Sun™ Integrated Lights Out Manager 2.0 ユーザーズガイド

Sun Microsystems, Inc.
www.sun.com

Part No. 820-2698-10
2007 年 7 月, Revision A

コメントの送付: http://www.sun.com/hwdocs/feedback

原典: *Sun Integrated Lights Out Manager 2.0 User's Guide*
Part No: 820-1188-10
Revision A

目次

はじめに

『Sun Integrated Lights Out Manager 2.0 ユーザーズガイド』では、ILOM をサポートする Sun ラック搭載型サーバーまたはブレードサーバーに共通の ILOM 機能およびタスクについて説明します。これらの機能へのアクセスやタスクの実行は、ILOM が管理している Sun サーバープラットフォームにかかわらず、同じ方法で行うことができます。使用しているサーバープラットフォームに固有の ILOM 機能やタスクは、ほかのユーザーマニュアルで説明しています。ILOM のプラットフォーム固有の情報は、システムに付属のマニュアルセットで確認できます。

本書を読む前に

このユーザーズガイドでは、ILOM で管理されるすべてのサーバープラットフォームに共通の ILOM 機能について、詳細な情報を提供します。このユーザーズガイドで説明されている情報を完全に理解し、タスクを完全に実行するには、このマニュアルを、使用している特定のサーバープラットフォームに付属の ILOM マニュアルと一緒に使用することをお勧めします。

マニュアルの構成

このマニュアルには、次の情報が含まれています。

第 1 章では、ILOM の機能の概要について説明します。

第 2 章では、ILOM との初期通信を確立する方法と、さまざまな接続を使用して実行できるタスクの種類について説明します。

第 3 章では、ILOM のコマンド行インタフェース (CLI) の使用方法と、CLI を使用した ILOM へのログイン方法について説明します。

第 4 章では、ILOM Web インタフェースの使用方法と、Web インタフェースを使用した ILOM へのログイン方法について説明します。

第 5 章では、Active Directory、LDAP、および RADIUS の設定方法に加えて、ILOM CLI または Web インタフェースを使用したユーザーアカウントの管理方法について説明します。

第 6 章では、部品情報を表示および変更する方法、部品を取り外す準備や部品をサービスに復帰させる準備を行う方法、およびポリシーの設定方法について説明します。

第 7 章では、センサー、インジケータ、およびイベントログを使用してシステムを監視する方法や、警告を管理する方法について説明します。

第 8 章では、ILOM ネットワーク設定の概要と、ILOM CLI または Web インタフェースを使用してネットワーク設定を行うために実行する必要のあるタスクについて説明します。

第 9 章では、Intelligent Platform Management Interface と IPMItool について説明します。

第 10 章では、SNMP の仕組みと、ILOM CLI または Web インタフェースを使用した SNMP ユーザーの管理方法について説明します。

第 11 章では、ILOM CLI または Web インタフェースを使用して ILOM ファームウェアをアップグレードおよびリセットする方法について説明します。

第 12 章では、ILOM リモートコンソールアプリケーションについて、およびリモートコンソールを起動および設定してサーバープラットフォームを遠隔で管理する方法について説明します。

付録 A では、ILOM CLI コマンドのリファレンスを提供し、コマンドの使用方法について説明します。

付録 B は、このユーザーズガイドで使用されている単語や語句の一部の定義がまとめられた用語集です。

表記上の規則

書体または記号*	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	% **su** Password:
AaBbCc123	コマンド行の可変部分。実際の名前や値と置き換えてください。	rm *filename* と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	% **grep '^#define ** **XV_VERSION_STRING'**

* 使用しているブラウザにより、これらの設定と異なって表示される場合があります。

関連マニュアル

このマニュアルは、使用している特定のプラットフォームに付属の ILOM プラットフォーム用補足マニュアルと一緒に使用することをお勧めします。

マニュアル、サポート、およびトレーニング

Sun のサービス	URL
マニュアル	http://jp.sun.com/documentation/
サポート	http://jp.sun.com/support/
トレーニング	http://jp.sun.com/training/

Sun 以外の Web サイト

このマニュアルで紹介する Sun 以外の Web サイトが使用可能かどうかについては、Sun は責任を負いません。このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、広告、製品、またはその他の資料についても、Sun は保証しておらず、法的責任を負いません。また、このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、商品、サービスの使用や、それらへの依存に関連して発生した実際の損害や損失、またはその申し立てについても、Sun は一切の責任を負いません。

コメントをお寄せください

マニュアルの品質改善のため、お客様からのご意見およびご要望をお待ちしております。コメントは下記よりお送りください。

http://www.sun.com/hwdocs/feedback

ご意見をお寄せいただく際には、下記のタイトルと Part No. を記載してください。

『Sun Integrated Lights Out Manager 2.0 ユーザーズガイド』、Part No. 820-2698-10

第1章

ILOM の概要

Sun™ Integrated Lights Out Manager (ILOM) 2.0 は、さまざまな Sun サーバープラットフォームの監視、管理、および構成を行うために使用できるシステム管理ファームウェアです。

この章には次の節があります。

ILOM とは

Integrated Lights Out Manager (ILOM) は、一部の Sun サーバープラットフォームにプリインストールされているシステム管理ファームウェアです。ILOM を使用すると、サーバーシステムにインストールされたコンポーネントをアクティブに管理および監視できます。ILOM を使用すると、ハードウェア構成の参照、システム情報の監視、システム警告の管理などを行うことによって、システムを予防保守的に監視および管理することができます。ILOM では、SNMP ユーザーインタフェースと IPMI ユーザーインタフェースのほかに、ブラウザベースの Web インタフェースとコマンド行インタフェースも提供されています。システムに電源が投入されるとすぐに、

ILOM は自動的に初期化されます。ILOM は、ホストのオペレーティングシステムの状態に関係なく処理を継続するため、システムは「完全自動」の管理システムとなります。

ILOM の主要な機能は次のとおりです。

- 独自のプロセッサおよびリソース上で動作する
- システムリソースを消費することなく、サーバーを管理できる
- サーバーの電源が切断されているときでも、スタンバイ電源を使用して管理を続行する
- データネットワークとは別の独立した管理ネットワークを提供する
- ハードウェアインベントリと環境の簡潔なビューを提供する
- 電源の制御、部品の管理、ホストコンソールへのアクセスを行うための機能を提供する
- Sun N1™ System Manager、Sun 以外のアプリケーションなどのほかの管理ツールの統合ポイントとして動作する
- サービスプロセッサ (SP) ファームウェアと BIOS の変更のダウンロードを可能にする
- ホットプラグ可能なシステムコンポーネントのインベントリを管理する

SP および CMM 上の ILOM

ILOM は、ラック搭載型サーバーやブレードサーバーなど、各種 Sun サーバープラットフォームでサポートされています。ILOM ファームウェアは、ラック搭載型サーバーまたはブレードサーバーのサービスプロセッサ (SP) にプリインストールされています。または、使用しているサーバープラットフォームで適用可能な場合、ILOM ファームウェアはシャーシ監視モジュール (CMM) にプリインストールされています。

ILOM は、システムを管理するために、直接 SP を使用する方法と、適用可能な場合には CMM を使用する方法の 2 つをサポートしています。

- **サービスプロセッサを直接使用する** − SP またはブレードと直接通信して、ラック搭載型サーバーの SP を管理すると、個々のシステムまたはブレードの操作を管理することができます。この方法は、サービスプロセッサの障害追跡や、マルチテナントシステムを使用している場合は特定のシステムまたはブレードへのアクセスの制御に役立つ場合があります。
- **シャーシ監視モジュールを使用する** − システムに CMM が含まれている場合、CMM からシステムを管理すると、システム全体のすべてのコンポーネントを設定して管理したり、個々のブレードサーバーの SP までドリルダウンして管理することもできます。

ILOM インタフェース

ILOM はさまざまなインタフェースから使用可能です。

- **Web インタフェース** − Web インタフェースには使いやすいブラウザインタフェースが用意されており、これを使用して SP にログインし、システム管理、監視、および IPMI タスクを実行できます。ILOM の Web インタフェースに関する情報は、第 4 章を参照してください。
- **コマンド行インタフェース (CLI)** − コマンド行インタフェースでは、キーボードコマンドを使用して ILOM を操作できます。このコマンド行インタフェースは、業界標準の CLI とスクリプトプロトコルの DMTF の「SMASH」CLP に準拠しています。端末エミュレータソフトウェアを実行している端末または PC をシステムのシリアルポートに直接接続できます。または、Secure Shell (SSH) を使用して Ethernet 管理ネットワークポートに接続することもできます。CLI に関する情報は、第 3 章を参照してください。
- **リモートコンソール** − ILOM リモートコンソールを使用すると、サーバーのコンソールに遠隔からアクセスすることができます。キーボード、マウス、およびビデオ画面をリダイレクトし、ローカルマシンの CD ドライブやフロッピーディスクドライブからの入出力もリダイレクトできます。リモートコンソールに関する情報は、第 12 章を参照してください。
- **Intelligent Platform Management Interface (IPMI)** − IPMI v1.5 および v2.0 と IPMItool ユーティリティーを使用すると、CLI を使用してデバイスを管理および構成し、システムの Baseboard Management Controller (BMC) から情報を取得できます。IPMItool を使用すると、遠隔からのハードウェアコンポーネントの状態の監視、システムログの監視、交換可能コンポーネントに関するレポートの受信、およびサーバーコンソールのリダイレクトを行うことができます。IPMI に関する情報は、第 9 章を参照してください。
- **SNMP (ネットワーク管理用プロトコルの一種。Simple Network Management Protocol の略) インタフェース** − ILOM は、外部のデータセンター管理アプリケーション、たとえば Sun N1™ System Manager や、Hewlett-Packard OpenView®、IBM Tivoli® などの Sun 以外のアプリケーション用に SNMP v3.0 インタフェース (SNMP v1 および SNMP v2c のサポートに限定) も提供します。SNMP に関する情報は、第 10 章を参照してください。

ILOM 管理ネットワーク

Sun サーバープラットフォームには、ネットワーク管理ポートおよびデータポートがあります。これらの独立した物理的な Ethernet 接続は、ILOM と、ホストハードウェア上で実行しているオペレーティングシステム用です。専用ネットワーク管理

ポートに接続して、ILOM を使用したサーバープラットフォームの管理を行うことができます。ネットワーク管理ポートから ILOM に接続することを選択した場合、ILOM へのトラフィックは、オペレーティングシステムのホストが行うデータ転送とは別になります。ネットワークポートを介して渡されるデータトラフィックはありません。このため、必要に応じて、管理トラフィックを個別のネットワーク上で完全に独立させることが可能です。

ネットワーク管理ポートの場所とラベル付けは、システム固有です。また、サーバープラットフォームの種類によって、内部管理通信の提供方法が決まります。たとえば、ブレードサーバーシステムでは、ネットワークポートがシャーシ内のすべての CMM と SP への通信を提供します。使用しているプラットフォームのマニュアルを参照して、システムでの管理通信の提供方法を確認してください。

サーバーの管理に ILOM とネットワーク管理ポートを使用しないことを選択する場合、環境の監視、IPMI 管理、Web インタフェースなどの多数の拡張機能を使用できなくなります。ホストオペレーティングシステムのデータポートを使用して、Sun 以外のネットワーク管理アプリケーション、SNMP ツール、またはオペレーティングシステムのユーティリティーにアクセスできますが、これらのソリューションではプラットフォームの限定されたビューしか使用できません。端末エミュレータソフトウェアを実行している PC または端末を使用して、サーバーのシリアルポートを介して接続すると、ローカルでサーバーを管理することもできます。ILOM に直接接続する方法を使用しない場合は、Sun サーバープラットフォームを遠隔管理することができません。

ILOM の接続方法

ILOM に接続する方法は、サーバープラットフォームによって異なります。

次の表に、ILOM への接続に使用できるさまざまな方法を示します。

表 1-1 ILOM の接続方法

接続方法	ラック搭載	ブレード	サポートされるインタフェース	説明
Ethernet ネットワーク管理接続	はい	はい	CLI と Web インタフェース	Ethernet ネットワーク管理ポートに接続します。ILOM の IP アドレスが既知である必要があります。この方法は Web インタフェースとコマンド行インタフェースをサポートします。

表 1-1　ILOM の接続方法 (続き)

接続方法	ラック搭載	ブレード	サポートされるインタフェース	説明
シリアル接続、サーバーまたはブレードから	はい	いいえ	CLI のみ	サーバーまたはブレード上のシリアル管理ポートに直接接続します。必要に応じて、シリアルアダプタケーブルを使用してシリアルポートに接続します。この方法はコマンド行インタフェースのみをサポートします。
シリアル接続、CMM から	いいえ	はい	CLI のみ	CMM のシリアルポートに接続します。この方法はコマンド行インタフェースのみをサポートします。

注 – ILOM は、シリアル、Secure Shell (SSH)、および Web インタフェースセッションを含む、最大 10 個のアクティブセッションをサポートしています。

ILOM の Web インタフェースまたは CLI を使用して管理ネットワークにアクセスするには、管理する CMM または SP の IP アドレスが必要です。内部システムの設定中に、各 CMM と SP に一意の IP アドレスが割り当てられます。SP と CMM に初期 IP アドレスを割り当てる方法は、第 2 章を参照してください。

ILOM ユーザーアカウントの役割

ILOM のユーザーアカウントには、ILOM のユーザーアクセスと権限を決定する役割が定義されています。管理者は、ILOM の Web インタフェースまたは CLI を使用してユーザーアカウントを管理できます。ILOM アカウントに割り当てられた役割は次のとおりです。

- **管理者** − ILOM のすべての機能やコマンドにアクセスできます。
- **オペレータ** − ホストシステムの管理および監視を完全に実行するためのアクセスが可能です。また、ILOM 構成への読み取り専用アクセスを提供します。

事前構成された ILOM 管理者アカウント

ILOM は、1 つの管理者アカウントが事前構成された状態でプリインストールされています。

- ユーザー名: `root`
- パスワード: `changeme`

事前定義された管理者アカウントである root は、削除することも変更することもできませんが、デフォルトのパスワード (changeme) をリセットすることはできます。このアカウントでは、ILOM のすべての機能やコマンドに対して組み込み型の管理権限 (読み取りおよび書き込みアクセス) が提供されます。

SP または CMM レベルではじめて ILOM にアクセスするときは、root として、デフォルトの changeme パスワードを使用してログインする必要があります。ILOM にログインしてシステムへのネットワーク接続を確立したら、ILOM の root アカウントに関連付けられたデフォルトの changeme パスワードをリセットすることをお勧めします。承認されていないアクセスからシステムを保護するには、システムに取り付けられている各 SP および CMM でこのパスワードをリセットします。ILOM の root アカウントのパスワードのリセットについては、209 ページの「ILOM SP をリセットする」を参照してください。

ILOM の機能

表 1-1 に、ILOM をサポートしている Sun のシステムに共通する ILOM の機能とタスクを示します。使用しているシステムでこの機能がサポートされるかどうかについては、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

表 1-2 ILOM の機能

機能	利点
インタフェース	
Web インタフェース	• Sun の標準に基づくブラウザベースのユーザーインタフェースを提供します。
コマンド行インタフェース	• 業界標準の CLI とスクリプトプロトコルの DMTF「SMASH」CLP をサポートします。 • 既存のスクリプトを Sun のシステムで再利用し、使い慣れたインタフェースを使用してタスクを自動化します。

表 1-2　ILOM の機能 (続き)

機能	利点
システム管理インタフェース	• 業界標準の SNMP v1、v2c、v3、および IPMI v1.5 と v2.0 をサポートします。プラットフォーム MIB では、IPMI に加えて SNMP を使用してプラットフォームを管理できます。コントロール MIB では、カスタム管理アプリケーションまたは Sun 以外の管理アプリケーションを ILOM と統合できます。 • ILOM リモートコンソールを使用して、遠隔システムにアクセスできます。
セキュリティー	
SSH 2.0 のサポート	• CLI へのセキュリティー保護されたアクセスが可能です。
LDAP、MSFT Active Directory、RADIUS	• 既存の環境へ簡単に統合するための、業界標準の認証プロトコルおよび承認プロトコルをサポートします。
ユーザー管理	• 管理者とオペレータの役割をサポートします。システムのセキュリティーおよび制御を向上させるためにアクセスレベルを構成できます。
root のパスワードのリセット機能	• 承認されていないアクセスからシステムを保護します。パスワードをデフォルトにリセットするには、プッシュボタンまたはジャンパを使用します。
SSL 証明書	• デフォルトの SSL 証明書と HTTPS アクセス用の自己署名鍵を使用すると、セキュリティー保護された通信が可能です。
ローカルアクセスと遠隔アクセス	
ホストの電源が切断されているときの SP へのアクセス	• ホストのオペレーティングシステムの状態に関係なく、ILOM の処理を継続することができます。
専用ネットワーク管理ポート	• ネットワーク管理トラフィックとデータネットワークトラフィックを分離します。
リモートコンソール	• 遠隔システムにアクセスするためのシンプルな Web インタフェースを提供します。リモートコンソールを起動するために、SP にログインする必要はありません。
編集可能なホスト名データフィールド	• 管理者は、システムの識別用に、IP アドレスに加えてホスト名データフィールドを使用できます。
Web インタフェースのオンとオフの切り替え	• ILOM アクセスを制限し、CLI アクセスのみを可能にします。
監視とロギング	

表 1-2　ILOM の機能 (続き)

機能	利点
SNMP と IPMI の監視と制御	• 業界標準の SNMP コマンドと IPMI IPMItool ユーティリティーを使用して、コンポーネントを監視します。
イベントログ	• すべての「サービス」データをロギングするための一貫性のある方法を提供します。
構成可能な警告のしきい値	• システムのしきい値を超えたときに IPMI PET 警告を送信するように、ユーザーが SP を構成できます。
電子メールイベント通知	• すばやく便利なイベント通知を提供します。
ECC メモリーエラーと同様に、SP ログ、syslog、遠隔ログホストにレポートされるハードウェアおよびシステムに関するエラー	• より迅速な障害の診断と分離が可能なため、停止時間が減少します。
電源制御	
強制的電源切断	• システムの緊急の電源切断が可能です。
正常な停止と電源の再投入	• システムの電源切断の前に、ユーザーがホストのオペレーティングシステムを停止できます。
遠隔の電源投入および電源切断	• ユーザーは、システムの電源を遠隔から制御できます。
ファームウェア	
Web インタフェースまたは CLI から識別されるファームウェアのバージョン	• ファームウェアバージョンを識別する簡単な方法を提供します。
Web インタフェースまたは CLI を使用したファームウェアの更新	• ファームウェアを更新するための簡単な手順を提供します。
構成	
BIOS インタフェース、シリアルまたは Ethernet SP ポート、あるいはホストの OS を介した、IP アドレスなどの SP の手動構成	• 初期構成を簡略化します。
ローカルのキーボードおよびモニターからプログラム可能な SP IP アドレス	• データセンター内のシステムに対する手動での IP 構成を容易にします。

ILOM 2.0 の新機能

- Active Directory
- 電子メール警告
- 新たに更新された Sun 固有の MIB
- SNMP トラップ
- リモートコンソールの国際化

その他の管理ツール

Sun のサーバーは、システムの管理に使用できるさまざまなシステム管理ツールをサポートしています。ILOM のほかに、システム管理ツールには次のようなものがあります。

- **Sun N1 System Manager** − Sun N1 System Manager は、個別に購入できる包括的なシステム管理ツールです。このツールは、SPARC 版、x64 版 Sun Fire サーバー、および Sun Blade サーバーモジュールのインフラストラクチャー管理を簡単にする柔軟な機能を提供します。Sun N1 System Manager を使用すると、IT 管理者は Sun N1 管理ステーションから複数のシステムを遠隔で監視、保守、およびプロビジョニングすることができます。Sun N1 System Manager に関する情報は、次のサイトを参照してください。

  `http://www.sun.com/software/products/system_manager`

- **Sun 以外のシステム管理ツール** − Sun のシステムでは、HP Systems Insight Manager、IBM Tivoli などの Sun 以外のシステム管理ツールと統合するために、SNMP (v1、v2c、v3) と IPMI (v1.5 および v2.0) の両方をサポートしています。Sun 以外の主なシステム管理ツールとそれらの Sun x64 システムのサポート状況の一覧は、次のサイトで確認できます。

  `http://www.sun.com/x64/system-management/tools.jsp`

第2章

ILOM との初期通信の確立

サーバーまたは CMM のシリアル管理ポートへのコンソール接続、あるいはサーバーまたは CMM のネットワーク管理ポートへの Ethernet 接続を使用して、ILOM との通信を確立することができます。

ILOM に対して確立する接続の種類によって、実行できるタスクの種類が決まります。たとえば、ILOM のあらゆるシステム管理機能に遠隔からアクセスするには、サーバー SP やさらに該当する場合は CMM への Ethernet 接続と IP 割り当ての両方が必要です。

この章には次の節があります。

ILOM の初期設定について

ILOM との通信を確立する前に、次のトピックを確認することをお勧めします。

初期設定ワークシート

表 2-1 のワークシートを使用して、ILOM との通信をはじめて確立するために必要な情報を収集します。

表 2-1　ILOM との通信を確立するための初期設定ワークシート

設定のための情報	要件	説明
ローカルシリアルコンソール接続	任意 ― 初期 IP アドレスを割り当てるために DHCP を使用する場合 必須 ― 初期 IP アドレスを割り当てるために DHCP サーバを利用しない場合	IP アドレスをサーバー SP または CMM に割り当てるために DHCP サーバーを利用しない場合は、サーバーまたはシャーシ監視モジュール (CMM) のシリアル管理ポートを使用して、ILOM へのローカルシリアルコンソール接続を確立する必要があります。 シリアルコンソールをサーバーまたは CMM に接続する方法については、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。
遠隔 Ethernet 管理接続	任意	ネットワーク (Ethernet) ケーブルをサーバーまたは CMM のネットワーク管理ポートに接続します。ネットワーク管理ポートのラベルは、サーバープラットフォームによって異なる場合があります。一部のサーバーおよび CMM ネットワーク管理ポートには、NET MGT または MGT というラベルが付いています。ネットワーク管理ポートのラベルについての質問や、Ethernet ケーブルを管理ポートに接続する方法については、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。 ILOM の管理機能のすべてにアクセスするには、ローカルエリアネットワークをサーバーまたは CMM のネットワーク管理ポートに接続する必要があります。 ネットワーク管理ポートは、すべてのラック搭載型の Sun スタンドアロンサーバーで提供されています。ただし、このポートは Sun Blade サーバーモジュールでは提供されていません。ブレードサーバーモジュールとの Ethernet 通信では、CMM のネットワーク管理ポートを使用します。
SP IP の割り当て	必須	DHCP または静的 IP アドレスをサーバー SP または CMM に割り当てるかどうかを指定します。ILOM とのすべての遠隔システム管理通信では、サーバー SP または CMM の管理ネットワークを使用します。 詳細は、次のトピックを参照してください。 • 14 ページの「DHCP IP 割り当てに関する考慮事項」 • 18 ページの「静的 IP 割り当てに関する考慮事項」 • 23 ページの「Sun サーバープラットフォーム SP インタフェースへの IP アドレスの割り当て」

表 2-1　ILOM との通信を確立するための初期設定ワークシート (続き)

設定のための情報	要件	説明
ILOM インタフェース	必須	サーバー SP または CMM の IP アドレスを確立または変更するときは、次の ILOM インタフェースのいずれかを使用します。 • **コマンド行インタフェース (CLI) ― 初期 IP アドレスを確立する場合に使用します。**IP アドレスがサーバー SP または CMM に割り当てられていない場合は、ローカルシリアルコンソールを介して ILOM に接続し、IP アドレスを割り当てることができます。 一般に CLI は、シリアル接続 (ローカルシリアルコンソール、端末エミュレーションアプリケーション、または遠隔 SSH 接続) を介して ILOM で実行されるすべてのタスクに対して使用されます。 • **Web インタフェース ― 既存の IP アドレスを編集する場合に使用します。**IP アドレスがサーバー SP または CMM に割り当てられている場合、LAN 接続が MGT ポートに対して確立されていれば、Web インタフェースを使用して ILOM に接続し、割り当てられている既存の IP アドレスを編集することができます。 一般に Web インタフェースは、Ethernet 管理接続を介して ILOM で実行されるすべてのタスクに対して使用されます。 ILOM インタフェースについては、第 3 章および第 4 章を参照してください。
ILOM ファイアウォールアクセス	任意	ファイアウォールアクセスを必要とする Ethernet ネットワークでの ILOM のネットワークポートの使用方法を確認します。詳細は、20 ページの「ILOM ネットワークポートの割り当て」を参照してください。
SP ホスト名の割り当て	任意	任意で、わかりやすいホスト名をサーバー SP に割り当てることができます。詳細は、22 ページの「サーバー SP および CMM のホスト名の識別情報」または 33 ページの「ホスト名またはシステム識別子の割り当て」を参照してください。
システム識別子の割り当て	任意	任意で、システム識別子 (わかりやすい名前) を Sun サーバーに割り当てることができます。詳細は、22 ページの「サーバー SP および CMM のホスト名の識別情報」または 33 ページの「ホスト名またはシステム識別子の割り当て」を参照してください。

DHCP IP 割り当てに関する考慮事項

動的ホスト構成プロトコル (DHCP) サーバーを使用して、IP アドレスをサーバー SP または CMM に割り当てることを計画している場合は、次のトピックを確認してください。

- 15 ページの「Sun サーバープラットフォームの DHCPDISCOVER パケットのブロードキャスト」
- 15 ページの「DHCP 割り当ての要件」
- 15 ページの「SP ネットワークインタフェースの MAC アドレス」
- 17 ページの「DHCP 後の要件」

Sun サーバープラットフォームの DHCPDISCOVER パケットのブロードキャスト

Sun サーバープラットフォームに電源が供給されると、Sun サーバー SP または CMM は、DHCPDISCOVER パケットを自動的にブロードキャストします。ネットワーク上に DHCP サーバーが確立されている場合、DHCP サーバーは、要求元であるサーバー SP または CMM に対して、IP アドレスとその他のネットワーク設定情報が含まれる DHCPOFFER パケットを自動的に返します。

注 – DHCP サーバーが Ethernet IP アドレスを割り当てるように選択するか、SP の MAC アドレスを指定することによって特定の Ethernet IP アドレスを割り当てるように DHCP サーバーを設定することができます。詳細は、DHCP サーバーのユーザーマニュアルを参照してください。サーバー SP または CMM の MAC アドレスを取得する方法については、15 ページの「SP ネットワークインタフェースの MAC アドレス」を参照してください。

DHCP 割り当ての要件

DHCP サーバーを使用して IP アドレスを Sun サーバー SP インタフェースに割り当てるには、次の条件を満たす必要があります。

- Ethernet ケーブルが、サーバー管理ポートまたは CMM 管理ポートに差し込まれている必要があります。
- DHCP サーバーが、Sun サーバープラットフォームと同じサブネットに接続されている必要があります。
- DHCP サーバーが、新しいメディアアクセス制御 (MAC) アドレスを受け入れるように設定されている必要があります。
- ILOM の DHCP 構成設定が有効になっている必要があります。この設定はデフォルトで有効になっています。

SP ネットワークインタフェースの MAC アドレス

DHCP サーバーを使用して IP アドレスを SP ネットワークインタフェースに割り当てることを計画している場合は、サーバー SP または CMM の MAC アドレスが必要になることがあります。

サービスプロセッサの MAC アドレスは、表 2-2 で説明するいずれかの方法で取得できます。

表 2-2　SP の MAC アドレスを取得する方法

ILOM のカテゴリ	方法	説明
ラック搭載型サーバー SP ブレードサーバー SP	内部ラベルの確認	通常、管理ネットワークでのサーバー SP の MAC アドレスのラベルは、サーバーに貼り付けられたステッカーに表示されています。 サーバーに貼り付けられたステッカーに MAC アドレスが表示されていない場合は、Sun サーバープラットフォームに付属のユーザーマニュアルを確認してください。
CMM	内部ラベルの確認	通常、管理ネットワークでの CMM の MAC アドレスのラベルは、CMM に貼り付けられたステッカーに表示されています。 CMM に貼り付けられたステッカーに MAC アドレスが表示されていない場合は、Sun サーバープラットフォームに付属のユーザーマニュアルを確認してください。
すべて	Customer Information Sheet	Sun サーバープラットフォームに付属の Customer Information Sheet を参照してください。

DHCP 後の要件

DHCP サーバーが IP アドレスを SP ネットワークインタフェースに割り当てたら、表 2-3 に示すいずれかの方法を使用して、DHCP サーバーによって割り当てられた IP アドレスを識別することができます。

表 2-3 DHCP サーバーによって割り当てられた IP アドレスを識別する方法

方法	説明
DHCP のログファイル (このログファイルは、ILOM の一部ではなく、DHCP サーバー上にあるログファイルです。)	DHCP のログファイルを開き、次の手順を実行します。 1. MAC アドレスフィールドでサービスプロセッサの MAC アドレスを探します。 2. MAC アドレスフィールドの MAC アドレスに対応する IP アドレスフィールドに割り当てられた IP 値を特定します。 3. Web インタフェースを使用して遠隔で ILOM と通信するには、手順 2 で特定した IP アドレスを使用します。 **ヒント**: 通常、DHCP ログファイルのエントリは、次のようにコンマで区切られたフィールドを持つ個別の行です。 ID, Date, Time, Description, IP Address, Host Name, MAC Address
シリアルコンソール接続	サーバーまたは CMM のシリアルポートに対するシリアルコンソール接続を確立します。 CLI を使用して ILOM に root としてログインし、次のいずれかのコマンドを入力します。 • ラック搭載型のスタンドアロンサーバーの場合: `show /SP/network` • シャーシブレードサーバーモジュールの場合: `show /CH/BLn/SP network` • スロット 0 のシャーシ CMM の場合: `show /CMM/network/CMM0` • スロット 1 のシャーシ CMM の場合: `show /CMM/network/CMM1`

静的 IP 割り当てに関する考慮事項

静的 IP アドレスをサーバー SP または CMM に割り当てることを計画している場合は、次のトピックを確認してください。

- 18 ページの「静的 IP 割り当ての要件」
- 19 ページの「シリアルデバイス ― 端末エミュレーションソフトウェアの設定」
- 19 ページの「静的 IP 割り当て後」

静的 IP 割り当ての要件

最初に静的 IP アドレスをサーバー SP または CMM に割り当てるには、表 2-4 に記載された要件を満たす必要があります。

表 2-4 静的 IP 割り当ての要件

要件	手順	説明
シリアルコンソール接続の確立	1	端末エミュレーションソフトウェアを実行している端末または PC をサーバーまたは CMM のシリアルポートに接続して、サーバー SP または CMM に対するシリアルコンソール接続を確立します。 シリアル端末または PC をサーバーまたは CMM のシリアルポートに接続する方法については、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。 CMM が構成されている Sun サーバープラットフォームの場合は、CMM ILOM コマンド行インタフェースを使用して、シャーシに取り付けられたブレード SP に対して静的 IP アドレスを設定することができます。
シリアルポートの設定	2	端末デバイスまたは端末エミュレーションソフトウェアに必要なシリアル設定を行います。 詳細は、19 ページの「シリアルデバイス ― 端末エミュレーションソフトウェアの設定」を参照してください。
ILOM CLI を使用した静的 IP アドレスの割り当て	3	ILOM CLI を使用して静的 IP アドレスを割り当てます。 詳細は、使用しているシステム構成に該当する次のいずれかのトピックを参照してください。 • 25 ページの「シリアル接続を使用してサーバー SP に静的 IP アドレスを割り当てる」 または • 27 ページの「シリアル接続を使用して CMM に静的 IP アドレスを割り当てる」

シリアルデバイス — 端末エミュレーションソフトウェアの設定

シリアルコンソールを使用して ILOM に接続するときは、次のシリアル設定を使用するように端末デバイスまたは端末エミュレーションソフトウェアを設定する必要があります。

- 8N1: 8 データビット、パリティーなし、1 ストップビット
- 9600 ボー
- ハードウェアのフロー制御無効 (CTS/RTS)
- ソフトウェアのフロー制御無効 (XON/XOFF)

次の CLI `show` コマンドを使用すると、サーバーまたは CMM の外部シリアルポートに関連付けられたプロパティーおよび値を表示することができます。

```
show <target>
```

例

- CMM の場合: `show /CMM/serial/external`
- ラック搭載型のサーバーの場合: `show /SP/serial/external`
- ブレードサーバーモジュールの場合: `show /CH/BLn/SP/serial/external`

静的 IP 割り当て後

次の要件を満たしてから、ILOM Web インタフェースまたは CLI を使用して IP アドレスを遠隔で管理することができます。

- サーバー SP または CMM への IP アドレスの割り当て
- サーバーまたは CMM ネットワーク管理ポートに対する Ethernet 接続の確立

Ethernet ネットワーク管理接続を使用した IP アドレスの割り当ての管理については、29 ページの「Ethernet 管理接続を使用した IP アドレスの割り当ての編集」を参照してください。

管理ネットワーク IP アドレスの設定

ILOM の IP 接続は、通常、SP ネットワークインタフェースに対して設定されるため、管理トラフィックとデータトラフィックを分離することができます。サーバー SP または CMM に割り当てる DHCP または静的 IP アドレスは、データネットワーク IP アドレスと混同しないように、「管理ネットワーク IP アドレス」とも呼ばれます。

データネットワーク IP アドレスは、サーバーにホストオペレーティングシステムをインストールしたあとに設定されます。データネットワーク IP アドレスと管理ネットワーク IP アドレスでは目的が異なるため、これらを区別することは重要です。

このマニュアルでは、これ以降、管理ネットワーク IP アドレスを参照する場合は、「サーバー SP の IP アドレス」または「CMM の IP アドレス」と表記します。一般に、ILOM Web インタフェースまたは ILOM CLI に対して接続する手順を説明するときに、この表記を使用しています。

ILOM の管理ネットワークについては、3 ページの「ILOM 管理ネットワーク」を参照してください。

データネットワーク IP アドレスをサーバーに割り当てる方法については、ホストオペレーティングシステムに付属のユーザーマニュアルを参照してください。

ILOM ネットワークポートの割り当て

表 2-5 と表 2-6 に、ILOM で使用されるデフォルトのネットワークポートを示します。これらのネットワークポートのほとんどは、設定可能です。ILOM に対するファイアウォールによるセキュリティーアクセスを設定する場合は、ファイアウォールサービスで現在使用されている適切なポートでこれらのポートを設定するようにしてください。

表 2-5 サーバー SP の ILOM ポートの直接割り当て

ポート	プロトコル	適用
80	HTTP over TCP	SP - ILOM ユーザー設定可能ポート
443	HTTPS over TCP	SP - ILOM ユーザー設定可能ポート
5120	TCP	SP - ILOM リモートコンソール: CD
5123	TCP	SP - ILOM リモートコンソール: フロッピーディスク
5121	TCP	SP - ILOM リモートコンソール: キーボードおよびマウス
7578	TCP	SP - ILOM リモートコンソール: ビデオ
22	SSH over TCP	SSH - Secure Shell
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol

表 2-5　サーバー SP の ILOM ポートの直接割り当て (続き)

123	NTP over UDP	NTP - 時間情報プロトコル
161	SNMP over UDP	SNMP - Simple Network Management Protocol
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (送信ポート)
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (ユーザー設定可能ポート)
514	Syslog over UDP	Syslog - (送信ポート)
546	DHCP over UDP	DHCP - 動的ホスト構成プロトコル (クライアント)
623	IPMI over UDP	IPMI - Intelligent Platform Management Interface
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial In User Service

表 2-6　CMM の ILOM ネットワークポートの直接割り当て

ポート	プロトコル	適用
80	HTTP over TCP	CMM - ILOM (ユーザー設定可能ポート)
443	HTTPS over TCP	CMM - ILOM (ユーザー設定可能ポート)
8000 ～ 8009	HTTP over TCP	CMM - ILOM ドリルダウン (BL0 ～ BL9)
8400 ～ 8409	HTTPS over TCP	CMM - ILOM ドリルダウン (BL0 ～ BL9)
22	SSH over TCP	SSH - Secure Shell
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol
123	NTP over UDP	NTP - 時間情報プロトコル
161	SNMP over UDP	SNMP - Simple Network Management Protocol
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (ユーザー設定可能ポート)
514	Syslog over UDP	Syslog - (送信ポート)
546	DHCP over UDP	DHCP - 動的ホスト構成プロトコル (クライアント)
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial In User Service

サーバー SP および CMM のホスト名の識別情報

IP アドレスの代わりにホスト名を使用して、ネットワークの特定のサーバー SP または CMM を識別することができます。また、ホスト名を使用して、サーバー SP ILOM または CMM ILOM との通信を確立することもできます。通常、この種類のシステム識別および接続では、ネームサービス (DNS、NIS、SMB など) でホスト名をサーバー SP (または CMM) の IP アドレスに関連付けることが必要です。使用しているネットワーク環境でホスト名を使用してサーバー SP または CMM を識別する場合は、「System Identification」ページでサーバー SP (または CMM) のホスト名を入力することにより、ILOM で同じ識別方法をサーバー SP または CMM に任意で適用することも可能です。詳細は、33 ページの「Web インタフェースを使用してホスト名およびシステム識別子を割り当てる」を参照してください。

Sun サーバーのシステム識別子テキスト文字列

システム識別子は、Sun システムのコンポーネントを識別できるように設定可能なテキスト文字列です。たとえば、システムの場所、ラック内の特定のサーバー、またはシステムの目的に関する説明などを識別するシステム識別子を作成できます。

システム識別子は、SNMP トラップにも含まれます。これらのシステム識別子を使用すると、システムで実行中の特定の ILOM インスタンスとトラップとを関連付けることができます。

ILOM でシステム識別子を設定するときは、システムまたはコンポーネントを説明する任意のテキスト文字 (引用符を除く) を使用できます。ILOM でシステム識別子を指定する方法については、33 ページの「ホスト名またはシステム識別子の割り当て」を参照してください。

Sun サーバープラットフォーム SP インタフェースへの IP アドレスの割り当て

次の手順を使用して、IP アドレスを Sun サーバープラットフォームの SP ネットワークインタフェースに割り当てます。

- 23 ページの「Ethernet 管理接続を使用して DHCP IP アドレスを割り当てる」
- 25 ページの「シリアル接続を使用してサーバー SP に静的 IP アドレスを割り当てる」
- 27 ページの「シリアル接続を使用して CMM に静的 IP アドレスを割り当てる」
- 33 ページの「Web インタフェースを使用してホスト名およびシステム識別子を割り当てる」
- 34 ページの「CLI を使用してホスト名およびシステム識別子を割り当てる」

▼ Ethernet 管理接続を使用して DHCP IP アドレスを割り当てる

次の手順に従って、DHCP を使用して IP アドレスを割り当てます。

1. **DHCP サーバーが新しいメディアアクセス制御 (MAC) アドレスを受け入れるよう設定されていることを確認します。**

   使用している DHCP サーバーソフトウェアに付属のマニュアルを参照してください。

2. **Ethernet ケーブルが次のいずれかのポートに接続されていることを確認します。**
   - CMM の Ethernet ポート (NET MGT) (該当する場合)
   - ラック搭載型のスタンドアロンサーバーの Ethernet ポート (MGT) (該当する場合)

注 – ILOM がこれまで静的 IP アドレスで設定されていなかった場合、ILOM は自身の SP ネットワークインタフェースにおける MAC アドレスの ID を使用して DHCPDISCOVER パケットを自動的にブロードキャストします。ILOM がこれまで静的 IP アドレスで設定されていた場合は、「Network Settings (ネットワーク設定)」タブで静的 IP アドレスの設定を無効にする必要があります。IP アドレス設定の編集については、29 ページの「Ethernet 管理接続を使用した IP アドレスの割り当ての編集」を参照してください。

---

3. ネットワーク上の DHCP サーバーは、IP アドレスやその他の情報を含む DHCPOFFER パケットを返します。次に、サービスプロセッサが、DHCP サーバーによって割り当てられた IP アドレスの「リース」状況を管理します。

4. 次のいずれかの方法を使用して、SP ネットワークインタフェースに割り当てられた DHCP IP アドレスを取得します。

   - シリアル接続を使用した ILOM - CMM

     CMM の背面パネルに接続されたシリアルコンソールを使用して、ILOM に管理者としてログインします。たとえば、ログインプロンプトで、事前構成されている管理者ユーザー名 `root` とそのデフォルトのパスワード `changeme` を入力して、Enter を押します。

     - アクティブな CMM の作業用ディレクトリを設定するには、次のように入力します。
       `cd /CMM/network/CMM0`
     - アクティブな CMM の IP アドレスを表示するには、次のように入力します。
       `show`
     - 各ブレードの IP アドレスをドリルダウンして表示するには、次のように入力します。
       `show /CH/BL0/SP/network`

注 – CMM0 は、スロット CMM0 に取り付けられた CMM を表します。BL0 は、スロット BL0 に取り付けられたブレードを表します。ターゲットの CMM またはブレードを指定するには、モジュールが取り付けられているスロットの番号を指定する必要があります。ブレードのスロットの範囲は 0 ～ 9 です。CMM のスロットの範囲は 0 ～ 1 です。

   - シリアル接続を使用した ILOM - サーバー SP

     ブレードのフロントパネルに接続されたシリアルコンソールを使用して、ILOM に管理者としてログインします。たとえば、ログインプロンプトで、事前構成されている管理者ユーザー名 `root` とそのデフォルトのパスワード `changeme` を入力して、Enter を押します。

     - ブレード SP の IP アドレスを表示するには、次のように入力します。
       `show /SP/network`

   - DHCP サーバーログ

     詳細は、17 ページの「DHCP 後の要件」、または DHCP サーバーのマニュアルを参照してください。

▼ シリアル接続を使用してサーバー SP に静的 IP アドレスを割り当てる

次の手順に従って、シリアル接続を使用して静的 IP アドレスをサーバー SP に割り当てます。

1. **サーバー SP に対するローカルシリアルコンソール接続を確立します。**

   サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

2. **接続したシリアルコンソールに表示される端末ウィンドウで、次の設定を行います。**
   - 8N1: 8 データビット、パリティーなし、1 ストップビット
   - 9600 ボー
   - ハードウェアのフロー制御無効 (CTS/RTS)
   - ソフトウェアのフロー制御無効 (XON/XOFF)

3. **Enter を押して、シリアルコンソールと SP インタフェースの間の接続を確立します。**

   最終的に ILOM のログインプロンプトが表示されます。

   例: *host name* `Login:`

4. **管理者のユーザー名およびパスワードを入力して管理者としてログインしてから、Enter を押します。**

   注 – ILOM の出荷時に事前構成されている管理者アカウント `root/changeme` を使用して ILOM にログインできます。詳細は、6 ページの「事前構成された ILOM 管理者アカウント」を参照してください。

   デフォルトのプロンプト (->) が表示されます。システムでは、ネットワーク設定を確立する CLI コマンドを受信する準備ができました。

5. **次のコマンドを入力して、作業用ディレクトリを設定します。**

   `cd /SP/network`

6. 次の CLI コマンドを使用して、IP、ネットマスク、およびゲートウェイのアドレスを指定します。

コマンド	説明および例
`set pendingipaddress=`	このコマンドに続けて、サーバー SP に割り当てる静的 IP アドレスを入力します。 たとえば、次のように入力します。 `set pendingipaddress=129.144.82.26` これは、`129.144.82.26` を IP アドレスとしてサーバー SP に割り当てるように、ILOM に指示します。
`set pendingipnetmask=`	このコマンドに続けて、サーバー SP に割り当てる静的ネットマスクアドレスを入力します。 たとえば、次のように入力します。 `set pendingipnetmask=255.255.255.0` これは、`255.255.255.0` をネットマスクアドレスとしてサーバー SP に割り当てるように、ILOM に指示します。
`set pendingipgateway=`	このコマンドに続けて、サーバー SP に割り当てる静的ゲートウェイアドレスを入力します。 たとえば、次のように入力します。 `set pendingipgateway=129.144.82.254` これは、`129.144.82.254` をゲートウェイアドレスとしてサーバー SP に割り当てるように、ILOM に指示します。
`setpendingipdiscovery=`	サーバー SP に静的 IP アドレスを設定するように ILOM に指示するには、次のコマンドを入力します。 `set pendingipdiscovery=static`

`set commitpending=true`	このコマンド (`true`) を入力すると、指定したネットワーク設定が割り当てられます。
	
	例:
	`set pendingipaddress=129.144.82.26`
	`set pendingipnetmask=255.255.255.0`
	`set pendingipnetmask=129.144.82.254`
	`set commitpending=true`

通常、IP アドレスの割り当てまたは変更を行うと、以前の IP アドレスを使用して確立された ILOM への接続はタイムアウトします。ILOM に接続するには、新しく割り当てた IP アドレスを使用します。

▼ シリアル接続を使用して CMM に静的 IP アドレスを割り当てる

次の手順に従って、シリアル接続を使用して静的 IP アドレスを CMM に割り当てます。

1. **アクティブな CMM に対するシリアル接続が動作していることを確認します。**

   シリアルコンソールを CMM に接続する方法については、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

2. **管理者のユーザー名およびパスワードを入力して管理者としてログインしてから、Enter を押します。**

注 – ILOM の出荷時に事前構成されている管理者アカウント `root/changeme` を使用して ILOM にログインできます。詳細は、6 ページの「事前構成された ILOM 管理者アカウント」を参照してください。

デフォルトのプロンプト (->) が表示され、システムではネットワーク設定を確立する CLI コマンドを実行する準備ができました。

3. **ILOM CLI を使用して CMM に静的 IP アドレスを設定するには、次のコマンドを入力して作業用ディレクトリを設定します。**

   `cd /CMM/network/CMM0`

注 – CMM0 は、スロット CMM0 に取り付けられた CMM を表します。ターゲット CMM は、CMM のスロット番号を参照して指定します。

---

4. 次のコマンドを使用して、IP、ネットマスク、およびゲートウェイのアドレスを指定します。

コマンド	説明および例
`set pendingipaddress=`	このコマンドに続けて、CMM に割り当てる静的 IP アドレスを入力します。 たとえば、次のように入力します。`set pendingipaddress=129.144.82.26` これは、`129.144.82.26` を CMM IP アドレスとして割り当てるように、ILOM に指示します。
`set pendingipnetmask=`	このコマンドに続けて、CMM に割り当てる静的ネットマスクアドレスを入力します。 たとえば、次のように入力します。`set pendingipnetmask=255.255.255.0` これは、`255.255.255.0` を CMM ネットマスクアドレスとして割り当てるように、ILOM に指示します。
`set pendingipgateway=`	このコマンドに続けて、CMM に割り当てる静的ゲートウェイアドレスを入力します。 たとえば、次のように入力します。 `set pendingipgateway=129.144.82.254` これは、`129.144.82.254` を CMM ゲートウェイアドレスとして割り当てるように、ILOM に指示します。
`set pendingipdiscovery=`	静的 IP アドレスを設定するように ILOM に指示するには、次のコマンドを入力します。 `set pendingipdiscovery=static`

`set commitpending=true`	このコマンド (`true`) を入力すると、指定したネットワーク設定が割り当てられます。
	
	例:
	`set pendingipaddress=129.144.82.26`
	`set pendingipnetmask=255.255.255.0`
	`set pendingipgateway=129.144.82.254`
	`set comitpending=true`

遠隔 SSH 接続を使用して ILOM に接続した場合、以前の IP アドレスを使用して確立された ILOM への接続はタイムアウトします。ILOM に接続するには、新しく割り当てた IP アドレスを使用します。

Ethernet 管理接続を使用した IP アドレスの割り当ての編集

次の手順を使用して、Ethernet 管理接続でサービスプロセッサの IP 割り当てを管理します。

- 29 ページの「Web インタフェースを使用して ILOM の既存の IP アドレスを編集する」
- 31 ページの「CLI を使用して ILOM の既存の IP アドレスを編集する」

▼ Web インタフェースを使用して ILOM の既存の IP アドレスを編集する

サーバー SP または CMM に以前に割り当てられた既存の IP アドレスを、ILOM Web インタフェースを使用して編集するには、次の手順を実行します。

1. **ブラウザベースのクライアントを使用して、サーバー SP または CMM の IP アドレスをブラウザのアドレスボックスに入力し、Enter を押します。**

   ILOM のログイン画面が表示されます。

2. **ILOM のログイン画面で、管理者のユーザー名およびパスワードを入力して管理者としてログインします。**

   参考 – ILOM の出荷時に事前構成されている管理者アカウント `root/changeme` を使用して ILOM にログインできます。詳細は、6 ページの「事前構成された ILOM 管理者アカウント」を参照してください。

   ILOM インタフェースが表示されます。

3. **ILOM インタフェースの右区画で、「Configuration (設定)」-->「Network (ネットワーク)」をクリックします。**

   サーバーまたは CMM の「Network Settings (ネットワーク設定)」ページが表示されます。

図 2-1　　ILOM サーバー SP ー「Network Settings (ネットワーク設定)」ページ

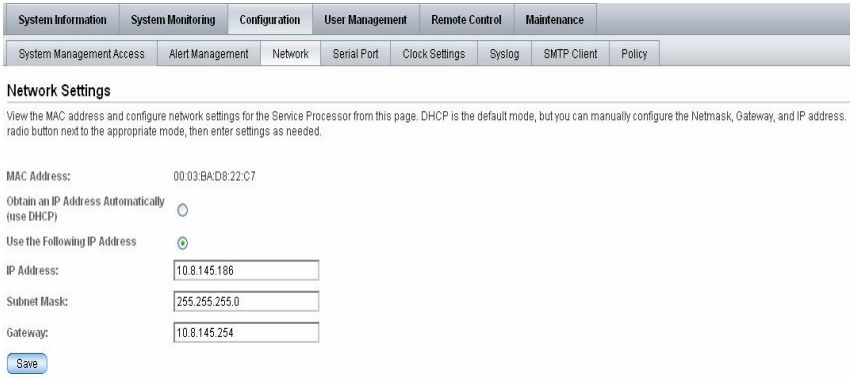
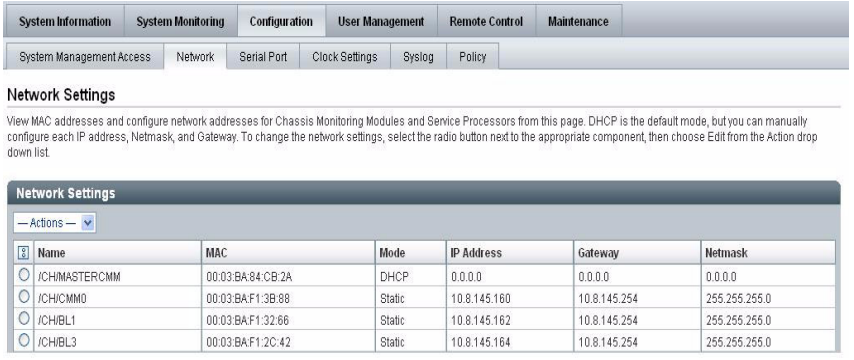


図 2-2　　ILOM CMM ー「Network Settings (ネットワーク設定)」ページ



4. SP インタフェースに割り当てられた IP アドレスを編集するには、次の手順を実行します。

   a. 「Use the Following IP Address (次の IP アドレスを使用)」のラジオボタンを選択します。

   b. テキストボックスに IP アドレス、サブネットマスク、およびゲートウェイの値を入力します。

   c. 「Save (保存)」をクリックして新しい設定を有効にします。

   通常、IP アドレスの割り当てまたは変更を行うと、以前の IP アドレスを使用して確立された ILOM への接続はタイムアウトします。ILOM に接続するには、新しく割り当てた IP アドレスを使用します。

▼ CLI を使用して ILOM の既存の IP アドレスを編集する

サーバー SP または CMM に以前に割り当てられた既存の IP アドレスを、ILOM CLI を使用して編集するには、次の手順を実行します。

1. **サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。**
   - **ローカルシリアルコンソール接続**

     サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

     詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

   または

   - **遠隔 Secure Shell (SSH) 接続**

     サーバー SP または CMM との Secure Shell 接続を確立します。

     遠隔クライアントから、root としてサーバー SP または CMM へのセキュリティー保護された接続を確立します。たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

     ```
     ssh -l root server_ip_address
     ```

     ```
     パスワード: changeme
     ```

   デフォルトのプロンプト (->) が表示され、システムではネットワーク設定を確立する CLI コマンドを実行する準備ができました。

2. **次のいずれかのコマンドを入力して、SP の作業用ディレクトリを設定します。**
   - ラック搭載型のスタンドアロンサーバーの場合: `cd /SP/network`
   - シャーシブレードサーバーモジュールの場合: `cd /SP/network`
   - スロット 0 のシャーシ CMM の場合: `cd /CMM/network/CMM0`
   - スロット 1 のシャーシ CMM の場合: `cd /CMM/network/CMM1`
3. **次のように `show` コマンドを入力して、割り当てられている IP アドレスを表示します。**
   - ラック搭載型のスタンドアロンサーバーの場合: `show /SP/network`
   - シャーシブレードサーバーモジュールの場合: `show /CH/BL`*n*`/SP network`
   - スロット 0 のシャーシ CMM の場合: `show /CMM/network/CMM0`
   - スロット 1 のシャーシ CMM の場合: `show /CMM/network/CMM1`

4. 次のコマンドを入力して、割り当てられている既存の IP アドレスを変更します。

コマンド	説明および例
`set pendingipaddress=`	このコマンドに続けて、サーバー SP または CMM に割り当てる静的 IP アドレスを入力します。 たとえば、次のように入力します。 `set pendingipaddress=129.144.82.26` これは、`129.144.82.26` を IP アドレスとしてサーバー SP に割り当てるように、ILOM に指示します。
`set pendingipnetmask=`	このコマンドに続けて、サーバー SP または CMM に割り当てる静的ネットマスクアドレスを入力します。 たとえば、次のように入力します。 `set pendingipnetmask=255.255.255.0` これは、`255.255.255.0` をネットマスクアドレスとしてサーバー SP または CMM に割り当てるように、ILOM に指示します。
`set pendingipgateway=`	このコマンドに続けて、サーバー SP または CMM に割り当てる静的ゲートウェイアドレスを入力します。 たとえば、次のように入力します。 `set pendingipgateway=129.144.82.254` これは、`129.144.82.254` をゲートウェイアドレスとしてサーバー SP または CMM に割り当てるように、ILOM に指示します。
`setpendingipdiscovery=`	サーバー SP または CMM に対して静的 IP アドレスを設定するように ILOM に指示するには、次のコマンドを入力します。 `set pendingipdiscovery=static`

`set commitpending=true`	このコマンド (`true`) を入力すると、指定したネットワーク設定が割り当てられます。
	
	例:
	`set pendingipaddress=129.144.82.26`
	`set pendingipnetmask=255.255.255.0`
	`set pendingipnetmask=129.144.82.254`
	`set commitpending=true`

遠隔 SSH 接続を使用して ILOM に接続した場合、以前の IP アドレスを使用して確立された ILOM への接続はタイムアウトします。ILOM に接続するには、新しく割り当てた IP アドレスを使用します。

ホスト名またはシステム識別子の割り当て

ネットワークの Sun サーバー SP または CMM を識別するためにホスト名を使用する場合は、サーバー SP または CMM と同じ識別情報 (ホスト名) をバナーに表示するように ILOM を設定することができます。また、ネットワークでのシステムの識別に役立つ、わかりやすいテキスト文字列で ILOM を設定することもできます。ILOM でホスト名またはシステム識別のテキスト文字列を割り当てる詳細な手順については、次の節を参照してください。

- 33 ページの「Web インタフェースを使用してホスト名およびシステム識別子を割り当てる」
- 34 ページの「CLI を使用してホスト名およびシステム識別子を割り当てる」

ホスト名の割り当てに関する詳細情報や、システム識別子テキスト文字列の例については、22 ページの「サーバー SP および CMM のホスト名の識別情報」、または 22 ページの「Sun サーバーのシステム識別子テキスト文字列」を参照してください。

▼ Web インタフェースを使用してホスト名およびシステム識別子を割り当てる

次の手順に従って、Web インタフェースを使用して、ILOM でホスト名またはシステム識別子を割り当てます。

1. **ブラウザベースのクライアントを使用して、サーバー SP の IP アドレスをブラウザのアドレスボックスに入力し、Enter を押します。**

   ILOM のログインダイアログが表示されます。

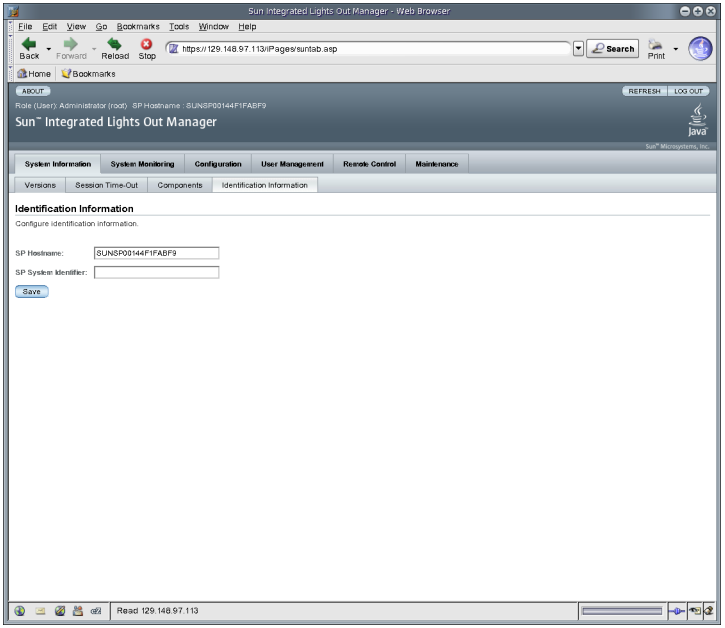
2. **ILOM のログインダイアログで、管理者のユーザー名およびパスワードを入力して管理者としてログインします。**

   ILOM インタフェースが表示されます。

3. **「System Information (システム情報)」-->「Identification Information」を選択します。**

   「Identification Information」ページが表示されます。

図 2-3　「Identification Information」ページ



4. 「SP Hostname」フィールドで、SP ホスト名を入力します。

   ホスト名には英数字を使用でき、ハイフンを含めることができます。

5. 「SP System Identifier」フィールドで、システムを識別するために使用するテキストを入力します。

   システム識別子には、標準的なキーボードの任意のキーを使用したテキスト文字列を使用できます。ただし、引用符は除きます。

6. 「Save (保存)」をクリックして設定を有効にしてください。

▼ CLI を使用してホスト名およびシステム識別子を割り当てる

次の手順に従って、CLI を使用して、ILOM でホスト名またはシステム識別子を割り当てます。

1. サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。

   ■ ローカルシリアルコンソール接続

サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

または

- **遠隔 Secure Shell (SSH) 接続**

  サーバー SP または CMM との Secure Shell 接続を確立します。

  遠隔クライアントから、root としてサーバー SP または CMM へのセキュリティー保護された接続を確立します。たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

  ```
  ssh -l root server_ip_address
  ```

  ```
  パスワード: changeme
  ```

デフォルトのプロンプト (->) が表示され、システムではネットワーク設定を確立する CLI コマンドを実行する準備ができました。

2. **SP ホスト名およびシステム識別子のテキストを設定するには、コマンドプロンプトで次のように入力します。**

   -> **set /SP hostname=***text_string*

   -> **set /SP system_identifier=***text_string*

   ホスト名には英数字を使用でき、ハイフンを含めることができます。システム識別子には、標準的なキーボードの任意のキーを使用したテキスト文字列を使用できます。ただし、引用符は除きます。

第3章

ILOM コマンド行インタフェースおよびログイン

ILOM コマンド行インタフェース (CLI) を使用すると、キーボードコマンドを使用して多くの ILOM の機能を設定および管理することができます。ILOM Web インタフェースを使用して実行可能なあらゆるタスクに対して、同等の ILOM CLI コマンドが用意されています。

この章には次の節があります。

注 – この章の構文例では、`/SP/` で始まるターゲットを使用しますが、使用している Sun サーバープラットフォームによっては、`/CMM/` で始まるターゲットに置き換わる場合があります。サブターゲットは、すべての Sun サーバープラットフォームで共通です。

CLI の概要

ILOM コマンド行インタフェース (CLI) は、Distributed Management Task Force 仕様の『Server Management Command-Line Protocol Specification, version 11.0a.8 Draft』(DMTF CLP) に準拠しています。この仕様全体は、次のサイトで参照できます。

`http://www.dmtf.org/standards/published_documents/DSP0214.pdf`

DMTF CLP には、サーバーの状態、アクセス方法、またはインストールされているオペレーティングシステムにかかわらず、1 つ以上のサーバーを対象にした管理インタフェースがあります。

DMTF CLP アーキテクチャーでは、階層的なネームスペースをモデル化しており、システム管理下にあるすべてのオブジェクトを含むツリーがあらかじめ定義されています。このモデルでは、少数のコマンドを使用してターゲットの大きなネームスペースを操作します。ターゲットは、オプションやプロパティーで変更できます。このネームスペースでは、各コマンド動詞のターゲットが定義されています。

CLI 階層アーキテクチャー

次の表に、ILOM CLI で使用できるさまざまな階層方式を示します。使用できる方式は、使用している特定の Sun サーバープラットフォームによって異なります。

表 3-1 ILOM のターゲットの種類

ターゲットの種類	説明
* `/SP`	このターゲットの種類の下にあるターゲットおよびプロパティーは、ILOM サービスプロセッサ (SP) の設定や、ログおよびコンソールの表示に使用されます。
* `/CMM`	ブレードプラットフォームでは、このターゲットの種類が `/SP` の代わりになり、ILOM シャーシ監視モジュール (CMM) の設定に使用されます。
* `/SYS`	このターゲットの種類の下にあるターゲットおよびプロパティーは、インベントリ、環境、およびハードウェアの管理を提供します。ターゲットは、すべてのハードウェアコンポーネントの命名法に直接対応しており、その一部は物理的なハードウェアに印字されています。

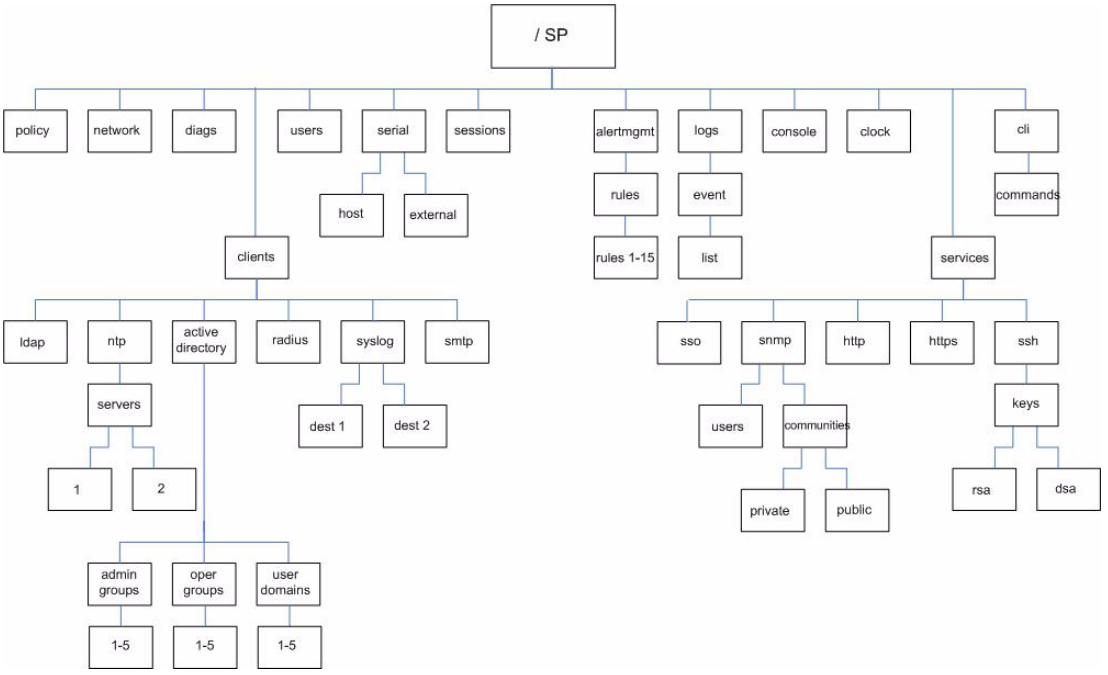
表 3-1　ILOM のターゲットの種類 (続き)

ターゲットの種類	説明
* /CH	ブレードプラットフォームでは、このターゲットの種類が /SYS の代わりになり、シャーシレベルのインベントリ、環境、およびハードウェアの管理を提供します。ターゲットの種類は、すべてのハードウェアコンポーネントの命名法に直接対応しており、その一部は物理的なハードウェアに印字されています。
* /HOST	このターゲットの種類の下にあるターゲットおよびプロパティーは、ホストオペレーティングシステムの監視および管理に使用されます。これは、SPARC システムでのみ使用可能です。

注 – 階層内のこれらのサブツリーの一部にアクセスする方法は、使用している Sun サーバープラットフォームによって異なります。

サービスプロセッサは、/SP ネームスペースと、システム全体のネームスペースである /SYS の 2 つのネームスペースにアクセスできます。/SP ネームスペースでは、サービスプロセッサの管理および設定を行うことができます。/SYS ネームスペースでは、管理対象システムハードウェアのセンサーおよびその他の情報にアクセスできます。

図 3-1　　ILOM CLI ターゲットツリーにおける /SP の例



ユーザーの権限レベルについては、5 ページの「ILOM ユーザーアカウントの役割」を参照してください。

CLI コマンド構文

ILOM CLI を使用するときは、情報を次の順序で入力します。

コマンド構文: `<command> <options> <target> <properties>`

次の節で、構文の各部分に関する詳細情報について説明します。

CLI コマンド

ILOM CLI では、次の表に示す DMTF CLP コマンドをサポートしています。

CLI コマンドの大文字と小文字は区別されます。

表 3-2 CLI コマンド

コマンド	説明
cd	オブジェクトのネームスペースを操作します。
create	ネームスペースにオブジェクトを作成します。
delete	ネームスペースからオブジェクトを削除します。
exit	CLI のセッションを終了します。
help	コマンドとターゲットに関するヘルプ情報を表示します。
load	指定されたソースから指定されたターゲットにファイルを転送します。
reset	ターゲットの状態をリセットします。
set	ターゲットのプロパティを指定した値に設定します。
show	ターゲットとプロパティについての情報を表示します。
start	ターゲットを起動します。
stop	ターゲットを停止します。
version	実行中のサービスプロセッサのバージョンを表示します。

コマンドのオプション

ILOM CLI では、次のオプションをサポートしていますが、コマンドによってはサポートしていないオプションがあります。help オプションと examine オプションは、どのコマンドでも使用できます。

表 3-3 CLI オプション

長文形式オプション	省略形式	説明
-default		コマンドのデフォルト機能のみを実行します。
-destination		データの宛先を指定します。
-display	-d	ユーザーが表示したいデータを表示します。
-help	-h	ヘルプ情報を表示します。

表 3-3　CLI オプション (続き)

長文形式オプション	省略形式	説明
-level	-l	現在のターゲットと、特定レベルのすべてのターゲットのコマンドを実行します。
-output	-o	コマンド出力の内容と形式を指定します。ILOM では、表形式でターゲットおよびプロパティーを表示する -o table のみをサポートしています。
-script		コマンドに関連する通常の警告またはプロンプトをスキップします。
-source		ソースイメージの場所を表示します。

コマンドのターゲット

ネームスペースのすべてのオブジェクトはターゲットです。

コマンドのプロパティー

プロパティは、設定可能な属性であり、各オブジェクトに固有です。

コマンドの実行

ほとんどのコマンドでは、実行するにはターゲットの場所を指定してからコマンドを入力します。これらの操作は、個別に実行することも、同じコマンド行で組み合わせることもできます。

▼ コマンドを個別に実行する

1. cd コマンドを使用して、ネームスペースに移動します。

   例:

   ```
   cd /SP/services/http
   ```

2. コマンド、ターゲット、および値を入力します。

例:

```
set port=80
```

または

```
set prop1=x
set prop2=y
```

▼ 組み合わせたコマンドを実行する

- <command><target>=*value* という構文を使用して、単一のコマンド行でコマンドを入力します。

例:

```
set /SP/services/http port=80
```

または

```
set /SP/services/http prop1=x prop2=y
```

次の表に、個別のコマンドおよび組み合わせたコマンドの実行方法についての例と説明を示します。

表 3-4 個別のコマンドおよび組み合わせたコマンドの実行

コマンド構文	コマンドの説明
コマンドを個別に実行する場合: > **cd /SP/services/http**	ネームスペース /SP/services/http に移動する
> **set port=80**	コマンド、ターゲット、および値を入力して、「port」に「80」を設定する
組み合わせたコマンドを実行する場合: > **cd /SP/services/http port=80**	ネームスペース /SP/services/http で、ターゲット「port」に「80」を設定する

CLI を使用した ILOM への接続

この節では、ILOM に対するログインおよびログアウトの方法について説明します。まず、ILOM CLI にログインする前に、ILOM を設定する方法について 23 ページの「Sun サーバープラットフォーム SP インタフェースへの IP アドレスの割り当て」を参照しておくことをお勧めします。

ILOM は、シリアル、SSH、および Web インタフェースセッションを含む、最大 10 個のアクティブセッションをサポートしています。ILOM への Telnet 接続はサポートされていません。

▼ ILOM にログインする

ILOM CLI には、Secure Shell (SSH) またはシリアル接続によって遠隔でアクセスできます。Secure Shell 接続はデフォルトで有効になっています。

次の手順に、UNIX システムで SSH クライアントを使用する例を示します。使用しているオペレーティングシステムに適した SSH クライアントを使用します。デフォルトのユーザー名は `root`、デフォルトのパスワードは `changeme` です。

デフォルトの有効な SSH 接続を使用して ILOM にログインするには、次の手順に従います。

1. ILOM にログインするには、次のコマンドを入力します。

   ```
   $ ssh root@ipaddress
   ```

   ipaddress はサーバー SP の IP アドレスです。

2. プロンプトが表示されたら、このパスワードを入力します。

   ```
   Password: changeme
   ```

   デフォルトのユーザー名およびパスワードを使用して ILOM にログインしたら、ILOM の root アカウントのパスワード (`changeme`) を変更するようにしてください。root アカウントのパスワードの変更については、69 ページの「CLI を使用して ILOM の root アカウントのパスワードを変更する」を参照してください。

▼ ILOM からログアウトする

ILOM からログアウトするには、次の手順に従います。

- ILOM からログアウトするには、次のコマンドを入力します。

  ```
  -> exit
  ```

第4章

ILOM Web インタフェースおよびログイン

ILOM では、多くの Web ブラウザで動作する、使いやすい Web インタフェースをサポートしています。この Web インタフェースを使用して、ILOM が提供するすべての機能にアクセスできます。

この章には次の節があります。

Web インタフェースの概要

ILOM Web インタフェースはブラウザからアクセス可能で、Sun 標準のインタフェースを使用しています。ILOM Web インタフェースを使用すると、ローカルおよび遠隔システムの監視および管理をすることができます。ILOM のもっとも強力な機能の 1 つに、サーバーのグラフィカルコンソールをローカルのワークステーションまたはラップトップシステムにリダイレクトする機能があります。ホストのコンソールをリダイレクトすると、ローカルシステムのキーボードおよびマウスを、サーバーのマウスおよびキーボードとして動作するように設定することができます。さらに、遠隔システムのフロッピーディスクドライブまたは CD-ROM ドライブを、Sun システムに接続した仮想デバイスとして設定することができます。これらの機能には、

ILOM リモートコンソールアプリケーションを使用してアクセスできます。リモートコンソールの詳細は、第 12 章を参照してください。Web インタフェースでは、役割と権限が定義されたユーザーアカウントが用意されています。権限のレベルの詳細は、5 ページの「ILOM ユーザーアカウントの役割」を参照してください。

ブラウザおよびソフトウェアの要件

Web インタフェースは、新たにリリースされた Mozilla、Firefox、および Internet Explorer Web ブラウザで正常にテストされていますが、ほかの Web ブラウザとも互換性がある可能性があります。

単体のブラウザでは、ILOM Web インタフェースの 1 つのインスタンスのみを起動できます。同じブラウザで ILOM Web インタフェースの複数のインスタンスを起動しようとすると、Web インタフェースの最初のインスタンスのみが表示されます。

次のオペレーティングシステムと Web ブラウザは、ILOM と互換性があることが分かっています。

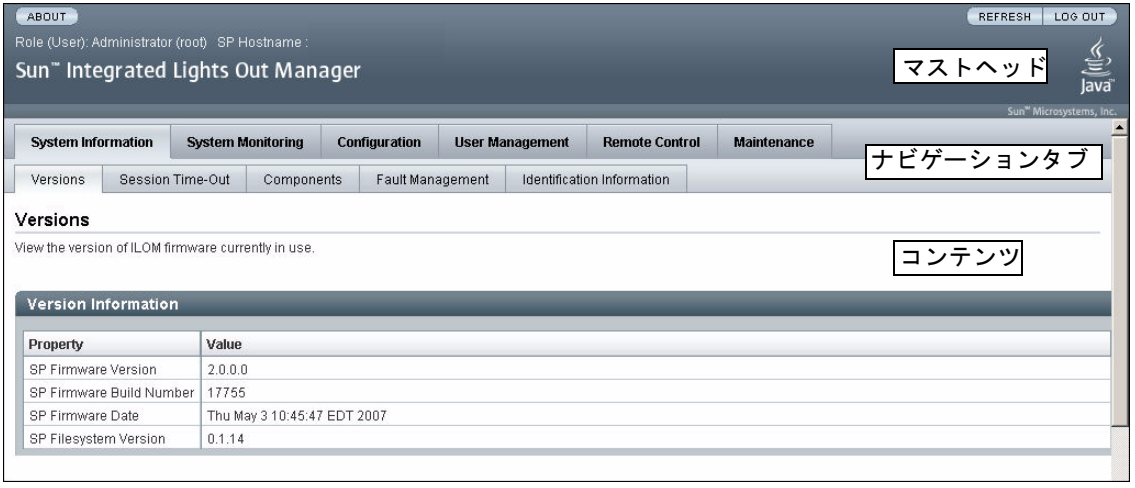
- Solaris (9 および 10)
  - Mozilla 1.4 および 1.7
  - Firefox 1.x 以降
- Linux (Red Hat、SuSE、Ubuntu)
  - Mozilla 1.x 以降
  - Firefox 1.x 以降
  - Opera 6.x 以降
- Microsoft Windows (98、2000、XP、Vista)
  - Internet Explorer 5.5、6.x、7.x
  - Mozilla 1.x 以降
  - Firefox 1.x 以降
  - Opera 6.x 以降
- Macintosh (OSX v10.1 以降)
  - Internet Explorer 5.2
  - Mozilla 1.x 以降
  - Firefox 1.x 以降
  - Safari すべて

注 – ILOM は Sun のシステムにプリインストールされており、リモートコンソールアプリケーションも含まれています。ILOM リモートコンソールを実行するには、Java Runtime Environment 1.5 (JRE 1.5) またはそれ以降のバージョンの JRE ソフトウェアがローカルクライアントにインストールされている必要があります。JRE ソフトウェアをダウンロードするには、`http://java.com` にアクセスしてください。リモートコンソールの詳細は、第 12 章を参照してください。

Web インタフェースのコンポーネント

ILOM Web インタフェースのメインページは次のようになっています。

図 4-1 ILOM Web インタフェースのメインページ



Web インタフェースの各ページには、マストヘッド、ナビゲーションタブ、およびコンテンツという 3 つのメインエリアがあります。

注 – シャーシ監視モジュール (CMM) で ILOM Web インタフェースを使用する場合、Web インタフェースにはナビゲーション区画と呼ばれる別のコンポーネントがあります。

マストヘッドには、Web インタフェースの各ページにおいて、次のボタンと情報が提供されます。

- **「About (このソフトウェアについて)」ボタン** − クリックすると、製品情報および著作権情報を表示します。
- **「User (ユーザー)」フィールド** − Web インタフェースの現在のユーザーのユーザー名とユーザーの役割を表示します。
- **「Server (サーバー)」フィールド** − ILOM SP または CMM のホスト名を表示します。
- **「Refresh (リフレッシュ)」ボタン** − クリックすると、ページのコンテンツエリアの情報を再表示します。「Refresh」ボタンは、ページで入力または選択した新しいデータを保存しません。
- **「Log Out (ログアウト)」ボタン** − クリックすると、Web インタフェースの現在のセッションを終了します。

注 – Web インタフェースの使用中は、Web ブラウザの「Refresh (リフレッシュ)」ボタンを使用しないでください。

ILOM Web インタフェースのナビゲーション構造にはタブおよび第 2 レベルのタブがあります。これをクリックして特定のページを開くことができます。メインのタブをクリックすると、第 2 レベルのタブが表示され、さらにオプションが表示されます。追加情報は、48 ページの「ナビゲーションタブのコンポーネント」を参照してください。

コンテンツエリアは、特定のトピックまたは操作に関する情報が表示される場所です。

ナビゲーションタブのコンポーネント

次の節では、Web インタフェースのもっとも一般的な ILOM コンポーネントにある各種タブおよび第 2 レベルのタブについて説明します。これらの各エリアに関する詳細は、このマニュアルの個々の章で説明しています。

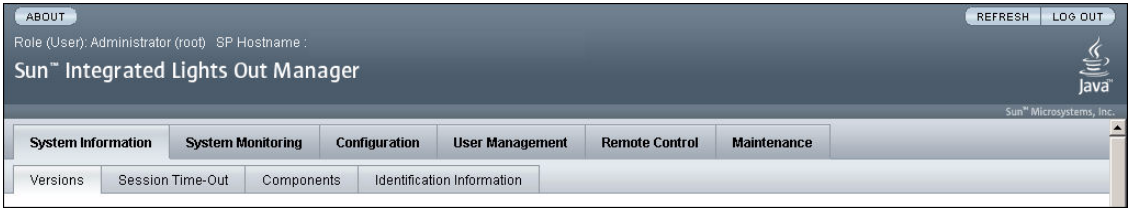
「System Information (システム情報)」タブ

ILOM を開くと、次に示す図のように、デフォルトで「System Information (システム情報)」タブと第 2 レベルのタブが表示されます。「System Information (システム情報)」タブでは、次の第 2 レベルのタブにアクセスできます。

- 「Versions (バージョン)」タブ

- 「Session Time-Out (セッションタイムアウト)」タブ
- 「Components (部品)」タブ
- 「Identification Information」タブ

図 4-2　「System Information (システム情報)」タブ



「Versions (バージョン)」タブ

「Versions (バージョン)」セクションでは、実行している ILOM のバージョンを表示できます。詳細は、207 ページの「Web インタフェースを使用して ILOM バージョン情報を表示する」を参照してください。

「Session Time-Out (セッションタイムアウト)」タブ

「Session Time-Out (セッションタイムアウト)」セクションでは、ILOM セッションがアクティブな状態を維持するアイドル時間を設定できます。詳細は、60 ページの「セッションタイムアウトを設定する」を参照してください。

「Components (部品)」タブ

「Components (部品)」セクションでは、ILOM が監視している部品の名前、種類、および状態を表示できます。詳細は、109 ページの「Web インタフェースを使用して部品の情報を表示する」を参照してください。

「Identification Information」タブ

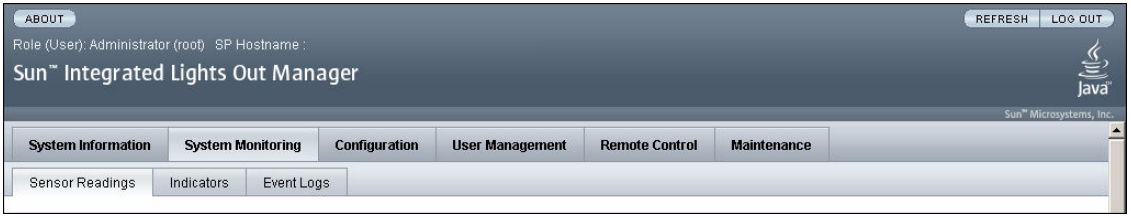
「Identification Information」セクションでは、SP の識別情報の入力または変更を行うことができます。詳細は、33 ページの「Web インタフェースを使用してホスト名およびシステム識別子を割り当てる」を参照してください。

「System Monitoring (システム監視)」タブ

「System Monitoring (システム監視)」タブをクリックすると、そのタブと第 2 レベルのタブが次に示す図のように表示されます。「System Monitoring (システム監視)」タブでは、次の第 2 レベルのタブにアクセスできます。

- 「Sensor Readings (センサー測定値)」タブ
- 「Indicators」タブ
- 「Event Logs (イベントログ)」タブ

図 4-3　「System Monitoring (システム監視)」タブ



「Sensor Readings (センサー測定値)」タブ

「Sensor Readings (センサー測定値)」セクションでは、センサーの名前、種類、および測定値を表示できます。詳細は、119 ページの「センサー測定値」を参照してください。

「Indicators」タブ

「Indicators」セクションでは、インジケータと LED の名前および状態を表示できます。詳細は、122 ページの「システムインジケータ」を参照してください。

「Event Logs (イベントログ)」タブ

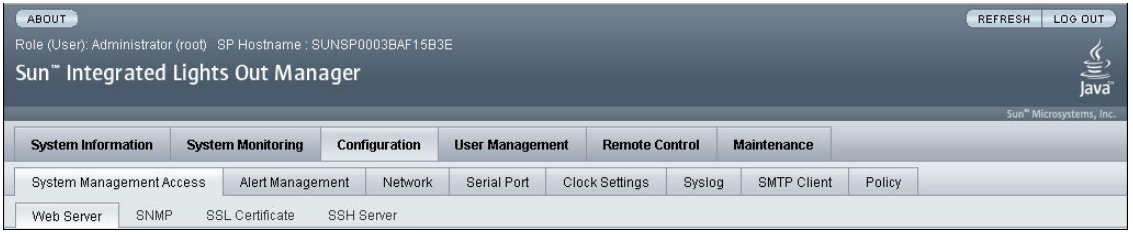
「Event Logs (イベントログ)」セクションでは、イベント ID、クラス、種類、重要度、日時、イベントの説明を含む、特定の各イベントに関するさまざまな詳細を表示できます。詳細は、125 ページの「ILOM イベントログ」を参照してください。

「Configuration (設定)」タブ

「Configuration (設定)」タブをクリックすると、そのタブと第 2 レベルのタブが次に示す図のように表示されます。「Configuration (設定)」タブでは、次の第 2 レベルのタブにアクセスできます。

- 「System Management Access (システム管理アクセス)」タブ
- 「Alert Management (警告の管理)」タブ
- 「Network (ネットワーク)」タブ
- 「Serial Port (シリアルポート)」タブ
- 「Clock Settings (クロック設定)」タブ
- 「Syslog」タブ
- 「SMTP Client」タブ
- 「Policy」タブ

図 4-4　「Configuration (設定)」タブ



「System Management Access (システム管理アクセス)」タブ

「System Management Access (システム管理アクセス)」セクションでは、Web サーバー、SNMP、および SSL 証明書の機能にアクセスできます。

「Web Server (ウェブサーバー)」タブ

「Web Server (ウェブサーバー)」セクションでは、HTTP Web サーバー、HTTP ポートなどの Web サーバーの設定を編集または更新できます。詳細は、174 ページの「Web インタフェースを使用して HTTP または HTTPS Web アクセスを有効にする」を参照してください。

「SNMP」タブ

「SNMP」セクションでは、SNMP の設定を編集または更新できます。詳細は、193 ページの「Web インタフェースを使用して SNMP の設定を行う」を参照してください。

「SSL Certificate (SSL 証明書)」タブ

「SSL Certificate (SSL 証明書)」セクションでは、デフォルトの SSL 証明書に関する情報を表示できます。また、新しい SSL 証明書を検索して入力するオプションもあります。詳細は、59 ページの「SSL 証明書をアップロードする」を参照してください。

「SSH Server」

「SSH Server」セクションでは、Secure Shell (SSH) サーバーのアクセスと鍵の生成について設定できます。詳細は、167 ページの「Web インタフェースを使用して SSH を有効または無効にする」を参照してください。

「Alert Management (警告の管理)」タブ

「Alert Management (警告の管理)」セクションでは、それぞれの警告に関する詳細を表示したり、設定された警告のリストを変更することができます。詳細は、144 ページの「ILOM Web インタフェースを使用した警告ルール設定の管理」を参照してください。

「Network (ネットワーク)」タブ

「Network (ネットワーク)」セクションでは、ILOM のネットワークの設定を表示および編集できます。詳細は、170 ページの「Web インタフェースを使用してネットワーク設定を表示する」を参照してください。

「Serial Port (シリアルポート)」タブ

「Serial Port (シリアルポート)」セクションでは、内部および外部のシリアルポートのボーレートを表示および編集できます。詳細は、172 ページの「Web インタフェースを使用してシリアルポート設定を表示する」を参照してください。

「Clock Settings (クロック設定)」タブ

「Clock Settings (クロック設定)」セクションでは、時刻および NTP の設定を表示および編集できます。詳細は、126 ページの「イベントログのタイムスタンプと ILOM のクロック設定」を参照してください。

「Syslog」タブ

「Syslog」セクションでは、syslog メッセージの送信先となるサーバーのアドレスを設定できます。詳細は、137 ページの「Web インタフェースを使用して遠隔 syslog 受信側の IP アドレスを設定する」を参照してください。

「SMTP Client」タブ

「SMTP」セクションでは、SMTP クライアントの状態を設定できます。これは、警告の電子メール通知の送信に使用されます。詳細は、155 ページの「Web インタフェースを使用して SMTP クライアントを有効にする」を参照してください。

「Policy」タブ

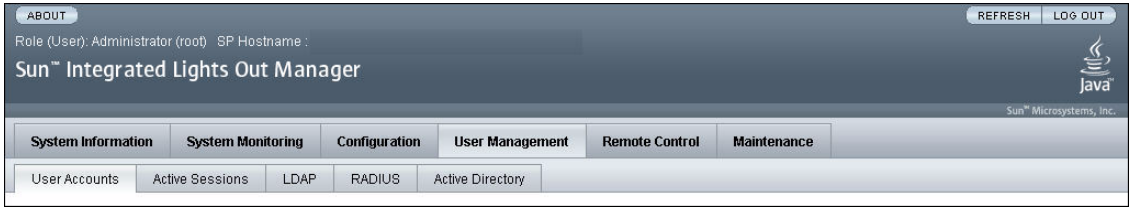
「Policy」セクションでは、電源投入ポリシーなど、システムの動作を制御する設定を有効または無効にすることができます。詳細は、115 ページの「ポリシーの設定」を参照してください。

「User Management (ユーザー管理)」タブ

「User Management (ユーザー管理)」タブをクリックすると、そのタブと第 2 レベルのタブが次に示す図のように表示されます。「User Management (ユーザー管理)」タブでは、次の第 2 レベルのタブにアクセスできます。

- 「User Accounts (ユーザーアカウント)」タブ
- 「Active Sessions (アクティブセッション)」タブ
- 「LDAP」タブ
- 「RADIUS」タブ
- 「Active Directory」タブ

図 4-5　「User Management (ユーザー管理)」タブ



「User Accounts (ユーザーアカウント)」タブ

「User Accounts (ユーザーアカウント)」セクションでは、ローカルの ILOM ユーザーアカウントを追加、削除、または変更できます。詳細は、74 ページの「Web インタフェースを使用してユーザーアカウントを追加し、権限を設定する」を参照してください。

「Active Sessions (アクティブセッション)」タブ

「Active Sessions (アクティブセッション)」セクションでは、ユーザーが開始したセッションの種類に加えて、現在 ILOM にログインしているユーザーを表示できます。詳細は、81 ページの「Web インタフェースを使用してユーザーセッションを表示する」を参照してください。

「LDAP」タブ

「LDAP」セクションでは、LDAP ユーザーの ILOM へのアクセスを設定できます。詳細は、98 ページの「Web インタフェースを使用して LDAP 用の ILOM を設定する」を参照してください。

「RADIUS」タブ

「RADIUS」セクションでは、RADIUS ユーザーの ILOM へのアクセスを設定できます。詳細は、102 ページの「Web インタフェースを使用して RADIUS を設定する」を参照してください。

「Active Directory」タブ

「Active Directory」セクションでは、Active Directory 設定を構成できます。詳細は、83 ページの「Web インタフェースを使用して Active Directory を設定する」を参照してください。

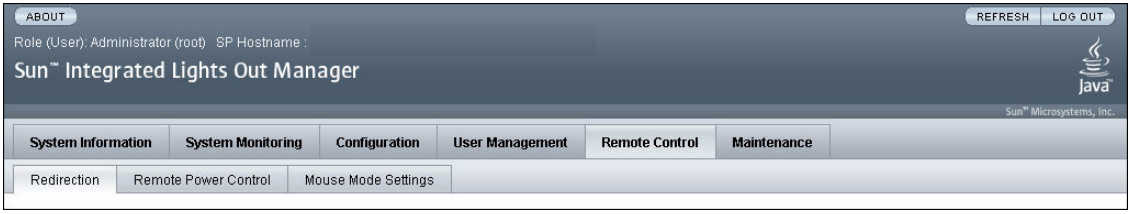
「Remote Control (リモートコントロール)」タブ

「Remote Control (リモートコントロール)」タブをクリックすると、そのタブと第 2 レベルのタブが次に示す図のように表示されます。「Remote Control (リモートコントロール)」タブでは、次の第 2 レベルのタブにアクセスできます。

- 「Redirection (リダイレクト)」タブ
- 「Remote Power Control (リモート電源制御)」タブ

- 「Mouse Mode Settings (マウスモード設定)」タブ

図 4-6　「Remote Control (リモートコントロール)」タブ



「Redirection (リダイレクト)」タブ

「Redirection (リダイレクト)」セクションでは、使用しているローカルマシンにシステムコンソールをリダイレクトすることにより、ホストを遠隔で管理できます。詳細は、219 ページの「Web インタフェースを使用して ILOM リモートコントロール設定を構成する」を参照してください。

「Remote Power Control (リモート電源制御)」

「Remote Power Control (リモート電源制御)」セクションでは、システムの電源を制御できます。詳細は、219 ページの「Web インタフェースを使用して ILOM リモートコントロール設定を構成する」を参照してください。

「Mouse Mode Settings (マウスモード設定)」

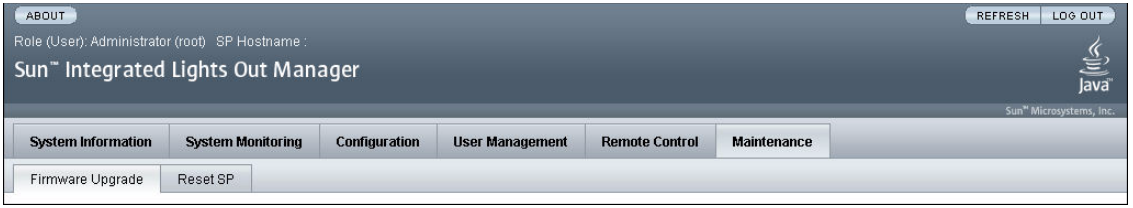
「Mouse Mode Settings (マウスモード設定)」セクションでは、ホストを遠隔で管理する際に使用するローカルのマウスのモードを選択できます。詳細は、219 ページの「Web インタフェースを使用して ILOM リモートコントロール設定を構成する」を参照してください。

「Maintenance (保守)」タブ

「Maintenance (保守)」タブをクリックすると、そのタブと第 2 レベルのタブが次に示す図のように表示されます。「Maintenance (保守)」タブでは、次の第 2 レベルのタブにアクセスできます。

- 「Firmware Upgrade (ファームウェアのアップグレード)」タブ
- 「Reset SP (SP のリセット)」タブ

図 4-7　「Maintenance (保守)」タブ



「Firmware Upgrade (ファームウェアのアップグレード)」タブ

「Firmware Upgrade (ファームウェアのアップグレード)」セクションでは、ILOM のファームウェアのアップグレードを取得する処理を開始できます。詳細は、207 ページの「Web インタフェースを使用して ILOM ファームウェアを更新する」を参照してください。

「Reset SP (SP のリセット)」タブ

「Reset SP (SP のリセット)」セクションでは、サービスプロセッサ (SP) をリセットする処理を開始できます。詳細は、209 ページの「ILOM SP をリセットする」を参照してください。

Web インタフェースを使用した ILOM への接続

この節では、SSL 証明書のアップロード方法とセッションのタイムアウトの設定方法に加えて、Web インタフェースのログインおよびログアウト方法について説明します。

▼ ILOM にログインする

この節では、ILOM Web インタフェースにログインする方法について説明します。

注 – Sun システムが AC 電源に接続されたとき、または電源が入っているシャーシにサーバーモジュールが挿入されたときに、ILOM は自動的に起動します。管理 Ethernet が接続されていない場合、または管理ネットワーク上に DHCP サーバーがないために ILOM の動的ホスト構成プロトコル (DHCP) の処理が失敗する場合には、ILOM の起動に時間がかかることがあります。

管理ネットワークへアクセスするためのブラウザのプロキシサーバー (使用している場合) を無効にすると、Web インタフェースの応答時間をより速くすることができます。

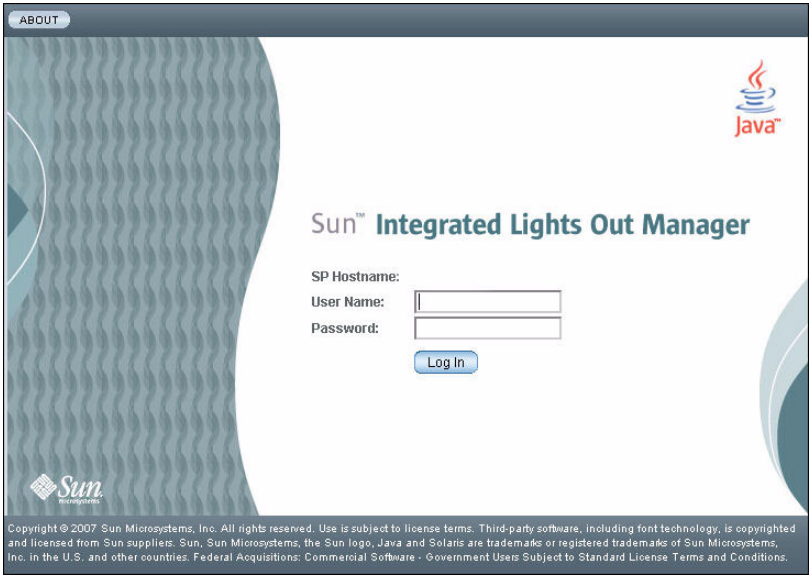
ILOM の IP アドレスが必要です。IP アドレスの表示および設定については、23 ページの「Sun サーバープラットフォーム SP インタフェースへの IP アドレスの割り当て」を参照してください。

次の手順に従って、ILOM Web インタフェースにログインします。

1. **Web インタフェースにログインするには、Web ブラウザに ILOM の IP アドレスを入力します。**

   Web インタフェースのログインページが表示されます。

図 4-8　　ログインページ



2. **ユーザー名およびパスワードを入力します。**

   デフォルトのユーザー名とパスワードを使用できます。

   - デフォルトのユーザー名 ー `root`
   - デフォルトのパスワード ー `changeme`

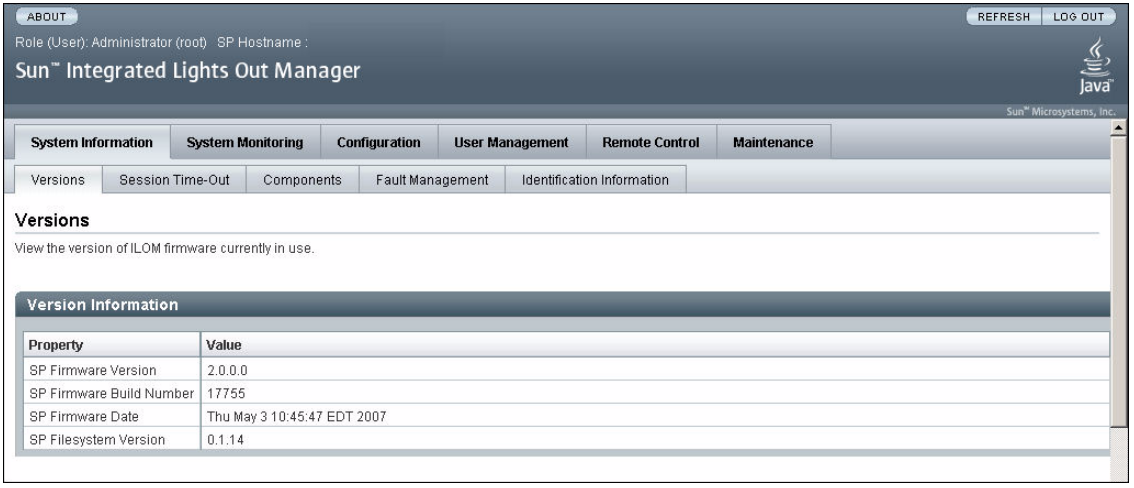
   デフォルトのユーザー名およびパスワードは小文字です。

   ローカルのユーザー ID が 1 つ事前に定義されており、ユーザー名は `root` で、管理者の役割が割り当てられています。このユーザー ID の削除および役割属性の変更はできません。初期パスワード `changeme` も提供されています。このパスワードは、コマンド行インタフェース (CLI)、Secure Shell (SSH)、および Web インタフェースへのログインに必要となります。

3. **「Log In (ログイン)」をクリックします。**

   Web インタフェースの「Versions (バージョン)」ページが表示されます。

図 4-9 「Versions (バージョン)」ページ



ILOM にログインしてシステムへのネットワーク接続を確立したら、承認されていないアクセスからシステムを保護するために、ILOM の root アカウントに関連付けられたデフォルトのパスワード (`changeme`) をリセットすることをお勧めします。ILOM の root アカウントのパスワードのリセットについては、66 ページの「Web インタフェースを使用して ILOM の root アカウントのパスワードを変更する」を参照してください。

▼ SSL 証明書をアップロードする

ILOM では、HTTPS アクセスを行うためのデフォルトの SSL 証明書と自己署名鍵が用意されています。

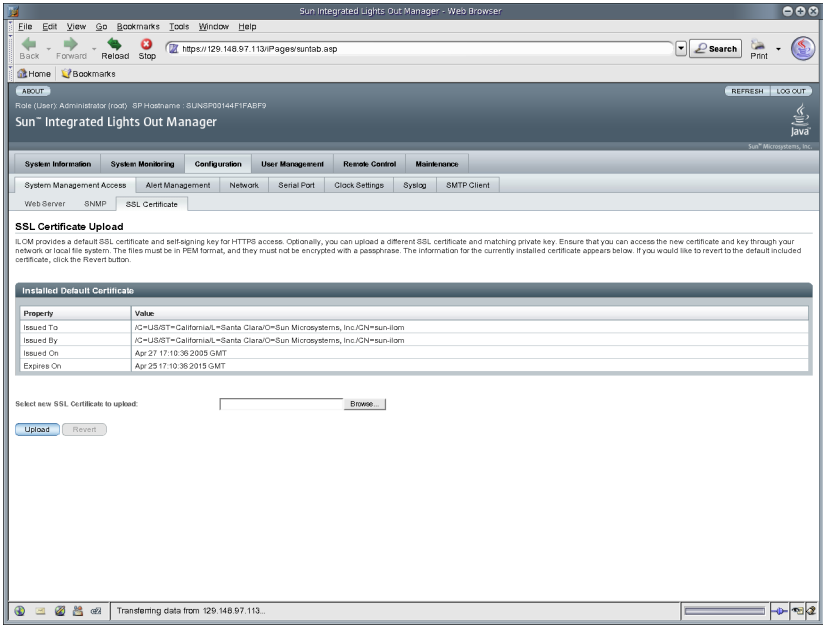
任意で、別の SSL 証明書とこれに一致する非公開鍵をアップロードできます。新しい証明書と鍵が、ネットワークまたはローカルのファイルシステムからアクセスできることを確認してください。

次の手順に従って、SSL 証明書をアップロードします。

1. ILOM にログインします。
2. 「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SSL Certificate (SSL 証明書)」の順に選択します。

   「SSL Certificate Upload (SSL 証明書アップロード)」ページが表示されます。

   図 4-10　「SSL Certificate Upload (SSL 証明書アップロード)」ページ



3. 新しい SSL 証明書のファイル名を入力するか、または「Browse (参照)」ボタンをクリックして新しい SSL 証明書を検索します。

   ファイル名には拡張子 .pem が付いています。サービスプロセッサはパスフレーズ方式の暗号化証明書をサポートしていません。

4. 「Upload (アップロード)」ボタンをクリックし、選択した SSL 証明書を取得します。

   「SSL Certificate Upload Status (SSL 証明書アップロード状況)」ダイアログボックスが表示されます。

5. **証明書と非公開鍵をアップロードしたら、「OK」ボタンをクリックして ILOM Web サーバーをリセットし、新しい SSL 証明書の使用を開始します。**

   新しい証明書を有効にするには、ILOM Web サーバーをリセットする必要があります。

▼ セッションタイムアウトを設定する

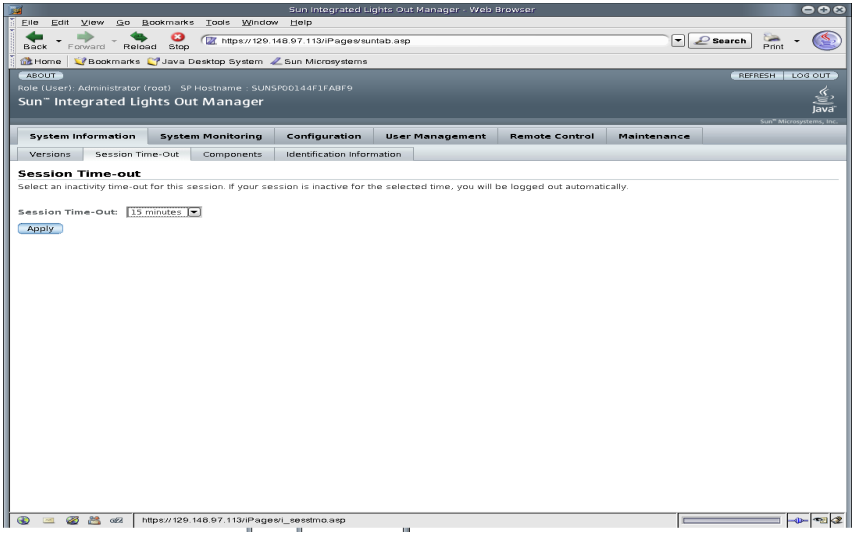
セッションタイムアウトの設定は、現在の ILOM セッションをログアウトしたあとは保持されません。ILOM Web インタフェースにログインするたびに、セッションタイムアウトをリセットする必要があります。

次の手順に従って、ILOM セッションがログアウトするまでにアイドル状態を維持する時間を設定します。

1. ILOM にログインします。
2. 「System Information (システム情報)」-->「Session Time-Out (セッションタイムアウト)」の順に選択します。

   「Session Time-Out (セッションタイムアウト」ページが表示されます。

図 4-11　「Session Time-Out (セッションタイムアウト)」ページ



3. 「Session Time-Out (セッションタイムアウト)」ドロップダウンリストから、ILOM が何も動作していないときに ILOM セッションがアイドル状態を維持する時間を選択します。

   選択した時間にわたってセッションがアクティブでない状態が続くと、ILOM から自動的にログアウトされます。

▼ ILOM からログアウトする

- Web インタフェースからログアウトするには、「Log Out (ログアウト)」ボタンをクリックします。

  「Log Out (ログアウト)」ボタンは Web インタフェースの右上の端にあります。

第5章

ユーザーアカウントの管理

ILOM は、最大 10 個のユーザーアカウントをサポートしています。これらのアカウントの 1 つは、事前構成された管理者アカウントです。このアカウントでは、すべての ILOM 機能やコマンドに対する読み取りおよび書き込みアクセスを行うことができます。ILOM の Web インタフェースまたはコマンド行インタフェース (CLI) を使用すると、ユーザーアカウントを追加、変更、または削除することができます。

この章には次の節があります。

- 74 ページの「Web インタフェースを使用してユーザーアカウントを管理する」
  - 74 ページの「Web インタフェースを使用してユーザーアカウントを追加し、権限を設定する」
  - 77 ページの「Web インタフェースを使用してユーザーアカウントを変更する」
  - 80 ページの「Web インタフェースを使用してユーザーアカウントを削除する」
  - 81 ページの「Web インタフェースを使用してユーザーセッションを表示する」
- 82 ページの「Active Directory」
  - 83 ページの「Web インタフェースを使用して Active Directory を設定する」
  - 87 ページの「Web インタフェースを使用して Active Directory テーブルの情報を編集する」
  - 89 ページの「ユーザーの承認レベルの決定」
  - 90 ページの「Active Directory 接続のセキュリティーの保護」
- 94 ページの「Lightweight Directory Access Protocol」
  - 97 ページの「LDAP サーバーを設定する」
  - 97 ページの「CLI を使用して LDAP 用の ILOM を設定する」
  - 98 ページの「Web インタフェースを使用して LDAP 用の ILOM を設定する」
- 100 ページの「RADIUS 認証」
  - 100 ページの「RADIUS クライアントとサーバー」
  - 101 ページの「RADIUS パラメータ」
  - 102 ページの「CLI を使用して RADIUS を設定する」
  - 102 ページの「Web インタフェースを使用して RADIUS を設定する」
  - 103 ページの「RADIUS コマンド」

注 – この章の構文例では、`/SP/` で始まるターゲットを使用しますが、使用している Sun サーバープラットフォームによっては、`/CMM/` で始まるターゲットに置き換わる場合があります。サブターゲットは、すべての Sun サーバープラットフォームで共通です。

ユーザーアカウントの管理のガイドライン

ユーザーアカウントを管理する場合は、次の一般的なガイドラインに従ってください。

- ILOM は最大 10 個のユーザーアカウントをサポートしており、そのうち 1 つは事前構成された管理者アカウントです。事前構成された管理者アカウントは削除できません。10 個のユーザーアカウントがすべて設定されている場合、新しいユーザーアカウントを追加するには既存のユーザーアカウントを削除する必要があります。
- 管理者権限のあるアカウントのみ、ユーザーアカウントの追加、修正、および削除を行うことができます。ただし、オペレータ権限を持つユーザーは、自分のパスワードを変更できます。
- アカウントのユーザー名は 4 文字以上 16 文字以下で指定してください。ユーザー名の大文字と小文字は区別され、先頭はアルファベットである必要があります。英数字とハイフン、アンダーラインが使用できます。ユーザー名にはスペースは使用できません。
- ローカルアカウントを設定するか、Active Directory、LDAP、RADIUS などの遠隔ユーザーデータベースに対する ILOM 認証アカウントを設定することができます。遠隔認証の場合は、ILOM インスタンスごとにローカルアカウントを設定するのではなく、中央ユーザーデータベースを使用することができます。また、遠隔認証を使用すると、ユーザーのパスワードをサーバーで 1 回変更できます。

ユーザーアカウントの役割と権限

ユーザーアカウントには 2 つの役割が定義されています。役割ごとに、ILOM ユーザーに特定の権限が与えられます。ユーザーの役割と権限は次のとおりです。

- **管理者** − ILOM のすべての機能やコマンドにアクセスできます。
- **オペレータ** − ILOM の一部の機能やコマンドにアクセスが制限されています。通常、オペレータは設定を変更できません。

事前構成された ILOM 管理者アカウント

事前構成された ILOM 管理者アカウント (固定ユーザーアカウントとも呼ばれる) の内容は次のとおりです。

ユーザー名: `root`

パスワード: `changeme`

ユーザー名 `root` は削除および変更できませんが、パスワード (`changeme`) をリセットすることはできます。このアカウントでは、ILOM のすべての機能やコマンドに対して組み込み型の管理権限 (読み取りおよび書き込みアクセス) が提供されます。

SP レベルまたは CMM レベルで最初に ILOM にアクセスするとき、`root` として、デフォルトのパスワード `changeme` を使用してログインする必要があります。ILOM にログインしてシステムへのネットワーク接続を確立したら、承認されていないアクセスからシステムを保護するために、ILOM の `root` アカウントに関連付けられたパスワード `changeme` のリセットを検討することをお勧めします。ブレードサーバーシステムを使用している場合は、システムシャーシに取り付けられている各 CMM およびブレードでこのパスワードをリセットしてください。ILOM の `root` アカウントのパスワードのリセットに関する詳細は、66 ページの「Web インタフェースを使用して ILOM の root アカウントのパスワードを変更する」を参照してください。

▼ Web インタフェースを使用して ILOM の root アカウントのパスワードを変更する

次の手順に従って、`root` アカウントのパスワードを変更します。

1. **Web ブラウザを開き、サーバー SP または CMM の IP アドレスを入力します。**

   ILOM Web インタフェースのログインページが表示されます。

2. **ILOM のログインページで、次の手順を実行します。**

   a. **デフォルトのユーザー名 (`root`) とパスワード (`changeme`) を入力します。**

   b. **「Log In (ログイン)」をクリックします。**

      ILOM Web インタフェースが表示されます。

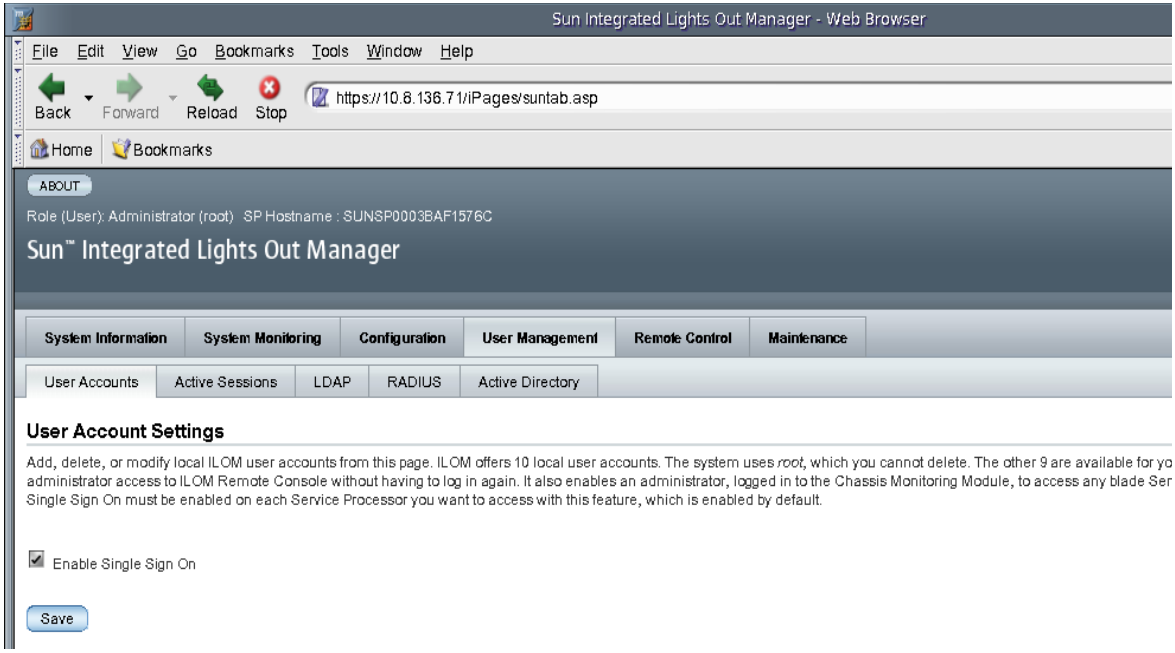
3. **ILOM Web インタフェースで、次の手順を実行します。**

   - 事前構成された管理者のパスワードを変更するには、左側のナビゲーション区画のデバイスをクリックして手順 4 に進みます。
   - ブレード SP レベルで事前構成された管理者のパスワードを変更するには、左側のナビゲーション区画の適切なブレードをクリックして手順 4 に進みます。

4. ILOM Web インタフェースで、「User Management (ユーザー管理)」-->「User Accounts (ユーザーアカウント)」をクリックします。

   「User Account Settings」ページが表示されます。

図 5-1　「User Account Settings」ページ

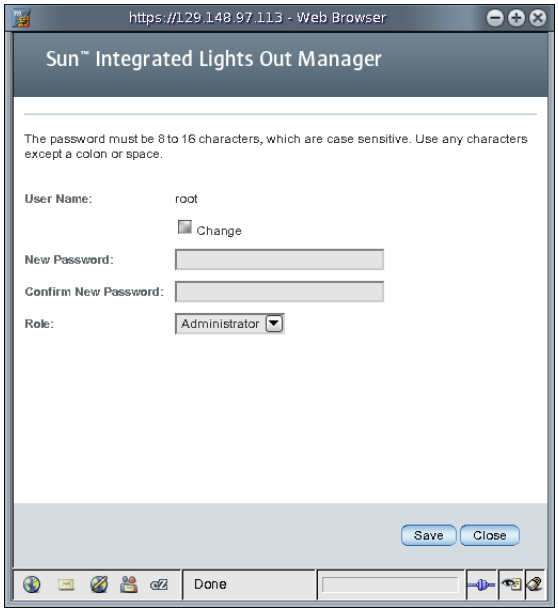


5. 「User Account Settings」ページで、`root` の隣のラジオボタンを選択してから「Edit (編集)」をクリックします。

   セキュリティーメッセージが表示されます。

6. 「OK」をクリックして続行します。「User Account Password」ダイアログが表示されます。

図 5-2　「User Account Password」ダイアログ



7. 「User Account Password」ダイアログで、次の手順を実行します。

   a. 「Change」の隣のボックスを選択します。

   b. 「New Password」テキストボックスに新しいパスワードを入力します。

   c. 「Confirm Password (パスワードの確認)」テキストボックスに新しいパスワードをふたたび入力します。

   d. 「Save (保存)」ボタンをクリックします。

      手順 7b と 7c で特定された新しいパスワードが、`root` 管理者アカウントで使用可能になります。

8. 必要に応じて、手順 2 から 7d までを繰り返して、取り付けられたデバイスごとにパスワードを変更します。

▼ CLI を使用して ILOM の root アカウントのパスワードを変更する

- ILOM の root アカウントのパスワードを変更するには、次のコマンドを入力します。

  -> set /SP/users/root password=*password*

  例:

```
-> set /SP/users/root password=password
Changing password for user /SP/users/root...
Enter new password again: ********
New password was successfully set for user /SP/users/root
```

シングルサインオン

シングルサインオンは、ILOM にアクセスする際に必要になるパスワードの入力回数を減らすための、便利な認証サービスです。シングルサインオンは、デフォルトで有効になっています。あらゆる認証サービスと同様に、認証資格はネットワークを介して渡されます。これが望ましくない場合は、シングルサインオン認証サービスを無効にすることを検討してください。

▼ CLI を使用してシングルサインオンを有効または無効にする

シングルサインオンは、デフォルトで有効になっています。管理者のみがシングルサインオンを有効または無効にできます。

- シングルサインオンを有効または無効にするには、次のコマンドを入力します。

  –> set /SP/services/sso state=*disabled* | *enabled*

▼ Web インタフェースを使用してシングルサインオンを有効または無効にする

次の手順に従って、シングルサインオンを有効または無効にします。

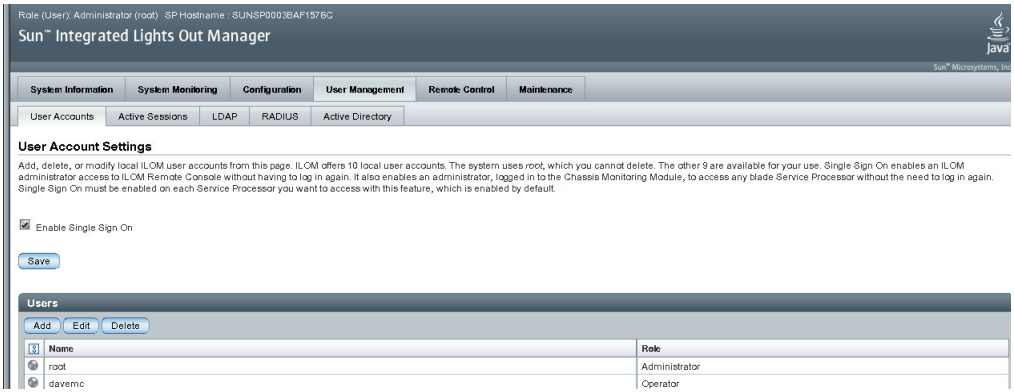
1. ILOM Web インタフェースに管理者としてログインします。

2. 「User Management (ユーザー管理)」-->「User Accounts (ユーザーアカウント)」を選択します。

   「User Account Settings」ページが表示されます。

3. 「Enable Single Sign On」の隣のチェックボックスをクリックして機能を有効にするか、チェックボックスの選択を解除して機能を無効にします。

   図 5-3　　シングルサインオンを有効にした場合の「User Account Settings」ページ



CLI を使用したユーザーアカウントの管理

この節では、ILOM のコマンド行インタフェース (CLI) を使用したユーザーアカウントの管理方法について説明します。

▼ CLI を使用してユーザーアカウントを追加する

- ローカルユーザーアカウントを追加するには、次のコマンドを入力します。

```
-> create /SP/users/username password=password role=
administrator|operator
```

例:

```
-> create /SP/users/davemc
Creating user...
Enter new password:********
Enter new password again:********
Created /SP/users/davemc
```

▼ CLI を使用してユーザーアカウントを変更する

- ローカルユーザーアカウントを変更するには、次のコマンドを入力します。

  –> set /SP/users/*username* **password=***password* **role=administrator|operator**

▼ CLI を使用してユーザーアカウントを削除する

1. ローカルユーザーアカウントを削除するには、次のコマンドを入力します。

   –> delete /SP/users/*username*

   例:

   -> delete /SP/users/davemc

   ```
   Are you sure you want to delete /SP/users/davemc (y/n)?
   ```

2. 削除する場合は y、取り消す場合は n を入力します。

▼ CLI を使用してユーザーアカウントのリストを表示する

- すべてのローカルユーザーアカウントに関する情報を表示するには、次のコマンドを入力します。

  –> show -display targets /SP/users

  例:

```
-> show -display targets /SP/users
 /SP/users
    Targets:
        root
        davemc
```

▼ CLI を使用して個々のユーザーアカウントを表示する

- 1 つの特定のユーザーアカウントに関する情報を表示するには、次のコマンドを入力します。

  –> show /SP/users/*username*

  例:

```
-> show /SP/users/davemc
/SP/users/davemc
   Targets:
  Properties:
        role = Operator
    password = *****
 Commands:
     cd
       set
      show
```

▼ CLI を使用してユーザーアカウントを設定する

`set` コマンドを使用すると、設定済みのユーザーアカウントのターゲット、プロパティー、パスワード、および値を変更できます。

- ローカルユーザーアカウントを設定するには、次のコマンドを入力します。

  –> set <*target***> [<***property***>=***value***]**

ターゲット、プロパティー、および値

次のターゲット、プロパティー、および値は、ローカルユーザーアカウントに対して有効です。

表 5-1 ローカルユーザーアカウントで有効なターゲット、プロパティー、および値

ターゲット	プロパティー	値	パスワード	デフォルト値
/SP/users/*username*	role	administrator | operator		operator
	password	<string>		

たとえば、user1 の役割を管理者からオペレータに変更するには、次のように入力します。

```
–> set /SP/users/user1 role=operator
```

user1 のパスワードを変更するには、次のように入力します。

```
–> set /SP/users/user1 password
Changing password for user /SP/users/user1/password...
Enter new password:********
Enter new password again:********
New password was successfully set for user /SP/users/user1
```

注 – ユーザーのプロパティを変更するには、管理者権限が必要です。

▼ CLI を使用してユーザーセッションのリストを表示する

- すべてのローカルユーザーセッションに関する情報を表示するには、次のコマンドを入力します。

  ```
  –> show /SP/sessions
  ```

  例:

```
-> show /SP/sessions
 /SP/sessions
    Targets:
        108
    Properties:
    Commands:
        cd
        show
```

▼ CLI を使用して個々のユーザーセッションを表示する

- 個々のユーザーセッションに関する情報を表示するには、次のコマンドを入力します。

–> show /SP/sessions/108

例:

```
-> show /SP/sessions/108
 /SP/sessions/108
    Targets:
    Properties:
        username = root
        starttime = Tue Jun  5 10:04:05 2007
        type = shell
    Commands:
        cd
        show
```

Web インタフェースを使用してユーザーアカウントを管理する

この節では、Web インタフェースを使用してユーザーアカウントを追加、変更、および削除する方法について説明します。

▼ Web インタフェースを使用してユーザーアカウントを追加し、権限を設定する

1. **ILOM Web インタフェースに管理者権限を持つユーザーとしてログインします。**

   管理者権限のあるアカウントのみ、ユーザーアカウントの追加、修正、および削除を行うことができます。ただし、オペレータは自分のパスワードを変更できます。

   新しいユーザーに管理者権限が認められている場合、コマンド行インタフェース (CLI) および Intelligent Platform Management Interface (IPMI) にも、ILOM に対して同じ権限が自動的に認められます。

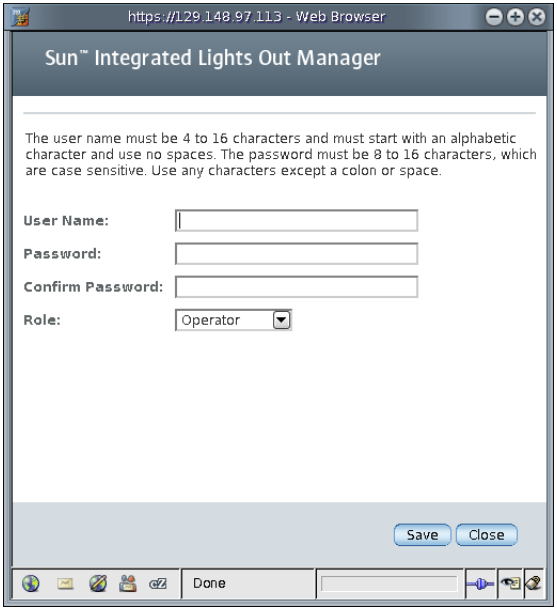
2. **「User Management (ユーザー管理)」-->「User Accounts (ユーザーアカウント)」を選択します。**

   「User Account Settings」ページが表示されます。

3. **「Users (ユーザー)」テーブルで「Add (追加)」をクリックします。**

   「Add User (ユーザーの追加)」ダイアログが表示されます。

図 5-4　「Add User (ユーザーの追加)」ダイアログ



4. 次の情報を入力します。

   a. 「User Name (ユーザー名)」フィールドに、ユーザー名を入力します。

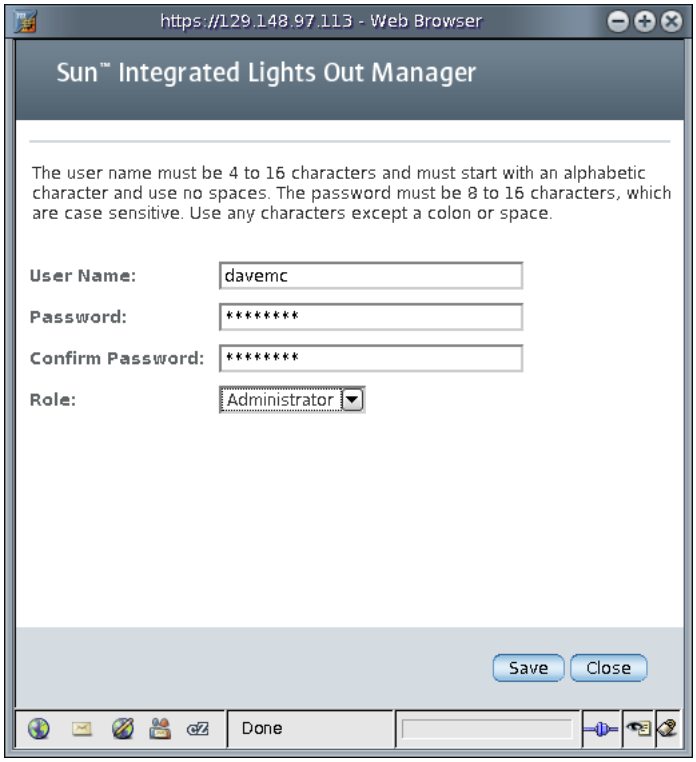
   b. 「Password (パスワード)」フィールドにパスワードを入力します。

      パスワードは、8 文字以上 16 文字以下にしてください。パスワードの大文字と小文字は区別されます。英数字のほか、セキュリティーを高めるため特殊文字も使用してください。コロン以外のすべての文字が使用できます。パスワードにはスペースは使用できません。

   c. 「Confirm Password (パスワードの確認)」フィールドにパスワードを再入力し、パスワードを確認します。

   d. 「Role」ドロップダウンリストで、「Administrator (管理者)」または「Operator (オペレータ)」を選択します。

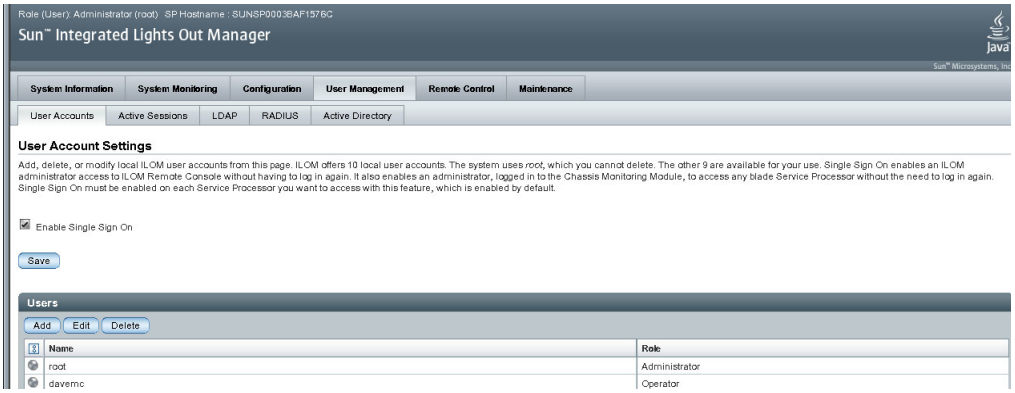
図 5-5　フィールドに値が入力された状態の「Add User (ユーザーの追加)」ダイアログ



e. 新しいユーザーの情報を入力し終わったら、「Save (保存)」ボタンをクリックします。

「User Account Settings」ページが再表示されます。「User Account Settings」ページには、新しいユーザーアカウントとその関連情報が表示されています。

図 5-6　　新しいユーザーが表示された「User Account Settings」ページ



▼ Web インタフェースを使用してユーザーアカウントを変更する

この節では、ILOM ユーザーアカウントを変更する方法について説明します。ユーザーアカウントの変更により、ユーザーのパスワードと、ネットワークおよびシリアル権限を変更することができます。

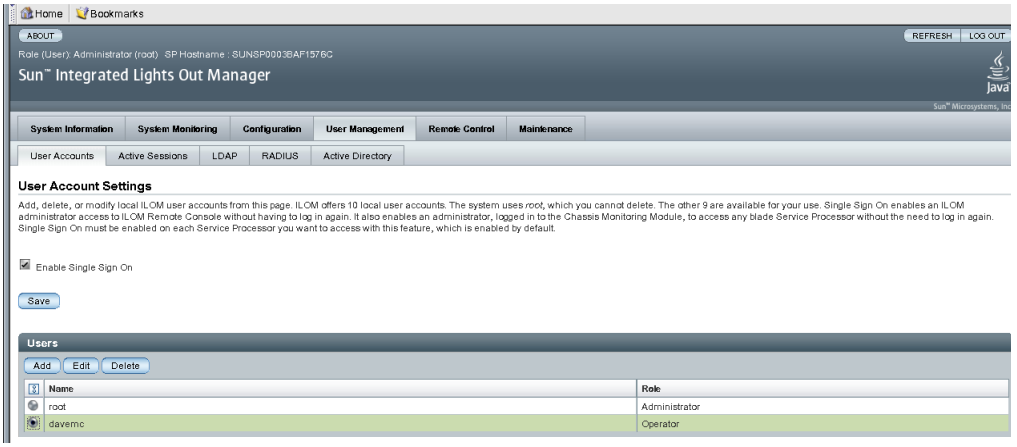
注 – 管理者権限のあるアカウントのみ、ユーザーアカウントの追加、修正、および削除を行うことができます。ただし、オペレータは自分のパスワードを変更できます。

新しいユーザーに管理者権限が付与されている場合は、コマンド行インタフェース (CLI) および Intelligent Platform Management Interface (IPMI) にも、ILOM に対する同じ権限が自動的に付与されます。

1. **管理者として ILOM にログインし、Web インタフェースを開きます。**
2. **「User Management (ユーザー管理)」-->「User Accounts (ユーザーアカウント)」を選択します。**

   「User Account Settings」ページが表示されます。

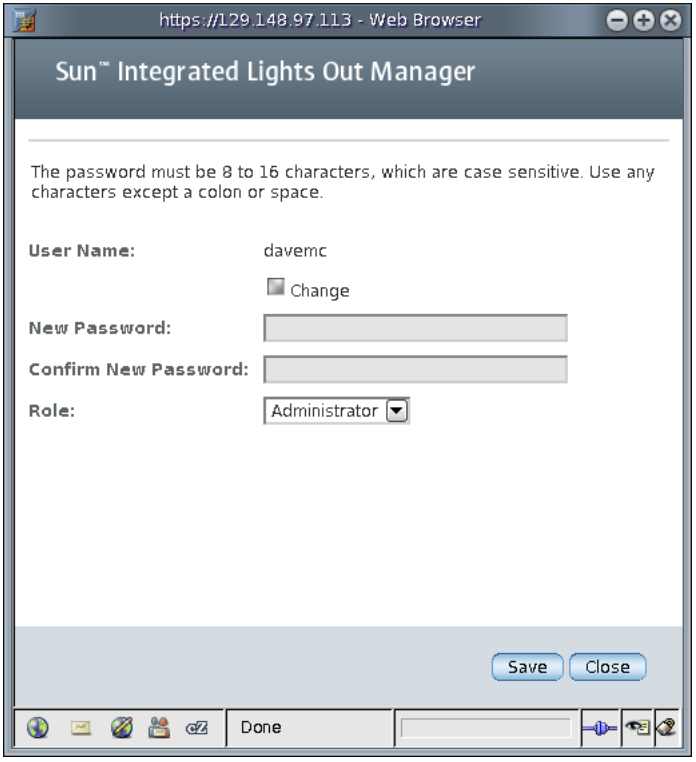
図 5-7　「User Account Settings」ページ



3. 「Users (ユーザー)」テーブルで、変更するユーザーアカウントの隣のラジオボタンを選択します。
4. 「Edit (編集)」をクリックします。

   「Edit User (ユーザーの編集)」ダイアログが表示されます。

図 5-8　「Edit User (ユーザーの編集)」ダイアログ



5. 必要に応じて、パスワードを修正します。

   a. ユーザーのパスワードを変更する場合は、「Change」チェックボックスを選択します。パスワードを変更しない場合は、チェックボックスの選択を解除します。

   b. 「New Password」フィールドに新しいパスワードを入力します。

      パスワードは 8 文字以上 16 文字以下で指定してください。パスワードの大文字と小文字は区別されます。英数字のほか、セキュリティーを高めるため特殊文字も使用してください。コロン以外のすべての文字が使用できます。パスワードにはスペースは使用できません。

   c. 「Confirm New Password」フィールドにパスワードを再入力し、パスワードを確認します。

6. 「Role」ドロップダウンリストで、「Administrator (管理者)」または「Operator (オペレータ)」を選択します。

7. アカウント情報を変更したあとで、「Save (保存)」をクリックするとその変更が有効になり、「Close (閉じる)」をクリックすると前の設定に戻ります。

   「User Account Settings」ページが再表示されます。

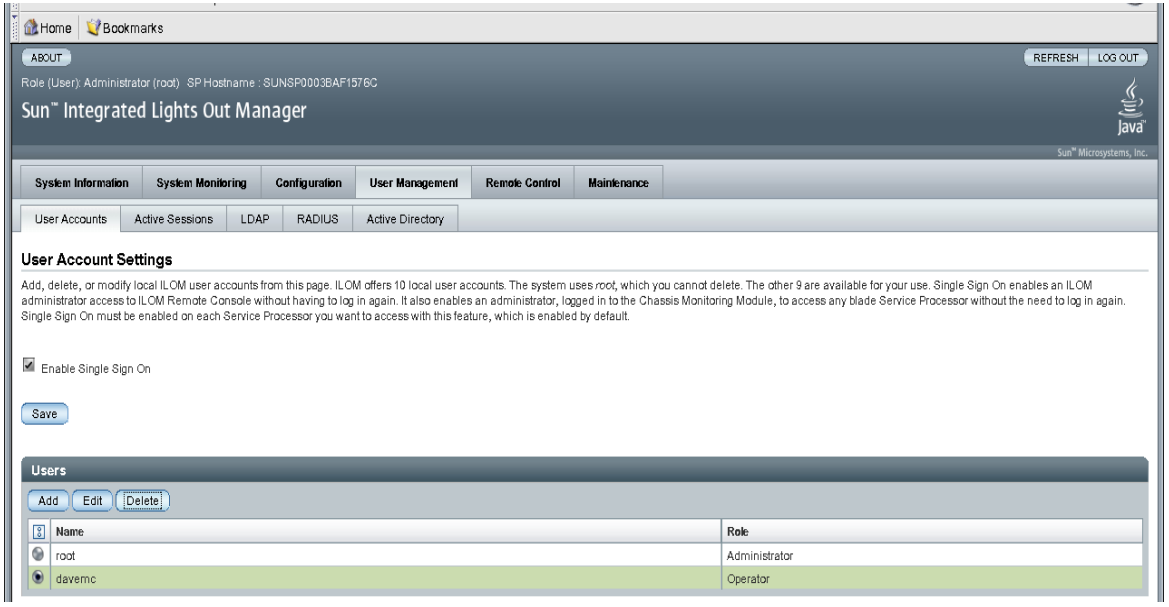
▼ Web インタフェースを使用してユーザーアカウントを削除する

1. 管理者として ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「User Accounts (ユーザーアカウント)」を選択します。

   「User Account Settings」ページが表示されます。
3. 削除するユーザーアカウントの隣のラジオボタンを選択します。

注 – root アカウントは削除できません。

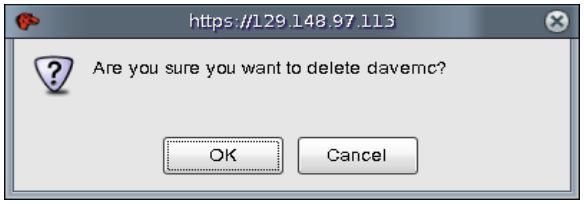
図 5-9　「User Account Settings」ページ



4. 「Users (ユーザー)」テーブルで「Delete (削除)」をクリックします。

   確認のダイアログが開きます。

図 5-10　ユーザー設定の削除ダイアログ



5. 「OK」をクリックしてアカウントを削除するか、「Cancel (キャンセル)」をクリックして処理を中止します。

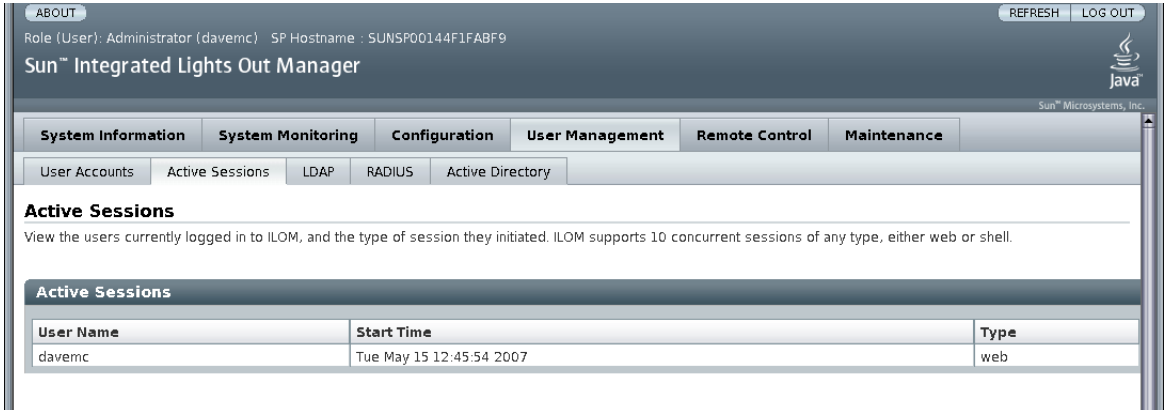
   「User Account Settings」ページが開きます。削除したユーザーアカウントは表示されていません。

▼ Web インタフェースを使用してユーザーセッションを表示する

1. ILOM Web インタフェースにログインします。
2. 「User Management (ユーザー管理)」-->「Active Sessions (アクティブセッション)」を選択します。

   「Active Sessions (アクティブセッション)」ページが表示されます。現在 ILOM にログインしているユーザーのユーザー名、そのユーザーがセッションを開始した日時、およびセッションの種類を確認できます。

図 5-11　「Active Sessions (アクティブセッション)」ページ



Active Directory

ILOM では、Microsoft Windows Server 2003 および Microsoft Windows 2000 Server オペレーティングシステムに導入されている分散ディレクトリサービスの Active Directory をサポートしています。

Active Directory について

ディレクトリサービスとは、データベースストレージシステム (ディレクトリストア) であり、ディレクトリストアのデータを安全に追加、変更、削除、検索する手段を提供する一連のサービスでもあります。分散環境において、ディレクトリサービスは、ネットワーク接続されたデバイスおよびサービスに関する情報や、それらを使用するユーザーに関する情報を格納するための中央の場所を提供します。また、ディレクトリサービスは、ユーザー、コンピュータ、およびアプリケーションがこの情報を使用できるようにするためのサービスも実装しています。

通常、Active Directory は次の 3 つのうちいずれかの目的で使用されます。

- **内部ディレクトリ** – 内部ディレクトリは、企業内のユーザーやリソースに関する情報を公開するために企業ネットワーク内で使用されます。
- **外部ディレクトリ** – 通常、これらのディレクトリは、企業のローカルエリアネットワーク (LAN) と公衆インターネットとの境界に位置する境界ネットワーク、つまり非武装ゾーン (DMZ) にあるサーバーに配置されます。
- **アプリケーションディレクトリ** – アプリケーションディレクトリは、そのアプリケーションにしか関係しない「プライベートな」ディレクトリデータをローカルディレクトリに格納します。アプリケーションと同じサーバー上であることもあり、Active Directory に対する追加設定は必要ありません。

Active Directory はユーザー資格の認証に使用できます。アクセスレベルは、設定することも、グループのメンバーシップに基づいてサーバーから取得することもできます。2 つ以上のユーザー「ドメイン」を使用できます。その場合、設定されたドメインは設定順に試行されます。

Active Directory の設定

Active Directory を設定するには、一部のグローバルプロパティーを設定し、次の内容を表す 3 つのテーブルに情報を入力する必要があります。

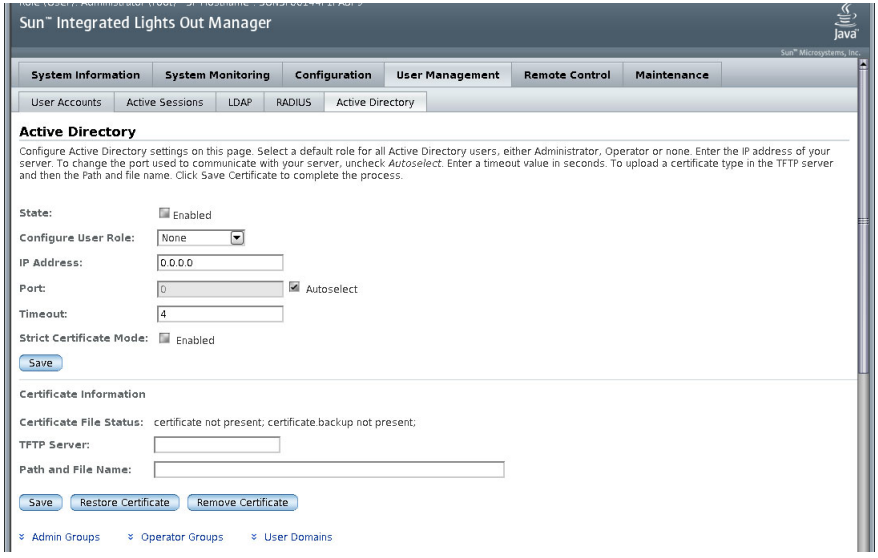
- ユーザードメイン
- 管理者グループ
- オペレータグループ

▼ Web インタフェースを使用して Active Directory を設定する

1. 管理者権限を持つユーザーとして ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「Active Directory」を選択します。

   「Active Directory」ページが表示されます。Active Directory 構成の設定と Active Directory テーブルは、このページの上半分にあります。

図 5-12　Active Directory 構成の設定



Active Directory 設定ページのプロパティー

表 5-2 に、Active Directory を使用するために必要な設定について説明します。

表 5-2 Active Directory 構成の設定 (グローバル変数)

プロパティー (Web)	プロパティー (CLI)	デフォルト値	説明
State (状態)	`adminState`	Enabled	Enabled | Disabled
Role	`defaultRole`	None	None | Administrator | Operator 単純な設定の場合に、認証されたすべてのユーザーに付与されるアクセスの役割。より統合された方法がデフォルトで使用できるように、このアクセスの役割はデフォルトでは設定されていません。アクセスレベルは Active Directory サーバーから取得されます。
IP Address (IP アドレス)	`ipaddress`		Active Directory サーバーの IP アドレス。
Port (ポート)	`port`	0 (autoselect)	サーバーとの通信に使用するポート。または `autoselect` を入力します。 SSL-LDAP トランザクションに標準のポートを使用することを示します。 使用している標準以外の TCP ポートで予期しないイベントが発生した場合に使用できます。
Timeout	`timeout`	5	秒単位のタイムアウトの値。 個々の LDAP トランザクションが完了するまで待機する秒数です。トランザクションの数は設定に応じて異なるため、この値はすべてのトランザクションの合計時間を表すわけではありません。 このプロパティーは、サーバーが応答していない場合や到達不可能な場合に待機する時間を調整するために使用できます。
Strict Certificate Mode	`strictcertmode`	Enabled	Enabled | Disabled 有効にすると、より制限的な証明書の検証を行うために、サーバー証明書のアップロードが必要になります。

表 5-2　Active Directory 構成の設定 (グローバル変数) (続き)

プロパティー (Web)	プロパティー (CLI)	デフォルト値	説明
Certificate File Status	`certfilestatus`		certificate present	not present; certificate.backup present	not present
対応する Web プロパティー なし	`getcertfile`	なし	必要に応じて、証明書ファイルのアップロードに使用する方法。ここから証明書を削除および復元することもできます。
TFTP Server	対応する CLI プロパティーなし	なし	証明書ファイルの取得に使用する TFTP サーバー。
Path and File Name	対応する CLI プロパティーなし	なし	サーバー上の証明書ファイルの完全なパス名およびファイル名
Restore Certificate	対応する CLI プロパティーなし	なし	既存の証明書ファイルに対して証明書ファイルをアップロードして上書きした場合に使用されます。既存のファイルはバックアップコピーとして格納されます。復元を行うと、バックアップコピーを取得し、これを現在のファイルに設定します。
Remove Certificate	対応する CLI プロパティーなし	なし	「Strict Certificate Mode」が有効な場合は、証明書を削除できません。

Active Directory ターゲットテーブル

Active Directory インタフェース (図 5-13) の下半分にある 3 つのテーブルは、ユーザーの認証と承認を行うためのドメインやグループの設定に使用されます。ターゲットテーブルには次に関する情報が含まれます。

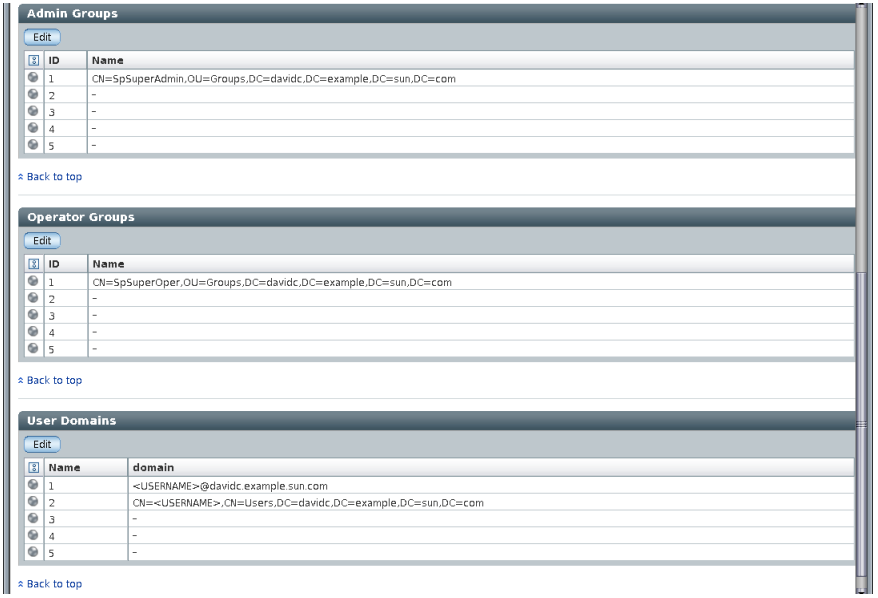
- 管理者グループ
- オペレータグループ
- ユーザードメイン

管理者グループとオペレータグループのテーブルのエントリには、識別名形式の MS Active Directory グループの名前が含まれます。ユーザーが特定のグループのメンバーである場合、ユーザーグループが対応するテーブルに応じて、そのユーザーにオペレータまたは管理者としてのアクセス権が付与されます。

ユーザードメインは、ユーザーが属する認証ドメインです。通常、ユーザーがログインする際に使用する名前は、これらのエントリで指定したドメイン/名前の形式になります。ユーザー認証は、入力したユーザードメインデータとユーザーが提供したログイン名に基づいて試行されます。

3 つのテーブルすべてにおいて、データの望ましい形式を示すために、デフォルトデータがいくつか入力されています。また、ユーザーが入力すべき内容を示すエラーメッセージも表示されます。

図 5-13　Active Directory テーブル



Active Directory ターゲットテーブルのプロパティー

表 5-3 および表 5-4 は、「Admin Groups」テーブルおよび「Operator Groups」テーブルの詳細を示したものです。完全修飾の識別名が「Name」列に表示されています。

表 5-3　「Admin Groups」テーブル

ID	名前
1	CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	

表 5-4　「Operator Groups」テーブル

ID	名前
1	CN=SpSuperOper,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com
2	
3	
4	
5	

表 5-5 は、図 5-13 に示した「User Domains」テーブルの詳細を示したものです。エントリ 1 に表示されているドメインは、認証を最初に試行する際に使用される原則の形式を示しています。エントリ 2 は完全な識別名 (dn) を示しています。これは、原則の形式を使用した認証の試行が失敗した場合に使用されます。

注 – 表 5-5 で使用されている例の <USERNAME> は置換文字列です。これは、ユーザーの実際のログイン名で置き換えられます。

表 5-5　「User Domains」テーブル

名前	ドメイン
1	`<USERNAME>@davidc.example.sun.com`
2	`CN=<USERNAME>,CN=Users,DC=davidc,DC=example,DC=sun,DC=com`
3	
4	
5	

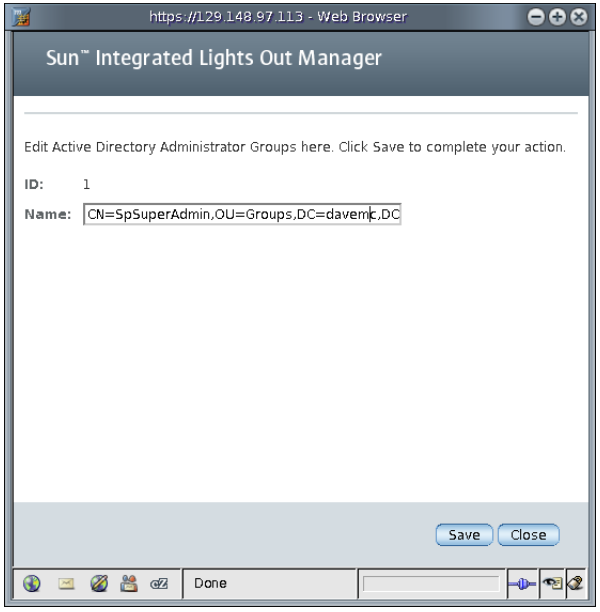
▼ Web インタフェースを使用して Active Directory テーブルの情報を編集する

1. 管理者権限を持つユーザーとして ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「Active Directory」を選択します。
   「Active Directory」ページが表示されます。

3. 「Active Directory」ページの一番下で、編集する情報が含まれる行のラジオボタンを選択し、「Edit (編集)」をクリックします。

   「Edit Active Directory Administrator Groups」ページ、「Edit Active Directory Operator Groups」ページ、「Edit Active Directory User Domains」ページのいずれかの適切なページが表示されます。各「編集」ページには、情報を追加または編集するための「Name」フィールドがあります。

図 5-14　Active Directory の管理者グループの編集ページ



4. 編集ページで、情報を追加または編集します。

5. 「Save (保存)」をクリックして変更を有効にします。

   「Active Directory」ページが表示されます。

6. 「User Domains」テーブルで、「Name」フィールドにテキストで情報を入力します。<USERNAME> 置換マーカーを使用して LDAP 要求におけるユーザー名の場所を確保します。

   例:

   ```
   domain = <USERNAME>@davemc.example.sun.com
   domain = CN=<USERNAME>,CN=Users,DC=davemc,DC=example,DC=sun,
   DC=com
   ```

   次の例に示すように、ユーザーは指定したいずれかの名前で ILOM にアクセスできるようになります。

コード例 5-1　　原則の形式を使用した Active Directory のログイン

```
/home/dc150698> ssh -l davemc 10.x.xxx.xxx
  Password:*******
  Sun(TM) Integrated Lights Out Manager
  Version 1.1
  Copyright 2005 Sun Microsystems, Inc. All rights reserved.
  ->
```

コード例 5-2　　識別名を使用した Active Directory のログイン

```
/home/dc150698> ssh -l "David A. Engineer" 10.x.xxx.xxx
  Password:*******
  Sun(TM) Integrated Lights Out Manager
  Version 1.1
  Copyright 2005 Sun Microsystems, Inc. All rights reserved.
  ->
```

ユーザーの承認レベルの決定

いったん認証が終わると、ユーザーのアクセスレベルを次の方法で決定することができます。もっとも単純な方法としては、オペレータまたは管理者のいずれかのユーザーアクセスが、SP の Active Directory の設定から直接取得されます。また、一連の LDAP クエリーを実行して、ユーザーに関連付けられた Active Directory グループを取得することにより、より統合された方法を使用することもできます。

- 1 つめの方法がもっとも簡単に設定できます。ユーザーは `defaultRole` を使用して認証されますが、グループのメンバーシップを判断するためのクエリーは必要ありません。Active Directory データベースでのユーザーの設定はより簡単です。この場合、必要になるのはパスワードのみで、グループのメンバーシップは考慮する必要がありません。SP では、`defaultRole` が `administrator` または `operator` のいずれかに設定されます。Active Directory を通じて認証されるすべてのユーザーには、この設定のみに基づき、管理者ユーザーまたはオペレータユーザーに関連した権限が割り当てられます。
- 2 つめの方法はより複雑で、各ユーザーの設定および認証の両方において、より多くのオーバーヘッドが必要になります。設定の際には、アクセスレベルの決定に使用する、Active Directory データベースの対応するグループ名を使用して、SP 管理者グループテーブルおよびオペレータグループテーブルを設定する必要があります。管理者を指定するために、最大 5 つの Active Directory グループを入力できます。また、オペレータ権限を割り当てるために、さらに 5 つ使用できます。

ユーザーのグループメンバーシップを使用して、SP に設定された Active Directory テーブルから各グループ名を検索し、管理者またはオペレータのいずれかの適切なアクセスレベルが識別されます。2 つめの方法を使用する場合、5 つのユーザーグループのリストがオペレータ権限を持つものとして識別され、5 つのユーザーグループが管理者権限を持つものとして識別されます。ユーザーのグループのリストが、定義された SP ユーザーグループのいずれかに存在しない場合、そのアクセスは拒否されます。

Active Directory 接続のセキュリティーの保護

接続のセキュリティー保護、「なりすまし攻撃」の防止、および LDAP トランザクションの保護を行うには、SSL 証明書認証を使用します。証明書の検証は、システムが必要とするセキュリティーレベルに応じて省略可能です。

CLI を使用した Active Directory 接続のセキュリティーの保護

次の手順では、CLI を使用して Active Directory 接続のセキュリティーを保護する方法について説明します。

▼ CLI を使用して `getcertfile` で処理を実行する

`getcertfile` は、必要に応じて、証明書ファイルのアップロードに使用する方法です。

- **証明書をアップロードするには、次のように入力します。**

  `-> set getcertfile=tftp://`*IP_address***`/`***file-path***`/`***filename***

- **証明書を削除または復元するには、次のように入力します。**

  `-> set getcertfile=remove|restore`

  例:

  ```
  -> set getcertfile=remove
  ```

  アップロードされた既存の証明書ファイルは削除されます。復元は、証明書ファイルのバックアップが現在存在する場合にのみ機能します。目的は、証明書がアップロードされたときにバックアップファイルを 1 つ保存することです。不具合が発生した場合に、古いファイルを復元することができます。

▼ CLI を使用して strictcertmode を有効にする

strictcertmode はデフォルトで無効になっています。SSL が使用されますが、制限的な証明書の検証が実行されます。strictcertmode を有効にした場合は、SSL ハンドシェーク中にサーバーの証明書が提供されると証明書の署名を検証できるように、サーバーの証明書がサーバーにすでにアップロードされている必要があります。

- strictcertmode を使用可能にするには、次のように入力します。

  -> set strictcertmode=enabled

▼ CLI を使用して certfilestatus を確認する

certfilestatus は、証明書のバックアップコピーだけでなく、現在の証明書の状態を反映する動作変数です。strictcertmode が無効になっている場合は、どちらも存在する必要はありません。ただし、strictcertmode が有効になっている場合は、証明書を読み込む必要があります。証明書のバックアップは常に省略可能です。これは、既存の証明書が上書きされる直前にのみ格納されます。

- 証明書の状態を確認するには、次のように入力します。

  -> show /SP/clients/activedirectory certfilestatus

  例:

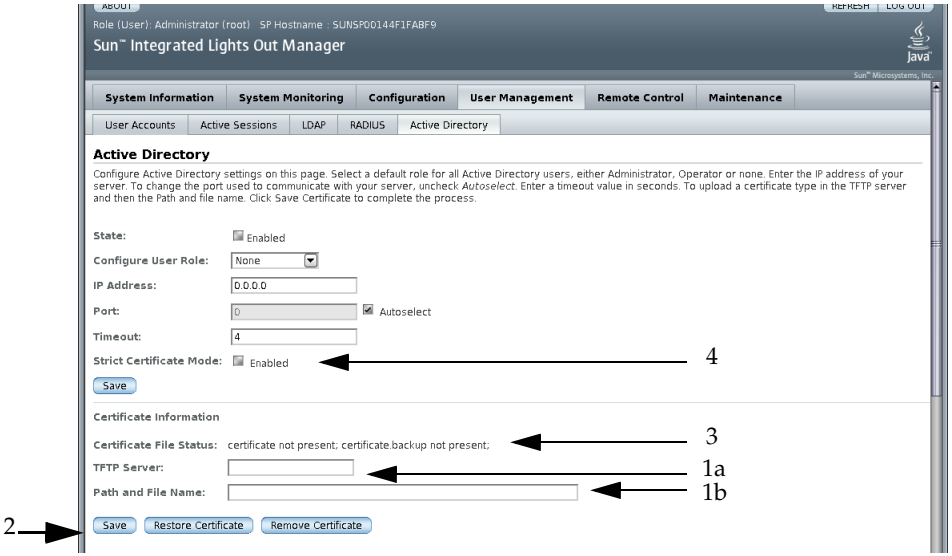
```
 -> show /SP/clients/activedirectory certfilestatus
    Properties:
certfilestatus = certificate not present;certificate.backup
not present;
```

Web インタフェースを使用した Active Directory 接続のセキュリティーの保護

次の手順では、Web インタフェースを使用して Active Directory 接続のセキュリティーを保護する方法について説明します。

図 5-15 に、Active Directory のセキュリティープロパティーと、データを入力する順序を示します。

図 5-15　Active Directory のセキュリティープロパティーとデータの入力順序



▼ Web インタフェースを使用して証明書をアップロードする

1. 管理者権限を持つユーザーとして ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「Active Directory」を選択します。

   「Active Directory」ページが表示されます。図 5-15 に、セキュリティーフィールドを入力する順序を示しています。
3. 「TFTP Server」および「Path and File Name」を入力します。図 5-15 の項目 1a と 1b を参照してください。

4. 「Save (保存)」ボタンをクリックして、証明書の転送を開始します。図 5-15 の項目 2 を参照してください。

注 – 復元と削除のオプションは必要に応じて使用可能です。「Restore Certificate」ボタンまたは「Remove Certificate」ボタンをクリックすると実行できます。

▼ Web インタフェースを使用して証明書ファイルの状態を確認する

1. 管理者権限を持つユーザーとして ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「Active Directory」を選択します。
   「Active Directory」ページが表示されます。図 5-15 の項目 3 を参照してください。
3. 証明書ファイルの状態を確認します。

▼ Web インタフェースを使用して厳密な証明書モードを有効にする

1. 管理者権限を持つユーザーとして ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「Active Directory」を選択します。
   「Active Directory」ページが表示されます。図 5-15 の項目 4 を参照してください。
3. 「Enable (有効)」の隣にあるチェックボックスをクリックして、厳密な証明書モードを有効にします。

Lightweight Directory Access Protocol

ILOM は、OpenLDAP ソフトウェアによるユーザーの Lightweight Directory Access Protocol (LDAP) 認証をサポートします。LDAP は汎用のディレクトリサービスです。ディレクトリサービスは、ディレクトリにあるエントリを管理する分配アプリケーションの集中データベースです。これにより、複数のアプリケーションが単一ユーザーデータベースを共有できます。LDAP の詳細情報は、`http://www.openldap.org/` を参照してください。

LDAP について

LDAP は、クライアントサーバーモデルに基づいています。LDAP にはディレクトリがあり、クライアントはディレクトリサービスを使用して、エントリにアクセスします。ディレクトリに保存されたデータは、複数の LDAP サーバーの間で分配されます。

LDAP のデータは、root を頂点として各エントリに分岐するように階層的に構成されています。階層トップレベルのエントリは、大きな会社や団体を表し、その下に小さな会社や団体のエントリがあります。階層の底辺には、個人または個別リソースのエントリがあります。

LDAP クライアントとサーバー

LDAP クライアントサーバーモデルでは、LDAP サーバーは人、会社や団体、およびリソースの情報に LDAP クライアントがアクセスできるようにします。クライアントは、通常 LDAP サーバーにバンドルされているクライアントユーティリティーを使用し、LDAP データベースを変更します。LDAP データベースを変更すると、すべてのクライアントアプリケーションはすぐに変更を参照し、個々の分散アプリケーションを更新する必要がないようにします。

たとえば、ディレクトリのエントリを更新するには、LDAP クライアントは、更新される属性情報とともにエントリの識別名を LDAP サーバーに送信します。LDAP サーバーは、識別名 (dn) を使用してエントリを検索し、変更操作を実行してディレクトリのエントリを更新します。更新された情報は、その LDAP サーバーを使用するすべての分配アプリケーションでただちに利用できます。

LDAP クライアントは、特に次のような操作を実行できます。

- ディレクトリからエントリを検索して取得します。
- ディレクトリに新しいエントリを追加します。
- ディレクトリのエントリを更新します。

- ディレクトリのエントリを削除します。
- ディレクトリのエントリ名を変更します。

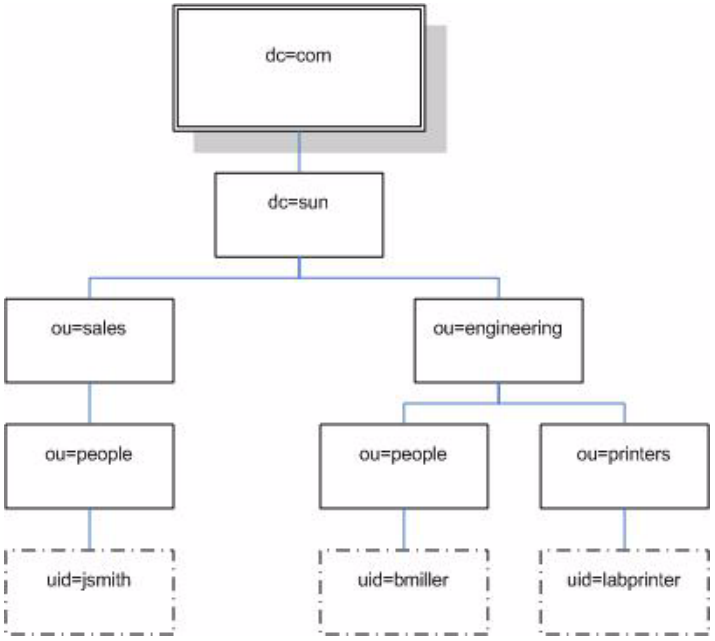
これらの LDAP 操作のいずれを行うにも、LDAP クライアントは LDAP サーバーと接続を確立する必要があります。LDAP は、サーバーがほかのポートで動作している場合でも、TCP/IP のポート番号 389 の使用を指定します。

Sun サーバーは、LDAP サーバーのクライアントになることができます。LDAP 認証を使用するには、Sun サーバーが認証を行うか、あるいはバインドできる LDAP サーバー上にユーザーを作成する必要があります。それにより、クライアントは LDAP サーバーの適切なディレクトリを検索する権限を持ちます。

LDAP サーバーのディレクトリ編成

図 5-16 に示すように、LDAP のデータは階層的に編成されています。

図 5-16　LDAP のディレクトリ構造



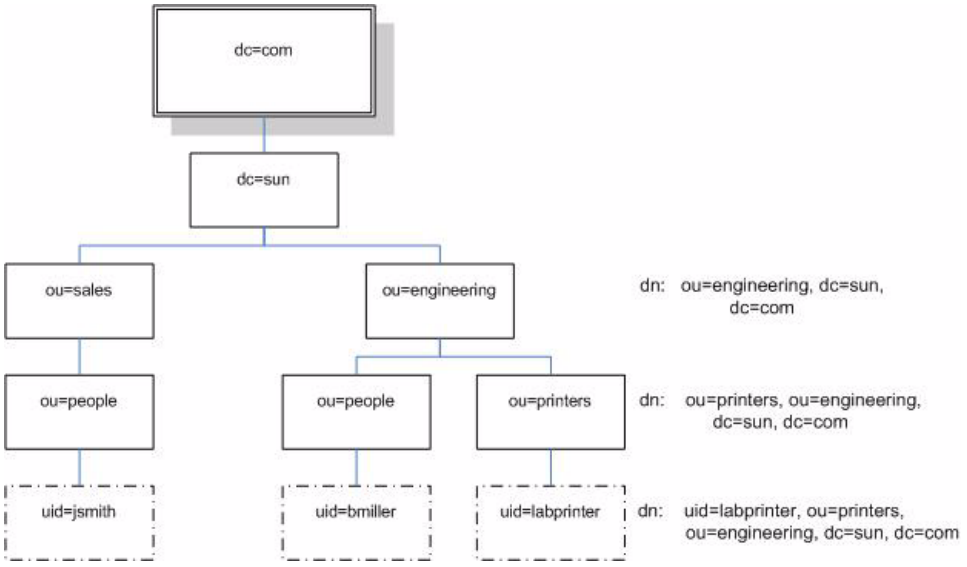
各エントリは、識別名 (dn) により一意に識別されます。DN には、その階層レベルのエントリを一意で識別する名前と、ツリーの root までのエントリを表示するパスがあります。

たとえば、jsmith の DN は次のようになります。

```
dn: uid=jsmith, ou=people, dc=sun.com
```

ここで、uid はエントリのユーザー ID、ou はエントリが属する組織単位、また dc はエントリが属するより大きな組織を意味します。次の図に、ディレクトリ階層で一意にエントリを識別するための識別名の使用方法を示します。

図 5-17　LDAP 識別名



LDAP の設定

LDAP を使用するには、LDAP サーバーのマニュアルに従って LDAP サーバーを設定する必要があります。また、ILOM CLI または Web インタフェースのいずれかを使用して ILOM も設定する必要があります。

次の手順では、使用している LDAP サーバーの設定に関する詳細な知識が必要になります。作業を開始する前に、IP アドレスなど、LDAP サーバーの基本的なネットワーク情報を収集してください。

注 – このタスクは、Linux または Solaris でネームサービスとして LDAP を設定する作業に類似しています。

▼ LDAP サーバーを設定する

1. ILOM に対して認証を行うすべてのユーザーが、「crypt」形式か、または一般的には「MD5 crypt」と呼ばれる、crypt の GNU 拡張で保存されたパスワードを使用していることを確認します。

   例:

   ```
   userPassword: {CRYPT}ajCa2He4PJhNo
   ```

   または

   ```
   userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
   ```

   ILOM は、これらの 2 種類の crypt 形式で保存されたパスワードによる LDAP 認証のみをサポートしています。

2. オブジェクトクラス `posixAccount` および `shadowAccount` を追加し、このスキーマ (RFC 2307) に必要なプロパティー値を入力します。

   表 5-6　LDAP のプロパティー値

必須プロパティー	説明
uid	ILOM にログインするためのユーザー名
uidNumber	任意の固有の数字
gidNumber	任意の固有の数字
userPassword	パスワード
homeDirectory	任意の値 (このプロパティーは、ILOM では無視される)
loginShell	任意の値 (このプロパティーは、ILOM では無視される)

3. LDAP サーバーのユーザーアカウントに対して ILOM のアクセスを許可します。

   LDAP サーバーが匿名バインドを許可するようにするか、または LDAP サーバーにプロキシユーザーを作成します。LDAP サーバーは、ILOM により認証されるすべてのユーザーアカウントに読み取り専用アクセスができます。

   詳細は、LDAP サーバーのマニュアルを参照してください。

▼ CLI を使用して LDAP 用の ILOM を設定する

1. プロキシユーザー名とパスワードを入力します。次のように入力します。

   –> set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales, dc=sun, dc=com" bindpw=*password*

2. LDAP サーバーの IP アドレスを入力します。次のように入力します。

   –> set /SP/clients/ldap ipaddress=*ldapipaddress*

3. LDAP サーバーとの通信に使用するポートを割り当てます。デフォルトのポートは 389 です。次のように入力します。

   –> set /SP/clients/ldap port=*ldapport*

4. ユーザーとグループを含む LDAP ツリー分岐の識別名を入力します。次のように入力します。

   –> set /SP/clients/ldap searchbase="ou=people, ou=sales, dc=sun, dc=com"

   これは、ユーザー認証を検索する LDAP ツリーの場所です。

5. LDAP サービスの状態を enabled に設定します。次のように入力します。

   –> set /SP/clients/ldap state=enabled

6. LDAP 認証の動作を確認するには、LDAP ユーザー名とパスワードを使用して、ILOM にログインします。

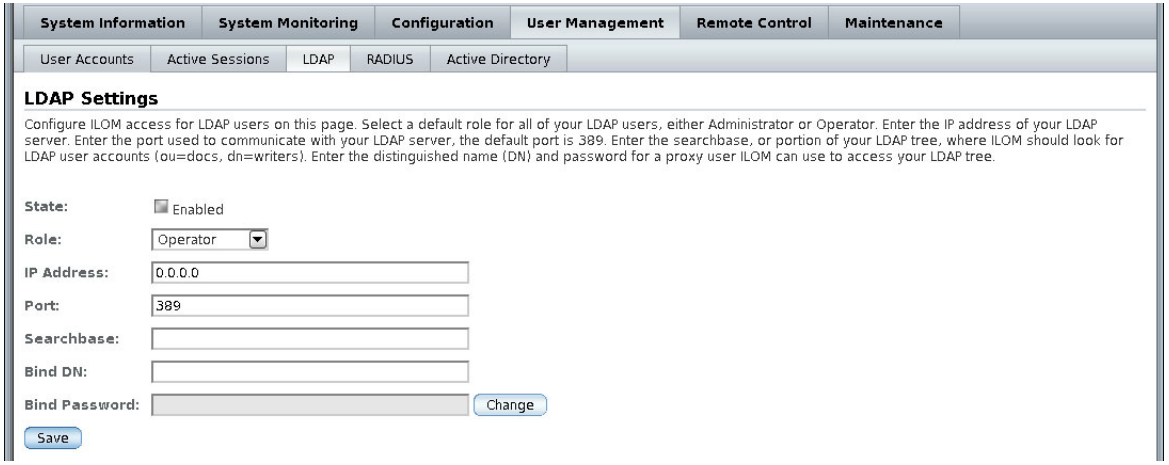
注 – ILOM は、LDAP ユーザーの前にローカルユーザーを検索します。LDAP ユーザー名がローカルユーザーとして存在する場合は、ILOM は認証にローカルアカウントを使用します。

▼ Web インタフェースを使用して LDAP 用の ILOM を設定する

1. 管理者として ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「LDAP」を選択します。

   「LDAP Settings (LDAP 設定)」ページが表示されます。

図 5-18　「LDAP Settings (LDAP 設定)」ページ



3. 次の値を入力します。
   - State (状態) − LDAP ユーザーを認証するには、「Enabled (有効)」チェックボックスを選択します。
   - Role − LDAP ユーザーのデフォルトの役割です。ドロップダウンリストから、「Operator (オペレータ)」または「Administrator (管理者)」を選択します。
   - IP Address (IP アドレス) − LDAP サーバーの IP アドレスです。
   - Port (ポート) − LDAP サーバーのポート番号です。
   - Searchbase (サーチベース) − ユーザーを検索するための LDAP サーバーの分岐を入力します。
   - Bind DN (バインド DN) − LDAP サーバー上の読み取り専用プロキシユーザーの識別名 (DN) を入力します。ILOM がユーザーの検索と認証を行うには、LDAP サーバーに対する読み取り専用のアクセス権が必要になります。
   - Bind Password (バインドパスワード) − 読み取り専用ユーザーのパスワードを入力します。
4. 「Save (保存)」ボタンをクリックします。
5. LDAP 認証の動作を確認するには、LDAP ユーザー名とパスワードを使用して、ILOM にログインします。

注 – ILOM は、LDAP ユーザーの前にローカルユーザーを検索します。LDAP ユーザー名がローカルユーザーとして存在する場合は、ILOM は認証にローカルアカウントを使用します。

RADIUS 認証

ILOM は Remote Authentication Dial-In User Service (RADIUS) 認証をサポートしています。RADIUS は中央ユーザー管理を容易にする認証プロトコルです。RADIUS は、多くのサーバーに中央データベースのユーザーデータへの共有アクセスを提供し、より高度なセキュリティーと容易な管理を実現します。RADIUS サーバーは、複数の RADIUS サーバーやその他の種類の認証サーバーと一緒に動作できます。

RADIUS クライアントとサーバー

RADIUS は、クライアントサーバーモデルに基づいています。RADIUS サーバーはユーザー認証データを提供し、アクセスを許可または拒否することができます。クライアントは、サーバーにユーザーデータを送信して、許可または拒否の応答を受信します。RADIUS のクライアントサーバーモデルでは、クライアントが RADIUS サーバーに Access-Request クエリーを送信します。サーバーはクライアントからの Access-Request メッセージを受信すると、データベース内でユーザーの認証情報を検索します。ユーザーの情報が見つからない場合、サーバーは Access-Reject メッセージを送信し、ユーザーは要求したサービスへのアクセスを拒否されます。ユーザーの情報が見つかった場合、サーバーは Access-Accept メッセージで応答します。Access-Accept メッセージによってユーザーの認証データは確認され、ユーザーは要求したサービスへのアクセスを許可されます。

RADIUS クライアントとサーバーの間のすべてのトランザクションは、共有シークレットと呼ばれる特定のテキスト文字列のパスワードを使用して認証されます。シークレットはネットワークを介して渡されることがないため、クライアントとサーバーのそれぞれでシークレットが既知である必要があります。ILOM 用に RADIUS 認証を設定する場合も、共有シークレットが既知である必要があります。

ILOM で RADIUS 認証を使用するには、ILOM を RADIUS クライアントとして設定する必要があります。

RADIUS パラメータ

表 5-7 に、Web インタフェースと CLI の RADIUS パラメータについて説明します。

表 5-7 RADIUS の Web インタフェースと CLI の設定

Web インタフェース	CLI	説明
State (状態)	**state** *enabled* | *disabled*	RADIUS ユーザーを認証する場合は有効にします。
Role	**defaultrole** *administrator* | *operator*	すべての RADIUS ユーザーのデフォルトの役割を設定します。Administrator (管理者) または Operator (オペレータ) を指定します。
IP Address (IP アドレス)	**ipaddress** *ipaddress*	RADIUS サーバーの IP アドレスです。
Port (ポート)	**port** *portnum*	RADIUS サーバーとの通信に使用するポート番号です。デフォルトのポートは 1812 です。
Shared Secret	**secret** *text*	RADIUS へのアクセスに使用する共有シークレットです。

RADIUS の設定

10 個を超えるローカルユーザーアカウントに ILOM アクセスを提供する必要がある場合は、RADIUS サーバーを適切に設定したあとで、RADIUS 認証を使用するように ILOM を設定できます。

この手順を完了する前に、63 ページの「ユーザーアカウントの管理」の説明に従って、使用している RADIUS 環境に関する適切な情報を収集してください。

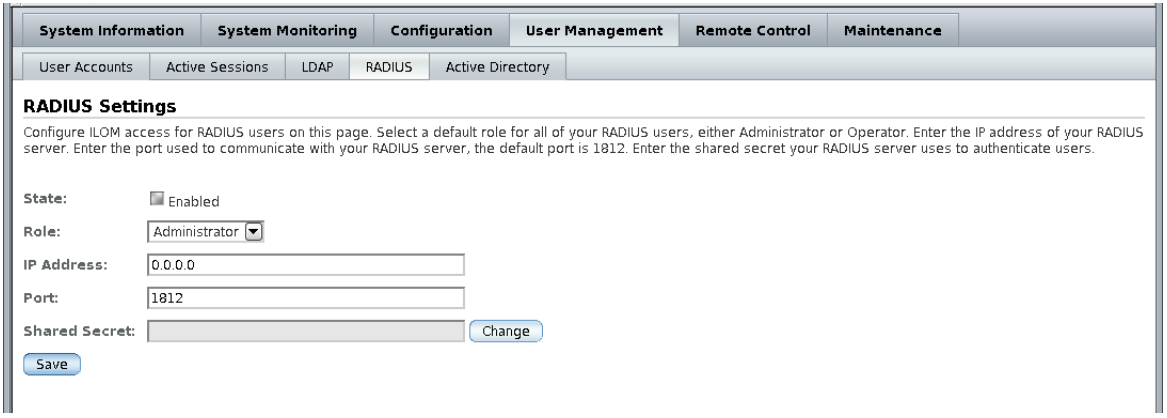
▼ CLI を使用して RADIUS を設定する

1. 管理者権限を持つユーザーで ILOM CLI にログインします。
2. `/SP/clients/radius` に移動します。103 ページの「RADIUS コマンド」を参照してください。
3. 表 5-7 に示されたパラメータを設定します。

▼ Web インタフェースを使用して RADIUS を設定する

1. 管理者として ILOM にログインし、Web インタフェースを開きます。
2. 「User Management (ユーザー管理)」-->「RADIUS」を選択します。
   「RADIUS Settings」ページが表示されます。

図 5-19　「RADIUS Settings」ページ



3. 設定を完了します。
   詳細は、表 5-7 を参照してください。
4. 「Save (保存)」をクリックして変更を有効にします。

RADIUS コマンド

この節では、RADIUS コマンドについて説明します。

show /SP/clients/radius

このコマンドは、管理者およびオペレータが使用できます。

用途

このコマンドは、RADIUS 認証に関連したプロパティーを表示する場合に使用します。

構文

```
show /SP/clients/radius
```

プロパティー

`defaultrole` − すべての RADIUS ユーザーに割り当てられる役割です。Administrator (管理者) または Operator (オペレータ) を指定します。

`ipaddress` − RADIUS サーバーの IP アドレスです。

`port` − RADIUS サーバーとの通信に使用するポート番号です。デフォルトのポートは 1812 です。

`secret` − 使用している RADIUS サーバーへのアクセスに使用する共有シークレットです。

`state` − RADIUS ユーザーへのアクセスを許可または拒否する場合は、この設定をそれぞれ有効または無効にします。

例

```
-> show /SP/clients/radius

  /SP/clients/radius
   Targets:

   Properties:
       defaultrole = Operator
       ipaddress = 129.144.36.142
       port = 1812
       secret = (none)
       state = enabled

   Commands:
       cd
       set
       show

->
```

set /SP/clients/radius

このコマンドは、管理者が使用できます。

用途

このコマンドは、サービスプロセッサ上の RADIUS 認証に関連したプロパティーを設定する場合に使用します。

構文

```
set /SP/clients/radius [defaultrole=[Administrator|Operator]
ipaddress=radiusserverIP port=port# secret=radiussecret state=
[enabled|disabled]]
```

プロパティー

- `defaultrole` − すべての RADIUS ユーザーに適用する権限レベルを割り当てる必要があります。Administrator (管理者) または Operator (オペレータ) を指定します。
- `ipaddress` − RADIUS サーバーの IP アドレスです。

- port − RADIUS サーバーとの通信に使用するポート番号です。デフォルトのポートは 1812 です。
- secret − 使用している RADIUS サーバーへのアクセスに使用する共有シークレットを入力します。これは暗号化鍵とも呼ばれます。
- state − RADIUS ユーザーへのアクセスを許可または拒否する場合は、それぞれ有効または無効にします。

例

```
 -> set /SP/clients/radius state=enabled ipaddress=10.8.145.77
Set 'state' to 'enabled'
Set 'ipaddress' to '10.8.145.77
```

show /SP/clients

このコマンドは、管理者およびオペレータが使用できます。

用途

このコマンドは、LDAP、NTP、RADIUS、SYSLOG クライアントなど、サービスプロセッサからデータを受信できるクライアントを表示するために使用します。

構文

```
show /SP/clients
```

例

```
-> show /SP/clients

 /SP/clients
   Targets:
      ldap
      ntp
      radius
      syslog

   Properties:

   Commands:
       cd
       show
```

注 – オペレータ権限を持つユーザーのみが ntp および syslog ターゲットを表示できます。radius および ldap ターゲットは非表示のままです。

第6章

インベントリと部品の管理

ILOM を使用すると、部品の名前、種類、障害の状態など、部品の詳細を表示できます。また、ILOM を使用して、部品の取り外しおよび取り付けに備えることもできます。

この章には次の節があります。

注 – この章の構文例では、**/SP/** で始まるターゲットを使用しますが、使用している Sun サーバーのプラットフォームによっては、**/CMM/** で始まるターゲットに置き換わる場合があります。サブターゲットは、すべての Sun サーバープラットフォームで共通です。

部品情報の表示およびインベントリの管理

次の手順では、部品の情報を表示する方法について説明します。管理者とオペレータのどちらも部品の情報を表示できます。

▼ CLI を使用して部品の情報を表示する

1. ILOM CLI に管理者またはオペレータとしてログインします。
2. コマンドプロンプトで、次のように入力します。

   -> **show** *component_name* **type**

   例:

```
-> show /SYS/MB type
    Properties:
        type = Motherboard
    Commands:
        show
```

インベントリ情報を表示するプロパティーを次に一覧で示します。表示できるプロパティーは、使用するターゲットの種類によって異なります。

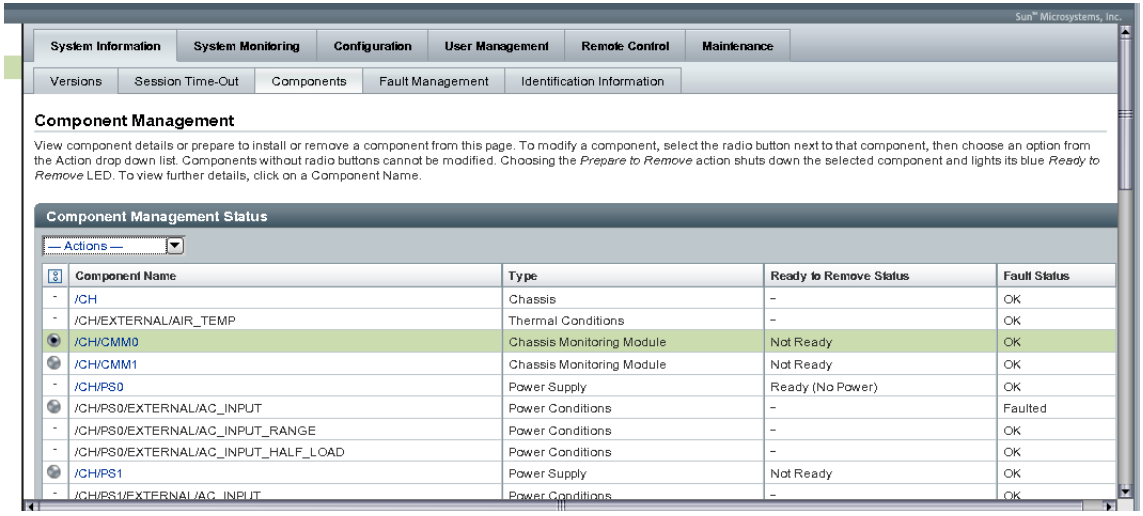
- fru_part_number
- fru_manufacturer
- fru_serial_number
- fru_name
- fru_description
- fru_version
- chassis_serial_number
- chassis_part_number
- product_name
- product_serial_number

- product_part_number
- customer_frudata

▼ Web インタフェースを使用して部品の情報を表示する

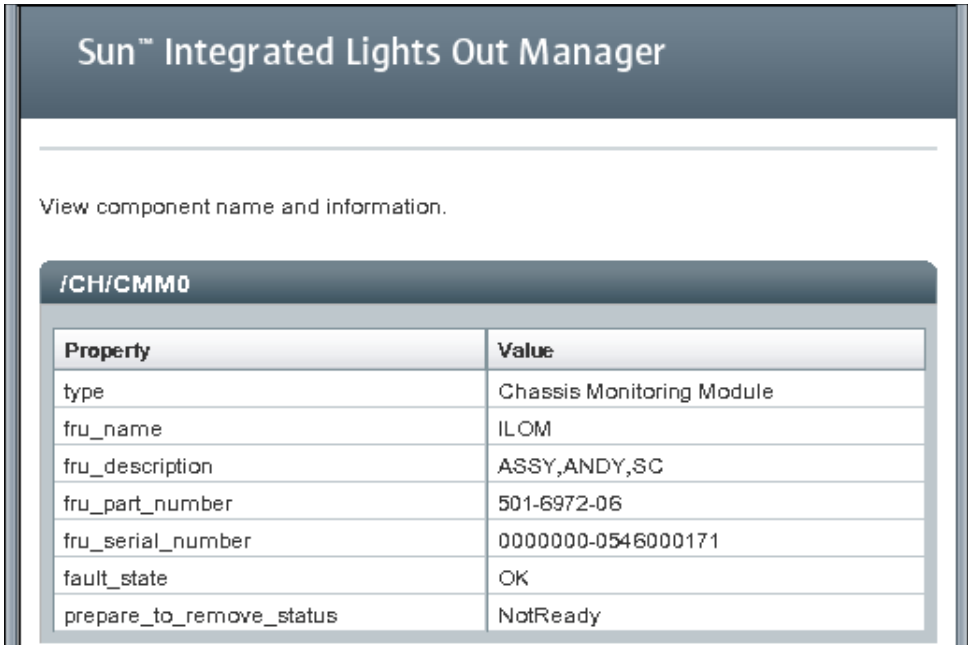
1. ILOM Web インタフェースに管理者またはオペレータとしてログインします。
2. 「System Information (システム情報)」 --> 「Components (部品)」を選択します。
   「Component Management」ページが表示されます。

図 6-1　「Component Management」ページ



3. 「Component Management Status」テーブルで部品の名前をクリックします。
   選択した部品に関する情報を示すダイアログボックスが表示されます。

図 6-2　部品情報のダイアログ



部品に対する操作の実行

インベントリを表示するだけでなく、部品に対して次の操作を実行することもできます。

- 取り外しの準備やサービスへの復帰 — 110 ページの「部品の取り外しおよび交換」を参照。
- 有効化と無効化 — 114 ページの「部品の有効および無効の切り替え」を参照
- 障害のクリアー — 128 ページの「障害管理」を参照。

部品の取り外しおよび交換

取り外しおよび交換の手順を使用すると、システムの実行中に多くの部品を交換できます。手順には、モジュールの取り外しとシステムへの挿入が含まれます。モジュールをシステムから取り外す前に、ILOM の CLI または Web インタフェースを使用してモジュールを準備する必要があります。

▼ CLI を使用して部品を取り外す準備を行う

1. ILOM CLI に管理者またはオペレータとしてログインします。
2. ILOM コマンドプロンプトで、次のように入力します。

   –> set <target> prepare_to_remove_action=true

   例:

   -> **set /CH/RFM0 prepare_to_remove_action=true**

   Set 'prepare_to_remove_action' to 'true'

▼ CLI を使用して部品を取り外す準備ができたかどうかを確認する

部品を取り外す準備ができたら、物理的に取り外せるようになっているかどうかを確認できます。

1. ILOM CLI に管理者またはオペレータとしてログインします。
2. ILOM コマンドプロンプトで、次のように入力します。

   –> show <target> prepare_to_remove_status

   例:

```
-> show /CH/RFM0 prepare_to_remove_status
    Properties:
        prepare_to_remove_status = Ready|NotReady
    Commands:
        cd
        set
        show
        start
        stop
```

この例の Ready|NotReady 文は、デバイスを取り外す準備ができたかどうかを示します。

▼ CLI を使用して部品をサービスに復帰させる

部品を取り外す準備が完了してから、この操作を取り消す場合は、遠隔で実行できます。

1. ILOM CLI に管理者またはオペレータとしてログインします。
2. ILOM コマンドプロンプトで、次のように入力します。

   –> set <target> return_to_service_action=true

   例:

   -> **set /CH/RFM0 return_to_service_action=true**

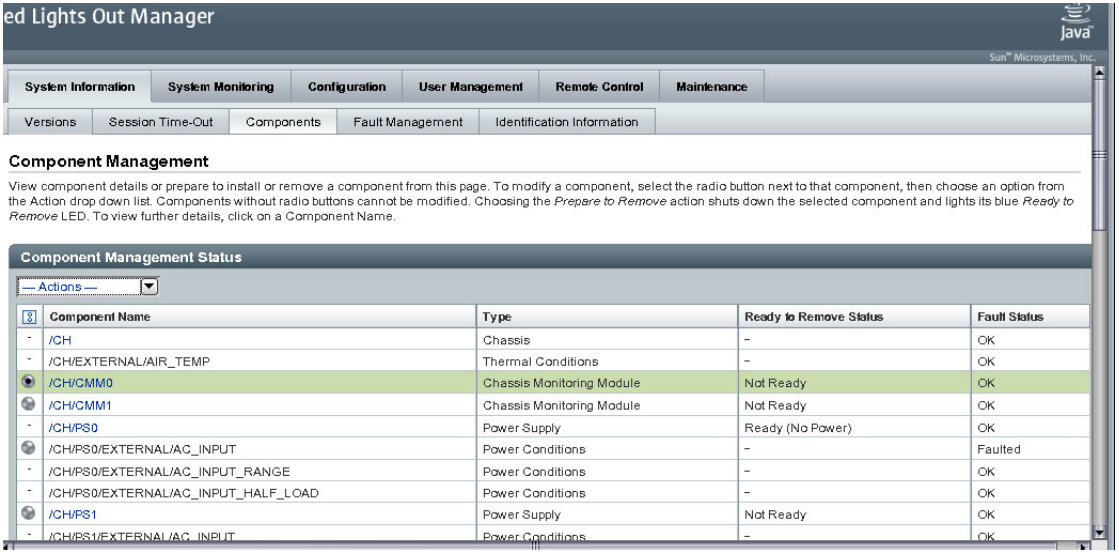
   Set 'return_to_service_action' to 'true'

▼ Web インタフェースを使用して部品を取り外す準備を行う

1. ILOM Web インタフェースに管理者またはオペレータとしてログインします。
2. 「System Information (システム情報)」 --> 「Components (部品)」を選択します。

   「Component Management」ページが表示されます。

図 6-3　「Component Management」ページ



3. 取り外す部品の横にあるラジオボタンを選択します。
   ラジオボタンが表示されていない部品は取り外せません。
4. 「Actions」ドロップダウンリストから「Prepare to Remove」を選択します。

▼ Web インタフェースを使用して部品をサービスに復帰させる

1. ILOM Web インタフェースに管理者またはオペレータとしてログインします。
2. 「System Information (システム情報)」 --> 「Components (部品)」を選択します。
   「Component Management」ページが表示されます。
3. サービスに復帰させる部品の横にあるラジオボタンを選択します。
4. 「Actions」ドロップダウンリストから「Return to Service」を選択します。

部品の有効および無効の切り替え

使用している Sun サーバープラットフォームによっては、特定の部品を有効または無効にできることがあります。詳細は、使用している Sun サーバープラットフォーム固有のマニュアルを参照してください。

▼ CLI を使用して部品を有効および無効にする

1. ILOM CLI に管理者としてログインします。
2. ILOM コマンドプロンプトで、次のように入力します。

```
-> set /SYS/MB/CMP0/P0/C0 component_state=enabled | disabled
```

▼ Web インタフェースを使用して部品を有効および無効にする

1. ILOM Web インタフェースに管理者としてログインします。
2. 「System Information (システム情報)」 --> 「Components (部品)」を選択します。
   「Component Management」ページが表示されます。
3. 有効または無効にする部品の横にあるラジオボタンを選択します。
4. 「Actions」ドロップダウンリストから「Enable (有効)」または「Disable (無効)」を選択します。
   選択した内容に応じて、部品が有効または無効になります。

ポリシーの設定

ポリシーとは、システムの動作を制御する設定です。ポリシーは、システムのデフォルトが設定された状態で出荷されており、ILOM の CLI または Web インタフェースを使用して簡単に修正できます。

▼ CLI を使用してポリシーの設定を構成する

1. ILOM CLI に管理者としてログインします。
2. ILOM コマンドプロンプトで、次のように入力します。

   —> show /CMM/policy

   例:

```
-> show /CMM/policy
 /CMM/policy
    Targets:
    Properties:
Policy1Name = enabled
Policy2Name = enabled
Policy2Name = enabled
    Commands:
        cd
        set
        show
```

3. ILOM コマンドプロンプトで、次のように入力します。

   —> set /CMM/policy

   例:

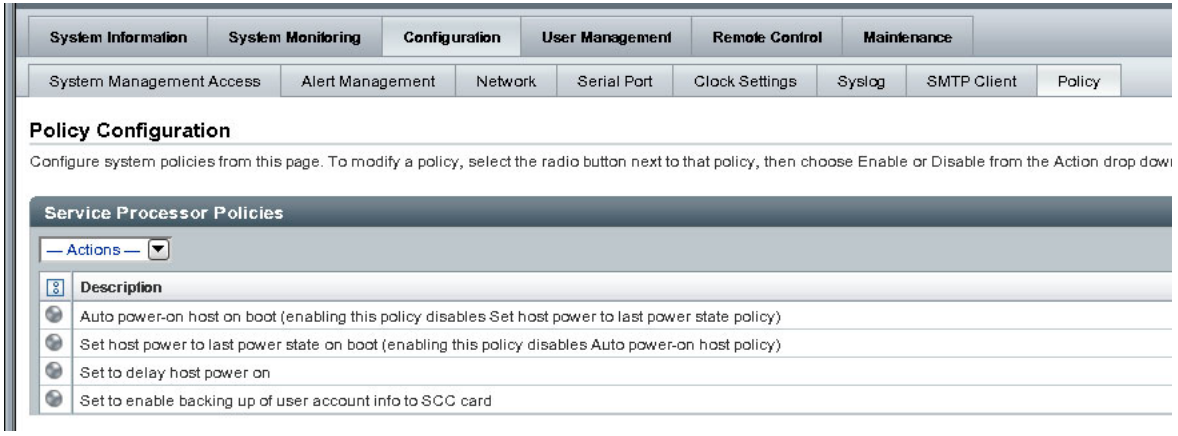
```
-> set /CMM/Policy1Name=enabled
/CMM/Policy1Name=enabled
```

▼ Web インタフェースを使用してポリシーの設定を構成する

使用している Sun サーバープラットフォームによっては、ポリシーを設定する機能が用意されていることがあります。

1. ILOM Web インタフェースに管理者としてログインします。
2. 「Configuration (設定)」 --> 「Policy」を選択します。
   「Policy Configuration」ウィンドウが表示されます。
3. 修正するポリシーの横にあるラジオボタンを選択します。
4. 「Actions」ドロップダウンリストから「Enable (有効)」または「Disable (無効)」を選択します。

図 6-4　「Policy Configuration」ページ



第7章

システム監視と警告管理

ILOM のシステム監視機能を使用すると、システムの健全性を予防保守的に監視することができます。ILOM の警告管理機能を使用すると、システムで発生するイベントの事前通知を受け取ることができます。ILOM のシステム監視機能および警告管理機能は、ILOM の Web インタフェースまたはコマンド行インタフェース (CLI) のいずれかで表示および管理できます。

この章では、次の項目について説明します。

システム監視について

ILOM のシステム監視機能を使用すると、システムの健全性を簡単に確認できます。また、エラーが発生したときに一目でエラーを検出することができます。たとえば、ILOM では次の操作を実行できます。

- システム部品の温度、電流、電圧、速度、および存在に関する瞬時のセンサー測定値を取得します。詳細は、119 ページの「センサー測定値」を参照してください。
- システム全体のインジケータの状態を判断します。詳細は、122 ページの「システムインジケータ」を参照してください。
- ILOM イベントログで、システムエラーを識別し、イベント情報を表示します。詳細は、125 ページの「ILOM イベントログ」を参照してください。
- システム部品の障害の状態を表示します。現在、この機能は Sun Fire X4100 または X4200 シリーズのサーバーを除くすべての Sun サーバープラットフォームで使用可能です。詳細は、128 ページの「障害管理」を参照してください。
- IPMI PET 警告、SNMP トラップ警告、または電子メール通知警告によって、事前にシステムイベントに関して生成された通知を受け取ります。詳細は、140 ページの「警告管理について」を参照してください。

センサー測定値

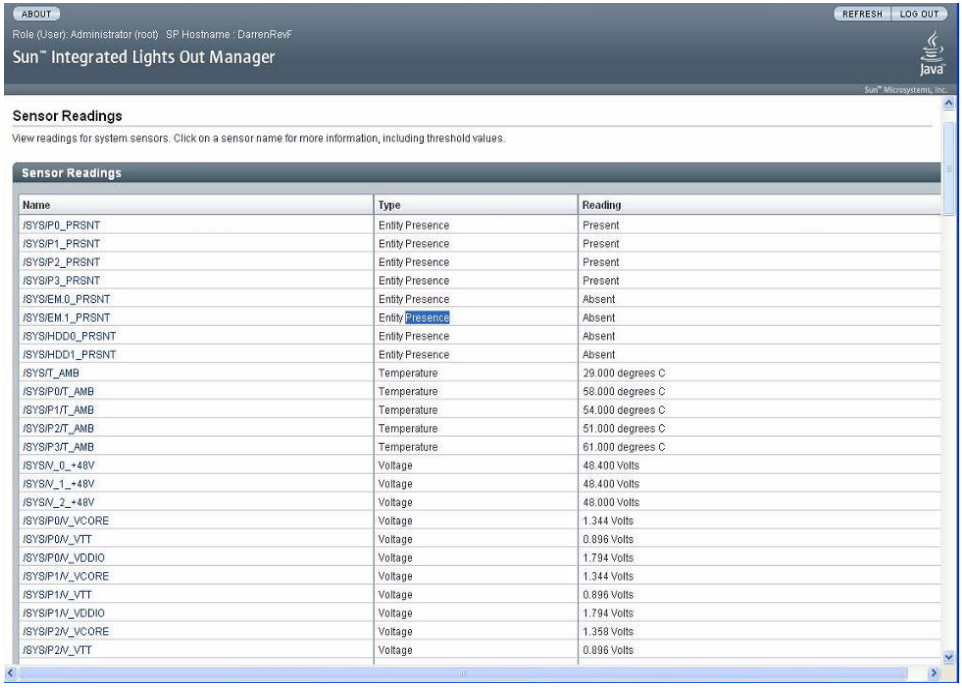
すべての Sun サーバープラットフォームには、電圧、温度、ファン速度、およびその他のシステムに関する属性を測定するセンサーが多数装備されています。ILOM の各センサーには、センサーの上限および下限のしきい値だけでなく、センサーの種類、センサークラス、センサー値などのセンサーに関連する各種設定を示す 9 つのプロパティーが含まれます。

ILOM は定期的にシステム内のセンサーをポーリングし、センサーの状態の変化やセンサーのしきい値を超えたことを検出すると、イベントを ILOM イベントログに報告します。さらに、超えているしきい値のレベルに対応する警告ルールがシステムで有効になっている場合、ILOM は定義された警告の宛先に対して警告メッセージを自動的に生成します。

Web インタフェースを使用したセンサー測定値の取得

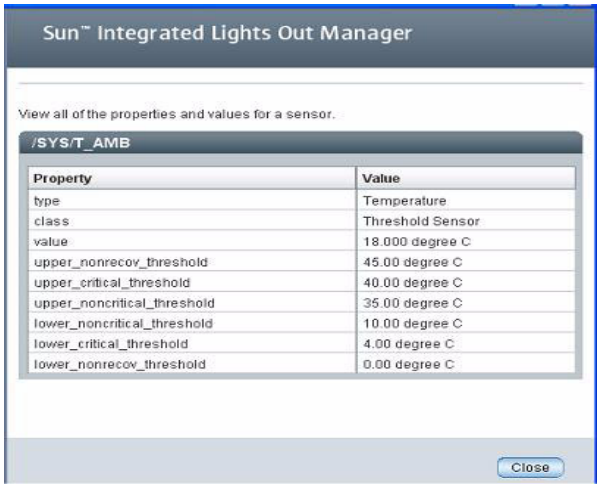
ILOM Web インタフェースでは、「System Monitoring (システム監視)」-->「Sensor Readings (センサー測定値)」ページで、システムの現場交換可能ユニット (FRU) またはほかのシステムインベントリに関する瞬時のセンサー測定値を取得できます。

図 7-1　「Sensor Readings (センサー測定値)」ページ



「Sensor Readings (センサー測定値)」ページには、各センサーの測定値が名前、種類、および測定値ごとに一覧で表示されます。しきい値センサーに関する詳細情報については、このページのしきい値センサー名をクリックして、その他のしきい値プロパティーを表示します。たとえば、しきい値センサー名 /SYS/T_AMB をクリックすると、このセンサーに関する追加情報を表示するダイアログが次のように表示されます。

図 7-2　/SYS/T_AMB の「Sensor Properties」ダイアログ



ILOM Web インタフェースからセンサー測定値を取得する方法の詳細は、131 ページの「Web インタフェースを使用してインジケータの状態を確認する」を参照してください。

CLI を使用したセンサー測定値の取得

ILOM CLI では、システム FRU、および /SYS または /CH ネームスペース内のほかのシステムインベントリに関する瞬時のセンサー測定値を取得できます。これらの両方のネームスペースは、アクセス可能な 2 つのクラスのセンサー測定値をサポートしています。これらのクラスは、「しきい値センサー測定値」および「ディスクリートセンサー測定値」と呼ばれます。これらのクラスの概要を次に説明します。

しきい値センサー

しきい値センサーは、定義済みの非クリティカルおよびクリティカルな上限および下限のしきい値に加えて、センサープロパティー値を示します。通常、しきい値センサーには温度測定値、電圧測定値、またはファン測定値が含まれます。

ILOM CLI を使用してセンサー測定値を取得するには、cd コマンドを使用して、センサーターゲットに移動してから、show コマンドを使用してセンサーのプロパティーを表示します。

たとえば、一部のサーバープラットフォームでは、次のパスを指定して、サーバーの吸気の温度測定値を取得します。

```
cd /SYS/T_AMB

show
```

センサーターゲットを説明するプロパティーが表示されます。たとえば、次のように表示されます。

- Type = Sensor
- Class = Threshold Sensor
- Value = 32.000 degree C
- Upper = non-recov_threshold = 80.00 degree C
- Upper critical_threshold = 75.00 degree C
- Upper noncritical_threshold = 70.00 degree C
- Lower non_recov_threshold = 0.00 degree C
- Lower critical_threshold = 0.00 degree C
- Lower noncritical_threshold = 0.00 degree C

アクセス可能なしきい値センサーターゲットの種類とそれらにアクセスするためのパスの詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

ディスクリートセンサー

ディスクリートセンサーは、センサーターゲットに関連付けられた一連の特定の値を示します。通常、ディスクリートセンサーはエンティティーの存在、エンティティーの障害、または電源状態に関する情報を提供します。

ILOM CLI を使用してディスクリートセンサーの測定値を取得するには、cd コマンドを使用してセンサーターゲットに移動してから、show コマンドを使用してターゲットのプロパティーを表示する必要があります。たとえば、一部の Sun サーバープラットフォームでは、次のパスを指定して、ハードディスクドライブがスロット 0 に存在するかどうかを判断できます。

```
cd /SYS/HDD0_PRSNT

show
```

ディスクリートセンサーターゲットを説明するプロパティーが表示されます。たとえば、次のように表示されます。

- Type = Entity Presence
- Class = Discrete Indicator
- Value = Present

アクセス可能なディスクリートセンサーターゲットの種類とそれらにアクセスするためのパスの詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

システムインジケータ

一般に、システムインジケータ LED は、Sun サーバープラットフォームのポリシーに基づき ILOM によってシステム上で点灯します。通常、次のいずれかの状況が発生した場合に、ILOM によってシステムインジケータ LED が点灯します。

- 部品で障害またはエラーが検出された。
- 現場交換可能ユニット (FRU) が保守を必要としている。
- ホットプラグモジュールの取り外しの準備ができている。
- FRU またはシステム上で活動が発生している。

システムインジケータの状態は、ILOM Web インタフェースまたは ILOM CLI から表示できます。また、状況によっては、システムインジケータの状態を変更できる場合もあります。

サポートされるシステムインジケータの状態

ILOM では、システムインジケータの次の状態をサポートしています。

- **消灯** − 通常の動作状態です。保守は不要です。
- **常時点灯** − 部品を取り外す準備ができています。
- **ゆっくり点滅** − 部品の状態が変わりつつあります。
- **高速点滅** − データセンター内のシステムの位置を確認する場合に役立ちます。
- **スタンバイ点滅** − 部品は起動の準備ができていますが、この時点では動作していません。

システムインジケータの状態の種類

ILOM では、「顧客変更可能」と「システム割り当て」の 2 つの種類のシステムインジケータの状態をサポートしています。

- **顧客変更可能状態** − ILOM の一部のシステムインジケータ LED は顧客変更可能状態を示します。通常、これらの種類のシステムインジケータは、各種システム部品の動作状態を示します。示される状態の種類は、システムインジケータによって異なります。たとえば、システムインジケータによっては、次のような顧客変更可能状態が示されることがあります。
  - **消灯** − 通常の動作状態です。保守は不要です。
  - **高速点滅** − データセンター内のシステムの位置を確認する場合に役立ちます。

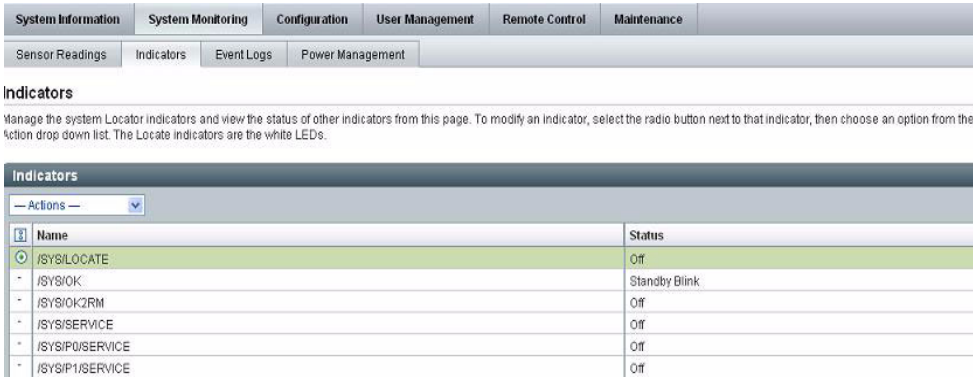
ILOM の Web インタフェースまたは CLI からのシステムインジケータの表示および管理に関する詳細は、123 ページの「Web インタフェースを使用したインジケータの表示および管理」または 124 ページの「CLI を使用したインジケータの表示および管理」を参照してください。

- **システム割り当て状態** – システム割り当てインジケータは顧客設定可能ではありません。これらの種類のシステムインジケータは、部品の動作状態についての読み取り専用の値を示します。ほとんどの Sun サーバープラットフォームで、システム割り当てインジケータは「保守要求 LED」です。通常、これらの種類の LED は次のいずれかの状況が検出された場合に点灯します。
  - システムコンポーネントで障害またはエラーが検出された。
  - ホットプラグモジュールの取り外しの準備ができている。
  - 現場交換可能ユニット (FRU) が保守を必要としている。

Web インタフェースを使用したインジケータの表示および管理

ILOM Web インタフェースでは、「Indicators」ページでシステムインジケータを表示および管理します。このページには、システムインジケータが名前および状態ごとに一覧で表示されます。顧客変更可能状態を示すシステムインジケータは、ラジオボタン付きで表示されます。顧客変更可能インジケータの状態を変更するには、このラジオボタンを選択して、「Actions」ドロップダウンリストから状態を選択します。

図 7-3　「Indicators」ページ



ILOM Web インタフェースを使用して瞬時のセンサー測定値を取得する方法の詳細は、132 ページの「Web インタフェースを使用してセンサー測定値を取得する」を参照してください。

CLI を使用したインジケータの表示および管理

ILOM CLI では、すべてのシステムインジケータが /SYS または /CH ネームスペースからアクセス可能です。通常は、cd コマンドを使用してシステムインジケータのターゲットに移動し、show コマンドを使用してターゲットのプロパティーを表示します。システムインジケータの状態は、set コマンドを使用して変更できます。set コマンドは、顧客変更可能状態を示すシステムインジケータでのみサポートされています。システムインジケータの状態を変更できるかどうかを判断するには、cd コマンドを使用してインジケータのターゲットに移動してから、show コマンドを使用してシステムインジケータのプロパティーを表示します。次に例を示します。

cd /SYS/*indicator target* または cd /CH/*indicator target*

show

システムインジケータに関連付けられたターゲット、プロパティー、およびコマンドが表示されます。次に例を示します。

```
Targets:
Properties:
Type = indicator
Value = Off
Commands:
  cd
  set
  show
```

Commands の一覧に set コマンドが表示された場合は、システムインジケータの状態を変更できます。システムインジケータの状態を変更するには、次の構文を使用します。

set value=*state_name*

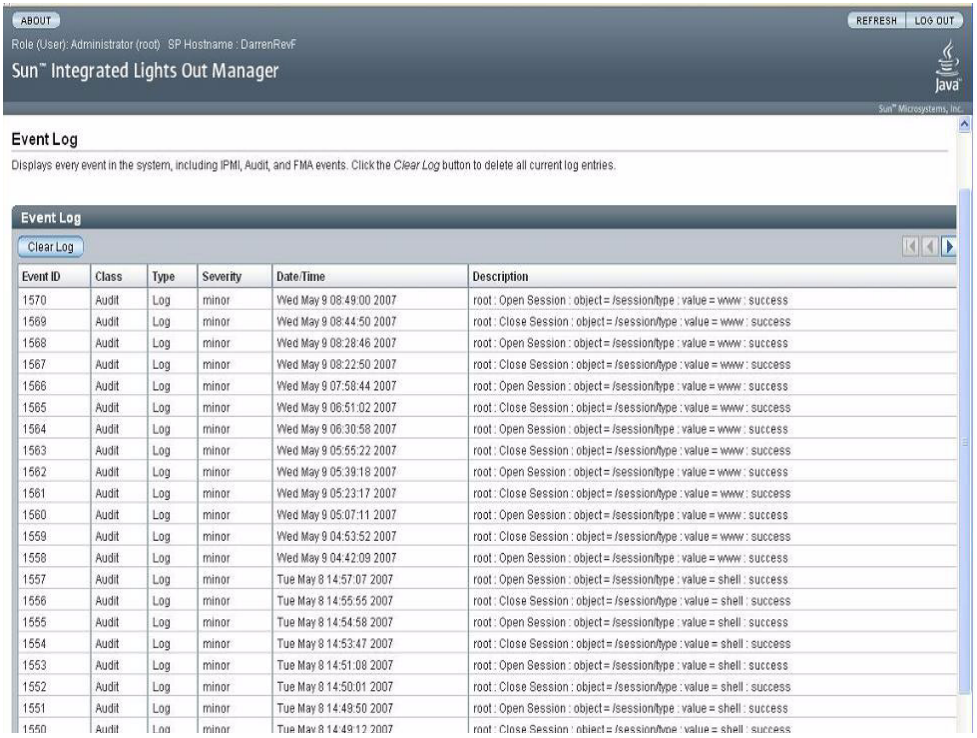
使用しているシステムでサポートされているシステムインジケータとそれらにアクセスするためのパスの詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

ILOM イベントログ

ILOM イベントログにより、システムで発生したすべてのイベントに関する情報を表示できます。これらのイベントには、IPMI イベントのほか、ILOM の設定の変更、ソフトウェアイベント、警告、アラート、部品の障害が含まれます。ILOM イベントログに記録されるイベントの種類は、Sun サーバープラットフォームによって異なります。ILOM イベントログに記録されるイベントに関する特定の情報については、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

ILOM イベントログは、ILOM Web インタフェースまたは CLI から表示および管理できます。ILOM イベントログを表示および管理する方法の詳細は、133 ページの「Web インタフェースを使用して ILOM イベントログを表示またはクリアする」または 134 ページの「CLI を使用して ILOM イベントログを表示またはクリアする」を参照してください。

図 7-4　ILOM イベントログの例



イベントログのタイムスタンプと ILOM のクロック設定

ILOM は、ホストサーバーの UTC/GMT タイムゾーンに基づいてイベントログのタイムスタンプを取得します。ただし、別のタイムゾーンに存在するクライアントシステムからイベントログを参照すると、タイムスタンプはクライアントシステムのタイムゾーンに合わせて調整されます。そのため、ILOM イベントログにある 1 つのイベントが、2 つのタイムスタンプで表示されることがあります。

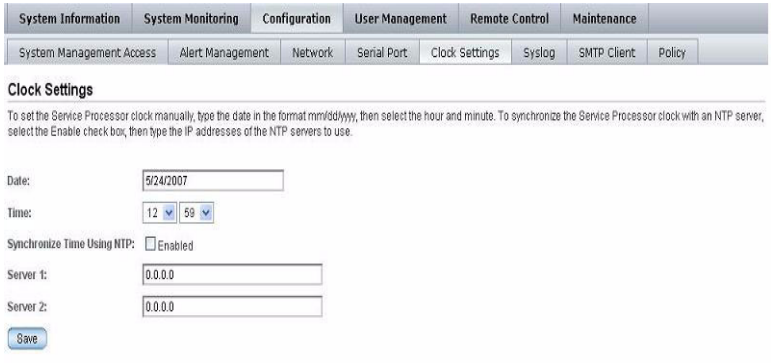
サポートされるクロック設定

ILOM では、ホストサーバーの UTC/GMT タイムゾーンに基づいて ILOM クロックを手動で設定するか、ILOM クロックに NTP サーバーの IP アドレスを設定してネットワーク上のほかのシステムと ILOM クロックを同期させることができます。

Web インタフェースを使用したクロック設定の表示および設定

ILOM Web インタフェースの「Configuration (設定)」-->「Clock Settings (クロック設定)」ページで、ILOM クロック設定を表示または設定できます。

図 7-5　「Clock Settings (クロック設定)」ページ



ILOM Web インタフェースからクロック設定を表示および設定する方法の詳細は、136 ページの「Web インタフェースを使用してクロック設定を表示および設定する」を参照してください。

CLI を使用したクロック設定の表示および設定

show コマンドを使用すると、ILOM CLI から ILOM クロック設定を表示できます。たとえば、一部のサーバープラットフォームでは、次のパスを指定してクロック設定を表示できます。

```
show /sp/clock
```

次の set コマンドの構文を使用すると、CLI から ILOM クロック設定を手動で設定できます。

```
set target property_name=value
```

また、ILOM CLI で、NTP サーバーの IP アドレスを設定して、ネットワーク上のほかのシステムと同期するように、ILOM クロック設定を設定することもできます。たとえば、一部の Sun サーバープラットフォームでは、次のパスを入力して NTP サーバーの IP アドレスを設定し、NTP 同期を使用可能にすることができます。

- NTP サーバーの IP アドレスを設定する例を次に示します。

  ```
  set /SP/clients/ntp/server/1 address=ip_address
  ```

- 同期を使用可能にする例を次に示します。

  ```
  set /SP/clock/usentpserver=enabled
  ```

ILOM CLI から ILOM クロック設定を設定する方法の詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

また、次の内容に関するプラットフォーム固有のクロック情報は、Sun サーバープラットフォームのユーザーマニュアルを参照してください。

- ILOM の現在の時間は SP を再起動しても維持されるかどうか。
- ILOM の現在の時間をホストの起動時にホストと同期させることができるかどうか。
- 時刻を格納するリアルタイムクロック要素があるかどうか。

syslog 情報

syslog は多くの環境で使用されている標準ログ機能です。syslog はイベントのログの一般的な機能セットと、イベントを遠隔ログホストに転送するためのプロトコルを定義しています。syslog を使用して、1 つの場所にある ILOM の複数のインスタンスのイベントを組み合わせることができます。ログエントリには、クラス、種類、重要度、説明などのローカル ILOM イベントログに表示される情報とすべて同じ情報が格納されます。syslog を 1 つまたは 2 つの IP アドレスに送信するように ILOM を設定する方法の詳細は、137 ページの「Web インタフェースを使用して遠隔 syslog 受信側の IP アドレスを設定する」または 139 ページの「CLI を使用して遠隔 syslog 受信側の IP アドレスを設定する」を参照してください。

障害管理

ほとんどの Sun サーバープラットフォームには、ILOM に障害管理ソフトウェア機能が含まれています。この機能を使用して、ハードウェア障害の発生時にそれらを診断するだけでなく、システムハードウェアの健全性を予防保守的に監視することができます。障害管理ソフトウェアは、システムハードウェアの監視に加えて、環境の状況を監視し、システムの環境が許容パラメータの範囲外になると報告します。システムコンポーネント上の各種センサーが絶え間なく監視されます。問題が検出されると、障害管理ソフトウェアは自動的に次の処理を実行します。

- 障害の発生したコンポーネントの保守要求 LED を点灯します。
- ILOM 管理インタフェースを更新し、障害状況を反映させます。
- ILOM イベントログに障害に関する情報を記録します。

障害の発生したコンポーネントの状態は、ILOM Web インタフェースまたは ILOM CLI から表示できます。詳細は、次を参照してください。

- 129 ページの「Web インタフェースを使用した障害状態の表示」
- 130 ページの「CLI を使用した障害状態の表示」

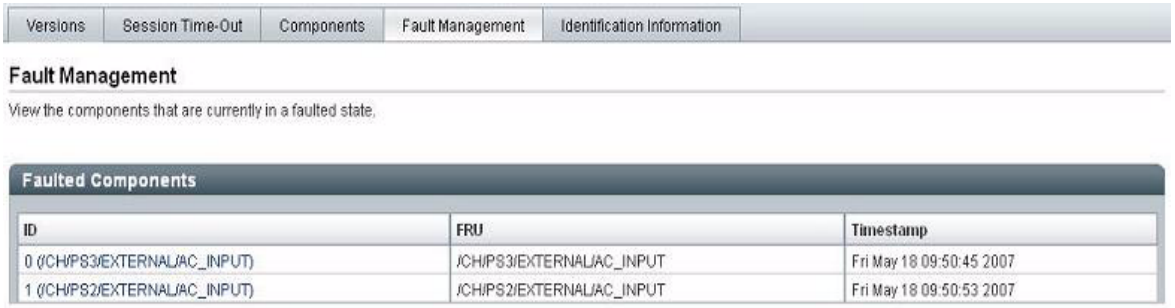
障害管理ソフトウェアによって監視されるシステムコンポーネントの種類および環境の状況は、Sun サーバープラットフォームによって異なります。障害管理ソフトウェアによって監視されるコンポーネントの詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

注 – 現在、ILOM 障害管理機能は Sun Fire X4100 または X4200 シリーズのサーバーを除くすべての Sun サーバープラットフォームで使用可能です。

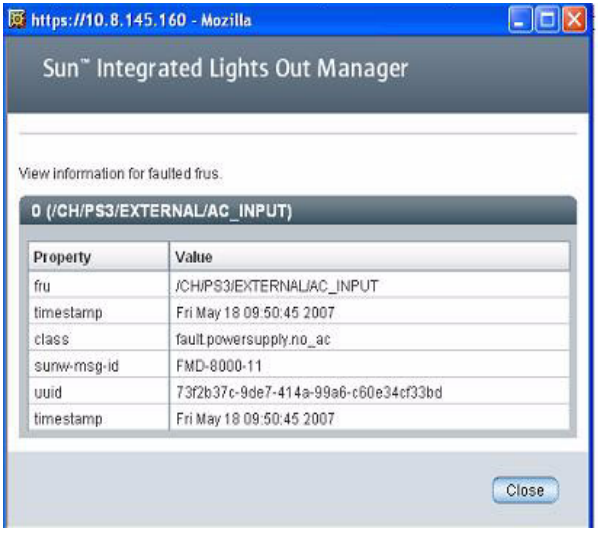
Web インタフェースを使用した障害状態の表示

ILOM Web インタフェースでは、「Fault Management」ページで、現在障害状態にあるシステムコンポーネントを表示できます。

図 7-6　「Fault Management」ページの例



「Fault Management」ページには、ID、FRU、およびタイムスタンプごとに障害の発生したコンポーネントが一覧で表示されます。障害の発生したコンポーネントの ID をクリックすると、障害の発生したコンポーネントに関する追加情報にアクセスできます。たとえば、障害の発生したコンポーネントの ID `0(CH/PS3/EXTERNAL/AC_INPUT)` をクリックすると、障害の発生したコンポーネントに関する追加の詳細を示すダイアログが次のように表示されます。



または、ILOM Web インタフェースの「Component Management」ページで、コンポーネントの障害状態を識別できます。

図 7-7　「Component Management」ページ − Fault Status

Component Management Status

Component Name	Type	Ready to Remove Status	Fault Status
/	Container	-	OK
/SYS	Host System	-	OK
/SYS/BIOS	BIOS	-	-
/SYS/P0	Host Processor	-	OK
/SYS/P0/D0	DIMM	-	OK
/SYS/P0/D1	DIMM	-	OK
/SYS/P1	Host Processor	-	OK
/SYS/P2	Host Processor	-	OK
/SYS/P3	Host Processor	-	OK
/SYS/HDD0	Hard Disk	-	OK

システムで提供されている ILOM 障害管理機能の詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

CLI を使用した障害状態の表示

ILOM CLI では、`show` コマンドを使用して、コンポーネントの障害の状態を表示できます。たとえば、Sun サーバープラットフォームに応じて、次のいずれかのパスを指定できます。

```
show /SP/faultmgmt
show /CH/faultmgmt
```

システムで提供されている ILOM 障害管理機能の詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

システムセンサー、インジケータ、ILOM イベントログの監視

システムセンサー、システムインジケータ、ILOM イベントログのイベントを監視するには、次の手順を参照してください。

▼ Web インタフェースを使用してインジケータの状態を確認する

ILOM Web インタフェースからシステムインジケータの状態を確認するには、次の手順に従います。

1. **Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。**

   ILOM Web インタフェースのログインページが表示されます。

2. **ILOM ログインページにユーザー名とパスワードを入力し、「OK」をクリックします。**

   ILOM Web インタフェースが表示されます。

3. **Web インタフェースページで、「System Monitoring (システム監視)」--> 「Indicators」を選択します。**

   「Indicators」ページが表示されます。

注 – サーバーの電源が切断されている場合は、多くのインジケータが「測定値なし」として表示されます。

---

4. **「Indicators」ページで、次の手順を実行します。**

   a. **表示するインジケータの名前を見つけます。**

b. インジケータの状態を切り替えるには、切り替えるインジケータに関連付けられているラジオボタンをクリックし、「Actions」ドロップダウンリストボックスをクリックして、「Turn LED Off」または「Set LED to Fast Blink」のいずれかを選択します。

変更を確認するダイアログが表示されます。

c. 「OK」をクリックして変更を確認します。

▼ Web インタフェースを使用してセンサー測定値を取得する

ILOM Web インタフェースからセンサー測定値を取得するには、次の手順に従います。

1. Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。

   ILOM Web インタフェースのログインページが表示されます。

2. ILOM ログインページにユーザー名とパスワードを入力し、「OK」をクリックします。

   ILOM Web インタフェースが表示されます。

3. Web インタフェースページで、「System Monitoring (システム監視)」-->「Sensor Readings (センサー測定値)」を選択します。

   「Sensor Readings (センサー測定値)」ページが表示されます。

注 – サーバーの電源が切断されている場合は、多くのコンポーネントが「測定値なし」として表示されます。

---

4. 「Sensor Reading (センサー測定値)」ページで、次の手順を実行します。

   a. 表示するセンサーの名前を見つけます。

   b. センサーの名前をクリックして、そのセンサーに関連付けられているプロパティー値を表示します。

アクセス可能なディスクリートセンサーのターゲットの種類とそれらにアクセスするためのパスの詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

▼ Web インタフェースを使用して ILOM イベントログを表示またはクリアする

ILOM Web インタフェースを使用して、ILOM イベントログのイベントを表示またはクリアするには、次の手順に従います。

1. **Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。**

   ILOM Web インタフェースのログインページが表示されます。

2. **ILOM ログインページにユーザー名とパスワードを入力し、「OK」をクリックします。**

   ILOM Web インタフェースが表示されます。

3. **Web インタフェースページで、「System Monitoring (システム監視)」-->「Event Logs (イベントログ)」を選択します。**

   「Event Logs (イベントログ)」ページが表示されます。

4. **「Event Logs (イベントログ)」ページで、次のいずれかの手順を実行します。**

   - **エントリ全体でページを操作する** − テーブルの上部および下部にあるページナビゲーションコントロールを使用して、テーブル内の使用可能なデータを前後に移動します。

     大量のエントリを選択すると、小数のエントリを選択した場合よりも Web インタフェースの応答が遅くなる場合があります。

   - **一覧をスクロールしてエントリを表示する** − 次の表に、ログに表示される各列について説明します。

列のラベル	説明
Event ID (イベント ID)	イベントの番号で、1 番から順に付けられます。
Class/Type	• Audit/Log − 設定が変更されるコマンド。説明には、ユーザー、コマンド、コマンドパラメータ、成功と失敗が記述されます。 • IPMI/Log − IPMI SEL に記録されたイベントは、管理ログにも記録されます。 • Chassis/State (状態) − インベントリの変更および全般的なシステム状態の変更。 • Chassis/Action − サーバーのモジュールおよびシャーシの停止イベント、FRU のホットインサート/リムーバブル、および押された「Reset Parameters」ボタンのカテゴリ。 • FMA/Fault − 障害管理アーキテクチャー (FMA) の障害。説明には、FMA によって検出された障害の時刻と疑われるコンポーネントが表示されます。 • FMA/Repair − FMA の修復。説明にはコンポーネントが表示されます。

列のラベル	説明
Severity	「Critical (重大)」、「Major」、または「Minor」。
Date (日付)/Time	イベントが発生した日時です。時間情報プロトコル (NTP) サーバーで ILOM 時間を設定できる場合、ILOM クロックは協定世界時 (UTC) を使用します。
説明	イベントの説明です。

- **イベントログをクリアする** – イベントログをクリアするには「Clear Event Log (イベントログのクリア)」ボタンをクリックします。確認のダイアログが表示されます。確認ダイアログで「OK」をクリックすると、エントリがクリアされます。

注 – ILOM イベントログには、IPMI エントリのコピーを含むさまざまな種類のイベントが蓄積されます。ILOM イベントログをクリアすると、IPMI エントリを含むログ内のすべてのエントリがクリアされます。ただし、ILOM イベントログエントリをクリアしても、IPMI ログに直接送信された実際のエントリはクリアされません。

▼ CLI を使用して ILOM イベントログを表示またはクリアする

ILOM CLI を使用して、システムイベントログのイベントを表示またはクリアするには、次の手順に従います。

1. **サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。**

   - **ローカルシリアルコンソール接続**

     サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

     詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

   または

   - **遠隔 Secure Shell (SSH) 接続**

     サーバー SP または CMM との Secure Shell 接続を確立します。

     遠隔クライアントから、root としてサーバー SP またはアクティブ CMM へのセキュリティー保護された接続を確立します。

     たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

     `ssh -l root` *server_ip_address*

     `Password:` **`changeme`**

   デフォルトのコマンドプロンプト (->) が表示されます。

2. 次のいずれかのコマンドパスを入力して、作業用ディレクトリを設定します。
   - ラック搭載型サーバーの SP の場合: **cd /SP/logs/event**
   - シャーシ内のブレードサーバーの SP の場合: **cd /CH/BL*n*/SP/logs/event**
   - CMM の場合: **cd /CMM/logs/event**
3. 次のコマンドパスを入力して、イベントログ一覧を表示します。

   show list

   イベントログの内容が表示されます。例を次に示します。

```
ID     Date/Time                 Class     Type      Severity
-----  ------------------------  --------  --------  --------
1522   Sun Jul 30 01:11:36 2006  Audit     Log       minor
       root : Close Session : object = /session/type : value = www : success
1521   Sun Jul 30 01:05:34 2006  Audit     Log       minor
       root : Close Session : session ID = 1307912184 : success
```

4. イベントログで、次のいずれかのタスクを実行します。
   - 一覧を下にスクロールし、エントリを表示する − 「q」以外の任意のキーを押します。次の表に、ログに表示される各列について説明します。

列のラベル	説明
Event ID (イベント ID)	イベントの番号で、1 番から順に付けられます。
Class/Type	• Audit/Log − 設定が変更されるコマンド。説明には、ユーザー、コマンド、コマンドパラメータ、成功と失敗が記述されます。 • IPMI/Log − IPMI SEL に記録されたイベントは、管理ログにも記録されます。 • Chassis/State (状態) - インベントリの変更および全般的なシステム状態の変更。 • Chassis/Action − サーバーのモジュールおよびシャーシの停止イベント、FRU のホットインサート/リムーバブル、および押された「Reset Parameters」ボタンのカテゴリ。 • FMA/Fault − 障害管理アーキテクチャー (FMA) の障害。説明には、FMA によって検出された障害の時刻と疑われるコンポーネントが表示されます。 • FMA/Repair − FMA の修復。説明にはコンポーネントが表示されます。
Severity	「Critical (重大)」、「Major」、または「Minor」。
Date (日付)/Time	イベントが発生した日時です。時間情報プロトコル (NTP) サーバーで ILOM 時間を設定できる場合、ILOM クロックは協定世界時 (UTC) を使用します。
説明	イベントの説明です。

- **イベントログを閉じる (ログの表示を中止する)** – 「q」キーを押します。
- **イベントログ内のエントリをクリアする** – 次の手順を実行します。

a. **set clear=true** と入力します。

確認のメッセージが表示されます。

b. 次のいずれかを入力します。

- エントリをクリアするには、**y** と入力します。
- ログのクリアを取り消すには、**n** と入力します。

注 – ILOM イベントログには、IPMI エントリのコピーを含むさまざまな種類のイベントが蓄積されます。ILOM イベントログをクリアすると、IPMI エントリを含むログ内のすべてのエントリがクリアされます。ただし、ILOM イベントログエントリをクリアしても、IPMI ログに直接送信された実際のエントリはクリアされません。

▼ Web インタフェースを使用してクロック設定を表示および設定する

この手順を完了するには、NTP サーバーの IP アドレスが必要です。

1. Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。

   ILOM Web インタフェースのログインページが表示されます。

2. ILOM ログインページにユーザー名とパスワードを入力し、「OK」をクリックします。

   ILOM Web インタフェースが表示されます。

3. Web インタフェースページで、「Configuration (設定)」-->「Clock Settings (クロック設定)」を選択します。

   「Clock Settings (クロック設定)」ページが表示されます。

4. 「Clock Settings (クロック設定)」ページで、次のいずれかの処理を実行します。

   - 既存の設定を表示します。
   - ホストサーバー SP の日時を手動で設定します。

   a. 「Date (日付)」テキストボックスに、mm/dd/yy の形式で日付を入力します。

   b. 「Time」ドロップダウンリストボックスで、時間と分を設定します。

   - NTP サーバーの IP アドレスを設定して、同期を使用可能にします。

   a. 「Synchronize Time Using NTP (NTP を使用して時刻を同期する)」の隣にある「Enabled (有効)」チェックボックスを選択します。

b. 「Server 1」テキストボックスに、使用する主 NTP サーバーの IP アドレスを入力します。

c. (省略可能)「Server 2」テキストボックスに、使用する副 NTP サーバーの IP アドレスを入力します。

5. 「Save (保存)」をクリックして変更を有効にします。

▼ Web インタフェースを使用して遠隔 syslog 受信側の IP アドレスを設定する

Web インタフェースを使用して、ILOM の遠隔 syslog 受信側の IP アドレスを設定するには、次の手順に従います。

1. Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。

   ILOM Web インタフェースのログインページが表示されます。

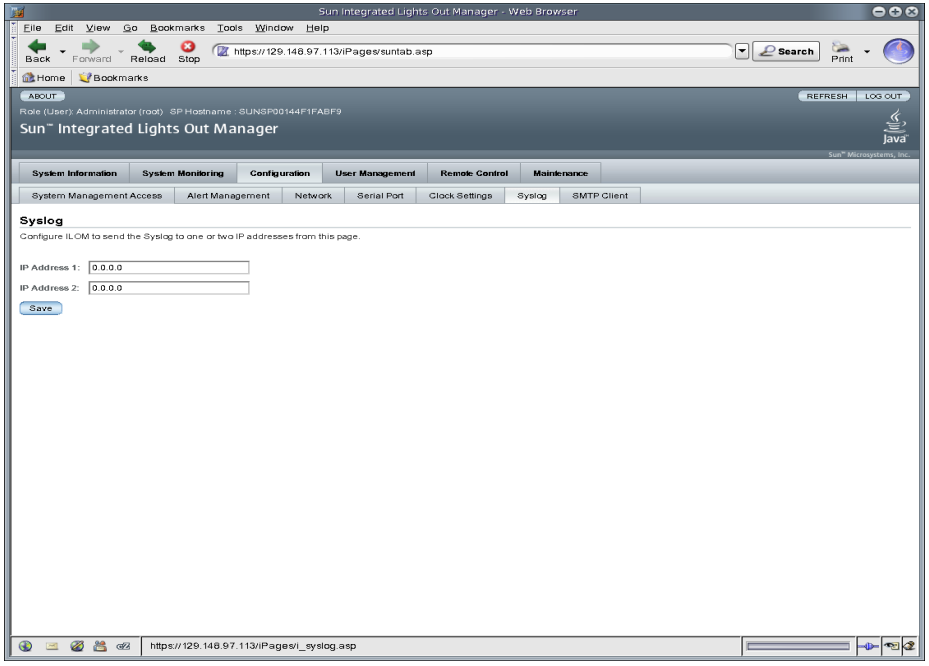
2. ILOM ログインページにユーザー名とパスワードを入力し、「OK」をクリックします。

   ILOM Web インタフェースが表示されます。

3. ILOM Web インタフェースで、「Configuration (設定)」-->「Syslog」を選択します。

   「Syslog」ページが表示されます。

図 7-8　「Syslog」ページ



4. 「IP Address 1」および「IP Address 2」フィールドに、syslog データの送信先の 2 つの場所の IP アドレスを入力します。
5. 「Save (保存)」をクリックして設定を有効にします。

▼ CLI を使用して遠隔 syslog 受信側の IP アドレスを設定する

CLI を使用して、遠隔 syslog 受信側の IP アドレスを設定するには、次の手順に従います。

1. **サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。**
   - **ローカルシリアルコンソール接続**

     サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

     詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

   または

   - **遠隔 Secure Shell (SSH) 接続**

     サーバー SP または CMM との Secure Shell 接続を確立します。

     遠隔クライアントから、root としてサーバー SP またはアクティブ CMM へのセキュリティー保護された接続を確立します。

     たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

     `ssh -l root` *server_ip_address*

     `Password:` **`changeme`**

   デフォルトのコマンドプロンプト (->) が表示されます。

2. **次のいずれかのコマンドパスを入力して、作業用ディレクトリを設定します。**
   - ラック搭載型サーバーの SP の場合: **`cd /SP/clients/syslog`**
   - シャーシ内のブレードサーバー SP の場合: **`cd /CH/BL`***n*`/SP/clients/syslog`**
   - CMM の場合: **`cd /CMM/clients/syslog`**

3. syslog プロパティーを表示するには、`show` コマンドを入力します。

   プロパティーが表示されます。たとえば、SP ではじめて syslog プロパティーにアクセスすると、次のように表示されます。

```
/SP/clients/syslog
Targets:
Properties:
   destination_ip1 = 0.0.0.0
   destination_ip2 = 0.0.0.0
Commands:
   cd
   set
   show
```

4. `set` コマンドを使用して、IP 1 (さらに、該当する場合は IP 2) の宛先 IP アドレスを特定します。たとえば、IP 宛先を IP アドレス 11.222.33.4 に設定するには、次のように入力します。

```
set destination_ip1=111.222.33.4
```

5. Enter を押して、設定を有効にします。

   IP アドレスの設定の結果が表示されます。たとえば、宛先の IP アドレスを 111.222.33.4 に設定した場合は、次のように表示されます。

```
Set 'destination_ip1' to '111.222.33.4'
```

警告管理について

警告では、発生する可能性のあるシステムの障害を事前に報告します。Sun の各サーバープラットフォームには、電圧、温度、およびその他の保守に関連するシステムの属性を測定するセンサーが多数装備されています。ILOM は、これらのセンサーを自動的にポーリングして、しきい値を超えるイベントを ILOM イベントログに送信し、1 つ以上のユーザー指定の警告の宛先に対して警告メッセージを生成します。

注意 – ILOM は、すべてのイベントまたは動作に LocalTime=GMT (または UTC) というタグを付けます。ブラウザクライアントには、LocalTime でこれらのイベントが表示されます。このため、イベントログに明らかな違いが発生する可能性があります。ILOM でイベントが発生すると、イベントログには UTC で示されますが、クライアントには LocalTime で示される場合があります。ILOM のタイムスタンプとクロック設定の詳細は、126 ページの「イベントログのタイムスタンプと ILOM のクロック設定」を参照してください。

警告ルールの設定

ILOM では、ILOM の Web インタフェースまたは CLI を使用して、最大 15 の警告ルールを設定できます。ILOM で設定する警告ルールごとに、警告の種類に応じて、警告に関する 3 つ以上のプロパティーを定義する必要があります。

「警告の種類」は、メッセージ形式と警告メッセージの送受信方法を定義します。ILOM は、次の 3 つの警告の種類をサポートしています。

- IPMI PET 警告
- SNMP トラップ警告
- 電子メール通知警告

Sun シャーシ監視モジュール (CMM) を除くすべての Sun サーバープラットフォームは、3 つの警告の種類をすべてサポートしています。Sun シャーシ監視モジュールは SNMP トラップ警告と電子メール通知警告をサポートしていますが、現在 IPMI PET 警告はサポートしていません。

各警告の種類についての簡単な説明と警告ルールの定義に使用できるその他のプロパティーは、141 ページの「警告ルールのプロパティーの定義」の節で詳しく説明します。

警告ルールのプロパティーの定義

ILOM では警告ルールを定義するための最大 5 つのプロパティー値を用意しています。これらは次のとおりです。

- 警告の種類
- 警告レベル
- 警告の宛先
- SNMP バージョン (SNMP トラップ警告のみ)
- SNMP コミュニティー名またはユーザー名 (SNMP トラップ警告のみ)

これらの各プロパティー値の詳細は、表 7-1 を参照してください。

表 7-1　警告ルール定義用のプロパティー

プロパティー名	要件	説明
警告の種類	必須	警告の種類プロパティーは、ILOM が警告メッセージを作成して送信する際に使用する、メッセージの形式および配信方法を指定します。次のいずれかの警告の種類を設定できます。 • **IPMI PET 警告。**IPMI Platform Event Trap (PET) 警告は、Sun シャーシ監視モジュール (CMM) を除くすべての Sun サーバープラットフォームおよびモジュールでサポートされています。 ILOM で設定する IPMI PET 警告ごとに、警告の宛先の IP アドレスとサポートされる 4 つの警告レベルのうちのいずれかを指定する必要があります。指定した警告の宛先が、IPMI PET メッセージの受信をサポートしている必要があります。警告の宛先が IPMI PET メッセージの受信をサポートしていない場合、警告の受信者は警告メッセージを復号化できません。 • **SNMP トラップ警告。**ILOM は、ユーザー指定の IP 宛先への SNMP トラップ警告の生成をサポートしています。指定したすべての宛先が、SNMP トラップメッセージの受信をサポートしている必要があります。 SNMP トラップ警告は、ラック搭載型サーバーとブレードサーバーモジュールでサポートされています。 • **電子メール通知警告。**ILOM は、ユーザー指定の電子メールアドレスへの電子メール通知警告の生成をサポートしています。ILOM クライアントが電子メール通知警告を生成できるようにするには、電子メール警告メッセージを送信する送信 SMTP 電子メールサーバーの名前を最初に ILOM で設定する必要があります。詳細は、155 ページの「Web インタフェースを使用して SMTP クライアントを有効にする」を参照してください。
警告の宛先	必須	警告の宛先プロパティーは、警告メッセージの送信先を指定します。警告の種類によって、警告メッセージの送信先として選択できる宛先が異なります。たとえば、IPMI PET および SNMP トラップ警告では、IP アドレスの宛先を指定する必要があります。電子メール通知警告では、電子メールアドレスを指定する必要があります。 警告の宛先が正しい形式で入力されていないと、ILOM はエラーを報告します。

表 7-1　警告ルール定義用のプロパティー (続き)

プロパティー名	要件	説明
警告レベル	必須	警告レベルは、警告の受信者が、受信することにもっとも関心のある警告メッセージのみを受信できるようにするフィルタメカニズムとして機能します。ILOM で警告ルールを定義するたびに、警告レベルを指定する必要があります。 警告レベルによって、警告を生成するイベントが決まります。もっとも低い警告レベルでは、そのレベルの警告とそのレベル以上のすべての警告が生成されます。 ILOM には次の警告レベルがあり、もっとも低いレベルの警告はマイナーです。 • **マイナー。**この警告レベルでは、情報イベント、下限および上限の非クリティカルイベント、上限および下限のクリティカルイベント、上限および下限の回復不可能イベントに関する警告が生成されます。 • **メジャー。**この警告レベルでは、上限および下限の非クリティカルイベント、上限および下限のクリティカルイベント、上限および下限の回復不可能イベントに関する警告が生成されます。 • **クリティカル。**この警告レベルでは、上限および下限のクリティカルイベント、上限および下限の回復不可能イベントに関する警告が生成されます。 • **停止。**この警告レベルでは、上限および下限の回復不可能なイベントに対してのみ警告が生成されます。 • **無効。**警告を無効にします。ILOM は警告メッセージを生成しません。 **注**:「無効」を除くすべての警告レベルにおいて、警告の送信が有効になります。 **重要**: ILOM は、すべての IPMI トラップおよび電子メール通知トラップの警告レベルフィルタリングをサポートしています。ILOM では SNMP トラップの警告レベルフィルタリングをサポートしていません。SNMP トラップの送信を有効にする (ただし、警告レベルによる SNMP トラップのフィルタリングは行わない) には、マイナー、メジャー、クリティカル、または停止のいずれかのオプションを選択できます。SNMP トラップの送信を無効にするには、「disabled (無効)」オプションを選択する必要があります。
SNMP バージョン	任意	SNMP バージョンプロパティーを使用すると、送信する SNMP トラップのバージョンを指定できます。1、2c、3 から選択して指定できます。 このプロパティー値は、SNMP トラップ警告にのみ適用されます。
SNMP コミュニティー名 または ユーザー名	任意	SNMP コミュニティー名またはユーザー名プロパティーを使用すると、SNMP トラップ警告で使用するコミュニティー文字列または SNMP v3 ユーザー名を指定できます。 • SNMP トラップ v1 または v2c の場合、SNMP 警告のコミュニティー名の値を指定できます。 • SNMP v3 の場合、SNMP 警告のユーザー名の値を指定できます。 **重要**: SNMP v3 ユーザー名の値を指定する場合は、ILOM にこのユーザー名を SNMP ユーザーとして定義する必要があります。このユーザーを SNMP ユーザーとして定義しないと、トラップ受信者は SNMP トラップ警告を復号化できません。ILOM での SNMP ユーザーの定義に関する詳細は、第 10 章を参照してください。

SMTP 設定	説明
SMTP State	この状態を有効にするには、このチェックボックスを選択します。
SMTP Server IP	電子メール通知を処理する送信 SMTP 電子メールサーバーの IP アドレスを入力します。
SMTP Port	送信 SMTP 電子メールサーバーのポート番号を入力します。

ILOM の警告ルール設定を管理および作成する方法の詳細は、次の節を参照してください。

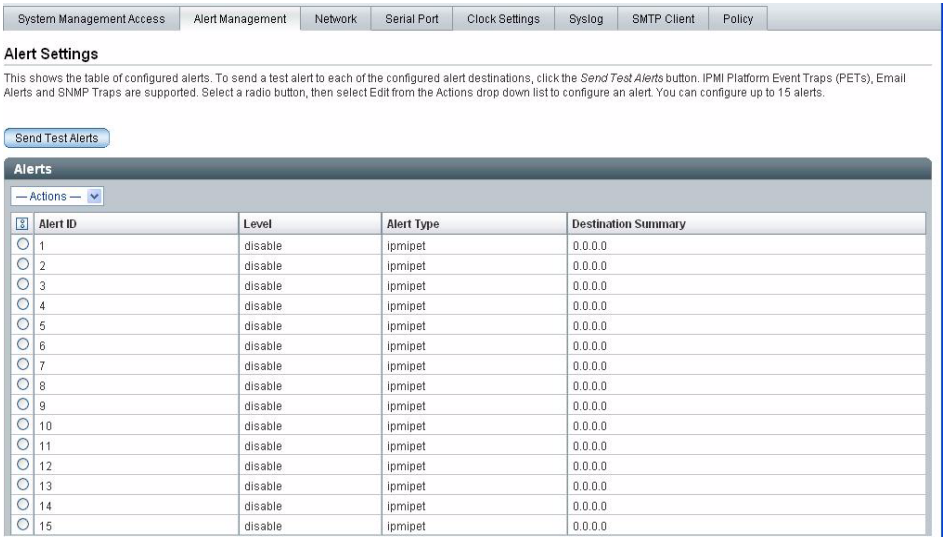
- 144 ページの「ILOM Web インタフェースを使用した警告ルール設定の管理」
- 149 ページの「ILOM CLI を使用した警告ルール設定の管理」
- 155 ページの「電子メール通知警告用の SMTP クライアントの設定」

ILOM Web インタフェースを使用した警告ルール設定の管理

ILOM の警告ルール設定は、「Alert Settings」Web インタフェースページから有効、変更、または無効にすることができます。このページに示されている 15 個のすべての警告ルール設定は、デフォルトで無効になっています。このページの「Actions」ドロップダウンリストボックスを使用して、警告ルールに関連付けられているプロパティーを編集できます。このページで警告ルールを有効にするには、警告の種類、警告レベル、および有効な警告の宛先を定義する必要があります。

「Alert Settings」ページには、「Send Test Alert (警告のテスト送信)」ボタンもあります。このテスト警告機能を使用すると、有効な警告ルールに指定されている警告の各受信者が警告メッセージを受け取ることを確認できます。

図 7-9　「Alert Settings」ページ



Web インタフェースを使用して ILOM の警告ルール設定を作成および管理する方法の詳細は、次の節を参照してください。

- 145 ページの「準備すべき事柄」
- 146 ページの「Web インタフェースを使用して警告ルール設定を変更する」
- 147 ページの「Web インタフェースを使用して警告ルール設定を無効にする」
- 148 ページの「Web インタフェースを使用して警告テストを生成する」

準備すべき事柄

- 電子メール通知警告を定義する場合は、電子メール通知の送信に使用する送信電子メールサーバーを ILOM で設定する必要があります。送信電子メールサーバーが設定されていないと、ILOM は正常に電子メール通知警告を生成できません。
- バージョンを SNMP v3 に設定して SNMP トラップ警告を定義する場合は、ILOM で SNMP ユーザーとして SNMP ユーザー名が定義されている必要があります。ILOM でユーザーが SNMP ユーザーとして定義されていないと、SNMP 警告ユーザーは SNMP 警告メッセージを復号化できません。ILOM での SNMP ユーザーの定義に関する詳細は、第 10 章を参照してください。
- ILOM の警告ルールを作成、変更、または無効にするには、管理者アカウントで ILOM にログインする必要があります。

▼ Web インタフェースを使用して警告ルール設定を変更する

ILOM の警告ルール設定を変更するには、次の手順を使用します。

1. **Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。**
   ILOM Web インタフェースのログインページが表示されます。
2. **ILOM ログインページで、管理者のユーザー名およびパスワードを入力して「OK」をクリックします。**
   ILOM Web インタフェースが表示されます。
3. **Web インタフェースページで、「Configuration (設定)」-->「Alert Management (警告の管理)」を選択します。**

注 – または、サーバー SP の警告ルール設定は、CMM Web インタフェースから管理できます。CMM からサーバー SP の警告ルール設定を管理するには、ページの左フレームのサーバー SP (ブレード) を選択してから、ページの右フレームで「Configuration (設定)」-->「Alert Management (警告の管理)」をクリックします。

「Alert Settings」ページが表示されます。

4. **「Alert Settings」ページで、次の手順を実行します。**
   a. **作成または編集する警告ルールのラジオボタンを選択します。**
   b. **「Actions」ドロップダウンリストボックスで、「Edit (編集)」を選択します。**
      警告ルールに関連付けられたプロパティー値を示すダイアログが表示されます。
   c. **このプロパティーダイアログボックスで、警告の種類、警告レベル、警告の宛先の値を指定します。**
      指定する警告の種類が SNMP トラップの場合、警告メッセージの受信を認証するためのコミュニティー名またはユーザー名の値を任意で定義できます。
      警告ルールに指定できるプロパティー値の詳細は、142 ページの「警告ルール定義用のプロパティー」を参照してください。
   d. **「Save (保存)」をクリックして、指定した値を適用し、プロパティーダイアログを閉じます。**

▼ Web インタフェースを使用して警告ルール設定を無効にする

ILOM の警告ルール設定を無効にするには、次の手順を使用します。

1. **Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。**
   ILOM Web インタフェースのログインページが表示されます。
2. **ILOM ログインページで、管理者のユーザー名およびパスワードを入力して「OK」をクリックします。**
   ILOM Web インタフェースが表示されます。
3. **Web インタフェースページで、「Configuration (設定)」-->「Alert Management (警告の管理)」を選択します。**

注 – または、サーバー SP の警告ルール設定は、CMM Web インタフェースから管理できます。CMM からサーバー SP の警告ルール設定を管理するには、ページの左フレームのサーバー SP (ブレード) を選択してから、ページの右フレームで「Configuration (設定)」-->「Alert Management (警告の管理)」をクリックします。

「Alert Settings」ページが表示されます。

4. **「Alert Settings」ページで、変更する警告ルールのラジオボタンを選択してから、「Actions」ドロップダウンリストボックスの「Edit (編集)」をクリックします。**
   警告ルールについて定義可能なプロパティーを示すダイアログが表示されます。
5. **このプロパティーダイアログボックスで、「Alert Levels (警告レベル)」ドロップダウンリストボックスの「Disabled (無効)」を選択します。**

▼ Web インタフェースを使用して警告テストを生成する

テスト警告を送信することによって、ILOM の有効な警告ルール設定をそれぞれテストできます。ILOM の警告ルール設定に指定した宛先へのテスト警告を生成するには、次の手順に従います。

1. **Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。**

   ILOM Web インタフェースのログインページが表示されます。

2. **ILOM ログインページで、管理者のユーザー名およびパスワードを入力して「OK」をクリックします。**

   ILOM Web インタフェースが表示されます。

3. **Web インタフェースページで、「Configuration (設定)」-->「Alert Management (警告の管理)」を選択します。**

   注 – または、サーバー SP の警告ルール設定は、CMM Web インタフェースから管理できます。CMM からサーバー SP の警告ルール設定を管理するには、ページの左フレームのサーバー SP (ブレード) を選択してから、ページの右フレームで「Configuration (設定)」-->「Alert Management (警告の管理)」をクリックします。

   「Alert Settings」ページが表示されます。

4. **「Alert Settings」ページで、「Send Test Alert (警告のテスト送信)」ボタンをクリックします。**

   ILOM は、「Alert Settings」ページで有効になっている各警告ルール設定に対してテスト警告を生成します。

ILOM CLI を使用した警告ルール設定の管理

ILOM の警告ルール設定は、コマンド行インタフェース (CLI) から有効、変更、または無効にすることができます。ILOM に定義されている 15 個のすべての警告ルール設定は、デフォルトで無効になっています。ILOM で警告ルール設定を有効にするには、警告の種類、警告レベル、および警告の宛先のプロパティーに値を設定する必要があります。

また、CLI から ILOM の有効な警告ルール設定に対してテスト警告を生成することもできます。このテスト警告機能を使用すると、有効な警告ルール設定に指定されている警告の受信者が警告メッセージを受け取ることを確認できます。

CLI を使用した ILOM の警告ルール設定の管理および作成に関する詳細は、次の節を参照してください。

- 149 ページの「警告ルール設定を管理するための CLI コマンド」
- 151 ページの「準備すべき事柄」
- 152 ページの「CLI を使用して警告ルール設定を変更する」
- 153 ページの「CLI を使用して警告ルール設定を無効にする」
- 154 ページの「CLI を使用して警告テストを生成する」

警告ルール設定を管理するための CLI コマンド

表 7-2 に、ILOM CLI を使用して警告ルール設定を管理する場合に、一般的に使用する必要がある CLI コマンドを示します。

表 7-2　警告ルール設定を管理するための CLI コマンド

CLI コマンド	説明
show	show コマンドを使用すると、フルパスまたは相対パスのいずれかを指定して、任意のレベルの警告管理コマンドツリーを表示できます。 例 • フルパスを使用して警告ルールとともにそのプロパティーを表示するには、コマンドプロンプトで次のように入力します。 **show /SP/alertmgmt/rules/1** /SP/alertmgmt/rules/1 Properties: community_or_username = public destination = 129.148.185.52 level = minor snmp_version = 1 type = snmptrap Commands: cd set show • フルパスを使用して 1 つのプロパティーを表示するには、コマンドプロンプトで次のように入力します。 **show /SP/alertmgmt/rules/1 type** Properties: type = snmptrap Commands: set show • 現在のツリーの場所が /SP/alertmgmt/rules である場合の相対パスを指定するには、コマンドプロンプトで次のようにコマンドを入力します。 **show 1/** /SP/alertmgmt/rules/1 Targets: Properties: community_or_username = public destination = 129.148.185.52 level = minor snmp_version = 1 type = snmptrap Commands: cd set show

表 7-2　警告ルール設定を管理するための CLI コマンド (続き)

CLI コマンド	説明
cd	cd コマンドを使用すると、作業用ディレクトリを設定できます。サーバー SP の作業用ディレクトリとして警告管理を設定するには、コマンドプロンプトで次のようにコマンドを入力します。 **cd /SP/alertmgmt**
set	set コマンドを使用すると、ツリー内の任意の場所からプロパティーに値を設定できます。ツリーの場所に応じて、プロパティーのフルパスまたは相対パスのいずれかを指定できます。次に例を示します。 • フルパスの場合は、プロンプトでコマンドパスに次のように入力します。 **set /SP/alertmgmt/rules/1 type=ipmipet** • 相対パス (ツリーの場所が /SP/alertmgmt) の場合、コマンドプロンプトで次のようにコマンドパスを入力します。 **set rules/1 type=ipmipet** • 相対パス (ツリーの場所が /SP/alertmgmt/rules/1) の場合、コマンドプロンプトで次のようにコマンドパスを入力します。 **set type=ipmipet**

準備すべき事柄

- 電子メール通知警告を定義する場合は、電子メール通知の送信に使用する送信電子メールサーバーを ILOM で設定する必要があります。送信電子メールサーバーが設定されていないと、ILOM は正常に電子メール通知警告を生成できません。
- バージョンを SNMP v3 に設定して SNMP トラップ警告を定義する場合は、ILOM で SNMP ユーザーとして SNMP ユーザー名が定義されている必要があります。ILOM でユーザーが SNMP ユーザーとして定義されていないと、SNMP 警告ユーザーは SNMP 警告メッセージを復号化できません。ILOM での SNMP ユーザーの定義に関する詳細は、第 10 章を参照してください。
- ILOM の警告ルールを作成、変更、または無効にするには、管理者アカウントで ILOM にログインする必要があります。

▼ CLI を使用して警告ルール設定を変更する

1. サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。

   - ローカルシリアルコンソール接続

     サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

     詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

   または

   - 遠隔 Secure Shell (SSH) 接続

     サーバー SP または CMM との Secure Shell 接続を確立します。

     遠隔クライアントから、root としてサーバー SP またはアクティブ CMM へのセキュリティー保護された接続を確立します。

     たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

     ```
     ssh -l root server_ip_address
     Password: changeme
     ```

   デフォルトのコマンドプロンプト (->) が表示されます。

2. 次のいずれかのコマンドパスを入力して、作業用ディレクトリを設定します。

   - ラック搭載型サーバーの場合: **cd /SP/alertmgmt**
   - ブレードサーバーモジュールの場合: **cd /SP/alertmgmt**
   - シャーシ CMM の場合: **cd /CMM/alertmgmt**

3. 警告ルールに関連付けられているプロパティーを表示するには、`show` コマンドを入力します。

   たとえば、最初の警告ルールに関連付けられているプロパティーを表示するには、次のいずれかを入力します。

   - ラック搭載型サーバーの場合: **show /SP/alertmgmt/rules/1**
   - ブレードサーバーモジュールの場合: **show /CH/BLn/SP/alertmgmt/rules/1**
   - シャーシ CMM の場合: **show /CMM/alertmgmt/CMM/rules/1**

4. 警告ルールに関連付けられているプロパティーに値を割り当てるには、`set` コマンドを入力します。

   たとえば、ルール 1 の警告の種類として IPMI PET を設定するには、次のようにコマンドパスを入力します。

   ```
   set type=ipmipet
   ```

注 – 警告ルール設定を有効にするには、警告の種類、警告レベル、および警告の宛先に値を指定する必要があります。SNMP 警告の種類を定義する場合は、SNMP トラップ警告の受信を認証するための値を任意で定義できます。

警告ルールに定義できる各プロパティー値の詳細は、142 ページの「警告ルール定義用のプロパティー」の表 7-1 を参照してください。

▼ CLI を使用して警告ルール設定を無効にする

CLI から ILOM の警告ルール設定を無効にするには、次の手順を使用します。

1. **サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。**

   - **ローカルシリアルコンソール接続**

     サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

     詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

   または

   - **遠隔 Secure Shell (SSH) 接続**

     サーバー SP または CMM との Secure Shell 接続を確立します。

     遠隔クライアントから、root としてサーバー SP またはアクティブ CMM へのセキュリティー保護された接続を確立します。

     たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

     ```
     ssh -l root server_ip_address
     Password: changeme
     ```

   デフォルトのコマンドプロンプト (->) が表示されます。

2. **`cd` コマンドを使用して、無効にする警告管理ルールを作業用ディレクトリとして設定します。**

   例:

   - ラック搭載型サーバー SP の場合、**`cd /SP/alertngnt/rules/`***n* と入力します。
   - ブレードサーバー SP の場合、**`cd /CH/BL`***n***`/SP/alertmgmt/rules/`***n* と入力します。
   - シャーシ CMM の場合、**`cd /CMM/alertmgmt/CMM/rules/`***n* と入力します。

     n は特定の警告ルール番号に相当し、1 ～ 15 の値になります。

3. 警告ルールを無効にするには、次のコマンドを入力します。

   set level=disable

▼ CLI を使用して警告テストを生成する

テスト警告を送信することによって、ILOM の有効な警告ルール設定をそれぞれテストできます。ILOM の警告ルール設定に指定した宛先へのテスト警告を生成するには、次の手順に従います。

1. サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。

   - ローカルシリアルコンソール接続

     サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

     詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

   または

   - 遠隔 Secure Shell (SSH) 接続

     サーバー SP または CMM との Secure Shell 接続を確立します。

     遠隔クライアントから、root としてサーバー SP またはアクティブ CMM へのセキュリティー保護された接続を確立します。

     たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

     ssh -l root *server_ip_address*

     Password: **changeme**

   デフォルトのコマンドプロンプト (->) が表示されます。

2. cd コマンドを使用して、作業用ディレクトリを警告管理ルールに設定します。

   例:

   - ラック搭載型サーバー SP の場合、**cd /SP/alertmgmt/rules** と入力します。
   - ブレードサーバー SP の場合、**cd /CH/BL***n***/SP/alertmgmt/rules** と入力します。
   - シャーシ CMM の場合、**cd /CMM/alertmgmt/CMM/rules** と入力します。

3. 次のコマンドを入力して、テスト警告を生成します。

   set testalert=true

電子メール通知警告用の SMTP クライアントの設定

設定済みの電子メール通知警告を生成するには、ILOM クライアントが SMTP クライアントとして動作し、電子メール警告メッセージを送信できるようにする必要があります。ILOM クライアントを SMTP クライアントとして有効にするには、電子メール通知を処理する送信 SMTP 電子メールサーバーの IP アドレスとポート番号を指定する必要があります。

ILOM の電子メール通知警告用に SMTP クライアントを設定する方法の詳細は、次の節を参照してください。

- 155 ページの「Web インタフェースを使用して SMTP クライアントを有効にする」
- 156 ページの「CLI を使用して SMTP クライアントを有効にする」

準備すべき事柄:

- ILOM クライアントを SMTP クライアントとして有効にする前に、送信 SMTP 電子メールサーバーの IP アドレスとポート番号を収集しておくことをお勧めします。

▼ Web インタフェースを使用して SMTP クライアントを有効にする

Web インタフェースを使用して、ILOM で SMTP クライアントを設定するには、次の手順に従います。

1. **Web ブラウザを開いて、サーバー SP または CMM の IP アドレスを入力します。**

   ILOM Web インタフェースのログインページが表示されます。

2. **ILOM ログインページで、管理者のユーザー名およびパスワードを入力して「OK」をクリックします。**

   ILOM Web インタフェースが表示されます。

3. **Web インタフェースページで、「Configuration (設定)」-->「SMTP Client」を選択します。**

4. **「SMTP Client」ページで、次の設定を指定して、電子メール通知警告の送信を有効にします。**

SMTP 設定	説明
SMTP State	この状態を有効にするには、このチェックボックスを選択します。
SMTP Server IP	電子メール通知を処理する送信 SMTP 電子メールサーバーの IP アドレスを入力します。
SMTP Port	送信 SMTP 電子メールサーバーのポート番号を入力します。

5. 「Save (保存)」をクリックして、SMTP 設定を適用します。

▼ CLI を使用して SMTP クライアントを有効にする

CLI を使用して、ILOM で SMTP クライアントを設定するには、次の手順に従います。

1. **サーバー SP または CMM とのローカルシリアルコンソール接続または SSH 接続を次のように確立します。**
   - **ローカルシリアルコンソール接続**

     サーバーまたは CMM のシリアルポートにシリアルコンソールを接続します。

     詳細は、Sun サーバープラットフォームに付属のユーザーマニュアルを参照してください。

   または

   - **遠隔 Secure Shell (SSH) 接続**

     サーバー SP または CMM との Secure Shell 接続を確立します。

     遠隔クライアントから、root としてサーバー SP またはアクティブ CMM へのセキュリティー保護された接続を確立します。

     たとえば次のように入力すると、遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立することができます。

     ```
     ssh -l root server_ip_address
     Password: changeme
     ```

   デフォルトのコマンドプロンプト (->) が表示されます。

2. **`cd` コマンドを使用して、作業用ディレクトリを `clients/smtp` に設定します。**

   例:

   - ラック搭載型サーバー SP の場合、**`cd /SP/clients/smtp`** と入力します。
   - ブレードサーバー SP の場合、**`cd /CH/BL`*n*`/SP/clients/smtp`** と入力します。

- シャーシ CMM の場合、**cd /CMM/clients/smtp** と入力します。

3. **SMTP プロパティーを表示するには、**show **コマンドを入力します。**

   たとえば、SP ではじめて SMTP プロパティーにアクセスすると、次のように表示されます。

```
show
/SP/clients/smtp
Targets
  Properties
  address = 0. 0. 0. 0
  port = 25
  state = enabled
Commands:
cd
set
show
```

4. **set コマンドを使用して、SMTP クライアントの IP アドレスを指定するか、ポートまたは状態プロパティー値を変更します。**

   次に例を示します。

```
set address=222.333.44.5
```

5. **Enter を押して、変更を有効にします。**

   たとえば、set address=222.333.44.5 と入力した場合、次のような結果が表示されます。

```
Set 'address=222.333.44.5'
```

第8章

ILOM の通信設定

詳細な ILOM 通信の設定には、ネットワーク、シリアルポート、および Web の設定が含まれます。

この章には次の節があります。

- 173 ページの「Web インタフェースを使用してシリアルポート設定を行う」
- 174 ページの「Web インタフェースを使用して HTTP または HTTPS Web アクセスを有効にする」

注 – この章の構文例では、**/SP/** で始まるターゲットを使用しますが、使用している Sun サーバーのプラットフォームによっては、**/CMM/** で始まるターゲットに置き換わる場合があります。サブターゲットは、すべての Sun サーバープラットフォームで共通です。

CLI を使用した ILOM ネットワーク設定の管理

この節では、ILOM のコマンド行インタフェース (CLI) を使用して、ILOM のネットワークを設定する方法について説明します。

ネットワーク設定について

ネットワーク設定には、pending と active という 2 つのプロパティーセットがあります。active 設定は、ILOM で現在使用中の設定です。これらの設定は読み取り専用です。設定を変更する場合は、更新する設定を pending 設定 (`pendingipaddress` または `pendingipgateway`) として入力してから、`commitpending` プロパティーを `true` に設定します。これにより、ポートとネットワーク設定両方が偶発的に切断されないようにします。

注 – 同一 IP アドレスが常に ILOM に割り当てられるようにしてください。これは、初期設定後に静的 IP アドレスを ILOM に割り当てるか、または DHCP サーバーを設定して常に同一 IP アドレスを ILOM に割り当てることによって行います。これにより、ネットワーク上で ILOM を簡単に検出できるようになります。

▼ CLI を使用してネットワーク設定を表示する

1. ILOM CLI に管理者またはオペレータとしてログインします。
2. コマンドプロンプトで、次のように入力します。

```
-> show /SP/network
```

▼ CLI を使用してネットワーク設定を行う

set コマンドを使用すると、ネットワーク設定のプロパティーと値を変更できます。

1. ILOM CLI に管理者としてログインします。
2. コマンドプロンプトで、次のように入力します。

```
-> set /SP/network
```

ターゲット、プロパティー、および値

ILOM のネットワーク設定では、次のターゲット、プロパティー、および値が有効です。

表 8-1　ILOM ネットワークのターゲット、プロパティー、および値

ターゲット	プロパティー	値	デフォルト値
/SP/network	ipaddress ipdiscovery ipgateway ipnetmask	これらの読み取り専用値は、システムによって更新される	
	macaddress	ILOM の MAC アドレス	
	commitpending	true|(なし)	(なし)
	pendingipaddress	<*ipaddress*|none>	none
	pendingipdiscovery	dhcp|static	dhcp
	pendingipgateway	<*ipaddress*|none>	none
	pendingipnetmask	<*ipdotteddecimal*>	255.255.255.255

例:

ILOM の IP アドレスを変更するには、次のように入力します。

```
-> set /SP/network pendingipaddress=nnn.nn.nn.nn commitpending=true
```

注 – IP アドレスを変更すると、ネットワーク経由で ILOM に接続している場合は、アクティブセッションが切断されます。

ネットワーク設定を DHCP から静的に割り当てた設定に変更するには、次のように入力します。

```
-> set /SP/network pendingipdiscovery=static pendingipaddress=
nnn.nn.nn.nn pendingipgateway=nnn.nn.nn.nn pendingipnetmask=nnn.nn.nn.nn
commitpending=true
```

注 – 設定は、commitpending を true に設定するとすぐに有効になります。

シリアルポート設定

シリアルポートを使用すると、ILOM Web インタフェース、コマンド行インタフェース (CLI)、およびシリアルポートリダイレクトを使用したシステムコンソールのストリームへのアクセスが可能になります。

- 内部シリアルポートは、ホストサーバーと ILOM 間の接続で、これによって、ILOM ユーザーがホストのシリアルコンソールにアクセスできるようになります。ILOM の内部シリアルポートの速度は、必ずホストサーバーの、多くの場合シリアルポート 0、COM1、または /dev/ttyS0 と呼ばれるシリアルコンソールポートの速度と一致させてください。

注 – 通常、ホストのシリアルコンソール設定は、ILOM のデフォルト設定 (9600 ボー、8N1 (データビット 8、パリティーなし、ストップビット 1)、フロー制御なし) に一致しています。

- 外部シリアルポートは、ILOM の RJ-45 シリアルポートです。通常、内部および外部シリアルポート接続は、ILOM の外部シリアルポートからホストコンソールに接続する際には、フロー制御の問題を避けるために同じ速度で動作するようにしてください。

▼ CLI を使用してシリアルポート設定を表示する

1. ILOM CLI に管理者またはオペレータとしてログインします。
2. コマンドプロンプトで、次のように入力します。
   - 外部シリアルポートの設定を表示するには、次のコマンドを入力します。

   ```
   >show /SP/serial/external
   ```

   - ホストのシリアルポートの設定を表示するには、次のコマンドを入力します。

   ```
   -> show /SP/serial/host
   ```

▼ CLI を使用してシリアルポート設定を行う

set コマンドを使用すると、シリアルポート設定のプロパティーと値を変更できます。ポート設定には、pending と active という 2 つのプロパティーセットがあります。active 設定は、ILOM で現在使用されている設定です。これらの設定は読み取り専用です。設定を変更するには、更新する設定を pending 設定として入力してから、commitpending プロパティーを true に設定します。これにより、ポートとネットワーク設定両方が偶発的に切断されないようにします。

1. ILOM CLI に管理者またはオペレータとしてログインします。
2. コマンドプロンプトで、次のように入力します。

```
-> set target [propertyname=value]
```

ターゲット、プロパティー、および値

ILOM のシリアルポート設定では、次のターゲット、プロパティー、および値が有効です。

表 8-2　ILOM のシリアルポートで有効なターゲット、プロパティー、および値

ターゲット	プロパティー	値	デフォルト値
/SP/serial/external	commitpending	true|(なし)	(なし)
	flowcontrol	none	none
	pendingspeed	<*decimal*>	9600
	speed	9600	9600
/SP/serial/host	commitpending	true|(なし)	(なし)
	pendingspeed	<*decimal*>	(なし)
	speed	9600	9600

例:

ホストシリアルポートの速度 (ボーレート) を 9600 から 57600 に変更するには、次のように入力します。

```
-> set /SP/serial/host pendingspeed=57600 commitpending=true
```

注 – ILOM がホストと適切に通信するために、ホストシリアルポートの速度は、ホストのオペレーティングシステムのシリアルポート 0、COM1、または /dev/ttys0 の速度設定と一致させてください。

▼ CLI を使用して HTTP または HTTPS Web アクセスを有効にする

ILOM では、HTTP および HTTPS の両方の接続をサポートしています。ILOM を使用すると、HTTP アクセスを自動的に HTTPS にリダイレクトすることができます。また、HTTP ポートと HTTPS ポートを設定することもできます。

1. ILOM CLI に管理者としてログインします。
2. コマンドプロンプトで、次のように入力します。

```
-> set /SP/services/http
```

プロパティーは /SP/services/http および /SP/services/https にあります。

ターゲット、プロパティー、および値

表 8-3 に、HTTP および HTTPS で有効なターゲット、プロパティー、および値を示します。

表 8-3 HTTP および HTTPS で有効なターゲット、プロパティー、および値

ターゲット	プロパティー	値	デフォルト値
/SP/services/http	secureredirect	enabled| disabled	enabled
	servicestate	enabled| disabled	disabled
	port	<*portnum*>	80
/SP/services/https	servicestate	enabled| disabled	enabled
	port	<*portnum*>	443

表 8-4 に、HTTP、HTTPS、および自動リダイレクトで使用可能な設定を示します。

表 8-4 HTTP、HTTPS、および自動リダイレクトで使用可能な設定

目的の状態	ターゲット	プロパティー	値
HTTP のみを有効にする	/SP/services/http	secureredirect	disabled
	/SP/services/http	servicestate	enabled
	/SP/services/https	servicestate	disabled
HTTP および HTTPS を有効にする	/SP/services/http	secureredirect	disabled

表 8-4　HTTP、HTTPS、および自動リダイレクトで使用可能な設定 (続き)

目的の状態	ターゲット	プロパティー	値
	/SP/services/http	servicestate	enabled
	/SP/services/https	servicestate	enabled
HTTPS のみを有効にする	/SP/services/http	secureredirect	disabled
	/SP/services/http	servicestate	disabled
	/SP/services/https	servicestate	enabled
HTTP を HTTPS に自動的にリダイレクトする	/SP/services/http	secureredirect	enabled
	/SP/services/http	servicestate	disabled
	/SP/services/https	servicestate	enabled

Secure Shell の設定

Secure Shell (SSH) は、ILOM コマンド行インタフェース (CLI) へのセキュリティー保護された遠隔接続にアクセスするために使用する標準プロトコルです。SSH を使用すると、ILOM とのすべての管理上の対話が暗号化され、セキュリティーが保護されます。サーバー接続の両端がデジタル鍵によって認証され、パスワードが暗号化によって保護されます。ILOM 接続は、RSA および DSA 鍵暗号化によって保護されます。

▼ CLI コマンドを実行するためにセキュリティー保護された遠隔接続を確立する

- **遠隔 SSH クライアントからサーバー SP へのセキュリティー保護された接続を確立する必要があります。セキュリティー保護された接続を確立するには、次のように入力します。**

  ssh -l username *server_ip_address*

  Password: **********

  デフォルトのプロンプト (->) が表示され、システムではネットワーク設定を確立する CLI コマンドを実行する準備ができました。

▼ CLI を使用して現在の鍵を表示する

鍵を表示するには高度な設定を必要とします。多くの場合、鍵を表示する必要はありません。公開鍵全体または鍵の省略されたフィンガプリントのいずれかを表示できます。

注 – /SP/services/ssh/keys/*rsa*|*dsa* の下のプロパティーはすべて読み取り専用です。

- RSA 鍵を表示するには、次のように入力します。

  -> show /SP/services/ssh/keys/rsa

  例:

```
/SP/services/ssh/keys/rsa
    Targets:
       Properties:
          fingerprint =
ca:c0:05:ff:b7:75:15:a0:30:df:1b:a1:76:bd:fe:e5
          length = 1024
            publickey
AAAAB3NzaC1yc2EAAAABIwAAAIEAthvlqgXbPIxN4OEvkukKupdFPr8GDaOsKGg
BESVlnny4nX8yd8JC/hrw3qDHmXIZ8JAFwoLQgjtZCbEsgpn9nNIMb6nSfu6Y1t
TtUZXSGFBZ48ROmU0SqqfR3i3bgDUR0siphlpgV6Yu0Zd1h3549wQ+RWk3vxqHQ
Ffzhv9c=
           Commands:
               cd
               show
```

- DSA 鍵を表示するには、次のように入力します。

  -> show /SP/services/ssh/keys/dsa

  例:

```
/SP/services/ssh/keys/dsa
     Targets:

     Properties:
        fingerprint =
6a:90:c7:37:89:e6:73:23:45:ff:d6:8e:e7:57:2a:60
        length = 1024
         publickey =
```

```
AAAAB3NzaC1kc3MAAACBAInrYecNH86imBbUqE+3FoUfm/fei2ZZtQzqrMx5zBm
bHFIaFdRQKeoQ7gqjc9jQbO7ajLxwk2vZzkg3ntnmqHz/hwHvdho2KaolBtAFGc
fLIdzGVxi4I3phVb6anmTlbqI2AILAa7JvQ8dEGbyATYR9A/pf5VTac/TQ70O/J
AAAAFQCIUavkex7wtEhC0CH3s25ON0I3CwAAAIBNfHUop6ZN7i46ZuQOKhD7Mkj
gdHy+8MTBkupVfXqfRE9Zw9yrBZCNsoD8XEeIeyP+puO5k5dJvkzqSqrTVoAXyY
qewyZMFE7stutugw/XEmyjq+XqBWaiOAQskdiMVnHa3MSg8PKJyWP8eIMxD3rIu
PTzkV632uBxzwSwfAQAAAIAtA8/3odDJUprnxLgHTowc8ksGBj/wJDgPfpGGJHB
B1FDBMhSsRbwh6Z+s/gAf1f+S67HJBTUPsVSMz+czmamc1oZeOazT4+zeNG6uCl
u/5/JmJSdkguc1FcoxtBFqfO/fKjyR0ecWaU7L4kjvWoSsydHJ0pMHasEecEBEr
lg==

      Commands:
          cd
          show
```

▼ CLI を使用して SSH を有効または無効にする

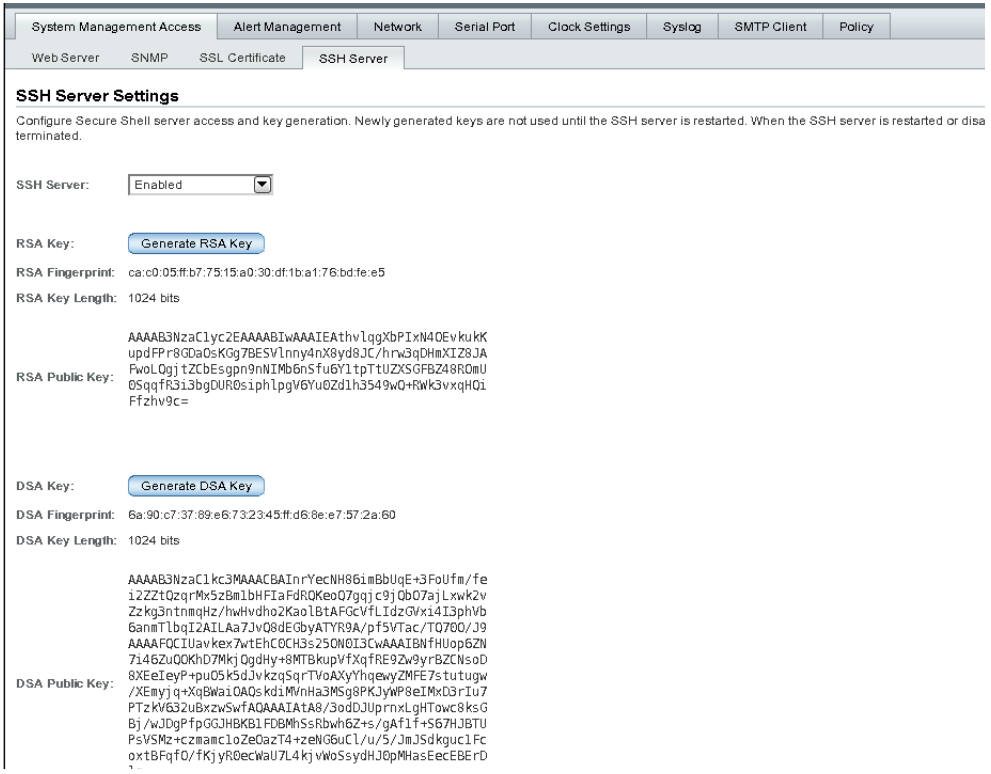
- ネットワーク経由でのアクセスを提供しない場合、または SSH を使用しない場合は、次のように入力します。

  -> set /SP/services/ssh state=*enabled* | *disabled*

▼ Web インタフェースを使用して SSH を有効または無効にする

1. ILOM に管理者としてログインします。
2. 「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SSH Server」の順に選択します。
3. 「SSH Server」ドロップダウンリストから、「Enabled (有効)」または「Disabled (無効)」を選択します。

図 8-1　「SSH Server Settings」ページ



▼ CLI を使用して新しい鍵を生成する

1. 次のように入力して、鍵の種類を設定します。

   -> set /SP/services/ssh generate_new_key_type=dsa | rsa

2. 操作を *true* に設定します。

   -> set /SP/services/ssh generate_new_key_action=true

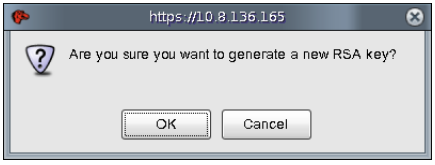
   フィンガプリントと鍵は異なって見えます。

▼ Web インタフェースを使用して新しい鍵を生成する

1. ILOM に管理者としてログインします。
2. 「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SSH Server」の順に選択します。
3. 「Generate RSA Key」ボタンをクリックして RSA を選択するか、「Generate DSA Key」ボタンをクリックして DSA を選択します。

   確認のメッセージが表示されたら、「OK」をクリックして選択を確認するか、または「Cancel (キャンセル)」をクリックして選択を取り消します。

図 8-2　確認ダイアログ



▼ CLI を使用して SSH サーバーを再起動する

新しい鍵は、SSH サーバーが再起動するまで有効になりません。

注 – 再起動によって、既存のすべての SSH 接続が終了します。

- SSH サーバーを再起動するには、次のように入力します。

```
-> set /SP/services/ssh restart_sshd_action=true
```

▼ Web インタフェースを使用して SSH サーバーを再起動する

新しい鍵は、SSH サーバーが再起動するまで有効になりません。

注 – 再起動によって、既存のすべての SSH 接続が終了します。

---

1. ILOM に管理者としてログインします。
2. 「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SSH Server」の順に選択します。
3. 「SSH Server」ドロップダウンリストから、「Restart SSH Server」を選択します。

Web インタフェースを使用して ILOM ネットワーク設定を管理する

この節では、ILOM Web インタフェースを使用して、ILOM のネットワークパラメータを設定する方法について説明します。

ILOM は、動的ホスト構成プロトコル (DHCP) を使用して IP 設定を自動的に行います。お手持ちのネットワークがこのプロトコルをサポートしていない場合には、パラメータを手作業で設定する必要があります。

▼ Web インタフェースを使用してネットワーク設定を表示する

1. 管理者またはオペレータとして ILOM にログインし、ILOM Web インタフェースを開きます。
2. 「Configuration (設定)」-->「Network (ネットワーク)」を選択します。

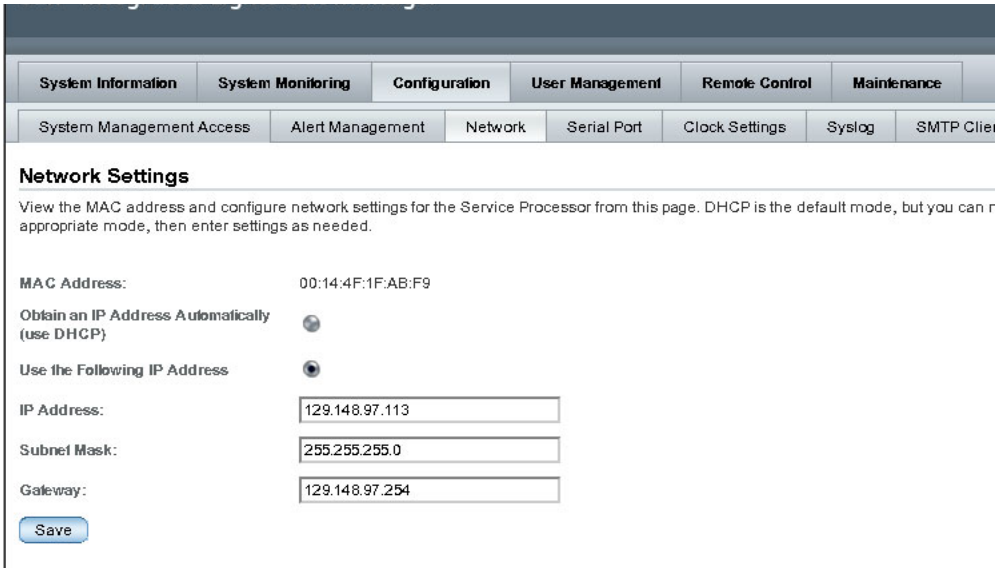
   「Network Settings (ネットワーク設定)」ページで、MAC アドレスを表示し、サーバーのシャーシ監視モジュールおよびサービスプロセッサのネットワークアドレスを設定できます。

注 – DHCP はデフォルトのモードですが、各 IP アドレス、ネットマスク、およびゲートウェイを手動で設定できます。

▼ Web インタフェースを使用してネットワーク設定を行う

1. 管理者として ILOM にログインし、ILOM Web インタフェースを開きます。
2. 「Configuration (設定)」-->「Network (ネットワーク)」を選択します。
   「Network Settings (ネットワーク設定)」ページが表示されます。

図 8-3　「Network Settings (ネットワーク設定)」ページ



3. 「Network Settings (ネットワーク設定)」ページに情報を入力します。
   情報を入力する際には、表 8-5 の説明を使用します。

表 8-5　「Network Settings (ネットワーク設定)」ページのフィールド

項目	説明
MAC Address (MAC アドレス)	ILOM のメディアアクセス制御 (MAC) アドレスは出荷時に設定されています。MAC アドレスは、各ネットワークデバイスに固有のハードウェアアドレスです。ILOM の MAC アドレスは、サーバーまたは CMM のラベル、出荷キットに含まれている Customer Information Sheet、BIOS 設定画面にあります。

表 8-5　「Network Settings (ネットワーク設定)」ページのフィールド (続き)

項目	説明
Obtain an IP Address Automatically (use DHCP) (IP アドレスを自動的に取得 (DHCP 使用))	ラジオボタンをクリックし、DHCP を使用して IP アドレスを取得します。
IP Address (IP アドレス)	ILOM の IP アドレスを入力します。IP アドレスは、システムを TCP/IP ネットワーク上で識別する一意の名前です。
Subnet Mask (サブネットマスク)	ILOM が属するネットワークのサブネットマスクを入力します。
Gateway (ゲートウェイ)	ILOM のゲートウェイアクセスアドレスを入力します。

4. 「Save (保存)」をクリックして設定を有効にしてください。

   「Save (保存)」をクリックするまで、設定は「待ち状態」とみなされます。IP アドレスを変更すると、ILOM セッションが終了します。

   Web ブラウザを閉じるように要求するプロンプトが表示されます。

5. 新しい IP アドレスを使用して、ILOM にふたたびログインします。

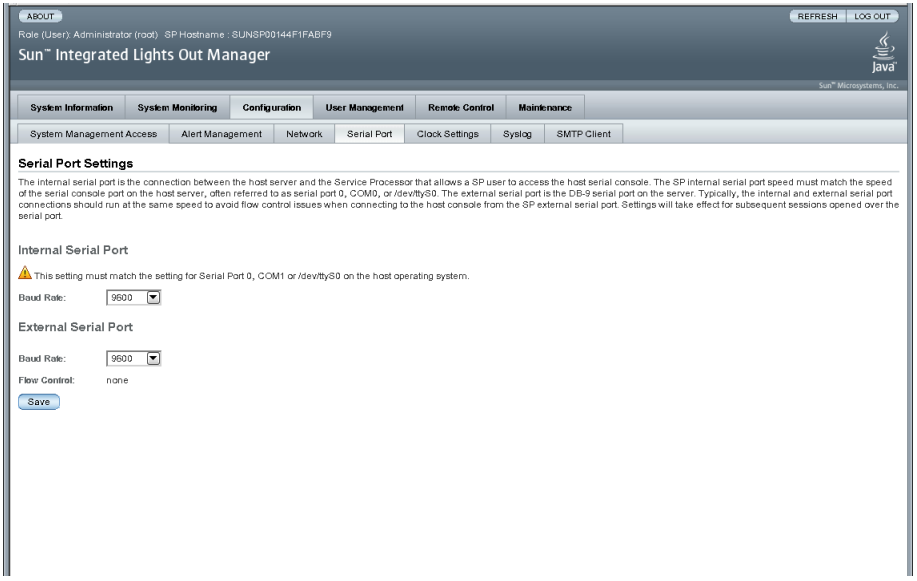
注 – ネットワーク設定を変更した場合には、新しいブラウザセッションでもう一度ログインし直すする必要がある場合があります。

▼ Web インタフェースを使用してシリアルポート設定を表示する

1. ILOM Web インタフェースに管理者またはオペレータとしてログインします。
2. 「Configuration (設定)」-->「Serial Port (シリアルポート)」を選択します。

   「Serial Port Settings (シリアルポート設定)」ページが表示されます。

図 8-4　「Serial Port Settings (シリアルポート設定)」ページ



3. 外部シリアルポートのボーレートを表示します。

▼ Web インタフェースを使用してシリアルポート設定を行う

この節では、ILOM シリアルポート設定を行う方法について説明します。デフォルトの設定は、9600 ボーとフロー制御なしです。

1. 管理者として ILOM にログインし、ILOM Web インタフェースを開きます。
2. 「Configuration (設定)」-->「Serial Port (シリアルポート)」を選択します。
   「Serial Port Settings (シリアルポート設定)」ページが表示されます。
3. 内部シリアルポートのボーレートを「Internal Serial Port Baud Rate」ドロップダウンリストから選択します。
   この設定は、ホストオペレーティングシステムのシリアルポート 0、COM1 または /dev/ttyS0 の設定と一致させてください。

   このボーレートの値は、BIOS のシリアルリダイレクト機能で指定されている速度 (デフォルトは 9600 ボー) と、ブートローダおよびオペレーティングシステムの設定で使用されている速度に一致させてください。

ILOM を使用してシステムコンソールに接続するには、ILOM をそのデフォルト設定 (9600 ボー、8N1 (データビット 8、パリティーなし、ストップビット 1)、フロー制御なし) に設定する必要があります。

4. **外部シリアルポートのボーレートを「External Serial Port Baud Rate」ドロップダウンリストから選択します。**

   この設定は、Sun サーバーの RJ-45 シリアルポートのボーレートと一致させてください。

5. **変更を有効にするには「Save (保存)」をクリックし、前の設定に戻すには「Cancel (キャンセル)」をクリックします。**

▼ Web インタフェースを使用して HTTP または HTTPS Web アクセスを有効にする

この節では、Web サーバーの設定を表示および変更する方法について説明します。

ILOM には、Web インタフェースへのアクセスを制御するオプションがあります。オプションは次の 4 種類です。

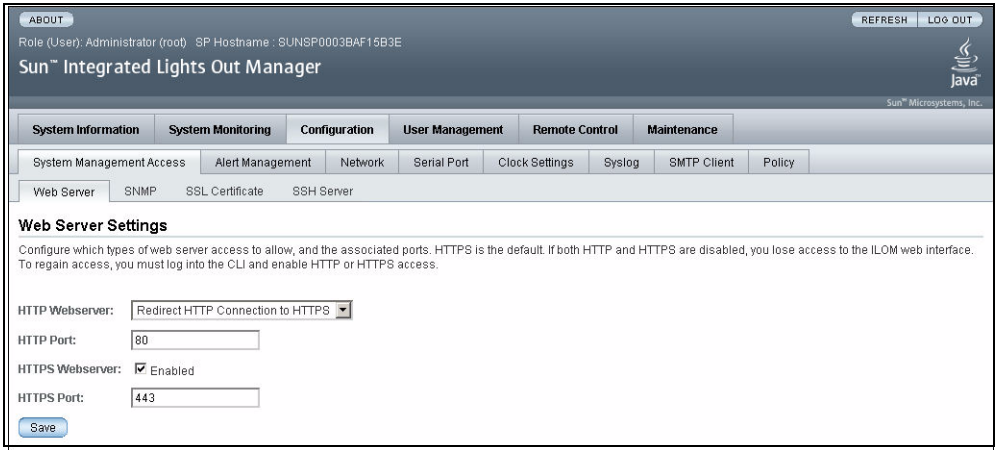
- HTTP のみ
- HTTPS のみ
- HTTP および HTTPS
- HTTPS および HTTP を自動的に HTTPS にリダイレクトする

HTTPS はデフォルトで有効になっています。

1. **管理者として ILOM にログインし、ILOM Web インタフェースを開きます。**
2. **「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「Web Server (ウェブサーバー)」の順に選択します。**

   「Web Server Settings (Web サーバー設定)」ページが表示されます。

図 8-5　「Web Server Settings (Web サーバー設定)」ページ



3. HTTP または HTTPS Web サーバーを選択します。
   - **HTTP を有効にする** – ドロップダウンリストボックスから「Enabled (有効)」を選択します。また、次を選択することもできます。
     - 「Redirect HTTP Connection to HTTPS (HTTP 接続を HTTPS にリダイレクト)」 – HTTP 接続が自動的に HTTPS にリダイレクトされます。
     - 「Disabled (無効)」 – HTTP を無効にします。
   - **HTTPS を有効にする** – 「HTTPS Web Server (HTTPS Web サーバー)」の「Enabled (有効)」チェックボックスを選択します。

   HTTPS Web サーバーはデフォルトで有効になっています。

注 – HTTP を無効にする、または「Redirect HTTP Connection to HTTPS (HTTP 接続を HTTPS にリダイレクト)」を選択してから、HTTPS を無効にすると、ILOM Web インタフェースにアクセスできなくなります。アクセスを回復するには、164 ページの「CLI を使用して HTTP または HTTPS Web アクセスを有効にする」での説明に従って、CLI の `/SP/services/http` コマンドまたは `/SP/services/https` コマンドを使用します。

---

4. HTTP または HTTPS ポート番号を割り当てます。
5. 「Save (保存)」をクリックして設定を有効にします。

第 9 章

Intelligent Platform Management Interface

ILOM は Intelligent Platform Management Interface (IPMI) をサポートしており、コマンド行インタフェースを使用して、サーバープラットフォームに関する情報を取得するだけでなく、サーバープラットフォームを監視および制御することができます。

この章には次の節があります。

IPMI の概要

Intelligent Platform Management Interface (IPMI) は、主に多くの異なる種類のネットワークのサーバーシステムの帯域外管理のために設計された、業界標準のオープンなインタフェースです。IPMI の機能には、現場交換可能ユニット (FRU) インベントリのレポート、システム監視、システムイベントのロギング、システム復旧 (ローカルおよび遠隔システムのリセットと電源の投入および切断も含む)、警告などがあります。IPMI は、メインプロセッサおよびオペレーティングシステムからは独立して機能します。

IPMI で使用できる独立した監視、ロギング、アクセス機能は、プラットフォームハードウェアに組み込まれおり、一定の管理容易性を提供します。また、特定のオペレーティングシステムで使用できるシステム管理ソフトウェアがない場合や、システム管理ソフトウェアのインストールまたはロードを行わないことを選択する場合は、IPMI がシステムをサポートします。

ILOM は IPMI v1.5 および v2.0 に準拠しています。

IPMI に関する詳細な仕様などの追加情報は、次のサイトから入手できます。

```
http://www.intel.com/design/servers/ipmi/spec.htm
```

```
http://openipmi.sourceforge.net
```

ILOM と IPMI

IPMI は、組み込みの管理サブシステムが通信する特定の方法を定義します。IPMI の情報は、IPMI に準拠したハードウェアコンポーネント上に配置される Baseboard Management Controller (BMC) を使用して交換されます。オペレーティングシステムではなく、下位のハードウェアインテリジェンスを使用することには、主に 2 つのメリットがあります。第 1 に帯域外のサーバー管理が可能になること、第 2 にシステム状態データを転送する際にオペレーティングシステムに負担をかけずに済むことです。

サーバーまたはブレード上のサービスプロセッサ (SP) は、IPMI v2.0 に準拠しています。IPMI の機能には、帯域内または帯域外のいずれかの IPMItool ユーティリティーを使用してコマンド行からアクセスできます。また、ILOM Web インタフェースから IPMI 固有のトラップを生成したり、IPMI v1.5 または v2.0 に準拠した外部の管理ソリューションから SP の IPMI 機能を管理することもできます。

IPMItool の使用

IPMItool は、IPMI に対応したデバイスの管理および構成に役立つ、オープンソースの簡単なコマンド行インタフェース (CLI) ユーティリティーです。IPMItool では、ローカルシステムまたは遠隔システムのどちらの IPMI 機能も管理できます。IPMItool ユーティリティーは、カーネルデバイスドライバまたは LAN インタフェースで IPMI 機能を実行する場合に使用できます。IPMItool は次のサイトからダウンロードできます。

```
http://ipmitool.sourceforge.net/
```

IPMItool を使用して、次の処理を実行できます。

- センサーデータレコード (SDR) リポジトリの読み取り
- センサーの値の出力
- システムイベントログ (SEL) の内容の表示
- 現場交換可能ユニット (FRU) のインベントリ情報の出力
- LAN 構成パラメータの読み取りおよび設定

■ 遠隔のシャーシの電源制御の実行

IPMItool の詳細は、次のサイトから入手可能なマニュアルページで提供されています。

`http://ipmitool.sourceforge.net/manpage.html`

IPMI の警告

ILOM では IPMI Platform Event Trap (PET) 形式の警告をサポートしています。警告では、発生する可能性のあるシステムの障害を事前に報告します。警告の構成は、サーバーまたはブレードの SP から実行できます。IPMI PET の警告は、シャーシ監視モジュール (CMM) 以外のすべての Sun のサーバープラットフォームおよびモジュールでサポートされています。

Sun の各サーバープラットフォームには、電圧や温度、およびその他の保守に関連するシステム属性を測定する、IPMI に準拠したセンサーが多数装備されています。ILOM はこれらのセンサーを自動的にポーリングし、しきい値を超えるとイベントを ILOM イベントログに記録します。また、ILOM は警告メッセージを生成して、IP アドレスで指定した 1 つ以上の警告の宛先に送信します。指定した警告の宛先は、IPMI PET メッセージの受信をサポートしている必要があります。警告の宛先が IPMI PET メッセージをサポートしていない場合、警告の受信者は警告メッセージを復号化できません。

IPMI PET 警告を設定する場合は、警告レベルも指定する必要があります。この警告レベルは、警告の受信者がもっとも関心のあるメッセージのみを受信できるように、警告メッセージをフィルタリングします。ILOM には 5 つの警告レベルがあり、もっとも低いレベルの警告はマイナーです。

- **マイナー** − 情報イベント、上限および下限の非クリティカルイベント、上限および下限のクリティカルイベント、上限および下限の回復不可能イベントに関する警告を生成します。
- **メジャー** − 上限および下限の非クリティカルイベント、上限および下限のクリティカルイベント、上限および下限の回復不可能イベントに関する警告を生成します。
- **クリティカル** − 上限および下限のクリティカルイベントと上限および下限の回復不可能イベントに関する警告を生成します。
- **停止** − 上限の回復不可能イベントと下限の回復不可能イベントのみに関する警告を生成します。
- **無効** − 警告を無効にします。ILOM は警告メッセージを生成しません。

警告ルールの変更、警告ルールの無効化、テスト警告の生成など、警告ルール設定の管理については、144 ページの「ILOM Web インタフェースを使用した警告ルール設定の管理」および 149 ページの「ILOM CLI を使用した警告ルール設定の管理」を参照してください。

警告ルール設定を管理するための ILOM CLI コマンドについては、149 ページの「警告ルール設定を管理するための CLI コマンド」を参照してください。

IPMItool の例

IPMItool の使用方法の例を次に示します。この例では、ILOM の IP アドレスは 10.8.136.165 です。コマンドはすべてのプラットフォームに共通です。ただし、出力 (センサー名、値、しきい値など) はプラットフォーム固有です。

▼ センサーとその値の一覧を表示する

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sdr list
/SYS/T_AMB       | 24 degrees C       | ok
/RFM0/FAN1_SPEED | 7110 RPM           | ok
/RFM0/FAN2_SPEED | 5880 RPM           | ok
/RFM1/FAN1_SPEED | 5880 RPM           | ok
/RFM1/FAN2_SPEED | 6360 RPM           | ok
/RFM2/FAN1_SPEED | 5610 RPM           | ok
/RFM2/FAN2_SPEED | 6510 RPM           | ok
/RFM3/FAN1_SPEED | 6000 RPM           | ok
/RFM3/FAN2_SPEED | 7110 RPM           | ok
/RFM4/FAN1_SPEED | 6360 RPM           | ok
/RFM4/FAN2_SPEED | 5610 RPM           | ok
/RFM5/FAN1_SPEED | 5640 RPM           | ok
/RFM5/FAN2_SPEED | 6510 RPM           | ok
/RFM6/FAN1_SPEED | 6180 RPM           | ok
/RFM6/FAN2_SPEED | 6000 RPM           | ok
/RFM7/FAN1_SPEED | 6330 RPM           | ok
/RFM7/FAN2_SPEED | 6330 RPM           | ok
/RFM8/FAN1_SPEED | 6510 RPM           | ok
/RFM8/FAN2_SPEED | 5610 RPM           | ok
```

注 – 上記の出力は省略されています。実際の出力では 163 個のセンサーが表示されます。

▼ 1 つのセンサーの詳細を表示する

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme sensor get
/SYS/T_AMB
Locating sensor record...
Sensor ID              : /SYS/T_AMB (0x8)
 Entity ID             : 41.0
 Sensor Type (Analog)  : Temperature
 Sensor Reading        : 24 (+/- 0) degrees C
 Status                : ok
 Lower Non-Recoverable : 0.000
 Lower Critical        : 4.000
 Lower Non-Critical    : 10.000
 Upper Non-Critical    : 35.000
 Upper Critical        : 40.000
 Upper Non-Recoverable : 45.000
 Assertions Enabled    : lnc- lcr- lnr- unc+ ucr+ unr+
 Deassertions Enabled  : lnc- lcr- lnr- unc+ ucr+ unr+
```

▼ ホストの電源を入れる

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme
chassis power on
```

▼ ホストの電源を切る

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme
chassis power off
```

▼ ホストの電源を再投入する

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme
chassis power cycle
```

▼ ホストを正常に停止する

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme
chassis power soft
```

▼ FRU の製造情報を表示する

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme fru print
FRU Device Description : Builtin FRU Device (ID 0)
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : SUN MICROSYSTEMS
 Product Name          : ILOM

FRU Device Description : /SYS (ID 4)
 Chassis Type          : Rack Mount Chassis
 Chassis Part Number   : 541-0251-05
 Chassis Serial        : 00:03:BA:CD:59:6F
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : SUN MICROSYSTEMS
 Product Name          : SUN BLADE X8400 SERVER MODULE
 Product Part Number   : 602-0000-00
 Product Serial        : 0000000000
 Product Extra         : 080020ffffffffffffff0003baf15c5a

FRU Device Description : /P0 (ID 5)
 Product Manufacturer  : ADVANCED MICRO DEVICES
 Product Part Number   : 0F21
 Product Version       : 2

FRU Device Description : /P0/D0 (ID 6)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
 Product Part Number   : 18VDDF12872Y-40BD3
 Product Version       : 0300
 Product Serial        : D50209DA
 Product Extra         : 0190
 Product Extra         : 0400

FRU Device Description : /P0/D1 (ID 7)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
 Product Part Number   : 18VDDF12872Y-40BD3
 Product Version       : 0300
 Product Serial        : D50209DE
 Product Extra         : 0190
 Product Extra         : 0400
```

▼ IPMI システムイベントログを表示する

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sel list
 100 | Pre-Init Time-stamp   | Power Unit #0x78 | State Deasserted
 200 | Pre-Init Time-stamp   | Power Supply #0xa2 | Predictive Failure Asserted
 300 | Pre-Init Time-stamp   | Power Supply #0xba | Predictive Failure Asserted
 400 | Pre-Init Time-stamp   | Power Supply #0xc0 | Predictive Failure Asserted
 500 | Pre-Init Time-stamp   | Power Supply #0xb4 | Predictive Failure Asserted
 600 | 04/05/2007 | 12:03:24 | Power Supply #0xa3 | Predictive Failure Deasserted
 700 | 04/05/2007 | 12:03:25 | Power Supply #0xaa | Predictive Failure Deasserted
 800 | 04/05/2007 | 12:03:25 | Power Supply #0xbc | Predictive Failure Deasserted
 900 | 04/05/2007 | 12:03:26 | Power Supply #0xa2 | Predictive Failure Asserted
 a00 | 04/05/2007 | 12:03:26 | Power Supply #0xa8 | Predictive Failure Deasserted
 b00 | 04/05/2007 | 12:03:26 | Power Supply #0xb6 | Predictive Failure Deasserted
 c00 | 04/05/2007 | 12:03:26 | Power Supply #0xbb | Predictive Failure Deasserted
 d00 | 04/05/2007 | 12:03:26 | Power Supply #0xc2 | Predictive Failure Deasserted
 e00 | 04/05/2007 | 12:03:27 | Power Supply #0xb0 | Predictive Failure Deasserted
 f00 | 04/05/2007 | 12:03:27 | Power Supply #0xb5 | Predictive Failure Deasserted
1000 | 04/05/2007 | 12:03:27 | Power Supply #0xba | Predictive Failure Asserted
1100 | 04/05/2007 | 12:03:27 | Power Supply #0xc0 | Predictive Failure Asserted
1200 | 04/05/2007 | 12:03:28 | Power Supply #0xa9 | Predictive Failure Deasserted
1300 | 04/05/2007 | 12:03:28 | Power Supply #0xae | Predictive Failure Deasserted
1400 | 04/05/2007 | 12:03:28 | Power Supply #0xb4 | Predictive Failure Asserted
1500 | 04/05/2007 | 12:03:28 | Power Supply #0xbe | Predictive Failure Deasserted
```

第 10 章

SNMP

ILOM では、SNMP をサポートしています。SNMP は、ネットワークアクティビティーに関するデータの交換に使用されます。SNMP は、業界標準のオープンなプロトコルです。

この章には次の節があります。

注 – この章の構文例では、/SP/ で始まるターゲットを使用しますが、使用している Sun サーバープラットフォームによっては、/CMM/ で始まるターゲットに置き換わる場合があります。サブターゲットは、すべての Sun サーバープラットフォームで共通です。

SNMP の概要

SNMP は、ネットワークおよびネットワークに接続されたデバイスまたはノードの管理を可能にするオープンな技術です。SNMP を使用して、管理対象デバイス (ノード) とネットワーク管理ステーションとの間でデータがやりとりされます。管理対象デバイスには、ホストやルータ、Web サーバー、またはネットワーク上のその他のサーバーなどの、SNMP が動作しているいずれのデバイスも含まれます。SNMP メッセージは、ユーザーデータグラムプロトコル (UDP) を使用して IP 経由で送信されます。SNMP をサポートする管理アプリケーションならサーバーを管理できます。

ILOM は、SNMP version 1、2c、および 3 をサポートしています。SNMP v3 は、SNMP v1 および v2c よりもセキュリティー、認証、およびプライバシー機能が優れているため、SNMP v3 の使用を強くお勧めします。

SNMP はオペレーティングシステムではなくプロトコルであるため、SNMP メッセージを使用するにはアプリケーションが必要です。使用している SNMP 管理ソフトウェアがこの機能を提供している場合があります。net-SNMP などのオープンソースツールも使用できます。net-SNMP は、次の URL からダウンロードできます。

```
http://net-snmp.sourceforge.net/
```

管理ステーションおよびエージェントはどちらも SNMP メッセージを使用してやりとりを行います。管理ステーションは、情報の送受信が可能です。エージェントは要求に応答し、トラップの形式で未承諾メッセージを送信できます。管理ステーションおよびエージェントは、次の機能を使用します。

- Get (取得)

- GetNext (次を取得)
- GetResponse (応答を取得)
- Set (設定)
- Trap (トラップ)

SNMP の仕組み

SNMP の機能には、次の 2 つのコンポーネントが必要です。

- **ネットワーク管理ステーション** – ネットワーク管理ステーションは、管理対象ノードを監視および制御する管理アプリケーションのホストになります。
- **管理対象ノード** – 管理対象ノードは、SNMP 管理エージェントをホストする、サーバー、ルーター、ハブなどのデバイスで、ILOM を実行している SP などの管理ステーションからの要求を実行します。

管理ステーションは、適切な情報を得るために、クエリーを使用して管理エージェントをポーリングして監視します。管理対象ノードは、トラップという形式で、状態が未承諾の情報を管理ステーションに提供することもできます。SNMP は、管理ステーションとエージェントの間で管理情報をやりとりするために使用されるプロトコルです。

SNMP エージェントは Sun のサーバープラットフォームにプリインストールされており、ILOM で実行されるため、すべての SNMP 管理は ILOM から行われます。この機能を使用するには、使用しているオペレーティングシステムに SNMP クライアントアプリケーションが必要です。

SNMP 管理情報ベースファイル

SNMP 実装の基本コンポーネントは、管理情報ベース (MIB) です。MIB は、管理対象ノードが使用できる情報と保存されている場所を記述するテキストファイルです。ツリーに似た階層システムによって、ネットワークのリソースに関する情報が分類されます。MIB は、SNMP エージェントがアクセス可能な変数を定義しています。管理ステーションが管理ノードからの情報を要求すると、そのエージェントは、そのリクエストを受信し、MIB から該当する情報を取得します。MIB によって、サーバーのネットワーク設定や状態、統計データにアクセスできる。

ILOM では次の SNMP MIB が使用されます。

- SNMPv2 MIB (RFC1907) のシステムグループと SNMP グループ
- SNMP-FRAMEWORK-MIB (RFC2271.txt)

- SNMP-USER-BASED-MIB (RFC 2574)
- SNMP-MPD-MIB (RFC 2572)
- ENTITY-MIB (RFC 2737) の entPhysicalTable
- SUN-PLATFORM-MIB

  この MIB は、すべてのセンサーやインジケータとその状態など、サーバーおよびシャーシハードウェアのインベントリを表します。
- SUN-ILOM-CONTROL-MIB

  この MIB は、ユーザーやアクセスの管理、警告など、Sun SP または CMM の設定を表します。
- SUN-HW-TRAP-MIB

  この MIB は、Sun SP または CMM が生成する可能性のあるハードウェア関連のトラップを表します。
- SUN-ILOM-PET-MIB

  この MIB は、Sun SP が生成する可能性のある IPMI Platform Event Trap (PET) を表します。PET に関する情報は、140 ページの「警告管理について」を参照してください。

警告と SNMP トラップ

ILOM を使用して、最大 15 個の警告ルールを設定できます。ILOM で設定する警告ルールごとに、警告の種類に応じて、警告に関する 3 つ以上のプロパティーを定義する必要があります。警告の種類には、メッセージ形式と警告メッセージの送受信方法を定義します。ILOM は、IPMI PET 警告、電子メール通知警告、SNMP トラップの 3 つの警告の種類をサポートしています。

ILOM は、ユーザー指定の IP アドレスへの SNMP トラップ警告の生成をサポートしています。指定するすべての宛先が、SNMP トラップメッセージの受信をサポートしている必要があります。

ILOM には、SNMP 管理アプリケーションに SNMP トラップを配信する SNMP エージェントがプリインストールされています。

この機能を使用するには、次の処理を実行する必要があります。

- プラットフォーム固有の MIB を SNMP ディレクトリに統合して保存します。
- 管理ステーションにサーバーについて通知します。
- 管理ステーションに SNMP トラップを送信するように ILOM を設定します。

デフォルトでは、トラップの宛先は設定されていません。デフォルトでは、エージェントはポート 161 で SNMP 要求を待機し、ポート 162 にトラップを送信します。

CLI を使用した SNMP ユーザーの管理

ILOM コマンド行インタフェース (CLI) を使用して、SNMP ユーザーアカウントおよびコミュニティーを追加、削除、または設定できます。

注 – ILOM CLI で作業する場合にセット要求が無効になっていると、すべての SNMP オブジェクトは読み取り専用になります。

▼ CLI を使用して SNMP ユーザーアカウントを追加する

1. ILOM CLI に管理者としてログインします。
2. SNMP v3 読み取り専用ユーザーアカウントを追加するには、次のコマンドを入力します。

   create /SP/services/snmp/users/*username* **authenticationpassword=***password*

▼ CLI を使用して SNMP ユーザーアカウントを編集する

1. ILOM CLI に管理者としてログインします。
2. SNMP v3 のユーザーアカウントを編集するには、次のコマンドを入力します。

   edit /SP/services/snmp/users/*username* **authenticationpassword=***password*

注 – SNMP ユーザーのパラメータを変更するときは、パスワードを変更しない場合でも `authenticationpassword` に値を指定してください。

▼ CLI を使用して SNMP ユーザーアカウントを削除する

1. ILOM CLI に管理者としてログインします。

2. SNMP v3 のユーザーアカウントを削除するには、次のコマンドを入力します。

   delete /SP/services/snmp/users/*username*

▼ CLI を使用して SNMP コミュニティーを追加または編集する

1. ILOM CLI に管理者としてログインします。
2. SNMP v1 または v2c のコミュニティーを追加するには、次のコマンドを入力します。

   create /SP/services/snmp/communities/*communityname*

▼ CLI を使用して SNMP コミュニティーを削除する

1. ILOM CLI に管理者としてログインします。
2. SNMP v1 または v2c のコミュニティーを削除するには、次のコマンドを入力します。

   delete /SP/services/snmp/communities/*communityname*

ターゲット、プロパティー、および値

次の表に、SNMP ユーザーアカウントで有効なターゲット、プロパティー、および値を示します。

表 10-1 SNMP ユーザーアカウントのターゲット、プロパティー、および値

ターゲット	プロパティー	値	デフォルト値
/SP/services/snmp/communities/*communityname*	permissions	ro|rw	ro
/SP/services/snmp/users/*username*	authenticationprotocol	MD5|SHA	MD5
	authenticationpassword*	<*string*>	(空文字列)
	permissions	ro|rw	ro
	privacyprotocol	none|DES	none
	privacypassword*	<*string*>	(空文字列)
/SP/services/snmp	engineid = none	<*string*>	(空文字列)
	port = 161	<*integer*>	161
	sets = enabled	enabled|disabled	disabled
	v1 = disabled	enabled|disabled	disabled
	v2c = disabled	enabled|disabled	disabled
	v3 = disabled	enabled|disabled	enabled

* privacyprotocol プロパティーに none 以外の値が指定されている場合は、privacypassword を設定してください。ユーザーを作成または修正する場合には、authenticationpassword を指定する必要があります (SNMP v3 のみ)。

たとえば、ユーザー a1 の privacyprotocol を DES に変更するには、次のように入力します。

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES
privacypassword=password authenticationprotocol=SHA
authenticationpassword=password
```

次のように入力しただけでは、変更は有効になりません。

```
-> set /SP/services/snmp/users/a1 privacyprotocol=DES
```

注 – SNMP ユーザーの権限は、プライバシプロパティーまたは認証プロパティーを再設定することなく変更できます。

▼ CLI を使用して SNMP トラップの宛先を設定する

SNMP トラップを送信する宛先を設定するには、次の手順に従います。

1. ILOM CLI に管理者としてログインします。
2. `show` コマンドを入力して、警告ルールの現在の設定を表示します。

   例:

```
-> show
/SP/alertmgmt/rules/1
   Targets:
   Properties:
      community_or_username = public
      destination = 0.0.0.0
      level = disable
      snmp_version = 1
      type = snmptrap
Commands:
  cd
  set
  show
```

3. `/SP/alertmgmt/rules/snmp` ディレクトリに移動します。次のように入力します。

   -> **cd /SP/alertmgmt/rules/snmp**

4. SNMP トラップの宛先を設定するルールをターゲット 1 ～ 15 の中から選択し、そのディレクトリに移動します。

   例:

   -> **cd 4**

5. そのルールのディレクトリ内で `set` コマンドを実行し、ルールのプロパティーを変更します。

   例:

   -> **set type=snmptrap level=critical destination=***IPaddress* **snmp_version=2c community_or_username=public**

Web インタフェースを使用した SNMP ユーザーの管理

この節では、ILOM Web インタフェースを使用して SNMP ユーザーおよびコミュニティーを管理する方法について説明します。

▼ Web インタフェースを使用して SNMP の設定を行う

SNMP の設定を行うには、次の手順に従います。

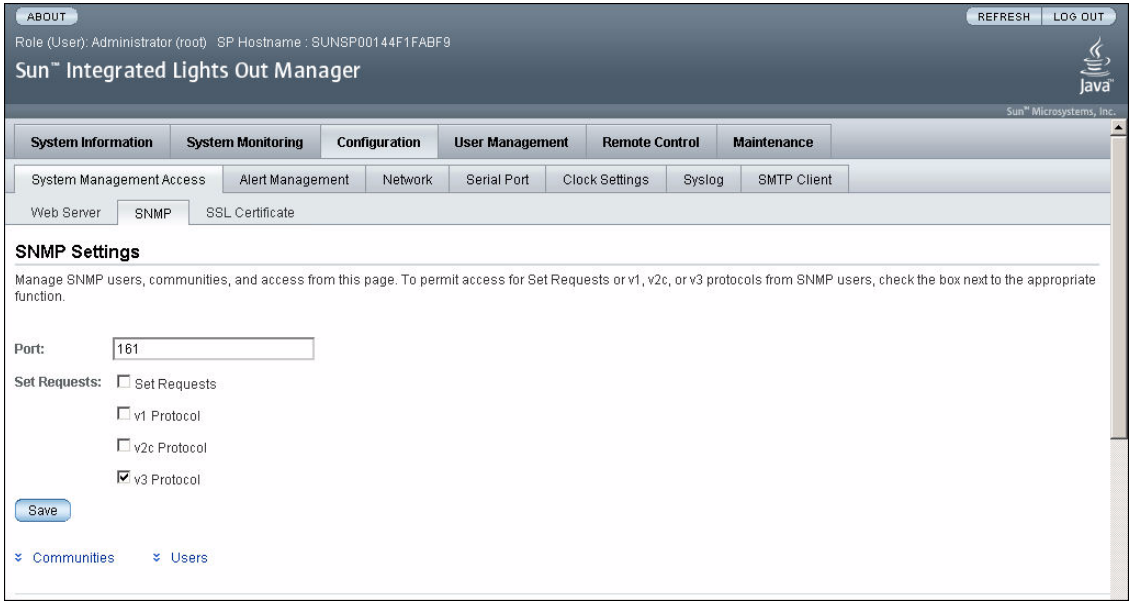
1. **管理者として ILOM にログインし、Web インタフェースを開きます。**

   管理者権限で ILOM にログインした場合にのみ、SNMP の設定を変更できます。

2. **「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SNMP」の順に選択します。**

   「SNMP Settings (SNMP 設定)」ページが表示されます。

図 10-1　「SNMP Settings (SNMP 設定)」ページ



3. 「Port (ポート)」テキストフィールドにポート番号を入力します。

4. 「Set Requests (セット要求)」チェックボックスを選択またはクリアして、「Set Requests (セット要求)」オプションを有効または無効にします。

   「Set Requests (セット要求)」が無効になっていると、すべての SNMP オブジェクトが読み取り専用になります。

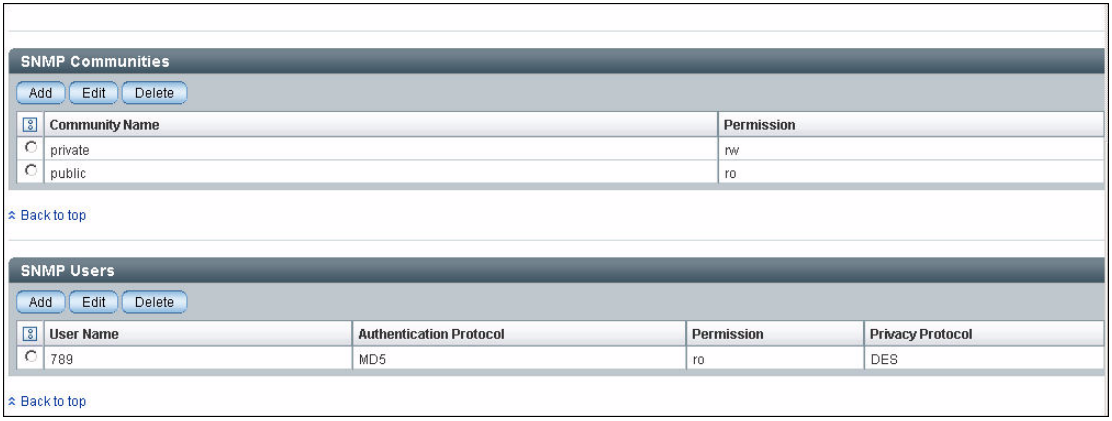
5. チェックボックスを選択して、SNMP v1、v2c、または v3 を有効にします。

   SNMP v3 がデフォルトで有効になっています。v1、v2c、および v3 のプロトコルバージョンは有効にしたり無効にしたりできます。

6. 「Save (保存)」ボタンをクリックします。

注 – 図 10-2 に示すように、ページの下部で、SNMP コミュニティーまたは SNMP ユーザーを追加、編集、または削除することもできます。

図 10-2　SNMP コミュニティーおよびユーザー



▼ Web インタフェースを使用して SNMP ユーザーアカウントを追加または編集する

SNMP v3 ユーザーアカウントを追加または編集するには、次の手順に従います。

1. **管理者として ILOM にログインし、Web インタフェースを開きます。**

   管理者権限で ILOM にログインした場合にのみ、SNMP ユーザーまたはユーザーアカウントを追加できます。

2. **「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SNMP」の順に選択します。**

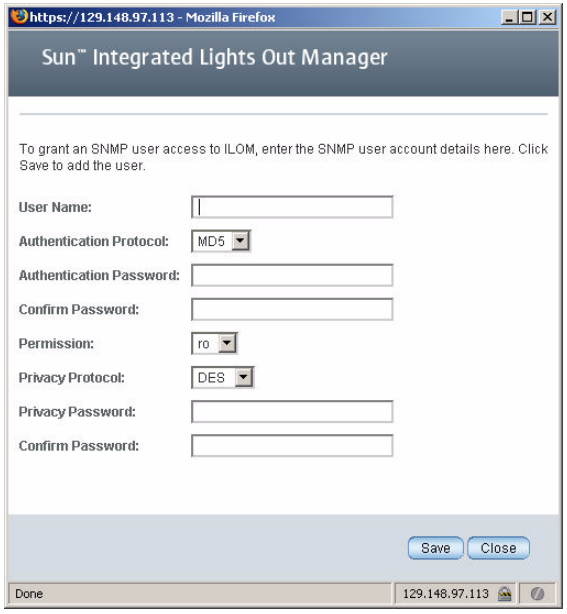
   「SNMP Settings (SNMP 設定)」ページが表示されます。

3. **「Users」リンクをクリックするか、「SNMP Users (SNMP ユーザー)」リストを下にスクロールします。**

4. **「SNMP Users (SNMP ユーザー)」リストの下の「Add (追加)」または「Edit (編集)」をクリックします。**

   図 10-3 に示すように、「Add (追加)」ダイアログボックスまたは「Edit (編集)」ダイアログボックスが表示されます。

図 10-3　「Add SNMP User」ダイアログ



5. 「User Name (ユーザー名)」テキストフィールドに、ユーザー名を入力します。

   ユーザー名は最大 35 文字まで入力できます。英字で始める必要があります。空白文字は使用できません。

6. 「Authentication Protocol (認証プロトコル)」ドロップダウンリストで、「MD5 (Message Digest 5)」または「SHA (Secure Hash Algorithm)」のいずれかを選択します。

7. 「Authentication Password」テキストフィールドにパスワードを入力します。

   認証パスワードは 8 文字以上 16 文字以下である必要があります。コロンまたは空白文字は使用できません。大文字と小文字は区別されます。

8. 「Confirm Password (パスワードの確認)」テキストフィールドに認証パスワードを再入力します。

9. 「Permissions (許可)」ドロップダウンリストで、「ro (読み取り専用)」または「rw (読み取りと書き込み)」を選択します。

10. 「Privacy Protocol」ドロップダウンリストで、「DES」または「None (なし)」を選択します。

11. 「Privacy Password」テキストフィールドにパスワードを入力します。

    プライバシパスワードは 8 文字以上 16 文字以下である必要があります。コロンまたは空白文字は使用できません。大文字と小文字は区別されます。

12. 「Confirm Password (パスワードの確認)」テキストフィールドにパスワードを再入力します。

13. 「Save (保存)」ボタンをクリックします。

▼ Web インタフェースを使用して SNMP ユーザーアカウントを削除する

SNMP v3 ユーザーアカウントを削除するには、次の手順に従います。

1. 管理者として ILOM にログインし、Web インタフェースを開きます。

   管理者権限でアカウントにログインした場合にのみ、SNMP の設定を変更できます。

2. 「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SNMP」の順に選択します。

   「SNMP Settings (SNMP 設定)」ページが表示されます。

3. 「Users」リンクをクリックするか、「SNMP Users (SNMP ユーザー)」リストを下にスクロールします。

4. 削除する SNMP ユーザーアカウントのラジオボタンを選択します。

5. 「SNMP Users (SNMP ユーザー)」リストの下の「Delete (削除)」をクリックします。

   確認のダイアログボックスが開きます。

6. 「OK」をクリックすると、ユーザーアカウントが削除されます。

▼ Web インタフェースを使用して SNMP コミュニティーを追加または編集する

SNMP v1 または v2c のコミュニティーを追加または編集するには、次の手順に従います。

1. 管理者として ILOM にログインし、Web インタフェースを開きます。

   管理者権限でアカウントにログインした場合にのみ、SNMP コミュニティーを追加または編集できます。

2. 「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SNMP」の順に選択します。

   「SNMP Settings (SNMP 設定)」ページが表示されます。

3. 「Communities」リンクをクリックするか、「Communities」リストを下にスクロールします。

4. 「SNMP Communities (SNMP コミュニティ)」リストの「Add (追加)」または「Edit (編集)」ボタンをクリックします。

   「Add (追加)」または「Edit (編集)」ダイアログボックスが表示されます。

5. 「Community Name (コミュニティ名)」フィールドにコミュニティーの名前を入力します。

   コミュニティー名は最大 35 文字まで入力できます。英字で始まる必要があります。空白文字は使用できません。

6. 「Permissions (許可)」ドロップダウンリストで、「ro (読み取り専用)」または「rw (読み取りと書き込み)」を選択します。

7. 「Save (保存)」ボタンをクリックします。

▼ Web インタフェースを使用して SNMP コミュニティーを削除する

SNMP v1 または v2c のコミュニティーを削除するには、次の手順に従います。

1. 管理者として ILOM にログインし、Web インタフェースを開きます。

   管理者権限でアカウントにログインした場合にのみ、SNMP コミュニティーを削除できます。

2. 「Configuration (設定)」-->「System Management Access (システム管理アクセス)」-->「SNMP」の順に選択します。

   「SNMP Settings (SNMP 設定)」ページが表示されます。

3. 「Communities」リンクをクリックするか、「Communities」リストを下にスクロールします。

4. 削除する SNMP コミュニティーのラジオボタンを選択します。

5. 「Delete (削除)」をクリックします。

   確認のダイアログボックスが表示されます。

6. 「OK」をクリックすると、SNMP コミュニティーが削除されます。

▼ Web インタフェースを使用して SNMP トラップの宛先を設定する

SNMP トラップを送信する宛先を設定するには、次の手順に従います。

1. 管理者として ILOM にログインし、Web インタフェースを開きます。

   管理者権限でアカウントにログインした場合にのみ、SNMP トラップの宛先を設定できます。

2. 「Configuration (設定)」-->「Alert Management (警告の管理)」を選択します。

   「Alert Settings」ページが表示されます。このページには、設定済みの警告の表が表示されます。

3. 「Actions」ドロップダウンリストから、「Edit (編集)」を選択します。

   「Create or Modify Alert」ダイアログが表示されます。

4. ダイアログで、ドロップダウンリストから警告のレベルを選択します。

5. 「Type」ドロップダウンリストで、「SNMP Trap」を選択します。

6. SNMP トラップの宛先の IP アドレス、SNMP のバージョン、またはコミュニティーかユーザー名を指定します。

7. 「Save (保存)」をクリックして変更を有効にします。

SNMP の例

この節では、net-snmp を使用して ILOM SP の SNMP エージェントに問い合わせを行うさまざまな例を示します。

最初に、使用している管理ステーションのオペレーティングシステムで動作する net-snmp の最新バージョン (version 5.2.1 以降) を次の URL からダウンロードしてインストールします。

```
http://net-snmp.sourceforge.net/
```

net-snmp によって、ILOM がサポートする標準の MIB (SNMPv2-MIB、SNMP-FRAMEWORK-MIB、および ENTITY-MIB) がすべてインストールされます。SUN-PLATFORM-MIB.mib、SUN-ILOM-CONTROL-MIB.mib、SUN-HW-TRAP-MIB.mib および SUN-ILOM-PET-MIB.mib ファイルをダウンロードして、net-snmp ツールが MIB を読み込むディレクトリにこれらのファイルを配置する必要があります。追加情報は、次の URL を参照してください。

http://net-snmp.sourceforge.net/wiki/index.php/TUT:Using_and_loading_MIBS

▼ SNMP の設定を表示および構成する

前の節で説明したように SP または CMM を設定してから、次の手順に従って SNMP の設定を表示および構成します。

1. 次のように入力して、/SP/services/snmp ディレクトリに移動します。

```
-> cd /SP/services/snmp
```

2. そのディレクトリ内で show コマンドを実行し、SNMP の設定を表示します。

```
-> show
   /SP/services/snmp
   Targets:
     communities
     users
   Properties:
     engineid = none
     port = 161
     sets = disabled
     v1 = disabled
     v2c = disabled
     v3 = enabled
   Commands:
     cd
     set
     show
```

3. SNMP の設定を行います。次に例を示します。
   - v2c を enabled に設定するには、次のように入力します。

```
-> set v2c=enabled
```

   - sets を enabled に設定するには、次のように入力します。

```
-> set sets=enabled
```

4. 次のように入力して、コミュニティーを表示します。

```
-> show communities
```

```
-> show communities
/SP/services/snmp/communities
Targets:
```

```
  public
Properties:
Commands:
  cd
  create
  delete
  show
```

5. 次のように入力して、public コミュニティーを表示します。

   -> **show communities/public**

```
-> show communities/public
/SP/services/snmp/communities/public
Targets:
Properties:
  permission = ro
Commands:
  cd
  set
  show
```

6. 次のように入力して、読み取りおよび書き込み権限を持つ private コミュニティーを作成します。

   -> **create communities/private permission=rw**

▼ snmpget または snmpwalk net-snmp コマンドを使用して情報を取得する

1. snmpget コマンドを入力して、特定の情報を取得します。

   例:

```
$ snmpget -v 2c -c public -m ALL <sp_ip> sysObjectID.0 sysUpTime.0 sysLocation.0
        SNMPv2-MIB::sysObjectID.0 =
        OID:SUN-FIRE-SMI-MIB::sunBladeX8400ServerModule
        SNMPv2-MIB::sysUpTime.0 = Timeticks: (17523) 0:02:55.23
        SNMPv2-MIB::sysLocation.0 = STRING:
```

2. snmpwalk コマンドを入力して、ディスクリートコンポーネントに関する情報を取得します。

例:

```
$ snmpwalk -v 2c -c public -m ALL <sp_ip> entPhysicalName
        ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
        ENTITY-MIB::entPhysicalName.2 = STRING: /SYS/OK2RM
        ENTITY-MIB::entPhysicalName.3 = STRING: /SYS/SERVICE
        ENTITY-MIB::entPhysicalName.4 = STRING: /SYS/OK
        ENTITY-MIB::entPhysicalName.5 = STRING: /SYS/LOCATE
        ENTITY-MIB::entPhysicalName.6 = STRING: /SYS/LOCATE_BTN
        ENTITY-MIB::entPhysicalName.7 = STRING: /SYS/POWER_BTN
        ENTITY-MIB::entPhysicalName.8 = STRING: /SYS/T_AMB
        ENTITY-MIB::entPhysicalName.9 = STRING: /SYS/P0
```

▼ snmpset を使用して情報を設定する

- デバイスの場所を変更するには、snmpset コマンドを入力します。

例:

$ **snmpset -v 2c -c private -m ALL** <*sp_ip*> sysLocation.0 s "<*location*>"

例:

```
SNMPv2-MIB::sysLocation.0 = STRING: ILOM Dev Lab
```

▼ snmptrapd を使用してトラップを受信する

- トラップ情報を受信するには、snmptrapd コマンドを入力します。

  例 :

```
$ /usr/sbin/snmptrapd -m ALL -f -Lo
SNMP trap example:
        2007-05-21 08:46:41 ban3c9sp4 [10.8.136.94]:
        SNMPv2-MIB::sysUpTime.0 = Timeticks: (1418) 0:00:14.18
        SNMPv2-MIB::snmpTrapOID.0 = OID:
        SUN-HW-TRAP-MIB::sunHwTrapPowerSupplyError
        SUN-HW-TRAP-MIB::sunHwTrapSystemIdentifier.0 = STRING:
        SUN-HW-TRAP-MIB::sunHwTrapChassisId.0 = STRING:
        ban6c4::0000000000 SUN-HW-TRAP-MIB::sunHwTrapProductName.0
        = STRING:   SUN-HW-TRAP-MIB::sunHwTrapComponentName.0 =
        STRING: /PS3/FAN_ERR
        SUN-HW-TRAP-MIB::sunHwTrapAdditionalInfo.0 = STRING: Predictive
        Failure Asserted    SUN-HW-TRAP-MIB::sunHwTrapAssocObjectId.0 =
        OID: SNMPv2-SMI::zeroDotZero
```

第 11 章

ILOM ファームウェアの更新

ILOM ファームウェアの更新プロセスでは、新しい ILOM ファームウェアをインストールしたり、使用しているプラットフォーム用のその他のモジュール (x64 用の BIOS、OpenBoot PROM、SPARC 用の Hypervisor ソフトウェアなど) を更新することができます。

この章には次の節があります。

ファームウェアの更新プロセス

ファームウェアを更新するときは、次の注意点やガイドラインと確認してください。

注意 – 処理を進める前に、ホストのオペレーティングシステムを停止してください。ILOM は、OS の正常な停止を試みます。正常に停止できない場合は、ILOM が強制的に停止するため、ファイルシステムが破損する場合があります。

- ファームウェアの更新プロセスの完了には、約 5 分かかります。この間、ILOM ではほかの作業を行わないようにしてください。

- ファームウェアファイルのアップロード中にネットワークで障害が発生すると、タイムアウトになります。この場合、ILOM は現在インストールされているバージョンの ILOM ファームウェアで再起動されます。

ILOM ファームウェアの更新の概要

1. 新しいファームウェアイメージをダウンロードします。
2. CLI で更新する場合は TFTP サーバーに、Web インタフェースで更新する場合はローカルファイルシステムに、イメージをコピーします。
3. 管理者権限を持つ任意のユーザーでログインします。
4. CLI または Web インタフェースを使用するシステムで、各サービスプロセッサ (SP) またはシャーシ監視モジュール (CMM)、あるいはその両方のファームウェアを更新します。
5. ファームウェアの更新が完了すると、システムが自動的に再起動します。

▼ CLI を使用して ILOM バージョン情報を表示する

1. **管理者権限を持つ任意のユーザーで Secure Shell にログインします。**
2. **コマンドプロンプトで `version` と入力します。**

   次の情報が表示されます。

```
SP firmware #.#.#.#
SP firmware build number: #####
SP firmware date: Fri Apr 27 14:03:21 EDT 2007
SP filesystem version: #.#.##
```

▼ CLI を使用して ILOM ファームウェアを更新する

1. **管理者権限を持つ任意のユーザーでログインします。**

2. 次のコマンドを入力し、新しい ILOM ファームウェアイメージをダウンロードします。

   ->load -source *tftpURL*

   例:

```
-> load -source tftp://xxx.xxx.xxx.xxx/filename.pkg

NOTE: A firmware upgrade will cause the server and ILOM to
      be reset. It is recommended that a clean shutdown of
      the server be done prior to the upgrade procedure.
      An upgrade takes about 6 minutes to complete. ILOM
      will enter a special mode to load new firmware. No
      other tasks can be performed in ILOM until the
      firmware upgrade is complete and ILOM is reset.

Are you sure you want to load the specified file (y/n)? y
Do you want to preserve the configuration (y/n)? y
. . . . . .
Preserving configuration. Please wait.
Done preserving configuration.


Firmware update is complete.
ILOM will now be restarted with the new firmware.
```

▼ Web インタフェースを使用して ILOM バージョン情報を表示する

1. 管理者権限を持つ任意のユーザーでログインします。
2. 「User Management (ユーザー管理)」-->「Versions (バージョン)」を選択します。

   現在のファームウェアのバージョン情報が表示されます。

▼ Web インタフェースを使用して ILOM ファームウェアを更新する

1. 管理者権限を持つ任意のユーザーでログインします。
2. 「Maintenance (保守)」-->「Firmware Upgrade (ファームウェアのアップグレード)」を選択します。

   「Firmware Upgrade (ファームウェアのアップグレード)」ページが表示されます。

3. 「Enter Upgrade Mode (アップグレードモードに入る)」をクリックします。

   ダイアログボックスが表示され、アップグレードモードに入ることを確認するように求められます。

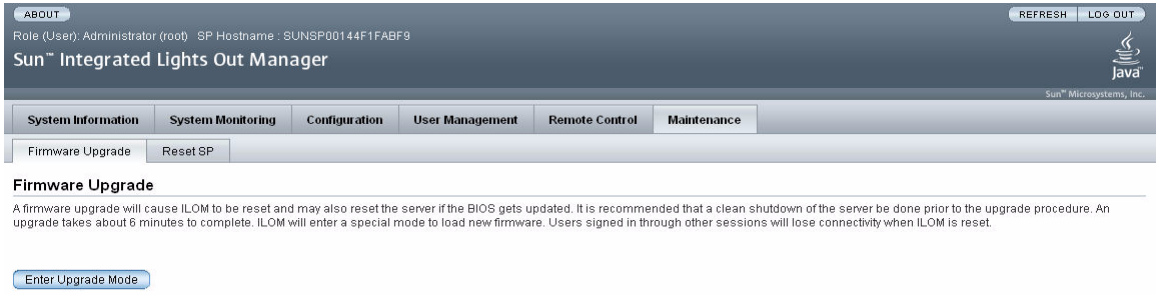
4. 「OK」をクリックしてアップグレードモードに入るか、「Cancel (キャンセル)」をクリックして処理を終了します。

   ILOM は通常の操作を停止し、フラッシュアップグレードの準備をします。

5. 「Select Image File to Upload」フィールドに新しい ILOM フラッシュイメージファイルのパスを入力するか、または「Browse (参照)」をクリックしてファームウェアアップデートファイルを探して選択してください。

   拡張子が .pkg または .ima であるファイルを使用できます。拡張子 .pkg が推奨されます。

図 11-1　「Firmware Upgrade (ファームウェアのアップグレード)」ページ



6. 「Upload (アップロード)」をクリックするか、「Cancel (キャンセル)」をクリックして処理を終了します。

   選択したファイルがアップロードされ、使用している SP または CMM に適したイメージアップデートであるかが確認されます。

   この処理には、高速ネットワーク接続で約 1 分かかります。

7. 「Verify Firmware Image (ファームウェアイメージの確認)」ページが表示されたら、「OK」をクリックします。

8. 「Preserve Configuration (設定を保存)」を選択して ILOM 設定を保存します。保存しないと、設定はファームウェアのデフォルトで上書きされます。

9. 「Start Upgrade」をクリックするか、「Cancel (キャンセル)」をクリックしてプロセスを終了します。

   「Start Upgrade」をクリックすると、進捗状況画面でファームウェアイメージが更新中であることが表示されます。更新の進捗状況が 100% に達すると、ファームウェアの更新は完了です。

   更新が完了すると、システムが自動的に再起動します。

10. SP または CMM、あるいはその両方の再起動が完了したら、ブラウザを使用して ILOM に再接続します。

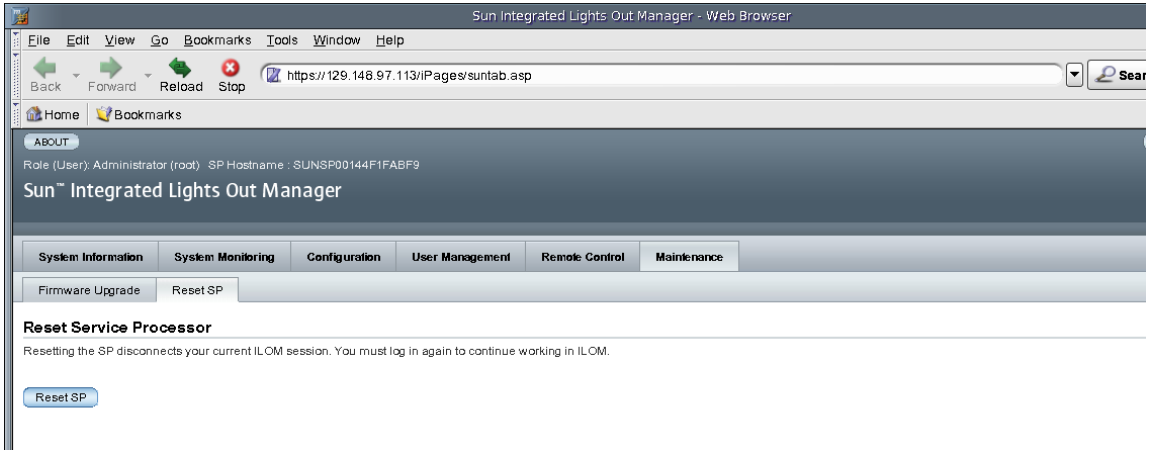
▼ ILOM SP をリセットする

ILOM サービスプロセッサ (SP) のリセットが必要な場合は、ホスト OS に影響を与えずにリセットできます。ただし、SP をリセットすると、現在の ILOM セッションが切断され、リセット中は SP が管理不可能な状態になります。

1. 管理者権限を持つ任意のユーザーでログインします。
2. 「Maintenance (保守)」-->「Reset SP (SP のリセット)」を選択します。

   「Reset Service Processor (サービスプロセッサのリセット)」ページが表示されます。

図 11-2　「Reset Service Processor (サービスプロセッサのリセット)」ページ



3. 「Reset SP (SP のリセット)」ボタンをクリックして ILOM のサービスプロセッサをリセットします。

   ILOM が再起動します。ILOM の再起動中は、Web インタフェースを使用できません。

第 12 章

Sun ILOM リモートコンソールを使用した x64 サーバーの遠隔管理

Sun ILOM リモートコンソールは、Sun x64 プロセッサベースのすべてのサーバーでサポートされています。Sun ILOM リモートコンソールは、現在、Sun SPARC サーバーではサポートされていません。

この章では、次の項目について説明します。

Sun ILOM リモートコンソールの概要

Sun ILOM リモートコンソールは、ILOM の Web インタフェースから起動できる Java アプリケーションです。Sun ILOM リモートコンソールを使用する場合、遠隔 x64 ホストサーバー上の次のデバイスを遠隔からリダイレクトおよび制御することができます。

- キーボード
- マウス
- ビデオコンソールディスプレイ
- ストレージデバイスまたはイメージ (CD/DVD、フロッピーデバイス)

Sun ILOM リモートコンソールを使用すると、ローカルクライアント上のデバイスを遠隔ホストサーバーに直接接続されているかのように動作させることができます。たとえば、遠隔ホストサーバーへのネットワーク接続を使用したリダイレクト機能により、次の処理を実行することができます。

- ローカルメディアドライブから遠隔ホストサーバーにソフトウェアをインストールします。
- 遠隔ホストサーバー上のコマンド行ユーティリティーをローカルクライアントから実行します。
- ローカルクライアントから遠隔ホストサーバー上の GUI ベースのプログラムにアクセスし、実行します。
- x64 プロセッサベースのサーバーの機能をローカルクライアントから遠隔で設定します。
- x64 プロセッサベースのサーバーのポリシーをローカルクライアントから遠隔で管理します。
- x64 プロセッサベースのサーバーの要素をローカルクライアントから遠隔で監視します。
- 通常は遠隔ホストサーバーから実行可能な、x64 プロセッサベースのソフトウェアタスクのほとんどすべてをローカルクライアントから実行します。

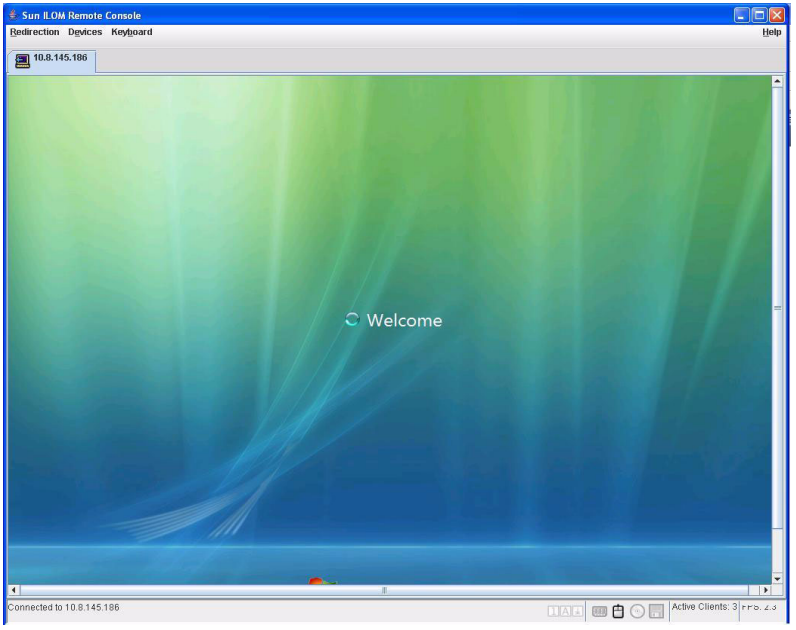
1 台構成または複数構成の遠隔ホストサーバー管理ビュー

Sun ILOM リモートコンソールは、1 台構成および複数台構成の遠隔サーバー管理ビューをサポートしています。1 台構成および複数台構成のサーバー管理ビューは、現在、すべての x64 プロセッサベースのサーバーでサポートされています。

- **1 台構成の x64 遠隔サーバー管理ビュー** – Sun ILOM リモートコンソールを起動して、1 つのウィンドウから 1 台の遠隔ホストサーバーを管理し、遠隔のキーボード、ビデオ、マウス、ストレージ (KVMS) 機能を利用できます。

注 – 1 台構成の遠隔サーバー管理ビューは、x64 サーバーのサービスプロセッサ (SP) の IP アドレスに接続する場合にサポートされます。詳細は、222 ページの「遠隔 x64 サーバー管理用の Sun ILOM リモートコンソールの起動および構成」を参照してください。

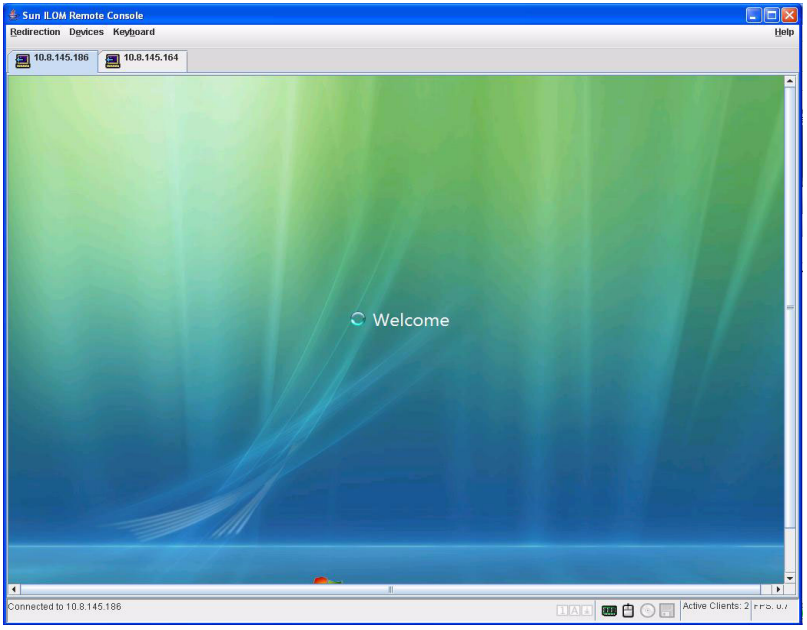
図 12-1　1 台構成のサーバー管理ビュー



- **複数台構成の x64 遠隔サーバー管理ビュー** – Sun ILOM リモートコンソールを起動して、1 つのウィンドウから複数台の遠隔 x64 サーバーを管理し、遠隔のキーボード、ビデオ、マウス、ストレージ (KVMS) 機能を利用できます。

注 – 複数台構成の遠隔サーバー管理ビューは、(1) x64 ブレードサーバーシャーシのシャーシ監視モジュール (CMM) の IP アドレスに接続する場合、(2) 別の遠隔 x64 サーバーを管理する新しい Sun ILOM リモートコントロールセッションを追加する場合のいずれかでサポートされます。詳細は、222 ページの「遠隔 x64 サーバー管理用の Sun ILOM リモートコンソールの起動および構成」を参照してください。

図 12-2　複数台構成のサーバー管理ビュー



インストール要件

Sun ILOM リモートコンソールでは、追加のハードウェアまたはソフトウェアをインストールする必要がありません。これは ILOM ソフトウェアに組み込まれています。ただし、ILOM リモートコンソールを実行するには、次のソフトウェアがローカルクライアントにインストールされている必要があります。

- **Web ブラウザ** – サポートされるブラウザは Internet Explorer 6.0 以降、Mozilla 1.7.5 以降、Mozilla Fire Fox 1.0 以降などです。
- **JRE 1.5 以降 (Java 5.0 以上)** – Java Runtime Environment 1.5 のダウンロードについては、`http://java.com` を参照してください。

ネットワーク通信ポートとプロトコル

Sun ILOM リモートコンソールは次のネットワークポートとプロトコルを使用して、リモートホストサーバーの SP と通信します。

表 12-1　SP ILOM リモートコンソールのネットワークポートとプロトコル

ポート	プロトコル	SP の ILOM リモートコンソール
5120	TCP	CD
5123	TCP	フロッピーディスク
5121	TCP	キーボードおよびマウス
7578	TCP	ビデオ

注 – CMM ILOM を使用してサーバーを遠隔で管理する場合は、すべての SP リモートコンソールポート (5120、5121、5123、および 7578) へのアクセスを設定する必要があります。

管理者役割のユーザーアカウント – サインイン認証の要求

ILOM Web インタフェースから Sun ILOM リモートコンソールを起動するには、最初に管理者役割のアカウント (管理者の役割ベースのユーザー名とパスワード) で ILOM にログインする必要があります。

- オペレータ役割のアカウントで ILOM にサインインし、Sun ILOM リモートコンソールを起動しようとすると、ILOM によって、ログインダイアログを使用して、有効な管理者役割のアカウントでサインインするように求めるプロンプトが表示されます。
- 最初に管理者役割のアカウントで ILOM にサインインし、Sun ILOM リモートコンソールを起動すると、Sun ILOM リモートコンソールのリダイレクトページが自動的に表示されます。ただし、Sun ILOM リモートコンソールでは、リダイレクトを停止および開始、つまりリダイレクトを再起動するたびにサインインを求めるプロンプトが表示されます。

注 – ILOM でシングルサインオン機能が無効になっている場合は、管理者の役割権限を持つユーザーに対して、ログインダイアログを使用してふたたび ILOM にサインインするように求めるプロンプトが表示されます。シングルサインオン機能の追加情報については、69 ページの「シングルサインオン」を参照してください。

遠隔管理用の ILOM の起動および構成

Sun ILOM リモートコンソールを起動する前に、ILOM Web インタフェースを起動して、遠隔管理用に ILOM を構成する必要があります。

- **ILOM Web インタフェースへの接続** – 遠隔で管理するサーバーの ILOM Web インタフェース (SP または CMM) に接続する必要があります。詳細は、217 ページの「ILOM Web インタフェースに接続する」を参照してください。
- **ILOM リモートコントロール設定の構成** – Sun ILOM リモートコンソールを使用して Sun x64 サーバーを遠隔で管理する前に、起動時の PC-Check 診断テストのほか、コンソールのリダイレト、サポートされるマウスモード、遠隔ホストの電源状態などの遠隔管理に関する ILOM 設定を最初に構成する必要があります。詳細は、219 ページの「Web インタフェースを使用して ILOM リモートコントロール設定を構成する」を参照してください。

注 – 通常、ILOM でのリモート管理コントロールの設定は一度行われます。ただし、遠隔ホストの電源状態は除きます。

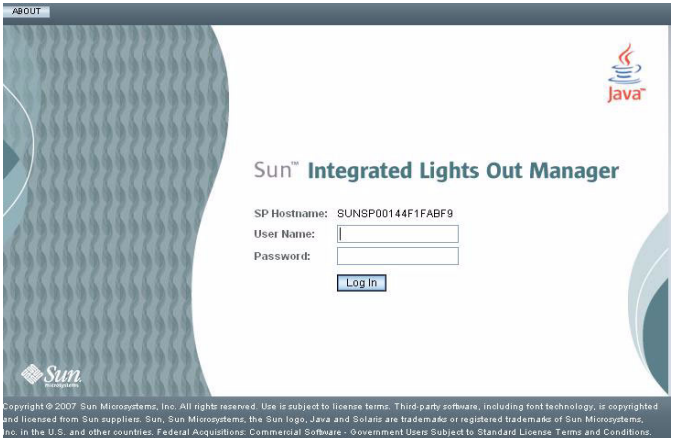
▼ ILOM Web インタフェースに接続する

次の手順に従って、ILOM Web インタフェースに接続します。

1. **Web ブラウザを開いて、遠隔で管理する x64 サーバー SP または x64 CMM の IP アドレスを指定してから、Enter を押します。**

   ILOM のログインページが表示されます。

図 12-3　　ILOM のログインページ



2. ILOM のログインページで、有効な管理者役割のアカウントのユーザー名とパスワードを入力してから、Enter を押します。

参考 – 出荷時の ILOM に事前構成されている管理者役割のアカウントは `root/changeme` です。この事前構成されたアカウントに関する追加情報は、66 ページの「事前構成された ILOM 管理者アカウント」を参照してください。

▼ Web インタフェースを使用して ILOM リモートコントロール設定を構成する

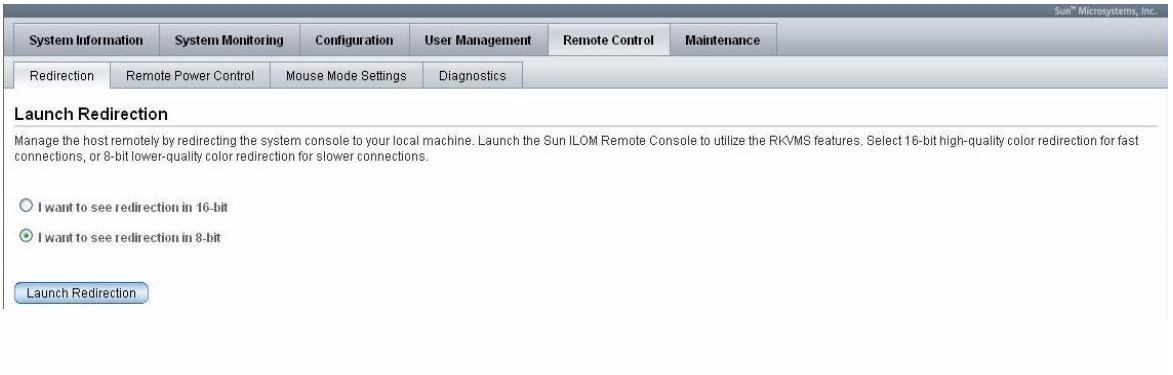
準備すべき事柄:

- 遠隔ホストサーバーの ILOM Web インタフェース (SP または CMM) への接続の確立。詳細は、217 ページの「ILOM Web インタフェースに接続する」を参照してください。

次の手順に従って、遠隔管理に関する ILOM の設定を構成します。

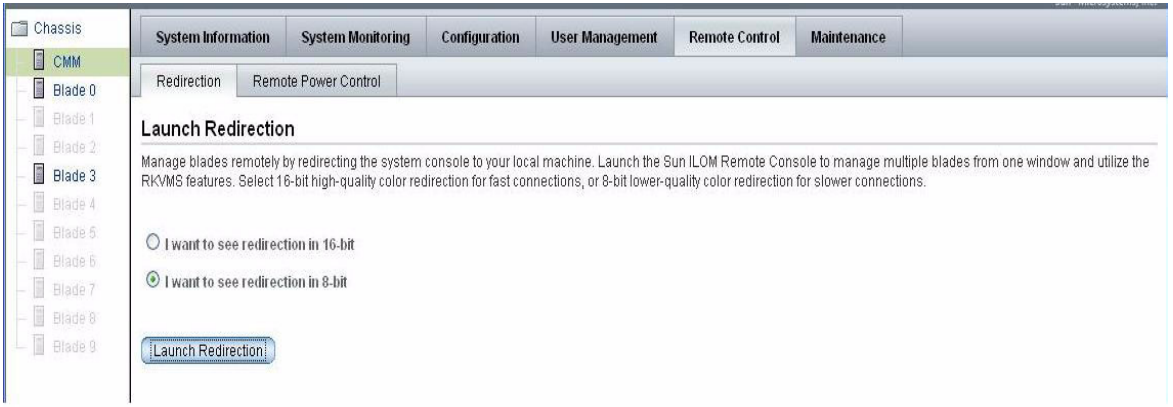
1. CMM または SP の ILOM Web インタフェースで、「Remote Control (リモートコントロール)」タブをクリックします。
   - **SP の ILOM Web インタフェースの場合。**「Redirection (リダイレクト)」、「Remote Power Control (リモート電源制御)」、「Mouse Mode Settings (マウスモード設定)」、および「Diagnostics」の 4 つのサブタブがある「Remote Control (リモートコントロール)」ページが表示されます。

図 12-4 SP の ILOM ー 「Remote Control (リモートコントロール)」タブ



   - **CMM の ILOM Web インタフェースの場合。**「Redirection (リダイレクト)」、「Remote Power Control (リモート電源制御)」の 2 つのサブタブがある「Remote Control (リモートコントロール)」ページが表示されます。

図 12-5　CMM の ILOM － 「Remote Control (リモートコントロール)」タブ



注 – もう 1 つの方法として、CMM と関連付けられた各サーバーの SP にリモートコントロール設定を構成することもできます。CMM の ILOM Web インタフェースに表示されるその他のサーバーの SP のリモートコントロール設定にアクセスするには、このページの左フレームでサーバーの SP をクリックしてから、右フレームで「Remote Control (リモートコントロール)」タブをクリックします。

---

2. **「Remote Control (リモートコントロール)」ページで、次のリモートコントロール設定を行います。**

Console Redirection Settings	「Redirection (リダイレクト)」タブをクリックし、次のコンソールカラーリダイレクションオプションのいずれかを選択します。 • 8-bit － 低速ネットワーク接続に 8 ビットのリダイレクションを選択します。 • 16-bit － 高速ネットワーク接続に 16 ビットのリダイレクションを選択します。
Mouse Mode Settings (マウスモード設定) (SP 設定のみ)	「Mouse Mode Settings (マウスモード設定)」タブをクリックし、次のマウスモード設定のいずれかを選択します。 • Absolute (絶対) － Solaris または Windows オペレーティングシステムを使用している場合に最大パフォーマンスを引き出すには、「Absolute (絶対)」マウスモードを選択します。「Absolute (絶対)」がデフォルトです。 • Relative (相対) － Linux オペレーティングシステムを使用している場合は「Relative (相対)」マウスモードを選択します。すべての Linux オペレーティングシステムで「Absolute (絶対)」モードがサポートされているわけではありません。

Power State Settings	「Remote Power Control (リモート電源制御)」タブをクリックし、次のホストサーバー電源状態のいずれかを選択します。 • **Immediate Power Off (ただちに電源オフ)** − 遠隔ホストサーバーの電源をただちに切断するには、「Immediate Power Off (ただちに電源オフ)」を選択します。 • **Graceful Shutdown and Power Off (適切な順序でシャットダウンして電源オフ)** − 遠隔ホストサーバーの電源を切断する前に OS を正常な停止を試みる場合は、「Graceful Shutdown and Power Off (適切な順序でシャットダウンして電源オフ)」を選択します。 • **Power On (電源オン)** − 遠隔ホストサーバーの電源を完全に投入するには、「Power On (電源オン)」を選択します。「Power On (電源オン)」がデフォルトです。 • **Power Cycle (パワーサイクル)** − 遠隔ホストサーバーの電源をただちに切断し、そのあとで遠隔ホストサーバーの電源を完全に投入するには、「Power Cycle (パワーサイクル)」を選択します。 • **Reset (リセット)** − 遠隔ホストサーバーをただちに再起動するには、「Reset (リセット)」を選択します。
PC-Check Diagnostic Settings (SP 設定のみ) **注**: PC-Check 設定は Sun Blade 8000 シリーズのシステムでのみサポートされています。	「Diagnostics」タブをクリックすると、次の PC-Check 診断設定を有効または無効にできます。 • **Disabled (無効)** − 遠隔ホストサーバーの起動時に、PC-Check 診断テストを実行しない場合は、「Disabled (無効)」を選択します。 • **Enabled (有効)** − 遠隔ホストサーバーの起動時に、基本的な PC-Check 診断テストを実行する場合は、「Enabled (有効)」を選択します。これらの基本診断テストの実行には、通常、3 分ほどかかります。 • **Extended** − 遠隔ホストサーバーの起動時に、拡張 PC-Check 診断テストを実行する場合は、「Extended」を選択します。これらの拡張診断テストの実行には、通常、30 分ほどかかります。

遠隔 x64 サーバー管理用の Sun ILOM リモートコンソールの起動および構成

x64 サーバーを遠隔で管理するには、Sun ILOM リモートコンソールを起動し、遠隔管理のために必要に応じてコンソール機能を構成する必要があります。詳細は、次の手順を参照してください。

▼ ILOM Web インタフェースを使用して Sun ILOM リモートコンソールを起動する

準備すべき事柄:

- ILOM Web インタフェース (SP または CMM) への接続の確立。詳細は、217 ページの「ILOM Web インタフェースに接続する」を参照してください。
- ILOM リモートコントロール設定の構成。詳細は、219 ページの「Web インタフェースを使用して ILOM リモートコントロール設定を構成する」を参照してください。

ILOM Web インタフェースを使用して Sun ILOM リモートコンソールを起動するには、次の手順に従います。

1. **サーバー SP または CMM SP のいずれかの ILOM Web インタフェースで、「Remote Control (リモートコントロール)」タブをクリックします。**

   「Remote Console (リモートコンソール)」ページが表示されます。

2. **「Remote Console (リモートコンソール)」ページで、「Redirection (リダイレクト)」タブをクリックします。**

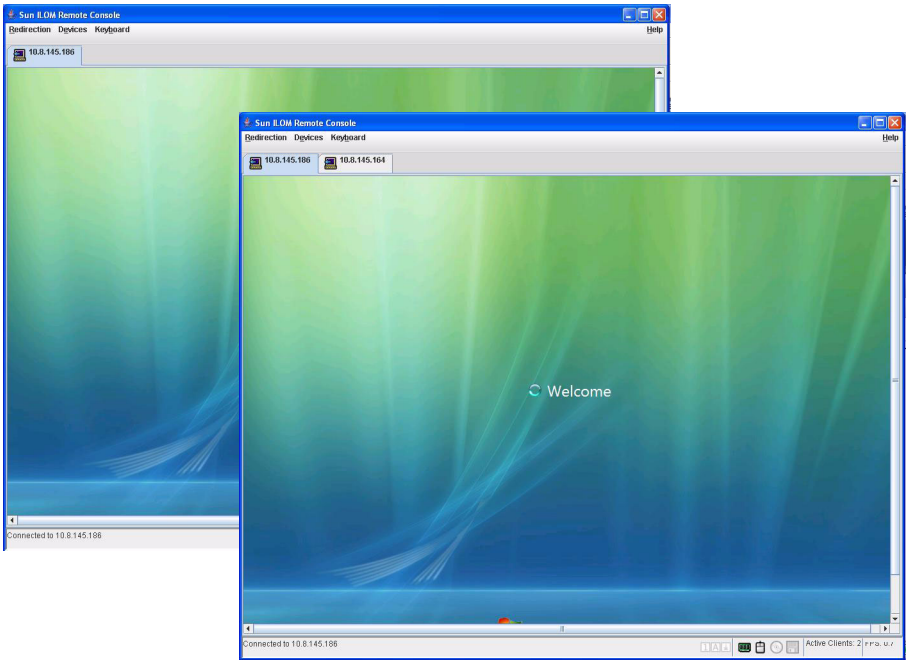
   「Redirection (リダイレクト)」ページが表示されます。

3. 「Redirection (リダイレクト)」ページで、「Launch Redirection (リダイレクトの起動)」をクリックします。

サイトの名前が証明書の名前と一致していないことを示す、証明書に関する警告メッセージが表示される場合があります。このメッセージが表示された場合は、「Run」をクリックして続行します。

「Sun ILOM Remote Console」ウィンドウが表示されます。x64 サーバー SP に接続している場合、サーバーセッションのタブが 1 つ表示されます。x64 CMM に接続している場合、サーバーセッションのタブが複数表示される場合があります (シャーシ内のサーバーごとに 1 つのタブ)。

図 12-6 Sun ILOM リモートコンソール



注 – 該当する場合は、もう 1 つの方法として、CMM ILOM Web インタフェースに表示されているサーバーの SP ごとに Sun ILOM リモートコンソールを起動することもできます。CMM に関連付けられたサーバーの Sun ILOM リモートコンソールを起動するには、ページの左フレームでサーバー SP をクリックしてから、「Remote Console (リモートコンソール)」-->「Redirection (リダイレクト)」-->「Launch Redirection (リダイレクトの起動)」をクリックします。

▼ 新規サーバーセッションを追加する

準備すべき事柄:

- Sun ILOM リモートコンソールへの接続の確立。詳細は、222 ページの「ILOM Web インタフェースを使用して Sun ILOM リモートコンソールを起動する」を参照してください。

次の手順に従って、ILOM リモートコンソールへの新規サーバーセッションを追加します。

1. **「Sun ILOM Remote Console」ウィンドウで、「Redirection (リダイレクト)」--> 「New Session」を選択します。**

   「New Session Creation」ダイアログが表示されます。

2. **「New Session Creation」ダイアログで、遠隔ホスト x64 サーバー SP の IP アドレスを入力してから、「OK」をクリックします。**

   ログインダイアログが表示されます。

3. **ログインダイアログで、管理者アカウントのユーザー名とパスワードを入力します。**

   新しく追加した遠隔ホストサーバーのセッションタブが、Sun ILOM リモートコンソールのタブセットに表示されます。

▼ デバイスのリダイレクトを開始、停止、またはリスタートする

準備すべき事柄:

- Sun ILOM リモートコンソールへの接続の確立。詳細は、222 ページの「ILOM Web インタフェースを使用して Sun ILOM リモートコンソールを起動する」を参照してください。

次の手順に従って、デバイスのリダイレクトを開始、停止、またはリスタートします。

1. **「Sun ILOM Remote Console」ウィンドウで、「Redirection (リダイレクト)」メニューをクリックします。**

2. **「Redirection (リダイレクト)」メニューで、必要に応じて、次のリダイレクトオプションを指定します。**

Start Redirection (リダイレクトの開始)	「Start Redirection (リダイレクトの開始)」を選択すると、デバイスのリダイレクトが有効になります。「Start Redirection (リダイレクトの開始)」はデフォルトで有効になっています。
Restart Redirection (リダイレクトのリスタート)	「Restart Redirection (リダイレクトのリスタート)」を選択すると、デバイスのリダイレクトを停止して開始します。通常、このオプションは有効なリダイレクトがまだ確立されている場合に使用します。
Stop Redirection (リダイレクトの停止)	「Stop Redirection (リダイレクトの停止)」を選択すると、デバイスのリダイレクトが無効になります。

リダイレクト設定を変更することを確かめる確認メッセージが表示されます。

3. 確認メッセージで、「Yes (はい)」をクリックして続行するか、「No (いいえ)」をクリックして操作を取り消します。

▼ キーボードとマウスデバイスをリダイレクトする

準備すべき事柄:

- Sun ILOM リモートコンソールへの接続の確立。詳細は、222 ページの「ILOM Web インタフェースを使用して Sun ILOM リモートコンソールを起動する」を参照してください。

次の手順に従って、ローカルクライアントに遠隔ホストサーバーのキーボードとマウスをリダイレクトします。

1. 「Sun ILOM Remote Console」ウィンドウで、次の処理を実行します。

   a. 「Devices (デバイス)」-->「Mouse (マウス)」を選択して、マウスのリダイレクトを有効または無効にします。

      「Enable (有効)」(チェックマーク) がデフォルトです。

   b. 「Devices (デバイス)」-->「Keyboard (キーボード)」を選択して、キーボードのリダイレクトを有効または無効にします。

      「Enable (有効)」(チェックマーク) がデフォルトです。

▼ キーボードモードとキー送信オプションを制御する

準備すべき事柄:

- Sun ILOM リモートコンソールへの接続の確立。詳細は、222 ページの「ILOM Web インタフェースを使用して Sun ILOM リモートコンソールを起動する」を参照してください。

次の手順に従って、キーボードモードと個々のキー送信オプションを制御します。

1. 「Sun ILOM Remote Console」ウィンドウで、「Keyboard (キーボード)」メニューをクリックします。
2. 「Keyboard (キーボード)」メニューで、必要に応じて、次のキーボード設定を指定します。

Auto-keybreak Mode	「Auto-keybreak Mode」を選択すると、キーを押すたびにキーブレークが自動的に送信されます。このオプションを使用すると、低速ネットワーク接続でキーボードに関する問題を解決する場合に役立ちます。 「Auto-keybreak Mode」はデフォルトで有効になっています。
Stateful Key Locking	クライアントがステートフルキーロック (XSun を実行する Solaris、OSX) を使用している場合は、「Stateful Key Locking」を選択します。 「Stateful Key Locking」は、Caps Lock、Num Lock、および Scroll Lock の 3 つのロックキーに適用されます。
Left Alt Key (左 Alt キー)	左側の Alt キーのオンとオフを切り替えるには、「Left Alt Key (左 Alt キー)」を選択します。
Right Alt Key (右 Alt キー)	英語以外のキーボードで右側の Alt キーのオンとオフを切り替えるには、「Right Alt Key (右 Alt キー)」を選択します。 このオプションが有効になっている場合は、キーの 3 番めのキー文字を入力できます。このキーボードオプションでは、Alt Graph キーと同じ機能を利用できます。
F10	F10 ファンクションキーを適用するには、「F10」を選択します (通常は BIOS で使用)。
Control Alt Delete	Control-Alt-Delete シーケンスを送信するには、「Control Alt Delete」を選択します。
Control Space	Control-Space シーケンスを送信し、遠隔ホストでの入力を有効にするには、「Control Space」を選択します。
Caps Lock	Caps Lock キーを送信し、ロシア語やギリシャ語のキーボードでの入力を有効にするには、「Caps Lock」を選択します。

▼ ストレージデバイスをリダイレクトする

準備すべき事柄:

- Sun ILOM リモートコンソールへの接続の確立。詳細は、222 ページの「ILOM Web インタフェースを使用して Sun ILOM リモートコンソールを起動する」を参照してください。
- Solaris クライアントシステムの場合、ストレージデバイスをリダイレクトする前に、次の手順を実行する必要があります。
  - ボリュームマネージャーが有効な場合は、この機能を無効にする必要があります。
  - 次のコマンドを入力して、Sun ILOM リモートコンソールを実行しているプロセッサに root 権限を割り当てます。

```
su to root

ppriv -s +file_dac_read pid_javarconsole
```

- 詳細は、229 ページの「CD とフロッピーディスクのリダイレクト処理のシナリオ」を参照してください。

次の手順に従って、ストレージデバイスまたは ISO イメージをリダイレクトします。

1. 「Sun ILOM Remote Console」ウィンドウで、「Devices (デバイス)」メニューを選択します。
2. 「Devices (デバイス)」メニューで、次の処理を実行します。

   a. 適切なストレージデバイスまたはイメージの設定を有効にします。

CD-ROM	ローカル CD デバイスを有効にするには、「CD-ROM」を選択します。このオプションを選択すると、CD デバイスが遠隔ホストサーバーに直接接続されているかのように、ローカル CD-ROM ドライブが動作します。
Floppy (フロッピー)	ローカルフロッピーデバイスを有効にするには、「Floppy (フロッピー)」を選択します。このオプションを選択すると、フロッピーデバイスが遠隔ホストサーバーに直接接続されているかのように、ローカルフロッピードライブが動作します。
CD-ROM Image (CD-ROM イメージ)	ローカルクライアントまたはネットワーク共有上の CD-ROM イメージの場所を指定するには、「CD-ROM Image (CD-ROM イメージ)」を選択します。
Floppy Image (フロッピーディスクイメージ)	ローカルクライアントまたはネットワーク共有上のフロッピーイメージの場所を指定するには、「Floppy Image (フロッピーディスクイメージ)」を選択します。

参考 – CD/DVD のリダイレクトには、2 つの選択肢しかありません。CD-ROM ドライブへのリダイレクト、または CD-ROM イメージへのリダイレクトのいずれかを選択できます。

参考 – 配布 CD/DVD からソフトウェアをインストールする場合は、リダイレクトされたドライブに CD/DVD を挿入し、CD-ROM ドライブを選択します。

参考 – ISO イメージからソフトウェアをインストールする場合は、ISO イメージをローカルクライアントまたはネットワーク共有ファイルシステムに配置してから、CD-ROM イメージを選択します。

ストレージドライブの場所またはイメージファイルの場所の指定を求めるダイアログが表示されます。

b. **ストレージドライブの場所またはイメージファイルの場所を指定するには、次のいずれかを実行します。**

- 「Drive Selection」ダイアログで、ドライブの場所を選択または入力し、「OK」をクリックします。

  または

- 「File Open」ダイアログで、イメージの場所を参照し、「OK」をクリックします。

3. **あとでホスト上のこれらのストレージ設定を再利用するには、「Devices (デバイス)」-->「Save as Host Default」をクリックします。**

▼ Sun ILOM リモートコンソールを終了する

次の手順に従って、Sun ILOM リモートコンソールを終了し、開かれたままになっている可能性のある遠隔サーバーセッションをすべて閉じます。

1. **「Sun ILOM Remote Console」ウィンドウで、「Redirection (リダイレクト)」メニューを選択します。**
2. **「Redirection (リダイレクト)」メニューで、「Quit (終了)」を選択します。**

CD とフロッピーディスクのリダイレクト処理のシナリオ

表 12-2 の情報を使用すると、リモートコンソールセッション中に CD ドライブまたはフロッピーディスクドライブのリダイレクト機能が動作する可能性のある、さまざまな事例シナリオの識別に役立ちます。

表 12-2 DVD ドライブとフロッピーディスクドライブを使用したリモートコンソールの操作

事例	状態	遠隔ホストから見た DVD	遠隔ホストから見たフロッピーディスク
1	リモートコンソールアプリケーションが起動していない、またはリモートコンソールは起動しているが DVD またはフロッピーディスクのリダイレクトが起動していない	DVD デバイスあり。ホストが問い合わせるたびに、メディアがないことを示すインジケーションが ILOM からホストに送信されます。	フロッピーディスクデバイスあり。ホストが問い合わせるたびに、メディアがないことを示すインジケーションが ILOM からホストに送信されます。
2	リモートコンソールアプリケーションが、ドライブにメディアがない状態で起動している	DVD デバイスあり。ホストが自動的に、またはホストのデバイスにアクセスする際に問い合わせるたびに、遠隔クライアントは状態メッセージ状態メッセージを送付します。この場合には、メディアがないため、状態はメディアなしになります。	フロッピーディスクデバイスあり。ホストが問い合わせると (たとえば、ドライブをダブルクリックした場合)、遠隔クライアントは状態メッセージを送付します。この場合には、メディアがないため、状態はメディアなしになります。
3	リモートコンソールアプリケーションがメディアなしで起動し、そのあとにメディアを挿入する	DVD デバイスあり。ホストが (自動または手動で) 問い合わせると、遠隔クライアントはメディアありの状態メッセージを送信し、さらにメディア変更を知らせます。	フロッピーディスクデバイスあり。ホストが (手動で) 問い合わせると、遠隔クライアントはメディアありの状態メッセージを送信し、さらにメディア変更を知らせます。
4	リモートコンソールアプリケーションが、メディアが挿入された状態で起動している	事例 3 と同じ。	事例 3 と同じ。
5	リモートコンソールアプリケーションが、メディアが挿入された状態で起動し、そのあとにメディアを取り出す	ホストからの次のコマンドは、メディアなしを知らせる状態メッセージを受け取ります。	ホストからの次のコマンドは、メディアなしを知らせる状態メッセージを受け取ります。
6	リモートコンソールアプリケーションが、イメージリダイレクトで起動している	事例 3 と同じ。	事例 3 と同じ。

表 12-2　DVD ドライブとフロッピーディスクドライブを使用したリモートコンソールの操作 (続き)

事例	状態	遠隔ホストから見た DVD	遠隔ホストから見たフロッピーディスク
7	リモートコンソールアプリケーションがイメージで起動したが、リダイレクトが停止している (これは ISO リダイレクトを停止する唯一の方法)	ドライバは、DVD リダイレクトが停止していることを知っているため、次のホストの問い合わせにメディアがないことを示す状態を送信します。	ドライバは、DVD リダイレクトが停止していることを知っているため、次のフロッピーディスクの問い合わせにメディアがないことを示す状態を送信します。
8	ネットワーク障害	このソフトウェアにはキープアライブの機構があります。ソフトウェアが、通信がないためにキープアライブ障害を検出して、クライアントから反応がないものと想定し、ソケットを閉じます。ドライバはメディアなしの状態をホストへ送信します。	このソフトウェアにはキープアライブの機構があります。ソフトウェアは、反応のないクライアントを検出してソケットを閉じると同時に、遠隔接続が消失したことをドライバに知らせます。ドライバはメディアなしの状態をホストへ送信します。
9	クライアントがクラッシュする	事例 8 と同じ。	事例 8 と同じ。

付録 A

ILOM コマンド行インタフェースのリファレンス

この付録には次の節があります。

CLI コマンドのクイックリファレンス

この節では、使用している Sun サーバーをコマンド行インタフェース (CLI) から管理するために使用する一般的な ILOM コマンドについて説明します。

注 – この章の構文例では、/SP/ で始まるターゲットを使用しますが、使用している Sun サーバープラットフォームによっては、/CMM/ で始まるターゲットに置き換わる場合があります。サブターゲットは、すべての Sun サーバープラットフォームで共通です。

表 A-1 コマンド構文と使用法

コンテンツ	字体	説明
ユーザーの入力	**固定幅、太字**	入力するテキスト。表示されているとおりに入力します。
画面上の出力	**固定幅、標準**	コンピュータに表示されるテキスト

表 A-1　コマンド構文と使用法 (続き)

コンテンツ	字体	説明
変数	**斜体**	選択する名前または値で置き換えます。
大括弧 [ ]		大括弧内のテキストは省略可能です。
縦棒 |		縦棒で区切られたテキストは、利用できる値を表します。1 つだけ選択します。

表 A-2　一般的なコマンド

説明	コマンド
すべての有効なターゲットを表示します	**help targets**
CLI からログアウトします	**exit**
ILOM で実行中の ILOM のファームウェアバージョンを表示します	**version**
クロック情報を表示します	**show /SP/clock**
CLI コマンドすべてを表示します	**show /SP/cli/commands**
アクティブな ILOM セッションを表示します	**show /SP/sessions**
コマンドとターゲットについての情報を表示します	**help**
特定のコマンドについての情報を表示します	**help** *create*
ILOM と BIOS ファームウェアを更新します	**load -source** *tftp://newSPimage*
ILOM のイベントログのリストを表示します	**show /SP/logs/event/list**

表 A-3　ユーザーコマンド

説明	コマンド
ローカルユーザーを追加します	**create /SP/users/**_user1_ **password=**_password_ **role=administrator|operator**
ローカルユーザーを削除します	**delete /SP/users/**_user1_
ローカルユーザーのプロパティーを変更します	**set /SP/users/**_user1_ **role=operator**

表 A-3　ユーザーコマンド (続き)

説明	コマンド
すべてのローカルユーザーについての情報を表示します	**show -display [**targets|properties|all**] -level all /SP/users**
LDAP 設定についての情報を表示します	**show /SP/clients/ldap**
LDAP 設定を変更します	**set /SP/clients/ldap binddn=***proxyuser* **bindpw=***proxyuserpassword* **defaultrole=administrator|operator ipaddress=***ipaddress*

表 A-4　ネットワークとシリアルポート設定のコマンド

説明	コマンド
ネットワーク設定情報を表示します	**show /SP/network**
ILOM のネットワークプロパティーを変更します。IP アドレスなどの特定のネットワークプロパティーを変更すると、アクティブセッションが切断されます	**set /SP/network pendingipaddress=***ipaddress* **pendingipdiscovery=dchp|static pendingipgateway=***ipgateway* **pendingipnetmask=***ipnetmask* **commitpending=true**
外部シリアルポートについての情報を表示します	**show /SP/serial/external**
外部シリアルポート設定を変更します	**set /SP/serial/external pendingspeed=***integer* **commitpending=true**
ホストへのシリアル接続についての情報を表示します	**show /SP/serial/host**
ホストシリアルポート設定を変更します。 注: この速度設定は、ホストのオペレーティングシステムのシリアルポート 0、COM1、または /dev/ttyS0 の速度設定と一致させてください	**set /SP/serial/host pendingspeed=***integer* **commitpending=true**

表 A-5　警告管理コマンド

説明	コマンド
警告についての情報を表示します。最大 15 件の警告を構成できます	**show /SP/alertmgmt/rules/1...15**
IPMI PET 警告を構成します	**set /SP/alertmgmt/rules/1...15 type=ipmipet destination=***ipaddress* **level=** down|critical|major|minor
v3 SNMP トラップ警告を構成します	**set /SP/alertmgmt/rules/1...15 type=snmptrap snmp_version=3 comunity_or_username=***username* **destination=***ipaddress* **level=** down|critical|major|minor
メール警告を構成します	**set /SP/alertmgmt/rules/1...15 type=email destination=***email_address* **level=** down|critical|major|minor

表 A-6　システム管理アクセスコマンド

説明	コマンド
HTTP 設定についての情報を表示します	**show /SP/services/http**
HTTPS への自動リダイレクトを有効にするなどの HTTP 設定を変更します	**set /SP/services/http port=***portnumber* **secureredirect enabled|disabled servicestate=**enabled|disabled
HTTPS アクセスについての情報を表示します	**show /SP/services/https**
HTTPS 設定を変更します	**set /SP/services/https port=***portnumber* **servicestate=** enabled|disabled
SSH DSA 鍵の設定を表示します	**show /SP/services/ssh/keys/dsa**
SSH RSA 鍵の設定を表示します	**show /SP/services/ssh/keys/rsa**

表 A-7　SNMP コマンド

説明	コマンド
SNMP 設定についての情報を表示します。デフォルトの SNMP ポート番号は 161 で、v3 が有効です	**show /SP/services/snmp engineid=***snmpengineid* **port=***snmpportnumber* **sets=**enabled|disabled **v1=**enabled|disabled **v2c=**enabled|disabled **v3=**enabled|disabled
SNMP ユーザーを表示します	**show /SP/services/snmp/users**
SNMP ユーザーを追加します	**create /SP/services/snmp/users/***snmpusername* **authenticationpassword=***password* **authenticationprotocol=**MD5|SHA **permissions=**rw|ro **privacypassword=***password* **privacyprotocol=**none|DES
SNMP ユーザーを削除します	**delete /SP/services/snmp/users/***snmpusername*
SNMP public (読み取り専用) コミュニティーについての情報を表示します	**show /SP/services/snmp/communities/public**
このデバイスを SNMP public コミュニティーに追加します	**create /SP/services/snmp/communities/ public/***comm1*
このデバイスを SNMP public コミュニティーから削除します	**delete /SP/services/snmp/communities/ public/***comm1*
SNMP private (読み書き可能) コミュニティーについての情報を表示します	**show /SP/services/snmp/communities/private**
このデバイスを SNMP private コミュニティーに追加します	**create /SP/services/snmp/communities/ private/***comm2*
このデバイスを SNMP private コミュニティーから削除します	**delete /SP/services/snmp/communities/ private/***comm2*

表 A-8　ホストシステムのコマンド

説明	コマンド
ホストシステムまたはシャーシの電源を起動します	**start /SYS** または **start /CH**
ホストシステムまたはシャーシの電源を停止します (正常な停止)	**stop /SYS** または **stop /CH**
ホストシステムまたはシャーシの電源を停止します (強制的に停止)	**stop -f /SYS** または **stop -f /CH**
ホストシステムまたはシャーシをリセットします	**reset /SYS** または **reset /CH**
ホストコンソールに接続するセッションを開始します	**start /SP/console**
ホストコンソールに接続していたセッションを停止します (正常な停止)	**stop /SP/console**
ホストコンソールに接続していたセッションを停止します (強制的に停止)	**stop -force [-f] /SP/console**

表 A-9　クロック設定コマンド

説明	コマンド
ILOM のクロックを設定して、主 NTP サーバーと同期させます	**set /SP/clients/ntp/server/1 address=***ntpIPaddress*
ILOM のクロックを設定して、副 NTP サーバーと同期させます	**set /SP/clients/ntp/server/2 address=** *ntpIPaddress2*

CLI コマンドリファレンス

このセクションには、CLI コマンドに関する参照情報を示します。

cd コマンドの使用

cd コマンドを使用すると、ネームスペースを操作できます。ターゲットの場所に cd を行うと、その場所がほかのすべてのコマンドのデフォルトターゲットになります。ターゲットなしで **-default** オプションを使用すると、最上位のネームスペースに戻ります。cd **-default** では、cd / を入力した場合と同じ結果が得られます。cd とだけ入力すると、ネームスペースの現在の場所が表示されます。help targets と入力すると、ネームスペース全体にあるすべてのターゲットのリストが表示されます。

構文

cd *target*

オプション

[-default] [-h|help]

ターゲットとプロパティー

ネームスペースの任意の場所。

例

emmett というユーザー名を作成するには、/SP/users に **cd** を行い、デフォルトのターゲットとして /SP/users を使用して create コマンドを実行します。

-> **cd /SP/users**

-> **create emmett**

自分の場所を表示するには、**cd** と入力します。

-> **cd /SP/users**

create コマンドの使用

create コマンドを使用すると、ネームスペースのオブジェクトを設定できます。create コマンドで特定のプロパティーを指定しないかぎり、プロパティーは空です。

構文

create [*options***] target [***propertyname=value***]**

オプション

[-h|help]

ターゲット、プロパティー、および値

表 A-10　create コマンドのターゲット、プロパティー、および値

有効なターゲット	プロパティー	値	デフォルト値
/SP/users/*username*	password	<string>	(なし)
	role	administrator|operator	operator
/SP/services/snmp/communities /*communityname*	permissions	ro|rw	ro
/SP/services/snmp/user/ *username*	authenticationprotocol	MD5	MD5
	authenticationpassword	<string>	(空文字列)
	permissions	ro|rw	ro
	privacyprotocol	none|DES	DES
	privacypassword	<string>	(空文字列)

例

-> **create /SP/users/susan role=administrator**

delete コマンドの使用

delete コマンドを使用すると、ネームスペースのオブジェクトを削除できます。delete コマンドを確認するプロンプトが表示されます。-script オプションを使用することで、このプロンプトの表示を省略できます。

構文

delete [*options***] [-script]** *target*

オプション

[-f|force] [-h|help] [-script]

ターゲット

表 A-11　delete コマンドのターゲット

有効なターゲット
/SP/users/*username*
/SP/services/snmp/communities/*communityname*
/SP/services/snmp/user/*username*

例

```
-> delete /SP/users/susan
-> delete /SP/services/snmp/communities/public
```

exit コマンドの使用

exit コマンドを使用すると、CLI のセッションを終了できます。

構文

exit [*options***]**

オプション

[-h|help]

help コマンドの使用

help コマンドを使用すると、コマンドとターゲットについてのヘルプ情報を表示できます。-output terse オプションを使用すると、使用法に関する情報のみが表示されます。-output verbose オプションでは、使用法、説明、およびコマンド使用法の例などの追加情報が表示されます。-output オプションを使用しない場合は、コマンドの使用法と簡単な説明が表示されます。

command targets を指定すると、/SP と /SYS にある固定ターゲットのうち、そのコマンドに有効なターゲットの詳細リストが表示されます。固定ターゲットとは、ユーザーが作成できないターゲットです。

command targets legal を指定すると、著作権情報と製品使用権が表示されます。

構文

help [*options***] command [***targets***]**

オプション

[-h|help] [-output terse|verbose]

コマンド

cd、create、delete、exit、help、load、reset、set、show、start、stop、version

例

-> **help load**

load コマンドは、サーバーからターゲットへのファイルの転送に使用されます。

使用法: **load -source** *URL* **[***target***]**

-source: 場所を指定してファイルを取得します。

```
-> help -output verbose reset
```

reset コマンドはターゲットのリセットに使用されます。

使用法: **reset [-***script***] [***target***]**

このコマンドの利用できるオプションには次のようなものがあります。

-script: yes/no を確認するプロンプトを表示せずに、yes が指定されたものとして動作します。

例:

```
-> reset /SYS
Are you sure you want to reset /SYS (y/n)? y
Performing hard reset on /SYS
-> reset
/SP Are you sure you want to reset /SP (y/n)? n
Command aborted. ->
```

load コマンドの使用

load コマンドを使用すると、Uniform Resource Indicator (URI) で特定されるソースからイメージファイルを転送し、ILOM のファームウェアを更新できます。URI によって、転送に使用するプロトコルと認証を指定できます。TFTP プロトコルのみがサポートされているため、URI の先頭には tftp:// を付けてください。認証が必要であっても指定しない場合は、パスワードの入力を求めるコマンドプロンプトが表示されます。-script オプションを使用すると、yes または no を確認するプロンプトの表示が省略され、yes が指定されたものとしてコマンドが動作します。

注 – このコマンドは、ILOM のファームウェアと BIOS を更新するために使用します。

構文

load -source *URI*

オプション

[-h|help] [-source] [-script]

例

-> **load -source tftp://<*ipaddress*>/newmainimage**

注 – ファームウェアをアップグレードすると、サーバーと ILOM はリセットされます。アップグレード処理の前に、サーバーの正常な停止を行うことをお勧めします。アップグレードの完了には、約 5 分かかります。ILOM は、特別なモードに入って、新しいファームウェアをロードします。ファームウェアのアップグレードが完了して ILOM がリセットされるまで、ほかのタスクは実行できません。

```
 -> load -source tftp://archive/newmainimage
Are you sure you want to load the specified file (y/n)? y
File upload is complete.
Firmware image verification is complete.
Do you want to preserve the configuration (y/n)? n
Updating firmware in flash RAM:
.
Firmware update is complete.
ILOM will not be restarted with the new firmware.
```

reset コマンドの使用

reset コマンドを使用すると、ターゲットの状態をリセットできます。リセット操作を確認するプロンプトが表示されます。**-script** オプションを使用することで、このプロンプトの表示を省略できます。

注 – reset コマンドは、ハードウェアデバイスの電源状態には影響を与えません。

構文

reset [*options***] target**

オプション

[-h|help] [-script]

ターゲット

表 A-12　reset コマンドのターゲット

有効なターゲット
/SP
/SYS

例

```
-> reset /SP
-> reset /SYS
```

set コマンドの使用

set コマンドを使用すると、ターゲットのプロパティーを指定できます。

構文

set [*options***] target [***propertyname***=***value***]**

オプション

[-h help]

ターゲット、プロパティー、および値

表 A-13　set コマンドのターゲット、プロパティー、および値

有効なターゲット	プロパティー	値	デフォルト値
/SP/users/*username*	password role	<string> administrator | operator	(なし) operator
/SP/alertmgmt/rules	testalert	true	(なし)

表 A-13　set コマンドのターゲット、プロパティー、および値 (続き)

有効なターゲット	プロパティー	値	デフォルト値
/SP/alertmgmt/rules/ *rulename* (*rulename* = 1 ～ 15)	community_or_username	<string>	public
	destination	email_address	(なし)
	level	down | critical | major | minor	(なし)
	snmp_version	1 | 2c | 3	3
	type	email | ipmipet | snmptrap	(なし)
/SP/clock	usentpserver	enabled | disabled	disabled
	datetime	day month date time year	<string>
/SP/services/http	port	<integer>	80
	secureredirect	enabled | disabled	enabled
	servicestate	enabled | disabled	disabled
/SP/services/https	port	<integer>	443
	servicestate	enabled | disabled	disabled
/SP/services/snmp	engineid	<hexadecimal>	*IP* アドレス
	port	<integer>	161
	sets	enabled | disabled	disabled
	v1	enabled | disabled	disabled
	v2c	enabled | disabled	disabled
	v3	enabled | disabled	enabled
/SP/services/snmp/communities/private	permission	ro | rw	rw
/SP/services/snmp/communities/public	permission	ro | rw	ro
/SP/services/snmp/user */username*	authenticationprotocol	MD5	MD5
	authenticationpassword	<string>	(空文字列)
	permissions	ro | rw	ro
	privacyprotocol	none | DES	DES
	privacypassword	<string>	(空文字列)
/SP/services/ssh	generate_new_key_action	true	(なし)
	generate_new_key_type	rsa | dsa	(なし)
	restart_sshd_action	true	(なし)
	state	enabled | disabled	enabled
/SP/services/sso	state		
/SP/users/*username*	role	administrator | operator	(なし)
	password	<string>	(なし)

表 A-13　set コマンドのターゲット、プロパティー、および値 (続き)

有効なターゲット	プロパティー	値	デフォルト値
/SP/clients/activedirectory	state	enabled | disabled	disabled
	certfilestatus	<string>	(なし)
	defaultrole	<string>	(なし)
	getcertfile	<string>	(なし)
	ipaddress	<string>	(なし)
	port	<string>	(なし)
	strictcertmode	enabled | disabled	disabled
	timeout	<integer>	(なし)
	name	<string>	(なし)
/SP/clients/activedirectory/admingroups/*n* *n* は 1 ～ 5	name	<string>	(なし)
/SP/clients/activedirectory/opergroups/*n* *n* は 1 ～ 5	name	<string>	(なし)
/SP/clients/activedirectory/userdomains/*n* *n* は 1 ～ 5	domain	<string>	(なし)
/SP/clients/ldap	binddn	<username>	(なし)
	bindpw	<string>	(なし)
	defaultrole	administrator | operator	operator
	ipaddress	<ipaddress> | none	(なし)
	port	<integer>	389
	searchbase	<string>	(なし)
	state	enable | disabled	disabled
/SP/clients/ntp/server/[1|2]	address	<ipaddress>	(なし)
/SP/clients/radius	defaultrole	administrator | operator	operator
	ipaddress	<ipaddress> | none	(なし)
	port	<integer>	1812
	secret	<string> | none	(なし)
	state	enable | disabled	disabled
/SP/clients/smtp	address	<ipaddress>	*IP* アドレス
	port	<integer>	25
	state	enabled | disabled	enabled

表 A-13　set コマンドのターゲット、プロパティー、および値 (続き)

有効なターゲット	プロパティー	値	デフォルト値
SP/clients/syslog	destination_ip1	<ipaddress>	*IP* アドレス
	destination_ip2	<ipaddress>	*IP* アドレス
/SP/network	commitpending	true	(なし)
	ipaddress	<ipaddress>	*IP* アドレス
	ipdiscovery	<ipaddress>	*IP* アドレス
	ipgateway	<ipaddress>	*IP* アドレス
	ipnetmask	<ipaddress>	*IP* アドレス
	pendingipaddress	<ipaddress> | none	(なし)
	pendingdiscovery	dhcp | static	dhcp
	pendingipgateway	<ipaddress> | none	(なし)
	pendingipnetmask	<点で区切られた IP の 10 進数>	255.255.255.255
/SP/serial/external	commitpending	true	(なし)
	flowcontrol	none	none
	pendingspeed	<リストの整数>	9600
	speed	<リストの整数>	9600
/SP/serial/host	commitpending	true	(なし)
	pendingspeed	<リストの整数>	9600
	speed		9600
/SP/	system_identifier	<string>	(なし)
/SP/	hostname	<string>	デフォルトは、MAC アドレスに基づく

例

```
-> set /SP/users/susan role=administrator

-> set /SP/clients/ldap state=enabled binddn=proxyuser bindpw=
ez24get
```

show コマンドの使用

show コマンドを使用すると、ターゲットとプロパティーについての情報を表示できます。

-display オプションは、表示される情報の種類を決定します。-display targets を指定すると、現在のターゲットの下にあるネームスペースのすべてのターゲットが表示されます。-display プロパティーを指定すると、ターゲットのす

べてのプロパティー名と値が表示されます。このオプションでは、特定のプロパティー名を指定することができ、これらの値のみ表示されます。-display all を指定すると、現在のターゲットの下にあるネームスペースのすべてのターゲットと、指定したターゲットのプロパティーが表示されます。-display オプションを指定しない場合、show コマンドは -display all が指定されたものとして動作します。

-level オプションは、show コマンドの深さを制御し、-display オプションのすべてのモードに適用されます。-level 1 を指定すると、オブジェクトが存在するネームスペースのレベルが表示されます。1 より大きい値の場合、ネームスペースのターゲットの現在のレベルおよび <指定した値> のレベルより下にあるレベルの情報を返します。-level all 引数を指定すると、ネームスペースの現在のレベルとそれより下のレベルの情報すべてが表示されます。

-o|output オプションは、コマンド出力の内容と形式を指定します。ILOM では、表形式でターゲットおよびプロパティーを表示する -o table のみをサポートしています。

構文

show [options] [-display targets|properties|all] [-level *value*|**all] target [***propertyname***]**

オプション

[-d|-display] [-l|level] [-o|output]

ターゲットとプロパティー

表 A-14　show コマンドのターゲット

有効なターゲット	プロパティー
/SYS	
/SP	
/SP/alertmgmt/rules/*rulename* (*rulename* = 1 ～ 15)	community	username destination level snmp_version type

表 A-14　show コマンドのターゲット (続き)

有効なターゲット	プロパティー
/SP/clients/activedirectory	state certfilestatus defaultrole getcertfile ipaddress port strictcertmode timeout
/SP/clients/activedirectory/admingroups/*n* *n* は 1 ～ 5	name
/SP/clients/activedirectory/opergroups/n *n* は 1 ～ 5	name
/SP/clients/activedirectory/userdomains/n *n* は 1 ～ 5	domain
/SP/clients/ldap	binddn bindpw defaultrole ipaddress port searchbase state
/SP/clients/ntp/server/[1|2]	ipaddress
/SP/clock	datetime usentpserver
/SP/logs/event	clear

表 A-14　show コマンドのターゲット (続き)

有効なターゲット	プロパティー
/SP/network	ipaddress ipdiscovery ipgateway ipnetmask macaddress pendingipaddress pendingdiscovery pendingipgateway pendingipnetmask
/SP/serial/external	flowcontrol pendingspeed speed
/SP/serial/host	pendingspeed speed
/SP/services/http	port secureredirect servicestate
/SP/services/https	port servicestate
/SP/services/snmp	engineid port sets v1 v2c v3
/SP/services/snmp/communities/private	permissions
/SP/services/snmp/communities/public	permissions
/SP/services/snmp/users/*username*	password role
/SP/services/ssh	state
/SP/services/ssh/keys/dsa	fingerprint length publickey
/SP/services/ssh/keys/rsa	fingerprint length publickey

表 A-14　show コマンドのターゲット (続き)

有効なターゲット	プロパティー
/SP/services/sso	state
/SP/sessions	username starttime date
/SP/sessions/*sessionid*	starttime source type user
/SP/users/*username*	role password

例

```
-> show -display properties /SP/users/susan
/SP/users/susan
Properties:
role = Administrator

-> show /SP/clients -level 2
/SP/clients
                Targets:
                                ldap
                                ntp
                Properties:
                Commands:
                                cd
                                show
/SP/clients/ldap
                Targets:
                Properties:
                                binddn = cn=Manager,dc=sun,dc=com
                                bindpw = secret
                                defaultrole = Operator
                                ipaddress = 129.144.97.180
                                port = 389
                                searchbase = ou=people,dc=sun,dc=com
                                state = disabled
                Commands:
                                cd
                                show
/SP/clients/ntp
                Targets:
                                server
                Properties:
                Commands:
                  cd
                  show
```

start コマンドの使用

start コマンドを使用すると、ターゲットの電源を入れるか、またはホストコンソールとの接続を開始できます。-script オプションを使用すると、yes または no を確認するプロンプトの表示が省略され、yes が指定されたものとしてコマンドが動作します。

構文

start [options] target

オプション

[-h|help] [-script]

ターゲット

表 A-15　start コマンドのターゲット

有効なターゲット	説明
/SYS または **/CH**	システムまたはシャーシを起動 (電源を投入) します。
/SP/console	コンソールストリームへインタラクティブセッションを開始します。

例

-> **start /SP/console**

-> **start /SYS**

stop コマンドの使用

stop コマンドを使用すると、ターゲットを停止するか、またはホストコンソールと別のユーザーの接続を終了することができます。stop コマンドを確認するプロンプトが表示されます。-script オプションを使用することで、このプロンプトの表示を省略できます。

構文

stop [options] [-script] target

オプション

[-f|force] [-h|help]

ターゲット

表 A-16　stop コマンドのターゲット

有効なターゲット	説明
/SYS または **/CH**	正常な停止を実行し、指定したシステムまたはシャーシの電源を切ります。-force オプションを使用すると、正常な停止をスキップして、ただちに電源を強制的に切ります。
/SP/console	ホストコンソールとほかのユーザーの接続を終了します。

例

-> **stop /SP/console**

-> **stop -force /SYS**

version コマンドの使用

version コマンドを使用すると、ILOM のバージョン情報を表示できます。

構文

version

オプション

[-h|help]

例

```
-> version
version SP firmware version: 1.0.0
SP firmware build number: 4415
SP firmware date: Mon Mar 28 10:39:46 EST 2005
SP filesystem version: 0.1.9
```

付録B

用語集

A

ASF プリブートまたは帯域外プラットフォーム管理仕様。これにより、インテリジェント Ethernet コントローラなどのデバイスが、マザーボード上の ASF 準拠センサーの電圧や温度その他について自立的にスキャンし、Remote Management and Control Protocol (RMCP) に Platform Event Trap (PET) 仕様に準じた警告を送ることができるようになります。ASF は、そもそも、クライアントデスクトップの帯域外管理機能のためのものでした。ASF は DMTF によって定義されています。

B

baseboard management controller (BMC) シャーシ環境や設定、サービス機能を管理し、システムのほかの部品からイベントデータを受信するのに使うデバイス。センサーインタフェースからデータを受信し、そのデータを、インタフェースを提供している SDR を使用して解釈します。BMC を使うことにより、システムイベントログ (SEL) へのまた別のインタフェースができます。BMC の典型的な機能には、プロセッサの温度や電源値、冷却ファンの状態の測定があります。BMC は、システムインテグリティを保つために自立的に動作できます。

BIOS (Basic Input/Output System) システム電源投入時にオペレーティングシステムの読み込みおよびハードウェアのテストを制御するシステムソフトウェア。BIOS は読み取り専用メモリー (ROM) に格納されています。

bps データ転送速度の単位。

D

DES データを暗号化および復元する共通アルゴリズム。

DMI コンピュータハードウェアおよびソフトウェアについての技術サポート情報にアクセスするための標準を定めた仕様。DMI は、ハードウェアおよびオペレーティングシステム (OS) から独立で、ワークステーションやサーバー、その他のコンピュータシステムを管理できます。DMI は DMTF によって定義されています。

DMTF 200 以上の団体によるコンソーシアムで、コンピュータシステムをリモート管理する能力を高めることを目的とした標準を記述および推進します。DTMF からの仕様には、DMI、CIM、ASF などがあります。

E

Ethernet ケーブルで直接接続されたシステム間のリアルタイム通信を可能にする構内通信網 (LAN) の業界標準形式。Ethernet では、アクセス方法として CSMA/CD アルゴリズムを使用しており、全ノードがリスンしていて、かつ、いずれのノードもデータ転送を開始できます。複数のノードが同時にデータ転送をしようとする場合には (コリジョン)、転送しようとしているノードが任意の時間待ってからふたたび転送を試みます。

F

Fast Ethernet 最大 100 Mbps でデータを転送する Ethernet 技術。Fast Ethernet は 10 Mbps Ethernet 機器と下位互換性があります。

FTP TCP/IP に基づいた基本的なインターネットプロトコル。これを使うと、ファイル転送に関連するシステムのオペレーティングシステムやアーキテクチャーにこだわることなく、インターネット上のシステム間でファイルの読み取りや保存ができます。

H

HTTPS Secure Sockets Layer (SSL) を使用した HTTP の拡張。TCP/IP ネットワーク上でのセキュア転送を可能にします。

I

ICMP ルーティング、信頼性、フロー制御、データの順序づけなどを提供する、インターネットプロトコル (IP) に対する拡張機能。ICMP は、IP で使用されるエラーおよび制御メッセージを指定します。

Integrated Lights Out Manager (ILOM) シャーシ内またはブレード内でのシステム管理のための、ハードウェアやファームウェア、ソフトウェアの統合ソリューション。

Intelligent Platform Management Interface (IPMI) 多くの異なる物理的相互接続上のサーバーシステムの帯域外管理のために主に設計された、ハードウェアレベルのインタフェース仕様。IPMI 仕様には、センサーに関する幅広い抽象概念が記載されています。これによって、オペレーティングシステム (OS) 上または遠隔システム内で実行されている管理アプリケーションは、システムの環境構成を把握でき、システムの IPMI サブシステムに登録してイベントを受信できるようになります。IPMI は異なるベンダー製の管理ソフトウェアと互換性があります。IPMI の機能には、現場交換可能ユニット (FRU) インベントリのレポート、システム監視、ロギング、システム復旧 (ローカルおよび遠隔システムのリセットと電源の投入/切断も含む)、警告などがあります。

IPMItool IPMI デバイスの管理に使用するユーティリティー。IPMItool では、ローカルシステムまたは遠隔システムのどちらの IPMI 機能も管理できます。機能には、現場交換可能ユニット (FRU) 情報や構内通信網 (LAN) 設定、センサー読み取り、遠隔システム電源制御、の管理などがあります。

J

Java(TM) Web Start アプリケーション Web アプリケーションランチャ。Java Web Start を使うと、Web リンクをクリックすることによってアプリケーションを起動できます。そのアプリケーションが手元のシステムにない場合には、Java Web Start はアプリケーション

をダウンロードし手元のシステム上にキャッシュします。アプリケーションは、いったんキャッシュにダウンロードすれば、デスクトップアイコンまたはブラウザから起動できるようになります。

K

KCS インタフェース レガシーパーソナルコンピュータ (PC) のキーボードコントローラに実装されているインタフェースの形式。データは、ビットごとのハンドシェイクを使って KCS インタフェース全体に転送されます。

L

LDAP ユーザープロファイルや配布一覧、設定データなどの情報の格納、取り出し、配布に使用するディレクトリサービスプロトコル。LDAP は TCP/IP 上で複数のプラットフォームに渡って動作します。

LDAP サーバー LDAP ディレクトリおよびそのディレクトリへのサービス問い合わせを保守するソフトウェアサーバー。Sun Directory Services および Netscape Directory Services は、LDAP サーバーの実装です。

LOM オペレーティングシステムが動作していなくてもサーバーとの帯域外通信を可能にする技術。これによってシステム管理者は、サーバーの電源オン/オフをしたり、システム温度やファン速度などを見たり、リモートロケーションからシステムをリスタートできます。

M

MD5 任意の長いデータ文字を唯一で固定長の短く要約したデータに変換する、セキュアなハッシュ関数。

N

NFS ユーザーに気づかせることなく、各種ハードウェア設定を協調して機能させるプロトコル。

NIS　UNIX システムが使用する、プログラムおよびデータファイルのシステム。コンピュータシステムネットワーク全体のコンピュータやユーザー、ファイルシステム、ネットワークパラメータに関する特定の情報の収集、照合、共有のために使用します。

NTP　TCP/IP ネットワークのインターネット標準。NTP は、UTC を使用して、ネットワークデバイスのクロック時間を NTP サーバーのミリ秒に同期します。

O

OpenBoot(TM) PROM　電源投入時の自己診断テスト (POST) が部品のテストを問題なく終了した後に、初期化されたシステムを制御するソフトウェアレイヤ。OpenBoot PROM は、メモリーにデータ構造を構築してオペレーティングシステムをブートします。

OpenIPMI　Intelligent Platform Management Interface (IPMI) へのアクセスを容易にする、オペレーティングシステムから独立した、イベント駆動型ライブラリ。

P

PEF　サービスプロセッサが、たとえば電源切断やシステムのリセット、警告の誘発などといったイベントメッセージを受信したときに、特定の動作をするように設定する仕組み。

PEM　プライバシーとデータインテグリティを保証するようにデータを暗号化した、インターネット電子メールの標準。

PET　ハードウェアまたはファームウェア (BIOS) イベントによって引き起こされる設定済みアラート。PET は Intelligent Platform Management Interface (IPMI) 仕様の SNMP トラップで、オペレーティングシステムから独立で動作します。

PXE　業界標準クライアント/サーバーインタフェースで、DHCP を使用して TCP/IP ネットワーク上のオペレーティングシステム (OS) をサーバーがブートできるようにします。PXE 仕様には、一次ブートストラッププログラムに基本的なネットワーク機能を提供するように、ネットワークアダプタカードおよび BIOS を協調して動作させる方法が記述されています。これによって、一次ブートストラッププログラムが、OS イメージの TFTP を介した読み込みなど、ネットワーク上で二次ブートストラップを実行できるようになります。したがって、一次ブートストラッププログラムは、PXE 標準に従ってコーディングされている場合、システムのネットワークハードウェアについての情報を必要としない。

R

RMCP システムの電源の投入または切断、あるいは再起動を強制することにより、管理者が遠隔で警告に応答できるようにするネットワークプロトコル。

RSA アルゴリズム RSA Data Security 社が開発した暗号化アルゴリズム。暗号およびデジタル署名の両方に使用できます。

S

SMTP メール送受信に使用する TCP/IP。

SNMP ネットワークアクティビティについてのデータ交換に使用する簡単なプロトコル。SNMP では、管理対象デバイスとネットワーク管理ステーション (NMS) との間でデータがやりとりされます。管理対象デバイスには、ホストやルータ、Web サーバー、またはネットワーク上のその他のサーバーなどの、SNMP が動作しているいずれのデバイスも含まれます。

SSH セキュアでないネットワーク上の遠隔システムで、セキュアで暗号化されたログインおよびコマンドの実行を可能にする、UNIX シェルプログラムおよびネットワークプロトコル。

SSL ネットワーク上のクライアントサーバー通信をプライバシーのために暗号化するプロトコル。SSL は、環境を確立するために鍵交換方式を使い、この方式では、交換されたデータすべては、盗聴や改ざんから保護するために暗号で暗号化されかつハッシュ化されています。SSL は Web サーバーと Web クライアントの間にセキュリティー保護された接続を作り出します。HTTPS では SSL を使用しています。

T

TCB 接続状態についての情報を記録して保守する TCP/IP の一部。

TCP/IP あるホストから別のホストへデータストリームを確実に送ることのできるインターネットプロトコル。TCP/IP は、Solaris や Microsoft Windows、Linux ソフトウェアシステムといった各種のネットワークシステム間でデータを転送します。TCP はデータ配信を保証し、パケットは送信された時のままのシーケンスで配信されます。

Telnet あるホストのユーザーがリモートホストにログインできるようにする仮想端末プログラム。リモートホストにログインしているあるホストの Telnet ユーザーは、そのリモートホストの通常の端末ユーザーのように対話できます。

TFTP システムにファイルを転送する簡単な転送プロトコル。TFTP は UDP を使用しています。

U

UDP インターネットプロトコル (IP) に信頼性と多重化をもたらすコネクションレス転送レイヤプロトコル。UDP によって、アプリケーションプログラムは、IP 経由でほかのコンピュータのほかのアプリケーションプログラムへデータグラムを配信できます。通常、SNMP が UDP 上に実装されます。

W

Web サーバー インターネットまたはイントラネットにアクセスするためのサービスを提供するソフトウェア。Web サーバーは Web サイトを主催し、HTTP/HTTPS およびその他のプロトコルをサポートし、サーバーサイドプログラムを実行します。

X

X ウィンドウシステム 一般的な UNIX ウィンドウシステムで、ワークステーションまたは端末が複数セッションを同時に制御できるようにします。

X.509 証明書 もっとも一般的な証明書標準。X.509 証明書は、公開鍵および関連するアイデンティティ情報を持ち、認証局 (CA) によってデジタル署名されたドキュメントです。

XIR ドメインのプロセッサに「ソフト」リセットを送る信号。XIR はドメインの再起動は行いません。XIR は通常、ハングしたシステムから脱出してコンソールプロンプトにたどり着くために使用されます。そうすることにより、ユーザーはコアダンプファイルを作成して、それをシステムがハングした原因の診断に役立てることができます。

あ

アクセス権 ユーザーまたはグループに許可あるいは拒否される権限のセットで、ファイルまたはディレクトリへの読み込みや書き込み、実行といったアクセスを指定します。アクセス制御のために、パーミッションには、そのディレクトリ情報へのアクセスが許可されているのか拒否されているのか、および、許可あるいは拒否されているアクセスのレベルが記載されています。

アクセス制御リスト (ACL) サーバーにアクセス権限を持つユーザーを制御するソフトウェア承認の仕組み。単独あるいは複数のユーザーまたはグループへアクセスを許可したり拒否したりすることにより、特定のファイルやディレクトリに特化した ACL ルールを定義できます。

アドレス ネットワークにおいて、ネットワーク内のノードを識別する固有のコード。「host1.sun.com」などの名前は、ドメインネームサービス (DNS) によって「168.124.3.4」のような、点で区切られた 4 つで 1 セットのアドレスに翻訳されます。

アドレス解決 インターネットアドレスを、物理メディアアクセス制御 (MAC) アドレスまたはドメインアドレスにマップする手段。

アドレス解決プロトコル (ARP) インターネットプロトコル (IP) アドレスをネットワークハードウェアアドレス (MAC アドレス) と関連づけるために使われるプロトコル。

い

イベント 管理対象オブジェクトの状態の変化。イベント処理サブシステムは通知を出すことができます。ソフトウェアシステムは、この通知に応答する必要がありますが、通知の要求や制御は行ないません。

インターネットプロトコル (IP) インターネットの基本的ネットワークレイヤプロトコル。IP は、あるホストから別のホストに対し、信頼性が低い状態での個々のパケットの送信を可能とします。IP では、パケットが送信されるかどうかや送信にかかる時間、また、複数のパケットが送信されたとおりの順序のまま送信されるかどうかについて、保証していません。IP の上に階層化されたプロトコルにより、接続の信頼性が高まります。

インターネットプロトコル (IP) アドレス TCP/IP において、ネットワーク上の各ホストまたはほかのハードウェアシステムを認識する、固有の 32 ビットの数字。IP アドレスは、「192.168.255.256」のように点で区切られた数字のセットで、イントラネットまたはインターネット上でのコンピュータの実際の位置を指定します。

え

エージェント 通常は特定のローカル管理対象ホストに対応しているソフトウェアプロセスで、管理者要求を実行し、ローカルのシステムおよびアプリケーション情報をリモートユーザーが使用できるようにします。

遠隔システム ユーザーが作業しているシステム以外のシステム。

遠隔手続き呼び出し (RPC) クライアントシステムがリモートサーバーの関数を呼び出せるようにする、ネットワークプログラミングの方法。クライアントがサーバーでプロシージャを開始すると、その結果がクライアントに転送されて戻ります。

お

オブジェクト識別子 (OID) グローバルオブジェクト登録ツリーにおけるオブジェクトの位置を識別する番号。ツリーのノードにはそれぞれ番号が割り当てられ、OID は一連の番号となっています。インターネットでの使用では、OID 番号はたとえば「0.128.45.12」といったように点で区切られています。LDAP において、OID は、オブジェクトクラスおよび属性タイプなどのスキーマ要素を一義的に識別するために使用される。

オペレータ 管理対象ホストシステムへの制限付き権限を持つユーザー。

か

カーネル オペレーティングシステム (OS) の核心で、ハードウェアを管理し、ファイリングおよびリソース割り当てといった、ハードウェアが提供していない基本的サービスを管理します。

拡張パラレルポート (EPP) 標準パラレルポートの 2 倍の速度でシステムがデータを転送できるようにする、ハードウェアおよびソフトウェアの標準。

完全修飾ドメイン名 (FQDN) 「www.sun.com」など、完全で固有なインターネット上のシステム名。FQDN には、ホストサーバー名 (www) や、第 1 レベル (.com) および第 2 レベル (.sun) ドメイン名などがあります。FQDN はシステムのインターネットプロトコル (IP) アドレスにマップすることができます。

管理者 (Administrator) 管理対象ホストシステムへの完全なアクセス (root) 権限を持っている人。

管理情報ベース (MIB) ネットワークのリソースについての情報を分類する、ツリーに似た階層システム。MIB では、マスター SNMP エージェントがアクセス可能な変数を定義しています。MIB によって、サーバーのネットワーク設定や状態、統計データにアクセスできる。SNMP を使うと、こういった情報をネットワーク管理ステーション (NMS) から見ることができます。業界協定により、各ディベロッパーにはツリー構造の一部分が割り当てられ、そこにディベロッパー独自のデバイスに特化した記述を加えることもできます。

き

キーボード、ビデオ、マウス、ストレージ (KVMS) キーボードやビデオ、マウス、ストレージイベントにシステムが応答できるようにする一連のインタフェース。

ギガビット Ethernet 最大 1000 Mbps でデータを転送する Ethernet 技術。

キャッシュ ローカルに格納されている元のデータの複製。通常、命令やもっとも頻繁にアクセスされた情報です。キャッシュされたデータは、要求された時に再度リモートサーバーから読み出す必要がありません。キャッシュによってメモリー転送速度およびプロセッサ速度が上がります。

協定世界時 (UTC) 世界標準時刻。UTC は、以前はグリニッジ標準時 (GMT) と呼ばれていました。UTC は、ネットワーク上のシステムとデバイスを同期させるために NTP サーバーが使用します。

く

クライアント クライアント/サーバーモデルにおいて、ネットワーク上のサーバーリソースにリモートでアクセスする、ネットワーク上のシステムまたはソフトウェア。

グラフィカルユーザーインタフェース (GUI) アプリケーションを使いやすくするために、キーボードおよびマウスに加えてグラフィックスを使用したインタフェース。

クリティカルイベント サービスに深刻な障害を及ぼし早急な対処を必要とするシステムイベント。

け

ゲートウェイ 2 つのネットワークを相互接続し、そのネットワーク間でデータパケットを渡すコンピュータまたはプログラム。ゲートウェイには 2 つ以上のネットワークインタフェースがあります。

警告 エラーイベントの収集および分析によって生成されたメッセージまたはログ。警告が出た場合、ハードウェアまたはソフトウェアの修正を行う必要があることを意味します。

現場交換可能ユニット (FRU) 顧客サイトで交換可能なシステム部品。

こ

コアファイル プログラムが機能不全となり終了した時に Solaris または Linux オペレーティングシステムが生成するファイル。コアファイルには、障害発生時にとらえられたメモリーのスナップショットが入っています。「crash dump file (クラッシュ時ダンプファイル)」とも呼ばれる。

広域通信網 (WAN) ファイル転送サービスを提供する数多くのシステムから構成されるネットワーク。WAN は広い物理範囲に、時には世界中に及びます。

公開鍵暗号 パブリックおよびプライベートなコンポーネントで作成された 2 つの部分からなる鍵 (コード) を使用する暗号方式。メッセージを暗号化するには、受取人の公表された公開鍵を使用します。メッセージを解読するには、受取人は、受取人のみが知っている非公開の秘密鍵を使用します。公開鍵を知っていても、対応する秘密鍵を推測することはユーザーにはできません。

構内通信網 (LAN) 接続するハードウェアおよびソフトウェア経由で通信できる至近距離にあるシステムの集まり。Ethernet が LAN 技術ではもっとも広範に使われます。

顧客交換可能ユニット (CRU) ユーザーが特別なトレーニングやツールなしで交換できるシステム部品。

コマンド行インタフェース (CLI) テキストベースのインタフェースで、ユーザーはこれを使用してコマンドプロンプトから実行命令を入力できます。

コンソール システムメッセージが表示される、端末または画面上の専用ウィンドウ。コンソールウィンドウによって、数々のサーバーソフトウェアコンポーネントの設定や監視、保守、トラブルシューティングができます。

さ

サーバー証明書 Web アプリケーションを認証するために HTTPS で使用する証明書。証明書は、自身で署名したものあるいは認証局 (CA) が発行したものとなります。

サーバーメッセージブロック (SMB) プロトコル ファイルおよびプリンタをネットワーク全体で共有できるようにするネットワークプロトコル。SMB プロトコルによって、クライアントアプリケーションが、ネットワーク内のサーバープログラムのファイルの読み書きおよびサーバープログラムからのサービスの要求ができるようになります。SMB プロトコルを使うと、Windows と UNIX システムの間でファイルシステムをマウントできます。SMB プロトコルは IBM が設計し、その後 Microsoft 社が修正しました。Microsoft 社は、このプロトコルを共通インターネットファイルシステム (CIFS) と改名しました。

サービスプロセッサ (SP) シャーシ環境や設定、サービス機能を管理し、システムのほかの部品からイベントデータを受信するのに使うデバイス。センサーインタフェースからデータを受信し、そのデータを、インタフェースを提供している SDR を使用して解釈します。SP を使用すると、システムイベントログ (SEL) への別のインタフェースが提供されます。SP の典型的な機能には、プロセッサの温度や電源値、冷却ファンの状態の測定があります。SP は、システムインテグリティを保つために自立的に動作できます。

再起動 システムを停止して起動する、オペレーティングシステムレベルの操作。電源が入っていることが前提条件です。

サブネット ルーティングを単純化するために、単一の論理ネットワークを小さな物理ネットワークに分割する動作体系。サブネットはホスト ID のブロックを認識するインターネットプロトコル (IP) アドレスの部分です。

サブネットマスク サブネットアドレッシングのためにインターネットアドレスからビットを選択するのに使うビットマスク。マスクは 32 ビット長で、インターネットアドレスのネットワーク部分およびローカル部分の 1 つまたは複数のビットを選択します。「アドレスマスク」とも呼ばれる。

し

しきい値 センサーが温度や電圧、電流、ファン速度を監視する際にこの範囲内で使用する最大値および最小値。

識別名 (DN) LDAP において、ディレクトリ内のエントリの名前および位置を識別する、固有のテキスト文字列。DN は、ツリーのルートからの完全なパスを持った完全修飾ドメイン名 (FQDN) である場合もあります。

システムイベントログ (SEL) システムイベント用の非揮発性ストレージを供給するログで、サービスプロセッサにより自発的にログ記録されるか、またはイベントメッセージと一緒にホストに直接送付されます。

シャーシ監視モジュール (CMM) 完全なシャーシ管理システムを形成するために、各ブレードのサービスプロセッサ (SP) と連携して動作する、一般に冗長でホットプラグ可能なモジュール。

出力先変更 システムの標準入出力へではなく、ファイルまたはデバイスへの入出力のチャネリング。出力先変更の結果、システムが通常表示する入出力をほかのシステムのディスプレイに送ります。

承認 ユーザーに特定のアクセス権を与えるプロセス。承認は、認証およびアクセス制御に基づいています。

証明書 エンティティーの属性を検証するために、信頼できる認証局 (CA) が割り当てた公開鍵データ。デジタル署名されたドキュメントです。クライアントおよびサーバーの両方が証明書を持つことができます。「公開鍵証明書」とも呼ばれる。

シリアルコンソール サービスプロセッサのシリアルポートに接続された端子または導線。シリアルコンソールは、システムがほかの管理タスクを行うように設定するために使用されます。

す

スーパーユーザー UNIX システムですべての管理機能を実行する権限を持っている特別なユーザー。「ルート (root)」とも呼ばれる。

スキーマ ディレクトリにエントリとして格納できる情報の種類を記述している定義。スキーマと一致しない情報がディレクトリに格納されている場合、ディレクトリにアクセスしようとしているクライアントは正しい結果を表示できないことがあります。

せ

セッションタイムアウト サーバーがユーザーセッションを無効化するまでの一定の時間。

センサーデータレコード (SDR) 機能の動的発見を容易にするために、Intelligent Platform Management Interface (IPMI) には、このレコードセットがあります。レコードセットには、存在するセンサー数、センサーの種類、センサーのイベント、しきい値情報などのソフトウェア情報が含まれます。センサーデータによって、ソフトウェアは、プラットフォームについての予備知識がなくてもセンサーデータの解釈および呈示ができます。

た

帯域外 (OOB) システム管理 オペレーティングシステムのネットワークドライバまたはサーバーが正常に機能していない時に使用可能なサーバー管理機能。

帯域内システム管理 オペレーティングシステムが初期化されていて、かつ、サーバーがきちんと機能している場合のみ使用可能な、サーバー管理機能。

帯域幅 通信リンク上で送信可能な情報量の尺度。通常、あるネットワークが配信可能な秒ごとのビット数として記述されます。

タイムアウト サーバーが、この時間を過ぎたら、ハングしたサービスルーチンを終了しようとする試みを停止するように指定された時間。

ダイレクトメモリーアクセス (DMA) プロセッサの指示なしで直接メモリーにデータ転送すること。

て

ディレクトリサーバー LDAP において、組織内の人員およびリソースに関する情報を論理的な中心位置から格納および提供するサーバー。

デジタル署名 デジタルデータの情報源の証明書。デジタル署名は、公開鍵暗号化プロセスから導き出される番号です。署名が作成された後にデータが改ざんされた場合、その署名は無効となります。このことにより、デジタル署名はデータインテグリティおよびデータ改ざんの発見を保証できます。

デジタル署名アルゴリズム (DSA) DSS が規定する暗号化アルゴリズム。DSA は、デジタル署名の作成に使用する標準アルゴリズムです。

電源投入時の自己診断テスト (POST) システムのスタートアップ時に初期化されていないシステムを受け取り、部品を丹念に調べてテストするプログラム。POST は、有用な部品を首尾一貫した初期化済みシステムとして設定し、そのシステムを OpenBoot PROM に渡します。POST は、テストが成功した部品のみの一覧を OpenBoot PROM に渡します。

電源の再投入 システムの電源をオフにしてからふたたびオンにするプロセス。

と

動的ホスト構成プロトコル (DHCP) DHCP サーバーが、TCP/IP ネットワーク上のシステムにインターネットプロトコル (IP) アドレスを動的に割り当てることができるようにするプロトコル。

ドメイン 名前によって識別する、ホストの系列化。こういったホストは通常、同一インターネットプロトコル (IP) ネットワークアドレスに属します。また、ドメインは、そのドメインを所有している団体または組織を識別する完全修飾ドメイン名 (FQDN) の最後の部分のことを指します。たとえば、「sun.com」は、FQDN の「docs.sun.com」でそのドメインの所有者としてサンマイクロシステムズを識別しています。

ドメインネームサーバー (DNS) ドメインにおいて通常はホスト名を管理するサーバー。DNS サーバーは「www.example.com」などといったホスト名を「030.120.000.168」などのインターネットプロトコル (IP) アドレスに変換します。

ドメインネームシステム (DNS) コンピュータがドメイン名によってネットワークあるいはインターネット上のほかのコンピュータを検索できるようにする、分散型名前解決システム。このシステムでは、「00.120.000.168」などの標準インターネットプロトコル (IP) アドレスを「www.sun.com」などのホスト名と関連付けます。コンピュータは、通常、この情報を DNS サーバーから受け取ります。

ドメイン名 インターネット上のシステムあるいはシステムグループに与えられた固有の名前。グループ内のシステムはすべて、ホスト名に「sun.com」など同一のドメイン名接尾辞が付いています。ドメイン名は右から左へと解釈されます。たとえば、「sun.com」はサンマイクロシステムズのドメイン名であり、かつ、トップレベル「.com」ドメインのサブドメインです。

トラップ 特定の状態が検知された時に SNMP エージェントが自らの主導権で作成するイベント通知。SNMP には形式的に 7 種のトラップが定義されていて、サブタイプを定義できます。

に

認証 通信セッションにおけるユーザー、または、コンピュータシステムにおけるデバイスやほかのエンティティーの属性を、システムリソースへアクセス可能になる前に検証するプロセス。セッション認証は 2 方向に動作します。サーバーは、アクセス制御を判断するためにクライアントの認証を行います。クライアントがサーバーを認証することもできます。クライアントは Secure Sockets Layer (SSL) を使ってサーバーを常に認証します。

認証局 (CA) 公開鍵証明書を発行しその証明書の所有者の身分証明書を提供する、信頼された組織。公開鍵認証局は、証明書に記載されたエンティティーと、そのエンティティーに属しかつその証明書に記載されている公開鍵との関係を示す証明書を発行します。

ね

ネームスペース LDAP ディレクトリのツリー構造における固有の名前のセットで、この名前からオブジェクト名が由来して解釈されます。たとえば、ファイルはファイルネームスペース内で命名され、プリンタはプリンタネームスペース内で命名されます。

ネットワークインタフェースカード (NIC) ワークステーションやサーバーをネットワークデバイスに接続する内部回路基盤またはカード。

ネットワーク管理ステーション (NMS) 1 つまたは複数のネットワーク管理アプリケーションがインストールされた高性能なワークステーション。NMS はネットワークをリモート管理するのに使用されます。

ネットワークマスク ローカルサブネットアドレスをほかの既知のインターネットプロトコル (IP) アドレスから区別するためにソフトウェアが使用する番号。

の

ノード ネットワーク上でアドレス参照可能なポイントまたはデバイス。ノードにより、コンピュータシステムや端末、各種周辺機器をネットワークに接続できます。

は

ハイパーテキスト転送プロトコル (HTTP) リモートホストからハイパーテキストオブジェクトを取り込むインターネットプロトコル。HTTP メッセージは、クライアントからサーバーへの要求およびサーバーからクライアントへの応答から構成されます。HTTP は TCP/IP に基づいています。

バインド LDAP (Lightweight Directory Access Protocol) において、ユーザーが LDAP ディレクトリにアクセスする際に LDAP が必要とする認証プロセスのこと。認証は、LDAP クライアントが LDAP サーバーに接続する際に行われます。

パリティー 受信したデータが送信されたデータと一致するかどうかを検査するのにコンピュータが使用する方式。また、ディスク上のデータと一緒に格納されている情報も指し、これを使用すると、ドライブ障害発生後にコントローラがデータを再構築することができます。

ひ

非揮発性メモリー システム電源がオフになった時にデータが失われないことを保証するメモリーの種類。

ふ

ブートローダ 読み取り専用メモリー (ROM) に格納されているプログラムで、システム電源投入時に自動的に実行され、システム初期化およびハードウェアテストの最初の段階を制御します。その結果、ブートローダは、オペレーティングシステムの読み込みを行うもっと複雑なプログラムへ制御を移管します。

ファームウェア 通常、システムの初期ブート段階およびシステム管理をサポートするのに使用されるソフトウェア。ファームウェアは読み取り専用メモリー (ROM) または PROM に組み込まれています。

ファイアウォール 通常はハードウェアおよびソフトウェア両方のネットワーク設定で、組織内のネットワークコンピュータを外部アクセスから保護します。ファイアウォールは、特定のサービスやホスト間で行き来する接続を監視または禁止できます。

ファイルシステム 情報を物理メディアに整理して格納する、安定した方法。通常、ファイルシステムはオペレーティングシステムごとに異なります。ファイルシステムは、ファイルおよびディレクトリのツリー構造ネットワークであることが多く、最上位にはルートディレクトリが、ルート以下には親および子ディレクトリがあります。

フェイルオーバー バックアップ機能を提供するために、あるシステム、または多くの場合サブシステムから、別のシステムへコンピュータサービスを自動的に移管すること。

物理アドレス メモリーの位置と一致する実際のハードウェアアドレス。仮想アドレスを参照するプログラムは、後に物理アドレスへとマップされます。

プロキシ プロトコル要求に応答して、あるシステムがほかのシステムの代理として動作する仕組み。

プロトコル ネットワーク上のシステムまたはデバイスが情報を交換する方法を記述した規則セット。

ほ

ポート TCP/IP 接続が確立される場所 (ソケット)。Web サーバーは従来からポート 80 を使用し、ファイル転送プロトコル (ftp) はポート 21 を、Telnet はポート 23 を使用します。ポートによって、クライアントプログラムは、ネットワーク上のコンピュータの特定のサーバープログラムを指定できます。サーバープログラムが起動するとはじめに、指定されたポート番号にバインドします。そのサーバーを使用しようとするすべてのクライアントは、指定されたポート番号にバインドするために要求を送る必要があります。

ポート番号 ホストマシンの個々の TCP/IP アプリケーションが指定する番号で、送信データの送付先を定めます。

ボーレート たとえば端末とサーバーの間といったデバイス間で送信される情報の速度。

ホスト インターネットプロトコル (IP) アドレスおよびホスト名を割り当てられた、バックエンドサーバーなどのシステム。ホストは、ネットワーク上のほかの遠隔システムからアクセスされます。

ホスト ID ネットワーク上のホストを識別するのに使用する 32 ビットのインターネットプロトコル (IP) アドレスの一部。

ホスト名 ドメイン内の特定のコンピュータの名前。ホスト名は常に特定のインターネットプロトコル (IP) アドレスへマップします。

ホットスワップ 稼働中のシステムから部品を取り外したり新しい部品を取り付けるだけで、インストールまたは取り外しができる部品のこと。部品が変更されたことをシステムが自動的に認識して設定を行うか、システムの設定をユーザーが対話的に行う必要があるかのどちらかです。ただし、いずれの場合も再起動の必要はありません。ホットスワップ可能な部品はすべてホットプラグ可能ですが、ホットプラグ可能な部品がすべてホットスワップ可能であるとは限りません。

ホットプラグ システム稼働中に取り外しをしても安全な部品のこと。ただし、部品を取り外す前に、システム管理者はシステムに対してホットプラグ操作の準備を行う必要があります。新しい部品を挿入したあとで、システム管理者はそのデバイスを含めてシステムを再構成するよう、システムに指示する必要があります。

ま

マイナーイベント システムイベントのうち、現時点でサービスに障害は発生していないが、さらに深刻になる前に修正を必要とするもの。

マニュアルページ オンライン UNIX ドキュメント。

め

メジャーイベント システムイベントのうち、深刻ではないがサービスに障害を与えるもの。

メディアアクセス制御 (MAC) アドレス 各構内通信網カード (NIC) に製造時にプログラムされる、世界で唯一の 48 ビットハードウェアアドレス番号。

ゆ

ユーザー ID (userid) システムのユーザーを識別する固有の文字列。

ユーザー ID 番号 (UID 番号) UNIX システムにアクセスしているユーザーにそれぞれ割り当てられる番号。システムが、ファイルおよびディレクトリの所有者を番号によって識別するのに UID 番号を使用します。

ユーザーアカウント システムに格納されている、不可欠なユーザー情報レコード。システムにアクセスするユーザーはそれぞれユーザーアカウントを 1 つ持ちます。

ユーザー名 システムでユーザーを識別する、文字または場合によっては番号の組み合わせ。

ユニバーサルシリアルバス (USB) 450Mbps (USB 2.0) のデータ転送レートをサポートする外部バス標準。USB ポートは、マウスポインタ、キーボード、モデム、プリンタなどのデバイスをコンピュータシステムに接続します。

り

リアルタイムクロック (RTC) システムの電源オフ時にでさえもシステムの時刻と日付を保守する、バッテリーバックアップ式の部品。

リセット システムの電源を切断してから投入する、ハードウェアレベルの操作。

る

ルータ ネットワークパケットまたはその他のインターネットトラフィックを送るパスを割り当てるシステム。ホストおよびゲートウェイの両者はルーティングを行うが、通常は「ルータ」という言葉が 2 つのネットワークを接続するデバイスを指す。

ルート (root) UNIX オペレーティングシステムのスーパーユーザー (root) の名前。root ユーザーは、全ファイルへのアクセス、および、一般ユーザーには許可していないほかの操作を実行することが許可されています。大まかに言うと、Windows Server オペレーティングシステムの管理者 (Administrator) ユーザー名と同等です。

ルートディレクトリ ベースディレクトリで、ほかのすべてのディレクトリは直接あるいは間接的にここから生じます。

ろ

ローカルホスト ソフトウェアアプリケーションが動作しているプロセッサまたはシステム。

索引

L

M

P

R

S

W

い

お

か

せ

て

と

な

ね

は

ふ

ほ

め

ゆ

り