが開きます。操作が完了するまで待ちます。
-

セキュア シェル サーバのイネーブル化

[Security] ページから、セキュア シェル サーバをイネーブルまたはディセーブルにすることができます。行った選択は、IMM の再起動後にのみ有効になります。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 が再起動するときに使用される値です。



(注) 有効なセキュア シェル サーバ秘密キーがインストールされている場合のみ、セキュア シェル サーバをイネーブルにすることができます。

セキュア シェル サーバをイネーブルにする手順は、次のとおりです。

-
- ステップ 1** ナビゲーション ペインで [Security] をクリックします。
 - ステップ 2** [Secure Shell (SSH) Server] 領域までスクロールします。
 - ステップ 3** [SSH Server] フィールドで [Enabled] をクリックします。

ステップ 4 ナビゲーション ペインで [Restart IMM] をクリックして IMM を再起動します。

セキュア シェル サーバの使用

Red Hat Linux バージョン 7.3 に含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に、ネットワーク アドレス 192.168.70.132 を使用して IMM へのセキュア 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 System フォワーディングがないことを示し、-l はセッションでユーザ ID *userid* を使用する必要があることを示しています。

設定ファイルの使用

ナビゲーション ペインで [Configuration File] を選択して、IMM の設定をバックアップおよび復元します。

重要 : [Security] ページの設定は、バックアップ操作では保存されず、復元操作で復元できません。

現在の設定のバックアップ

IMM Web インターフェイスを実行しているクライアント コンピュータに、現在の IMM の設定のコピーをダウンロードできます。誤って変更されたり、損傷したりした場合は、このバックアップ コピーを使用して IMM の設定を復元します。このバックアップ コピーをベースとして使用し、複数の IMM を同様の設定にすることができます。

この手順で保存される設定情報には、System x サーバ ファームウェアの設定や、IPMI 以外のユーザ インターフェイスとの共通性がない IPMI 設定は含まれません。

現在の設定をバックアップする手順は、次のとおりです。

-
- ステップ 1** 現在の設定をバックアップする IMM にログインします。詳細については、[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。
 - ステップ 2** ナビゲーション ペインで [Configuration File] をクリックします。
 - ステップ 3** [Backup IMM Configuration] 領域で、[View the current configuration summary] をクリックします。
 - ステップ 4** 設定を確認してから、[Close] をクリックします。
 - ステップ 5** この設定をバックアップするには、[Backup] をクリックします。
 - ステップ 6** バックアップの名前を入力し、ファイルを保存する場所を選択して、[Save] をクリックします。
Mozilla Firefox では、[Save File] をクリックしてから [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 の設定の復元と変更

保存された設定をすべて復元することも、保存された設定内の主要フィールドを変更してから IMM に設定を復元することもできます。設定ファイルを変更してから復元することによって、複数の IMM を同様の設定にすることができます。名前や IP アドレスなどの一意の値を必要とするパラメータは、共通する共有情報を入力することなく、迅速に指定できます。

現在の設定を復元または変更する手順は、次のとおりです。

- ステップ 1** 設定を復元する IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで [Configuration File] をクリックします。
- ステップ 3** [Restore IMM Configuration] 領域で、[Browse] をクリックします。
- ステップ 4** 必要な設定ファイルをクリックし、[Open] をクリックします。ファイル（フルパスを含む）が、[Browse] の横にあるボックスに表示されます。
- ステップ 5** 設定ファイルを変更する必要がない場合は、[Restore] をクリックします。IMM 設定情報を示す新規ウィンドウが開きます。この情報が、復元する設定であることを確認します。設定が適切でない場合は、[Cancel] をクリックします。

設定ファイルに変更を加えてから設定を復元する場合は、[Modify and Restore] をクリックして編集可能な設定要約ウィンドウを開きます。最初に、変更可能なフィールドだけが表示されます。この表示と完全な設定要約の表示を切り替えるには、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] をクリックしたときに、復元しようとしている設定ファイルが、タイプの異なるサービス プロセッサで作成されたものであるか、同じタイプでも搭載されているファームウェアが古い（そのため、機能が低い）サービス プロセッサで作成されたものであると、アラート ウィンドウが開く場合があります。このアラートメッセージには、復元の完了後に設定する必要があるシステム管理機能のリストが含まれます。機能によっては、複数のウィンドウでの設定が必要です。

- ステップ 6** このファイルを引き続き IMM に復元するには、[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きに、進捗状況インジケータが表示されます。更新が成功し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] ページでのセキュリティ設定は、復元操作では復元されません。セキュリティ設定を変更するには、「セキュア Web サーバおよびセキュア LDAP」(P.3-33) を参照してください。

- ステップ 7** 復元プロセスが完了したことを示す確認を受信したら、ナビゲーション ペインの [Restart IMM] をクリックし、[Restart] をクリックします。
- ステップ 8** [OK] をクリックして、IMM を再起動することを確認します。
- ステップ 9** [OK] をクリックして、現在のブラウザ ウィンドウを閉じます。
- ステップ 10** 再び IMM にログインするには、ブラウザを起動し、通常ログインプロセスを行います。

デフォルトの復元

スーパーバイザ アクセス権がある場合は、[Restore Defaults] リンクを使用して、IMM のデフォルト設定を復元します。

注意：[Restore Defaults] をクリックすると、IMM に対して行ったすべての変更が失われます。

IMM のデフォルトを復元する手順は、次のとおりです。

-
- ステップ 1** IMM にログインします。詳細については、[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。
 - ステップ 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復元します。これがローカル サーバの場合、TCP/IP 接続は失われ、接続を復元するためにネットワーク インターフェイスを再設定しなければなりません。
 - ステップ 3** IMM Web インターフェイスを使用するには、再びログインします。
 - ステップ 4** 接続が復元されるように、ネットワーク インターフェイスを再設定します。ネットワーク インターフェイスの詳細については、「[ネットワーク インターフェイスの設定](#)」(P.3-20) を参照してください。
-

IMM の復元

[Restart IMM] リンクを使用して、IMM を再起動します。この機能は、スーパーバイザ アクセス権がある場合のみ実行できます。イーサネット接続は一時的にドロップされます。IMM Web インターフェイスを使用するには、再びログインする必要があります。IMM を再起動する手順は、次のとおりです。

-
- ステップ 1** IMM にログインします。詳細については、[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。
 - ステップ 2** ナビゲーション ペインで [Restart IMM] をクリックして IMM を再起動します。TCP/IP またはモデム接続が失われます。
 - ステップ 3** IMM Web インターフェイスを使用するには、再びログインします。
-

ログオフ

IMM または別のリモート サーバ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。



CHAPTER 4

サーバステータスのモニタ

アクセスしているサーバのステータスを表示するには、ナビゲーションペインの [Monitors] 見出しの下にあるリンクを使用します。

[System Status] ページから、次の操作ができます。

- サーバの電源ステータスをモニタし、オペレーティングシステムの状態を表示します
- サーバの温度測定値、電圧のしきい値、およびファン速度を表示します
- 最新のサーバオペレーティングシステム障害の画面キャプチャを表示します
- IMM にログインするユーザの一覧を表示します

[Virtual Light Path] ページから、サーバで点灯されるすべての LED の名前、色、ステータスを表示できます。

[Event Log] ページから、次の操作ができます。

- IMM のイベントログに記録される特定のイベントを表示します
- イベントの重大度を表示します

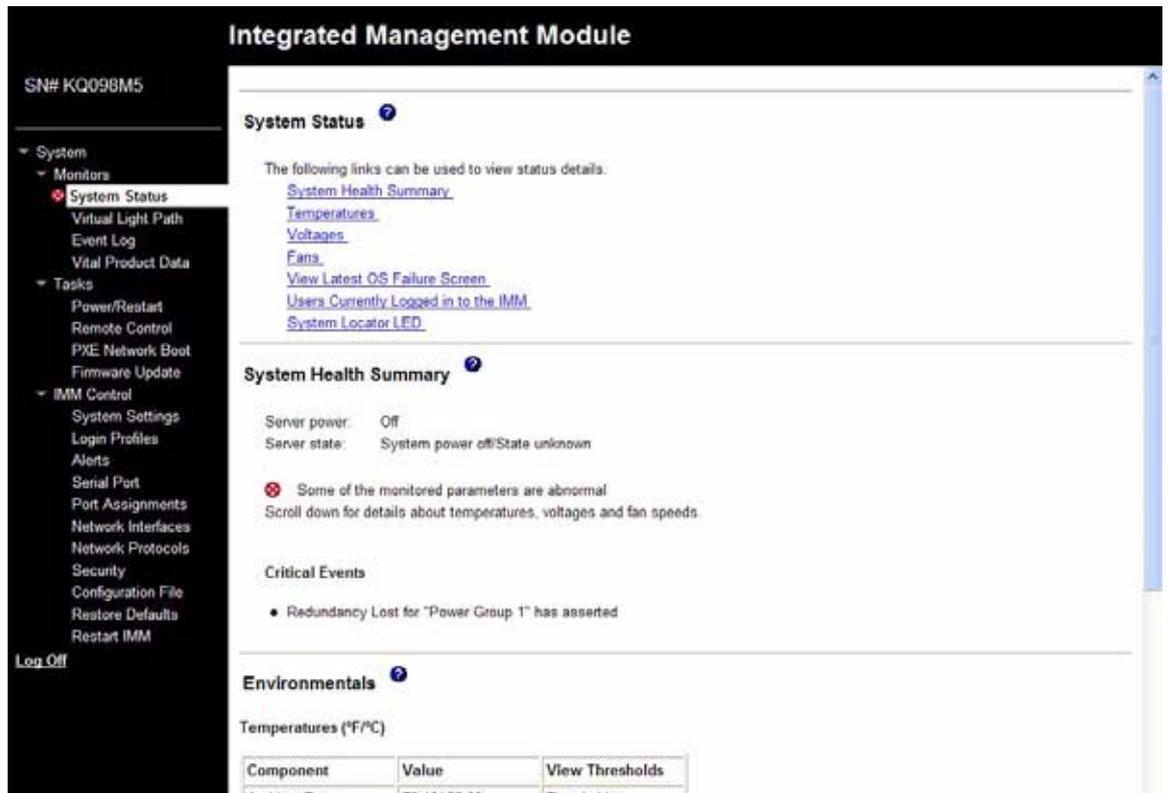
[Vital Product Data (VPD)] ページから、重要な製品データを表示できます。

システムステータスの表示

[System Status] ページで、サーバの温度測定値、電圧のしきい値、ファンステータスをモニタできます。最新のオペレーティングシステム障害画面、IMM にログインするユーザ、およびシステムロケータ LED を表示することもできます。

サーバのシステムヘルスおよび環境情報を表示するには、次の手順を実行します。

- ステップ 1** IMM にログインします。詳細については、[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。
- ステップ 2** ナビゲーションペインで、[System Status] をクリックして、ダイナミックに生成された全体的なサーバの状態のアップデートを表示します。次の図に示すようなページが表示されます。



サーバのステータスによって、[System Health Summary] ページの上部に表示されるメッセージが決定されます。次の記号のいずれかが表示されます。

- グリーンで点灯している円およびフレーズ「Server is operating normally.」
- X を含む赤い円または感嘆符を含む黄色い三角形、およびフレーズ「One or more monitored parameters are abnormal.」

モニタされるパラメータが正常範囲外で動作している場合、[System Health Summary] ページに特定の異常なパラメータの一覧が表示されます。

ステップ 3

ページの [Environmentals] セクション内の、温度、電圧、およびファン速度情報を含む [Temperature] 領域まで下方方向にスクロールします。

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 ドライブ バックプレーンなどのシステム コンポーネントの現在の温度測定値および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 (°F / °C)

Sensors	Noncritical	Critical	Fatal
Upper Threshold	100.40 / 38.00	105.80 / 41.00	113.00 / 45.00
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。温度のしきい値は、リモート サーバでプリセットされていて変更できません。

報告された温度は、次のしきい値範囲に対して測定されています。

[Non-Critical] : 温度が指定値に達すると、設定済みのリモート 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] 領域にある [Warning Alerts] チェックボックスか、または [Remote Alert Recipient] ページにある [Warning Alerts] チェックボックスをオンにする必要があります。

アラート オプションの選択の詳細については、「SNMP アラートの設定」(P.3-18) または「リモートアラート受信者の設定」(P.3-15) を参照してください。

[Critical] : 温度が警告値よりも高い指定値 (ソフト シャットダウンしきい値) に達すると、設定済みのリモート アラート受信者へ 2 番目の温度アラートが送信され、サーバはオペレーティングシステムのシャットダウンの順序でシャットダウン プロセスを開始します。その後サーバは自動的にオフになります。アラートを送信するには、[Alerts] ページの [SNMP Alerts Settings] 領域にある [Critical Alerts] チェックボックスか、または [Remote Alert Recipient] ページにある [Critical Alerts] チェックボックスをオンにする必要があります。

アラート オプションの選択の詳細については、「SNMP アラートの設定」(P.3-18) または「リモートアラート受信者の設定」(P.3-15) 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も高い指定値 (ハード シャットダウンしきい値) に達すると、サーバはただちにシャットダウンして、設定済みのリモート アラート受信者へ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] 領域にある [Critical Alerts] チェックボックスか、または [Remote Alert Recipient] ページにある [Critical Alerts] チェックボックスをオンにする必要があります。

アラート オプションの選択の詳細については、「SNMP アラートの設定」(P.3-18) または「リモートアラート受信者の設定」(P.3-15) を参照してください。

ステップ 4

[Voltage] 領域まで下方向にスクロールします。モニタされた電源電圧が指定した動作範囲を外れると、IMM は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	Noncritical	Critical	Fatal
Upper Threshold	N/A	3.56	N/A
Lower Threshold	N/A	3.04	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。電圧のしきい値は、リモート サーバでプリセットされていて変更できません。

IMM Web インターフェイスに、システム ボードおよび電圧レギュレータ モジュール (VRM) の電圧測定値が表示されます。システムでは、次のアクションが実行される電圧範囲を設定します。

[Non-Critical] : 電圧が指定した電圧範囲より低いまたは高い場合、設定済みのリモート 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] 領域にある [Warning Alerts] チェックボックスをオンにする必要があります。

アラート オプションの選択の詳細については、「[SNMP アラートの設定](#)」(P.3-18) を参照してください。

[Critical] : 電圧が指定した電圧範囲より低いまたは高い場合、設定済みのリモート アラート受信者へ電圧アラートが送信され、サーバはオペレーティングシステムのシャットダウンの順序でシャットダウンプロセスを開始します。その後サーバは自動的にオフになります。アラートを送信するには、[Alerts] ページの [SNMP Alerts Settings] 領域にある [Critical Alerts] チェックボックスをオンにする必要があります。

アラート オプションの選択の詳細については、「[SNMP アラートの設定](#)」(P.3-18) を参照してください。

[Fatal] : 電圧が指定した電圧範囲より低いまたは高い場合、サーバはただちにシャットダウンし、設定済みのリモート アラート受信者へ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] 領域にある [Fatal Alerts] チェックボックスをオンにする必要があります。



(注)

ハードシャットダウンアラートは、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にのみ送信されます。

アラート オプションの選択の詳細については、「[SNMP アラートの設定](#)」(P.3-18) を参照してください。

しきい値に達した場合、IMM は重要でないイベント、重要なイベント、または重大なイベントを生成して、必要に応じていずれかのシャットダウンアクションを生成します。

[Non-critical] : IMM がこのしきい値に達したことを示す場合、警告イベントが生成されます。

[Critical] : IMM がこのしきい値に達したことを示す場合、重要なイベントが生成されます。

[Fatal] : IMM がこのしきい値に達したことを示す場合、重大なイベントが生成されます。

ステップ 5

[Fan Speeds (% of max)] 領域まで、下方向にスクロールします。IMM Web インターフェイスに、サーバのファンの動作中の速度が表示されます (最大ファン速度のパーセンテージで表されます)。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	Noncritical	Critical	Fatal
Upper Threshold	N/A	N/A	N/A
Lower Threshold	N/A	530.00	N/A

ファン速度が許容できないレベルまで低下するか、ファンが停止した場合に、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] 領域にある [Critical Alerts] チェックボックスをオンにする必要があります。

アラート オプションの選択の詳細については、「[SNMP アラートの設定](#)」(P.3-18) を参照してください。



(注)

[View Latest OS Failure Screen] 機能はサポートされません。

ステップ 6

[Users Currently Logged in] 領域まで、下方向にスクロールします。IMM Web インターフェイスに、IMM にログインする各ユーザのログイン ID およびアクセス方式が表示されます。

- ステップ 7** [System Locator LED] 領域まで、下方向にスクロールします。IMM Web インターフェイスに、システムロケータ LED のステータスが表示されます。LED の状態を変更するボタンも提供されています。この領域に表示される図の意味については、オンラインヘルプを参照してください。

仮想ライトパスの表示

[Virtual Light Path] 画面に、サーバで点灯されるすべての LED の名前、色、ステータスが表示されます。

[Virtual Light Path] にアクセスして表示するには、次の手順を実行します。

- ステップ 1** IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで、[Virtual Light Path] をクリックして、そのサーバの最新のイベントの履歴を表示します。次の図に示すようなページが表示されます。

The screenshot shows the IMM web interface for a server with SN# KQ098M5. The left sidebar contains a navigation menu with categories like System, Monitors, Tasks, and IMM Control. The main content area is titled 'Virtual Light Path' and displays a table with the following data:

Name	Color	Status
Fault	Orange	On
Info	Not Applicable	Off
CPU	Not Applicable	Off
IPS	Orange	On
DASD	Not Applicable	Off
FAN	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
FAN 1	Not Applicable	Off
FAN 2	Not Applicable	Off
FAN 3	Not Applicable	Off
FAN 4	Not Applicable	Off
FAN 5	Not Applicable	Off
FAN 6	Not Applicable	Off

- ステップ 3** 下方向にスクロールして [Virtual Light Path] の内容すべてを表示します。



(注) LED がサーバで点灯していない場合は、[Virtual Light Path] テーブルの [Color] 列は、LED の色が [Not Applicable] であることを示します。

Web インターフェイスからのシステム イベント ログの表示



(注)

システム イベント ログは容量が制限されています。その制限に達すると、ファーストイン ファーストアウトの順で古いイベントが削除されます。

イベント ログにアクセスして表示するには、次の手順を実行します。

- ステップ 1** IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーションペインで、[Event Log] をクリックして、そのサーバの最新のイベントの履歴を表示します。次の図に示すようなページが表示されます。

Index	Sev	Date/Time	Text
1	I	04/05/2011, 06:15:48	Remote Login Successful. Login ID: USERID from Web at IP address 10.99.66.108
2	I	04/05/2011, 05:58:21	Remote Login Successful. Login ID: USERID from Web at IP address 10.99.66.108
3	I	04/05/2011, 05:45:02	Remote Login Successful. Login ID: USERID from Web at IP address 10.99.66.108
4	E	04/05/2011, 05:44:44	Remote access attempt failed. Invalid userid or password received. Userid is from WEB browser at IP add
5	E	04/05/2011, 05:44:21	Remote access attempt failed. Invalid userid or password received. Userid is from WEB browser at IP add
6	E	04/05/2011, 05:43:27	Remote access attempt failed. Invalid userid or password received. Userid is from WEB browser at IP add
7	E	04/05/2011, 05:43:07	Remote access attempt failed. Invalid userid or password received. Userid is from WEB browser at IP add
8	I	04/02/2011, 21:16:43	Remote Login Successful. Login ID: USERID from Web at IP address 10.21.125.156
9	E	04/01/2011, 22:33:19	Redundancy Lost for "Power Group 1" has asserted

- ステップ 3** 下方向にスクロールして、イベント ログの内容すべてを表示します。イベントでは、次の重大度のレベルが指定されています。

[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、サーバパフォーマンスに影響を及ぼす可能性のあるイベントに割り当てられます。

[Error] : この重大度レベルは、即時の注意が必要なイベントに割り当てられます。

IMM Web インターフェイスでは、重大度列で黄色の背景に文字 W のある警告イベントと赤い背景に文字 E のあるエラーイベントは区別されます。

- ステップ 4** [Save Log as Text File] をクリックして、イベント ログの内容をテキスト ファイルとして保存します。[Reload Log] をクリックして、イベント ログの表示をリフレッシュします。[Clear Log] をクリックして、イベント ログの内容を削除します。

重要な製品データの表示

サーバが開始すると、IMM はサーバ情報、サーバファームウェア情報、およびサーバ コンポーネントの重要な製品データ (VPD) を収集して、それを不揮発性メモリに保存します。ほとんどすべてのコンピュータから、いつでもこの情報にアクセスできます。[Vital Product Data] ページには、IMM がモニタしているリモートの管理対象サーバに関するキー情報が含まれます。

サーバ コンポーネントの重要な製品データを表示するには、次の手順を実行します。

- ステップ 1** IMM にログインします。詳細については、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。
- ステップ 2** ナビゲーション ペインで、[Vital Product Data] をクリックして、サーバ上のハードウェアおよびソフトウェア コンポーネントのステータスを表示します。
- ステップ 3** 下方向にスクロールして、次の VPD 測定値を表示します。

マシン レベル VPD

サーバの重要な製品データがこの領域に表示されます。VPD の表示で、マシンレベル VPD には汎用固有識別子 (UUID) が含まれます。



(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 ログはサーバがオンになっている場合のみ情報を提供します。

表 4-1 マシンレベルの重要な製品データ

フィールド	機能
Machine type and model	IMM がモニタしているサーバ タイプとモデル番号を識別します。
Serial number	IMM がモニタしているサーバのシリアル番号を識別します。
UUID	IMM がモニタしているサーバの汎用固有識別子 (UUID) を識別します (32 桁の 16 進数)。

コンポーネント レベル VPD

リモートの管理対象サーバのコンポーネントの重要な製品データがこの領域に表示されます。

表 4-2 コンポーネントレベルの重要な製品データ

フィールド	機能
FRU name	各コンポーネントの現場交換可能ユニット (FRU) を識別します。
Serial number	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業者 ID を識別します。

コンポーネント アクティビティ ログ

コンポーネント アクティビティの記録をこの領域で表示できます。

表 4-3 コンポーネント アクティビティ ログ

フィールド	機能
FRU name	コンポーネントの現場交換可能ユニット (FRU) 名を識別します。
Serial number	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業者を識別します。
Action	各コンポーネントに対して実行されるアクションを識別します。
Timestamp	コンポーネント アクションの日時を識別します。日付は、 <i>mm/dd/yy</i> 形式で表示されます。時刻は、 <i>hh:mm:ss</i> 形式で表示されます。

IMM VPD

リモートの管理対象サーバの IMM ファームウェア、System x サーバファームウェア、および Dynamic System Analysis ファームウェアの VPD をこの領域で表示できます。

表 4-4 コンポーネントレベルの重要な製品データ

フィールド	機能
Firmware type	ファームウェア コードのタイプを識別します。
Version string	ファームウェア コードのバージョンを識別します。
Release date	ファームウェアがリリースされた日付を識別します。



CHAPTER 5

IMM タスクの実行

IMM とサーバ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によって異なります。

次のタスクを実行できます。

- サーバの電源および再起動アクティビティを表示する
- リモートからサーバの電源ステータスを制御する
- リモートからサーバ コンソールにアクセスする
- リモートからディスクまたはディスク イメージをサーバに接続する
- IMM ファームウェアを更新する

サーバの電源および再起動アクティビティの表示

[Server Power/Restart Activity] 領域には、Web ページが生成された時点のサーバの電源ステータスが表示されます。

The screenshot displays the Integrated Management Module (IMM) web interface for a server with SN# KQ098M5. The left sidebar contains a navigation menu with categories like System, Monitors, System Status, Tasks, and IMM Control. The main content area is divided into two sections: 'Server Power / Restart Activity' and 'Server Power / Restart Control'. The activity section shows the current power state (Off), system state (System power off/State unknown), restart count (73), and power-on hours (2020). The control section lists various actions such as 'Power On Server Immediately', 'Power On Server at Specified Time', 'Power Off Server Immediately', 'Shut down OS and then Power Off Server', 'Shut down OS and then Restart Server', 'Restart the Server Immediately', and 'Schedule Daily/Weekly Power and Restart Actions'.

[Power] : このフィールドには、現在の Web ページが生成された時点のサーバの電源ステータスが表示されます。

[State] : このフィールドには、現在の Web ページが生成された時点のサーバの状態が表示されます。次の状態が示されます。

- System power off/State unknown
- System on/starting UEFI
- [System stopped in UEFI] (エラーが検出されました)
- System running in UEFI
- [Booting OS or in unsupported OS] (オペレーティング システムが IMM へのインバンド インターフェイスをサポートするように設定されていない場合、そのオペレーティング システムに示される可能性があります)
- OS booted

[Restart count] : このフィールドには、サーバが再起動した回数が表示されます。



(注)

カウンタは、IMM サブシステムが工場出荷時のデフォルトにクリアされるたびに、ゼロにリセットされます。

[Power-on hours] : このフィールドには、サーバの電源がオンにされていた合計時間数が表示されます。

サーバの電源ステータスの制御

IMM は、サーバに対し、電源オン、電源オフ、および再起動アクションによる完全な電源制御を提供します。さらに、電源オンおよび再起動の統計情報がキャプチャされて表示され、サーバハードウェアの可用性を示します。[Server Power/Restart Control] 領域にあるアクションを実行するには、IMM へのスーパーバイザ アクセス権を持っている必要があります。

サーバの電源および再起動アクションを実行するには、次の手順を実行します。



(注)

以下のオプションを選択するのは、緊急の場合、または現場を離れていてサーバが反応しない場合だけにしてください。

- ステップ 1** IMM にログインします。詳細については、[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。
- ステップ 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] 領域まで下方向にスクロールします。
- ステップ 3** 次のオプションのいずれかをクリックします。
- [Power on server immediately] : サーバの電源をオンにし、オペレーティング システムを起動します。
- [Power on server at specified time] : 指定した時刻にサーバの電源をオンにし、オペレーティング システムを起動します。
- [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てから、サーバの電源をオフにします。



(注)

[Shut down OS and then power off server] 要求の試行時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 モードだった場合、IMM はグレースフル シャットダウンを開始できない可能性があります。OS がまだ稼働中であっても、電源オフ遅延インターバルの経過後、IMM はハードリセットまたはシャットダウンを実行します。

[Shut down OS and then restart server] : オペレーティング システムを再起動します。



(注)

[Shut down OS and then restart server] 要求の試行時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 モードだった場合、IMM はグレースフル シャットダウンを開始できない可能性があります。OS がまだ稼働中であっても、電源オフ遅延インターバルの経過後、IMM はハードリセットまたはシャットダウンを実行します。

[Restart the server immediately] : 最初にオペレーティング 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の電源をオフにし（サーバを再起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、誤って選択した場合は操作をキャンセルできます。

IMM を管理するその他の方法

次のユーザ インターフェイスを使用して、IMM を管理および設定できます。

- IMM Web インターフェイス
- SNMPv1
- SNMPv3
- Telnet CLI
- SSH CLI



CHAPTER 6

コマンドライン インターフェイス

Web インターフェイスを使用せずに IMM にアクセスするには、IMM コマンドライン インターフェイス (CLI) を使用します。Web インターフェイスで提供される管理機能の一部を使用できます。

CLI には、Telnet または SSH セッションを使用してアクセスできます。CLI コマンドを実行するには、事前に IMM によって認証されている必要があります。

IPMI を使用した IMM の管理

出荷時の IMM には、ユーザ ID 2 に対して USERID というユーザ名と PASSWORD (文字 O ではなくゼロを使用) というパスワードが初期設定されています。このユーザには、スーパーバイザ アクセス権が与えられています。

重要：セキュリティを強化するために、初期設定時にこのデフォルトのパスワードを変更してください。

IMM は、次の IPMI リモート サーバ管理機能も提供します。

コマンドライン インターフェイス

コマンドライン インターフェイスでは、IPMI 2.0 プロトコルを使用してサーバ管理機能に直接アクセスできます。IPMITool を使用してコマンドを実行することにより、サーバの電源を制御したり、サーバ情報を表示したり、サーバを識別したりすることができます。

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。

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、次の手順を実行します。

-
- ステップ 1** IMM との接続を確立します。
 - ステップ 2** ユーザ名のプロンプトで、ユーザ ID を入力します。
 - ステップ 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。

コマンドラインにログインしました。コマンドラインプロンプトは、`system>` になります。コマンドラインセッションは、コマンドラインで `exit` を入力するまで持続します。入力すると、ログオフし、セッションが終了します。

コマンド構文

コマンドを使用する前に、次のガイドラインを確認してください。

- 各コマンドの形式は次のとおりです。

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

- コマンド構文では大文字と小文字が区別されます。
- コマンド名はすべて小文字です。
- すべての引数をコマンドのすぐ後に指定する必要があります。オプションは、引数のすぐ後に指定します。
- 各オプションの先頭には常にハイフン (-) が付きます。オプションには、短いオプション (1 文字) または長いオプション (複数文字) を使用できます。
- オプションに引数がある場合、その引数は必須になります。たとえば、次のようになります。

```
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、**eth0** は引数です。-i、-g、および -s はオプションです。この例では、3 つすべてのオプションに引数があります。

- 角カッコは、その中の引数またはオプションが省略可能であることを示します。角カッコは、コマンドの入力時には含めません。

機能および制限事項

CLI には、次の機能と制限事項があります。

- さまざまなアクセス方式 (Telnet または SSH) で同時に複数の CLI セッションを使用できます。最大で 2 つの Telnet コマンドラインセッションをいつでもアクティブにできます。



(注) Telnet セッションの数は設定可能です。有効な値は、0、1、および 2 です。値を 0 にすると、Telnet インターフェイスはディセーブルになります。

- 行ごとに 1 つのコマンドを入力できます (160 文字まで、スペースも含む)。
- 長いコマンド用の継続文字はありません。編集機能は、直前の入力した文字を消去する Back Space キーのみです。
- ↑キーと↓キーを使用して、直前の 8 つのコマンドを参照できます。**history** コマンドを使用すると、直前の 8 つのコマンドのリストが表示されます。次の例のように、これらをショートカットとして使用し、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 インターフェイスでは、出力バッファが 2 KB に制限されます。バッファリングは行われません。コマンドごとに 2048 文字までしか出力できません。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 リダイレクト中はデータがバッファリングされません）。
- コマンドの出力は、コマンドの実行が完了した後に画面に表示されます。そのため、コマンドは、リアルタイムで実行ステータスを報告することができません。たとえば、**flashing** コマンドの詳細モードの場合、フラッシングの進捗状況がリアルタイムで表示されません。コマンドの実行が完了した後に表示されます。
- 次の例のように、単純なテキスト メッセージを使用して、コマンドの実行ステータスが示されません。

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

- コマンド構文では大文字と小文字が区別されます。
- オプションとその引数の間には、1 つ以上のスペースが必要です。たとえば、`ifconfig eth0 -i192.168.70.133` は、間違った構文です。正しい構文は、`ifconfig eth0 -i 192.168.70.133` になります。
- すべてのコマンドには、**-h**、**-help**、および **?** オプションがあります。これらは構文ヘルプを表示します。次の例は、すべて同じ結果になります。

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

- 以降の項で説明されているコマンドのいくつかは、使用できないことがあります。サポートされているコマンドのリストを表示するには、次の例のように、**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 コマンド

ユーティリティ コマンドは次のとおりです。

- `exit`
- `help`
- `history`

exit コマンド

説明

コマンドライン インターフェイス セッションをログオフし、終了するには、**exit** コマンドを使用します。

help コマンド

説明

すべてのコマンドのリストとそれぞれの簡単な説明を表示するには、**help** コマンドを使用します。コマンドプロンプトで?を入力することもできます。

history コマンド

説明

最後に実行した 8 つのコマンドをインデックス付きの履歴リストで表示するには、**history** コマンドを使用します。インデックスは、この履歴リストからコマンドを再実行するためのショートカットとして使用できます (先頭に!を付けます)。

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 コマンド

モニタ コマンドは次のとおりです。

- clearlog

- fans
- readlog
- syshealth
- temps
- volts

clearlog コマンド

説明

IMM のイベント ログまたは IMM をクリアするには、**clearlog** コマンドを使用します。このコマンドを使用するには、イベント ログをクリアする権限が必要です。

fans コマンド

説明

サーバの各ファンの速度を表示するには、**fans** コマンドを使用します。

例

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

readlog コマンド

構文

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

説明

IMM イベント ログ エントリを一度に 5 つずつ表示するには、**readlog** コマンドを使用します。エントリは、新しいものから順に表示されます。

- **readlog** は、初めて実行されたとき、イベント ログ内の新しいエントリから順に最初の 5 つを表示します。それ以降は、呼び出されるたびに次の 5 つのエントリが表示されます。
- **readlog -f** を実行すると、カウンタがリセットされ、イベント ログ内の新しいエントリから順に最初の 5 つが表示されます。

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

説明

サーバのヘルスの要約を表示するには、**syshealth** コマンドを使用します。電源の状態、システムの状態、再起動の回数、および IMM ソフトウェアのステータスが表示されます。

例

```

system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>

```

temps コマンド

説明

温度および温度しきい値をすべて表示するには、**temps** コマンドを使用します。Web インターフェイ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)

- 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 (現在値)
 - SS : ソフト シャットダウン
 - HS : ハード シャットダウン
- 温度の値はすべて華氏/摂氏の形式で表示されています。

volts コマンド

説明

電圧および電圧しきい値をすべて表示するには、**volts** コマンドを使用します。Web インターフェイ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 : 低電圧時のハード シャットダウン
- SSL : 低電圧時のソフト シャットダウン
- WL : 低電圧時の警告
- WRL : 低電圧時の警告リセット
- V : 電圧 (現在値)
- WRH : 高電圧時の警告リセット
- WH : 高電圧時の警告
- SSH : 高電圧時のソフト シャットダウン
- HSH : 高電圧時のハード シャットダウン

vpd コマンド

構文

```
vpd sys
vpd IMM
vpd bios
vpd dsa
```

説明

システム (sys)、IMM、サーバファームウェア (bios)、および Dynamic System Analysis Preboot (dsa) の重要な製品データを表示するには、**vpd** コマンドを使用します。Web インターフェイスの場合と同じ情報が表示されます。

例

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

サーバの電源および再起動の制御コマンド

サーバの電源および再起動のコマンドは次のとおりです。

- power
- reset

power コマンド

構文

```
power on
power off [-s]
power state
power cycle [-s]
```

説明

サーバの電源を制御するには、**power** コマンドを使用します。**power** コマンドを実行するには、電源と再起動のアクセス権限が必要です。

- **power on** は、サーバの電源をオンにします。
- **power off** は、サーバの電源をオフにします。**-s** オプションを指定すると、オペレーティングシステムをシャットダウンしてからサーバの電源がオフになります。
- **power state** は、サーバの電源の状態（オンまたはオフ）とサーバの現在の状態を表示します。

- **power cycle** は、サーバの電源をオフにしてから、電源を再びオンにします。**-s** オプションを指定すると、オペレーティング システムをシャットダウンしてからサーバの電源がオフになります。

reset コマンド

構文

```
reset [option]
option:
-s
```

説明

サーバを再起動するには、**reset** コマンドを使用します。このコマンドを使用するには、電源と再起動のアクセス権限が必要です。**-s** オプションを指定すると、オペレーティング システムをシャットダウンしてからサーバが再起動されます。

コンフィギュレーション コマンド

コンフィギュレーション コマンドは次のとおりです。

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

dhcpinfo コマンド

構文

```
dhcpinfo eth0
```

説明

インターフェイスが DHCP サーバによって自動的に設定される場合、DHCP サーバが `eth0` に割り当てた IP 設定を表示するには、`dhcpcinfo` コマンドを使用します。DHCP は、`ifconfig` コマンドを使用してイネーブルまたはディセーブルにできます。

例

```
system> dhcpcinfo eth0
-server 192.168.70.29
-n IMMA00096B9E003A
-i 192.168.70.202
-g 192.168.70.29
-s 255.255.255.0
-d linux-test.cisco.com
-dns1 192.168.70.29
-dns2 0.0.0.0
-dns3 0.0.0.0
system>
```

次の表に、この例の出力の説明を示します。

オプション	説明
-server	設定を割り当てた DHCP サーバ
-n	割り当てられたホスト名
-i	割り当てられた IP 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名
-dns1	プライマリ DNS サーバの IP アドレス
-dns2	セカンダリ DNS の IP アドレス
-dns3	ターシャリ DNS サーバの IP アドレス

ifconfig コマンド

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
```

説明

イーサネット インターフェイスを設定するには、**ifconfig** コマンドを使用します。現在のイーサネット インターフェイス設定を表示するには、`ifconfig eth0` と入力します。イーサネット インターフェイス設定を変更するには、オプションを入力し、その後に値を指定します。インターフェイス設定を変更するには、最低でもアダプタのネットワークとセキュリティの設定権限が必要です。

次の表に、オプションの引数を示します。

オプション	説明	値
-state	インターフェイスの状態	disabled、enabled
-c	設定方法	dhcp、static、dthens (dthens は、Web インターフェイスでの [try dhcp server, if it fails use static config] オプションに対応します)
-i	スタティック IP アドレス	有効な IP アドレス形式
-g	ゲートウェイ アドレス	有効な IP アドレス形式
-s	サブネット マスク	有効な IP アドレス形式
-n	ホスト名	63 文字以下の文字列。英字、数字、ピリオド、アンダースコア、およびハイフンを含めることができます。
-r	データ レート	10、100、auto
-d	デュプレックス モード	full、half、auto
-m	MTU	60 ~ 1500 の数値
-l	LAA	MAC アドレス形式。マルチキャスト アドレスは指定できません (先頭バイトが偶数である必要があります)。

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` の `-b` オプションの表示は、Burned-In MAC Address に関するものです。Burned-In MAC Address は読み取り専用であり、設定することはできません。

ldap コマンド

構文

```
ldap [options]
options:
  -a loc|ldap|locId|ldloc
  -b anon|client|login
  -c client_dn
  -d search_domain
  -f group_filter
  -g group_search_attr
  -l string
  -m login|cfg|lthenc
  -n service_name
  -p client_pw
  -pc confirm_pw
  -r root_dn
  -s1ip host name/ip_addr
  -s2ip host name/ip_addr
  -s3ip host name/ip_addr
  -s1pn port_number
  -s2pn port_number
  -s3pn port_number
  -u search_attrib
  -v off|on
  -w on|off
  -h
```

説明

LDAP プロトコル設定パラメータを表示および設定するには、**ldap** コマンドを使用します。

次の表に、オプションの引数を示します。

オプション	説明	値
-a	ユーザ認証方式	ローカルのみ、LDAP のみ、ローカルの後に LDAP、LDAP の後にローカル
-b	バインド方式	匿名、ClientDN およびパスワードとのバインド、ユーザプリンシパルバインド (UPN)
-c	クライアント識別名	<i>client_dn</i> に 63 文字までの文字列
-d	検索ドメイン	<i>search_domain</i> に 31 文字までの文字列
-f	グループフィルタ	<i>group_filter</i> に 63 文字までの文字列
-g	グループ検索属性	<i>group_search_attr</i> に 63 文字までの文字列
-l	ログイン許可属性	<i>string</i> に 63 文字までの文字列
-m	ドメインソース	ログイン ID から検索ドメインを抽出する、設定された検索ドメインのみを使用する、ログインを先に試しその後に設定値を使用する
-n	サービス名	<i>service_name</i> に 15 文字までの文字列
-p	クライアントパスワード	<i>client_pw</i> に 15 文字までの文字列

オプション	説明	値
-pc	クライアント パスワードの確認	<i>confirm_pw</i> に 15 文字までの文字列 コマンドの使用方式 : <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ときに必要です。 <i>confirm_pw</i> 引数が <i>client_pw</i> 引数と比較され、それらが一致しなければコマンドは失敗します。
-r	ルート エントリの識別名 (DN)	<i>root_dn</i> に 63 文字までの文字列
s1ip	サーバ 1 のホスト名 /IP アドレス	<i>host name/ip_addr</i> に 63 文字までの文字列または IP アドレス
s2ip	サーバ 2 のホスト名 /IP アドレス	<i>host name/ip_addr</i> に 63 文字までの文字列または IP アドレス
s3ip	サーバ 3 のホスト名 /IP アドレス	<i>host name/ip_addr</i> に 63 文字までの文字列または IP アドレス
s1pn	サーバ 1 のポート番号	<i>port_number</i> に 5 桁までの数字のポート番号。
s2pn	サーバ 2 のポート番号	<i>port_number</i> に 5 桁までの数字のポート番号。
s3pn	サーバ 3 のポート番号	<i>port_number</i> に 5 桁までの数字のポート番号。
-u	UID 検索属性の文字列	<i>search_attrib</i> に 23 文字までの文字列
-v	DNS による LDAP サーバ アドレスの取得	off、on
-w	グループ名でのワイルドカードの使用許可	off、on
-h	コマンドの使用方式とオプションの表示	

ntp コマンド

構文

```
ntp [options]
options:
-en state
-i hostname
-f frequency
-synch
```

説明

ネットワーク タイム プロトコル (NTP) を表示および設定するには、**ntp** コマンドを使用します。

次の表に、オプションの引数を示します。

オプション	説明	値
-en	ネットワーク タイム プロトコルのイネーブル化またはディセーブル化	イネーブル、ディセーブル
-i	ネットワーク タイム プロトコル サーバの名前または IP アドレス	クロックの同期に使用される NTP サーバの名前。
-f	IMM のクロックがネットワーク タイム プロトコル サーバと同期される頻度 (分単位)	3 ~ 1440 分
-synch	ネットワーク タイム プロトコル サーバとただちに同期することを要求	このパラメータで使用される値はありません。

例

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

passwordcfg コマンド

構文

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

説明

パスワード パラメータを表示および設定するには、**passwordcfg** コマンドを使用します。

オプション	説明
-legacy	アカウント セキュリティを事前に定義されているレガシー レベルのデフォルト セットに設定
-high	アカウント セキュリティを事前に定義されている高レベルのデフォルト セットに設定
-exp	パスワードの最大有効期間 (0 ~ 365 日)。有効期限がない場合は 0 を設定します。
-cnt	再使用できない前のパスワードの数 (0 ~ 5)

オプション	説明
-nul	パスワードのないアカウントを許可 (yes または no)
-h	コマンドの使用方法和オプションの表示

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

構文

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

説明

シリアル ポートを設定するには、**portcfg** コマンドを使用します。シリアル ポート設定を変更するには、オプションを入力し、その後に値を指定します。シリアル ポート設定を変更するには、最低でもアダプタのネットワーキングとセキュリティの設定権限が必要です。

次のパラメータは、ハードウェアで設定されているため、変更することはできません。

- 8 データ ビット
- パリティなし
- 1 ストップ ビット

次の表に、オプションの引数を示します。

オプション	説明	値
-b	ボーレート	ボーレート 9600、19200、38400、57600、115200、230400
-climode	CLI モード	none、cliems、cliuser <ul style="list-style-type: none"> • none : コマンドライン インターフェイスはディセーブル • cliems : コマンドライン インターフェイスは EMS 互換のキーストローク シーケンスでイネーブル化 • cliuser : コマンドライン インターフェイスはユーザ定義のキーストローク シーケンスでイネーブル化

例

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

srcfg コマンド

構文

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

説明

シリアルリダイレクションを設定するには、**srcfg** コマンドを使用します。現在の設定を表示するには、**srcfg** と入力します。シリアルリダイレクト設定を変更するには、オプションを入力し、その後に値を指定します。シリアルリダイレクト設定を変更するには、最低でもアダプタのネットワーキングとセキュリティの設定権限が必要です。

次の表に、**-exitcliseq** オプションの引数を示します。

オプション	説明	値
-exitcliseq	コマンドライン インターフェイスを終了するキーストローク シーケンス	CLI を終了するためのユーザ定義のキーストローク シーケンス。詳細については、この表内の -entercliseq オプションの値を参照してください。

例

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

ssl コマンド

構文

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

説明



(注) SSL クライアントをイネーブルにするには、事前にクライアント証明書をインストールしておく必要があります。

Secure Sockets Layer (SSL) パラメータを表示および設定するには、**ssl** コマンドを使用します。

オプション	説明
-ce	SSL クライアントをイネーブルまたはディセーブルにします
-se	SSL サーバをイネーブルまたはディセーブルにします
-h	使用方法とオプションを表示します

パラメータ

次のパラメータは、**ssl** コマンドのオプション ステータス表示で示され、コマンドライン インターフェイスからのみ出力されます。

サーバセキュア トランスポート イネーブル

このステータス表示は、読み取り専用であり、直接設定することはできません。

サーバ Web/CMD キー ステータス

このステータス表示は、読み取り専用であり、直接設定することはできません。コマンドラインから出力される可能性のある値は次のとおりです。

```
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 サーバ CSR キー ステータス

このステータス表示は、読み取り専用であり、直接設定することはできません。コマンドラインから出力される可能性のある値は次のとおりです。

```
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 クライアント LDAP キー ステータス

このステータス表示は、読み取り専用であり、直接設定することはできません。コマンドラインから出力される可能性のある値は次のとおりです。

```
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 クライアント CSR キー ステータス

このステータス表示は、読み取り専用であり、直接設定することはできません。コマンドラインから出力される可能性のある値は次のとおりです。

```
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

構文

```
timeouts [options]
options:
-o OS_watchdog_option
-l loader_watchdog_option
```

説明

タイムアウト値を表示または変更するには、**timeouts** コマンドを使用します。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、オプションを入力し、その後に値を指定します。タイムアウト値を変更するには、最低でもアダプタ設定の権限が必要です。

次の表に、タイムアウト値の引数を示します。これらの値は、Web インターフェイスでのサーバタイムアウト用の段階的なスケールのプルダウン オプションと一致します。

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 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

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

構文

```
usbeth [options]  
options:  
-en <enabled|disabled>
```

説明

インバンドの LAN over USB インターフェイスをイネーブルまたはディセーブルにするには、**usbeth** コマンドを使用します。このインターフェイスをイネーブルまたはディセーブルにする方法の詳細については、「[USB インバンド インターフェイスのディセーブル化](#)」(P.3-6) を参照してください。

例

```
system>usbeth  
-en : disabled  
system>usbeth -en enabled  
ok  
system>usbeth  
-en : disabled
```

users コマンド

構文

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

説明

すべてのユーザ アカウントとそれらの権限レベルにアクセスしたり、新規のユーザ アカウントを作成したり、既存のアカウントを変更したりするには、**users** コマンドを使用します。

users コマンドに関する次のガイドラインを確認してください。

- ユーザ番号は 1 ~ 12 の範囲内にする必要があります。
- ユーザ名は、長さを 16 文字未満にする必要があります、数字、英字、ピリオド、およびアンダースコアのみを含めることができます。
- パスワードは、6 ~ 15 文字の長さにし、少なくとも英字と英字以外の文字を 1 つずつ含める必要があります。
- 権限レベルは、次のいずれかのレベルにできます。

- super (スーパーバイザ)
- ro (読み取り専用)
- 次の値の任意の組み合わせ (区切り文字は |) :
 - am (ユーザ 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 サーバの電源/再起動アクセス)
 - cel (イベント ログをクリア可能)
 - bc (アダプタ設定 (基本))
 - nsc (アダプタ設定 (ネットワークとセキュリティ))
 - ac (アダプタ設定 (詳細))

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. jacobyackenovics 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. jacobyackenovics 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 制御コマンドは次のとおりです。

- clearcfg
- clock

- identify
- resetsp
- update

clearcfg コマンド

説明

IMM 設定を出荷時の初期状態に設定するには、**clearcfg** コマンドを使用します。このコマンドを実行するには、最低でも詳細なアダプタ設定の権限が必要です。IMM の設定がクリアされた後、IMM は再起動されます。

clock コマンド

構文

```
clock [options]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

説明

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には、**clock** コマンドを使用します。日付、時刻、GMT オフセット、および夏時間を設定できます。

次の点に注意してください。

- +2 または +10 の GMT オフセットの場合、専用の夏時間設定が必要です。
- +2 の場合、夏時間オプションは次のとおりです。off、ee (東ヨーロッパ)、gtb (英国)、egt (エジプト)、fle (フィンランド)。
- +10 の場合、夏時間設定は次のとおりです。off、ea (東部オーストラリア)、tas (タスマニア)、vlad (ウラジオストク)。
- 年は 2000 ~ 2089 の範囲内にする必要があります。
- 月、日、時、分、および秒は、1 桁の値にすることもできます (たとえば、09:50:25 の代わりに 9:50:25)。
- GMT オフセットは、正のオフセットの場合は +2:00、+2、または 2、負のオフセットの場合は -5:00 または -5 の形式で指定できます。

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

構文

```
identify [options]  
options:  
-s on/off/blink  
-d seconds
```

説明

シャーシ識別 LED を点灯または消灯したり、点滅させたりするには、**identify** コマンドを使用します。**-d** オプションを **-s on** と組み合わせて使用することで、**-d** パラメータで指定した秒数だけ LED を点灯させることができます。指定された秒数が経過すると、LED は消灯します。

例

```
system> identify  
-s off  
system> identify -s on -d 30  
ok  
system>
```

resetsp コマンド

説明

IMM を再起動するには、**resetsp** コマンドを使用します。このコマンドを実行するには、最低でも詳細なアダプタ設定の権限が必要です。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>