



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 ローケーション 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。

The screenshot displays the IMM web interface with the following sections:

- System Settings** (Left Navigation Menu):
 - System
 - Monitors
 - System Status
 - Virtual Light Path
 - Event Log
 - Vital Product Data
 - Tasks
 - Power/Restart
 - Remote Control
 - PXE Network Boot
 - Firmware Update
 - IMM Control
 - System Settings** (Selected)
 - Login Profiles
 - Alerts
 - Serial Port
 - Port Assignments
 - Network Interfaces
 - Network Protocols
 - Security
 - Configuration File
 - Restore Defaults
 - Restart IMM
 - Log Off
- IMM Information**:
 - Name: SN# KQ098M5
 - Contact: [Empty Field]
 - Location: [Empty Field]
- Server Timeouts**:
 - OS watchdog: 0.0 minutes
 - Loader watchdog: 0.0 minutes
 - Power off delay: 0 minutes
- IMM Date and Time**:
 - Date (mm/dd/yyyy): 04/05/2011
 - Time (hh:mm:ss): 06:02:25
 - Link: [Set IMM Date and Time](#)
- Miscellaneous**:
 - Allow commands on USB interface: Enabled

A "Save" button is located at the bottom right of the page.

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せん。

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。

Integrated Management Module

SN# KQ098M5 [View Configuration Summary](#)

Login Profiles

To configure a login profile, click a link in the "Login ID" column or click "Add User."

| Slot No | Login ID | Access | Password Expires |
|---------|------------------------|------------|------------------|
| 1 | USERID | Supervisor | No expiration |

[Add User](#)

Global Login Settings

These settings apply to all login profiles.

User authentication method:

Lockout period after 5 login failures: minutes

Web inactivity session 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) |

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 User

SNMPv3 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。

Integrated Management Module

SN# KQ098M5 [View Configuration Summary](#)

Remote Alert Recipients

To configure a remote alert recipient, click a link in the "Name" column.

| Name | Status |
|----------------------------------|--------|
| 1. ~ not used ~ | |
| 2. ~ not used ~ | |
| 3. ~ not used ~ | |
| 4. ~ not used ~ | |
| 5. ~ not used ~ | |
| 6. ~ not used ~ | |
| 7. ~ not used ~ | |
| 8. ~ not used ~ | |
| 9. ~ not used ~ | |
| 10. ~ not used ~ | |
| 11. ~ not used ~ | |
| 12. ~ not used ~ | |

[Generate Test Alert](#)

Global Remote Alert Settings

These settings apply to all remote alert recipients.

Remote alert retry limit: 5 times

Delay between entries: 0.0 minutes

Delay between retries: 0.5 minutes

SNMP Alerts Settings

Select the alerts that will be sent to SNMP.

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 Incompatibility
- 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 times

Delay between entries minutes

Delay between retries 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る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 に割り当てることを要求されます。

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 IMMA 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。

- 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 ▼
 Search Domain
 Service Name

 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
 UID Search Attribute
 Binding Method ▼
 Client DN
 Password
 Confirm password
 Enhanced role-based security for Active Directory Users ▼
 Server Target Name

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す。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。このフィールドをブランクのままにすると、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 になります。

このフィールドをブランクのままにすると、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。

このフィールドをブランクのままにすると、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。

- **ネットワークキング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、ネットワークキング、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.3-34)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

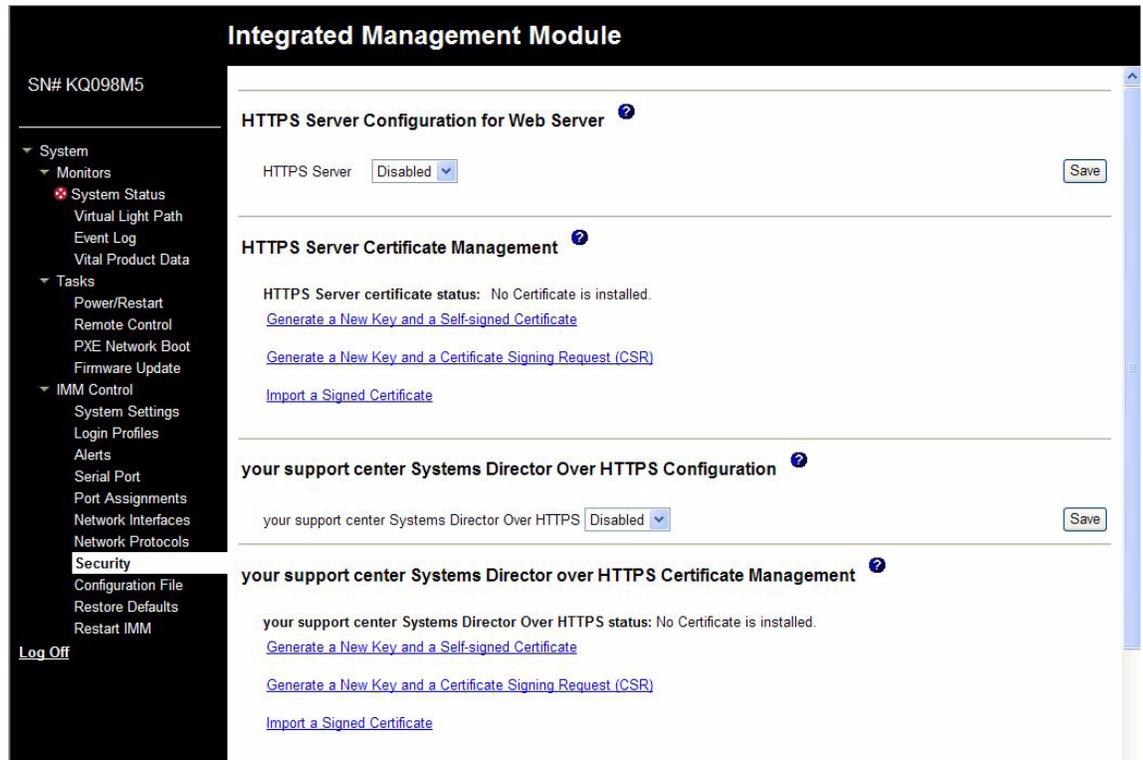
SSL サーバは、SSL をイネーブルにする前に、有効な証明書と対応する秘密暗号キーがインストールされていることを必要とします。秘密キーと必要な証明書を生成するには、自己署名証明書を使用する方法と、認証局が署名した証明書を使用する方法があります。SSL サーバの自己署名証明書の使用については、「自己署名証明書の生成」(P.3-35) を参照してください。SSL サーバの認証局署名証明書の

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) | <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"/> |

- 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。情報を入力し終えたら、[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"/> |

Generate CSR

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寄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.3-34) 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、通常のログイン 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。