FUJITSU

Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド

C120-E574-01

FUJITSU

Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド

マニュアル番号: C120-E574-01
Part No. 875-4567-10
2009 年 4 月、Revision A

本書には、富士通株式会社により提供および修正された技術情報が含まれています。

原典:	Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide Manual Code: C120-E574-01EN

目次

はじめに

『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』では、ILOM の必須セットアップ手順を実行する方法と、ILOM の機能にアクセスする際に実行する一般的な手順について説明します。

本書は、ネットワーキングの概念および基本的なシステム管理プロトコルについての知識があるシステム管理者を対象にしています。

注 – 本書の説明は、ILOM をサポートするサーバに限定されます。「すべてのサーバプラットフォーム」という説明は、ILOM をサポートしている富士通製のすべてのサーバを指します。使用するサーバによっては、ILOM の一部の機能がサポートされていないことがあります。ILOM の補足マニュアルと各サーバのプロダクトノートを事前に確認してください。

安全な使用のために

このマニュアルには当製品を安全に使用していただくための重要な情報が記載されています。当製品を使用する前に、このマニュアルを熟読してください。また、このマニュアルは大切に保管してください。
富士通は、使用者および周囲の方の身体や財産に被害を及ぼすことなく安全に使っていただくために細心の注意を払っています。本製品を使用する際は、マニュアルの説明に従ってください。

関連マニュアル

本書で説明されている情報を完全に理解するには、本書を次の表に示すマニュアルと一緒に使用することをお勧めします。SPARC Enterprise シリーズのすべてのマニュアルの最新版は、次の Web サイトから入手できます。

グローバルサイト

http://www.fujitsu.com/sparcenterprise/manual/

日本語サイト

http://primeserver.fujitsu.com/sparcenterprise/manual/

まず、『ILOM 3.0 概念ガイド』を読み、ILOM の特徴と機能を理解してください。ILOM がサポートしている新しいシステムをセットアップするには、『ILOM 3.0 入門ガイド』を参照してください。ここには、ネットワークに接続する手順、ILOM への初回ログイン手順、ユーザーアカウントやディレクトリサービスを設定する手順が記載されています。その後、その他の ILOM タスクを実行するために使用する ILOM インタフェースを決定してください。インタフェースが決定したら、選択したインタフェース用の ILOM 3.0 手順ガイドを参照してください。

次の表に、ILOM 3.0 に関する各種マニュアルを示します。

タイトル	説明	コード
Integrated Lights Out Manager (ILOM) 3.0 概念ガイド	ILOM の特徴および機能に関する情報	C120-E573
Integrated Lights Out Manager (ILOM) 3.0 入門ガイド	ネットワーク接続、ILOM への初回ログイン、およびユーザーアカウントやディレクトリサービスの設定に関する情報および手順	C120-E576
Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド	ILOM Web インタフェースを使用して ILOM 機能にアクセスするための情報および手順	C120-E574
Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド	ILOM CLI を使用して ILOM 機能にアクセスするための情報および手順	C120-E575
Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド	SNMP または IPMI 管理ホストを使用して ILOM 機能にアクセスするための情報および手順	C120-E579

ILOM 3.0 の各種マニュアルに加えて、関連する ILOM 補足マニュアルに、使用しているサーバプラットフォームに固有の ILOM 機能およびタスクが記載されています。ILOM 3.0 の各種マニュアルと、使用しているサーバプラットフォームに付属の ILOM 補足マニュアルを一緒に使用してください。

ILOM 3.0 のバージョン番号

ILOM 3.0 では、システムで動作している ILOM のバージョンを識別しやすいように、新しいバージョン番号体系が採用されています。この番号体系では、たとえば、`a.b.c.d.e` のように、5 つのフィールドを持つ文字列が使用されます。

- `a` – ILOM のメジャーバージョンを表します。
- `b` – ILOM のマイナーバージョンを表します。
- `c` – ILOM の更新バージョンを表します。
- `d` – ILOM のマイクロバージョンを表します。マイクロバージョンは、プラットフォームまたはプラットフォームグループごとに管理されます。詳細については、使用しているプラットフォームのプロダクトノートを参照してください。
- `e` – ILOM のナノバージョンを表します。ナノバージョンは、マイクロバージョンの増分イテレーションです。

たとえば、ILOM 3.1.2.1.a は、次のような意味になります。

- ILOM 3 は ILOM のメジャーバージョン
- ILOM 3.1 は ILOM 3 のマイナーバージョン
- ILOM 3.1.2 は ILOM 3.1 の 2 つ目の更新バージョン
- ILOM 3.1.2.1 は ILOM 3.1.2 のマイクロバージョン
- ILOM 3.1.2.1.a は ILOM 3.1.2.1 のナノバージョン

製品識別情報

製品識別情報により、システムは、それ自体を登録し、その識別情報に関連付けられたサービス契約に基づいて特定の自動サービスを使用できるようになります。製品識別情報を使用すると、システムを特定することができます。また、システムに関するサービスを依頼する際には、保守担当者に製品識別情報を提供する必要があります。製品識別情報には、次の情報が含まれます。

- `product_name`: 製品の販売名。
- `product_part_number`: 製品が固有のシリアル番号を持つように製造時に割り当てられるネームスペース。同じ製品パーツ番号が複数の製品に割り当てられることはありません。「602-3098-01」などです。
- `product_serial_number`: 製造時に製品の各インスタンスに割り当てられる固有の識別情報。「0615AM0654A」などです。
- `product_manufacturer`: 製品の製造元。「FUJITSU」などです。

表 P-1 では、ILOM で使用される共通の製品識別情報について説明します。

表 P-1 共通の製品識別情報

必要な情報	ターゲット	最小プロパティー

サーバ (ラック搭載型およびブレード) に関する基本製品情報	`/SYS`	`product_name`
		`product_part_number`
		`product_serial_number`
		`product_manufacturer`

シャーシ監視モジュール (Chassis Monitoring Module、CMM) に関する基本製品情報	`/CH`	`product_name`
		`product_part_number`
		`product_serial_number`
		`product_manufacturer`

ブレードに関する基本シャーシ情報	`/SYS/MIDPLANE`	`product_name`
		`product_part_number`
		`product_serial_number`
		`product_manufacturer`

シャーシ内でのブレードの位置	`/SYS/SLOTID`	`type`
		`class`
		`value`

ラック内でのシャーシの位置	`/CH`	`rack_location`

書体と記号について

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「システム部品の管理」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。

ご意見をお寄せください

本書に関するご意見、ご要望または内容に不明確な部分がございましたら、マニュアル番号、マニュアル名称、ページおよび具体的な内容を下記 URL の『お問い合わせ』から送付してください。

SPARC Enterprise マニュアルのサイト

http://primeserver.fujitsu.com/sparcenterprise/manual/

第1章

Web インタフェースの概要

項目

説明	リンク
ILOM Web インタフェースの特長と機能について学習する	• 2 ページの「Web インタフェースについて」 • 2 ページの「ブラウザおよびソフトウェアの要件」 • 3 ページの「Web インタフェースのコンポーネント」 • 4 ページの「ナビゲーションタブ」

関連項目

ILOM	章または節	ガイド
• 概念	• ILOM の概要	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• CLI の概要	『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
• SNMP および IPMI ホスト	• SNMP の概要 • IPMI の概要	『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

この章では、ILOM Web インタフェースを使用して手順を実行する前に知っておく必要のある基本的な情報を提供します。

Web インタフェースについて

ブラウザを通じて ILOM Web インタフェースにアクセスできます。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、サーバのキーボードおよびマウス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、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。

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。

ILOM は、次の表に示すブラウザをサポートしています。

表 1-1 サポートされている Web ブラウザ

オペレーティングシステム	Web ブラウザ
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アプリケーションがサポートする Web ブラウザおよびオペレーティングシステムのリストについては、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

次の図に、ILOM にログインすると表示される ILOM Web インタフェースのメインページを示します。

図 1-1 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 (Chassis Monitoring Module、CMM) で ILOM Web インタフェースを使用している場合、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。ナビゲーション区画は、ILOM の Web ページの左側に表示されます。

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」**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」**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役割を表示します。
- 「Server」**フィールド** − ILOM SP または CMM のホスト名を表示します。
- 「Refresh」**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」**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 – ILOM Web インタフェースに備わっている「Refresh」および「Log Out」ボタンを使用してください。Web インタフェースの使用中は、Web ブラウザの「Refresh」ボタンまたは「Log Out」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。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

次の表に、Web インタフェースを使用して ILOM のもっとも一般的な機能にアクセスするために使用できる各種タブおよびサブタブを示します。タブを選択すると表示される Web ページで機能を使用する方法の詳細は、このガイドの関連する章を参照してください。

注 – ILOM Web インタフェースのナビゲーションタブは、特定のプラットフォームに実装されている ILOM の機能によって多少異なります。このため、次の表に示すタブとは異なるタブにアクセスできる場合があります。使用しているシステムの ILOM インタフェースに関する情報は、お手持ちの ILOM 補足マニュアルを参照してください。

表 1-2　ILOM 3.0 Web インタフェースのタブ

メインタブ	第 2 および第 3 レベルのタブ	可能な操作
System Information		
	Versions	実行中の ILOM のバージョンを表示します。
	Session Time-Out	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します。
	Components	ILOM が監視しているコンポーネントの名前、種類、および状態を表示します。
	Fault Management	障害状態にあるコンポーネントに関する情報を表示します。
	Identification Information	ホスト名またはシステム識別子を割り当てることにより、サービスプロセッサの識別情報を入力または変更します。
System Monitoring		
	Sensor Readings	センサーの名前、種類、および測定値を表示します。
	Indicators	インジケータと LED の名前および状態を表示します。
	Event Logs	イベント ID、クラス、種類、重要度、日時、イベントの説明など、特定の各イベントに関するさまざまな詳細を表示します。
	Power Management	使用可能な電源管理インタフェースを使用して消費電力を監視し、電力使用を管理します。
Configuration		
	System Management Access --> Web Server	HTTP Web サーバ、HTTP ポートなど、Web サーバの設定を編集または更新します。
	System Management Access --> SSL Certificate	SSL 証明書に関する情報を表示し、任意で、新しい SSL 証明書を検索または入力します。
	System Management Access --> SNMP	SNMP の設定を編集または更新します。
	System Management Access --> SSH Server	Secure Shell (SSH) サーバのアクセスと鍵の生成に関する設定を行います。
	System Management Access --> IPMI	コマンド行インタフェースを使用して、サーバプラットフォームに関する情報を取得するだけでなく、サーバプラットフォームを監視および制御します。
	Alert Management	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したりします。
	Network	ILOM のネットワーク設定を表示および編集します。

表 1-2　ILOM 3.0 Web インタフェースのタブ (続き)

メインタブ	第 2 および第 3 レベルのタブ	可能な操作
	DNS	ホスト名を指定し、そのホスト名を、ドメインネームサービス (Domain Name Service、DNS) を使用して IP アドレスに解決します。
	Serial Port	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します。
	Clock	ILOM クロックの時間を表示および手動で編集したり、ILOM クロックを NTP サーバと同期させたりします。
	Timezone	サービスプロセッサによって表示されるタイムスタンプが、ほかの場所 (Solaris オペレーティングシステムなど) で作成されるログと対応するように、特定のタイムゾーンを指定します。
	Syslog	syslog メッセージの送信先となるサーバのアドレスを設定します。
	SMTP Client	警告の電子メール通知の送信に使用する SMTP クライアントの状態を設定します。
	Policy	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します。
User Management		
	User Accounts	ローカルの ILOM ユーザーアカウントを追加、削除、または変更します。
	Active Sessions	現在 ILOM にログインしているユーザーと、ユーザーが開始したセッションの種類を表示します。
	LDAP	LDAP ユーザーの ILOM へのアクセスを設定します。
	LDAP/SSL	Secure Socket Layer (SSL) テクノロジによって実現される高度なセキュリティー設定を使用して、LDAP ユーザーの ILOM へのアクセスを設定します。
	RADIUS	RADIUS ユーザーの ILOM へのアクセスを設定します。
	Active Directory	Active Directory ユーザーの ILOM へのアクセスを設定します。
Remote Control		
	Redirection	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、ホストをリモート管理します。
	KVMS	キーボード、ビデオ、マウス、またはストレージデバイスのリモート管理状態を有効または無効にします。
	Remote Power Control	電源の状態 (「Immediate Power Off」、「Graceful Shutdown and Power Off」、「Power On」、「Power Cycle」、または「Reset」) を選択します。

表 1-2　ILOM 3.0 Web インタフェースのタブ (続き)

メインタブ	第 2 および第 3 レベルのタブ	可能な操作
	Diagnostics	x64 プロセッサベースのシステムまたは SPARC プロセッサベースのシステムの診断を有効または無効にします。
Maintenance		
	Firmware Upgrade	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します。
	Backup/Restore	サービスプロセッサの設定を安全な方法で遠隔ホストまたは取り外し可能なストレージデバイスにバックアップしたり復元したります。
	Reset SP	サービスプロセッサをリセットします。
	Configuration Management	サービスプロセッサの設定データを管理します。
	Snapshot	環境、ログ、エラー、および FRUID に関するデータを収集して USB メモリや外部ホストに送信したり (CLI を使用)、ダウンロードされたファイルとして保存したりします。

第2章

Web インタフェースを使用するために準備すべき事柄

このガイドに示す手順を実行する前に、次の準備すべき事柄を確認してください。

準備すべき事柄

手順	説明	章または節	関連ガイド
1	ILOM SP (CMM またはサーバ) との初期通信を確立する必要があります。	• ILOM への接続	• 『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』
2	すでに ILOM でユーザーアカウントを作成している必要があります。	• ユーザーアカウントの追加と権限の割り当て (Web インタフェース) • ユーザーアカウントの追加と権限の割り当て (CLI)	• 『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ からダウンロードできます。

第3章

ILOM へのログインと ILOM からのログアウト

項目

説明	リンク
準備すべき事柄を確認する	• 12ページの「初回ログインの前に」
ILOM にはじめてログインする	• 13ページの「root ユーザーアカウントによる ILOM へのログイン」
ユーザーアカウントをセットアップする	• 14ページの「ユーザーアカウントのセットアップ」
一般ユーザーとして ILOM にログインする	• 14ページの「ユーザーとして ILOM へのログイン」
ILOM からログアウトする	• 15ページの「ILOM からのログアウト」

関連項目

ILOM	章または節	ガイド
• はじめに	• ILOM の使用開始プロセス • Web インタフェースを使用した ILOM 初期セットアップ手順	『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』
• CLI	• ILOM へのログインと ILOM からのログアウト	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』

ILOM 3.0 の各種マニュアルは、次の Web サイトで入手できます。
http://primeserver.fujitsu.com/sparcenterprise/manual/

この章は、ILOM のログインおよびログアウト手順のクイックリファレンスとして使用してください。詳細については、『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』で説明している初回ログインの作業と手順を参照してください。

初回ログインの前に

この章の手順を開始する前に、必ず、次の要件が満たされていることを確認してください。

- データセンター環境で使用するサーバでの ILOM のセットアップ方法を計画します。『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』の「ILOM との通信を確立するための初期設定ワークシート」を参照してください。
- ネットワーク接続を使用せずにシリアルポート経由で ILOM に接続するか、ネットワーク経由で ILOM にログインします。シリアル直接接続を使用してログインするには、ワークステーション、端末、または端末エミュレータと、サーバの SER MGT ポート (モジュラーシャーシシステムを使用している場合はシャーシ監視モジュール (Chassis Monitoring Module、CMM) ポート) にシリアルケーブルを接続します。ネットワーク接続を使用してログインする場合は、サーバまたは CMM の NET MGT ポートに Ethernet ケーブルを接続します。詳細は、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ください。
- ネットワーク設定を行います。DHCP 接続または静的ネットワーク接続を使用できます。デフォルトで、ILOM は、DHCP を使用してネットワーク設定を取得しようとします。『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』の「ILOM への接続」を参照してください。

ILOM へのログイン

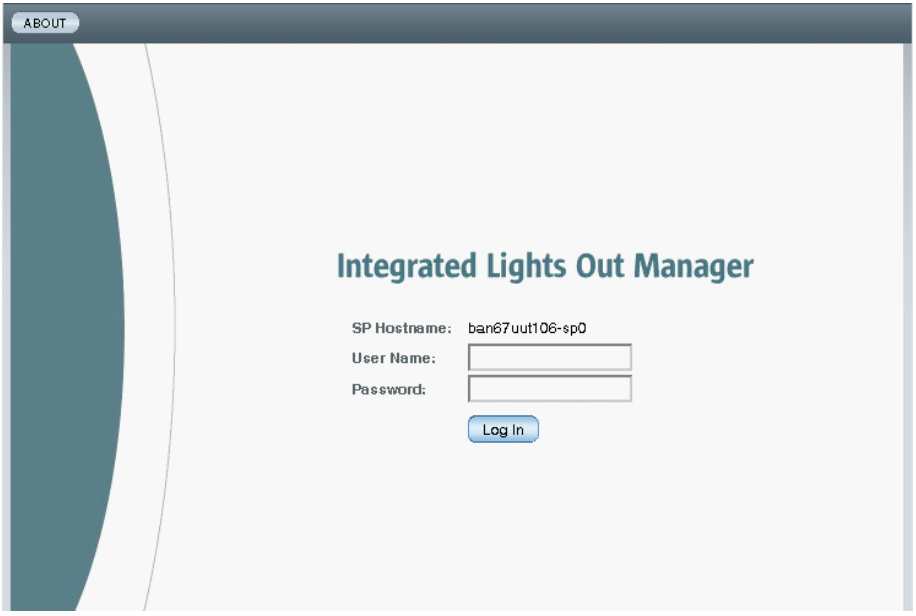
項目

説明	リンク
ILOM にログインしてユーザーアカウントをセットアップする	• 13ページの「root ユーザーアカウントによる ILOM へのログイン」 • 14ページの「ユーザーアカウントのセットアップ」 • 14ページの「ユーザーとして ILOM へのログイン」

▼ root ユーザーアカウントによる ILOM へのログイン

root ユーザーアカウントで ILOM Web インタフェースへの初回のログインを実行するには、Web ブラウザを開いて、次の手順を実行します。

1. **ブラウザに `http://`*system_ipaddress* と入力します。**
   Web インタフェースのログインページが表示されます。



2. **次のように、root ユーザーアカウントのユーザー名とパスワードを入力します。**
   User Name: **root**
   Password: **changeme**
3. **「Log In」をクリックします。**
   Web インタフェースの「Version」ページが表示されます。

▼ ユーザーアカウントのセットアップ

ILOM にログインしたら、一般 (root 以外の) ユーザーアカウントを作成する必要があります。この一般ユーザーアカウントを使用して、使用しているシステムおよび環境の ILOM 設定を行います。

次の手順に従って、ユーザーアカウントをセットアップします。

- **次の 5 つのユーザークラスのいずれかでユーザーアカウントをセットアップします。**
  - ローカルユーザー
  - Active Directory ユーザー
  - LDAP ユーザー
  - LDAP/SSL ユーザー
  - RADIUS ユーザー

  詳細な役割を使用して最大 10 のローカルユーザーアカウントを作成および設定するか、ディレクトリサービスを設定することができます。

  ユーザーアカウントのセットアップに関する情報は、34ページの「ユーザーアカウントの追加と役割の割り当て」を参照してください。

▼ ユーザーとして ILOM へのログイン

ここに示す手順を使用して、ILOM にログインし、ユーザーアカウントまたはディレクトリサービスが正常に機能していることを確認してください。

次の手順に従って、root 以外のユーザーアカウントを使用して ILOM にログインします。

1. **Web ブラウザで、`http://`*system_ipaddress* と入力します。**

   Web インタフェースのログインページが表示されます。

2. **設定したユーザーアカウントのユーザー名とパスワードを入力します。**

3. **「Log In」をクリックします。**

   ILOM の Web インタフェースで、「Version」ページが表示されます。

ILOM からのログアウト

項目	
説明	リンク
ILOM からログアウトする	• 15ページの「ILOM からのログアウト」

▼ ILOM からのログアウト

- **ILOM の Web インタフェースで、「Log Out」ボタンをクリックします。**

  「Log Out」ボタンは Web インタフェースの右上の端にあります。Web ブラウザの「Log Out」ボタンを使用して ILOM を終了しないでください。

次の手順

ユーザーアカウントのセットアップまたはディレクトリサービスの設定が完了したら、ILOM を設定できます。このガイドの残りの章では、ILOM の機能にアクセスするために実行できるタスクについて詳しく説明します。

第4章

ILOM の通信設定

項目

説明	リンク
ネットワークの設定	• 19 ページの「ホスト名およびシステム識別子の割り当て」 • 20 ページの「ネットワーク設定の表示と構成」 • 22 ページの「DNS 設定の表示と構成」 • 23 ページの「シリアルポート設定の表示と構成」 • 24 ページの「HTTP または HTTPS の Web アクセスを有効にする」 • 27 ページの「SSL 証明書をアップロードする」
Secure Shell の設定	• 28 ページの「SSH の有効化または無効化」 • 28 ページの「新しい SSH 鍵の生成」 • 29 ページの「SSH サーバの再起動」

関連項目

ILOM	章または節	ガイド
• 概念	• ILOM のネットワーク設定	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• 概要	• ILOM の使用を開始する	『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』
• CLI	• ILOM の通信設定	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• IPMI と SNMP ホスト	• ILOM の通信設定	『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

ネットワークの設定

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。動的ホスト構成プロトコル (Dynamic Host Configuration Protocol、DHCP) がデフォルト設定です。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。

項目

説明	リンク
準備すべき事柄を確認する	• 18 ページの「作業を開始する前に」
ネットワークの設定	• 19 ページの「ホスト名およびシステム識別子の割り当て」 • 20 ページの「ネットワーク設定の表示と構成」 • 22 ページの「DNS 設定の表示と構成」 • 23 ページの「シリアルポート設定の表示と構成」 • 24 ページの「HTTP または HTTPS の Web アクセスを有効にする」 • 27 ページの「SSL 証明書をアップロードする」

作業を開始する前に

ILOM の通信を設定する前に、常に ILOM に同じ IP アドレスが割り当てられるようにしてください。これは、初期設定のあとに静的 IP アドレスを ILOM に割り当てるか、または DHCP サーバ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。

デフォルトで、ILOM は、DHCP を使用してネットワーク設定を取得しようとします。

▼ ホスト名およびシステム識別子の割り当て

作業を開始する前に

- ホスト名とシステム識別子を割り当てるには、Admin (a) の役割を有効にする必要があります。

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. **ILOM Web インタフェースにログインします。**
2. **「System Information」-->「Identification Information」を選択します。**

   「Identification Information」ページが表示されます。
3. **「SP host name」フィールドで、SP ホスト名を入力します。**

   ホスト名は最大 60 文字まで入力できます。
4. **「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。
5. **「SP System Contact」フィールドで、連絡先の担当者の名前を入力します。**

   システムの連絡先には、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. **「SP System Location」フィールドで、システムの物理的な位置を記述するテキストを入力します。**

   システムの位置には、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。
7. **「Save」をクリックして設定を有効にします。**

▼ ネットワーク設定の表示と構成

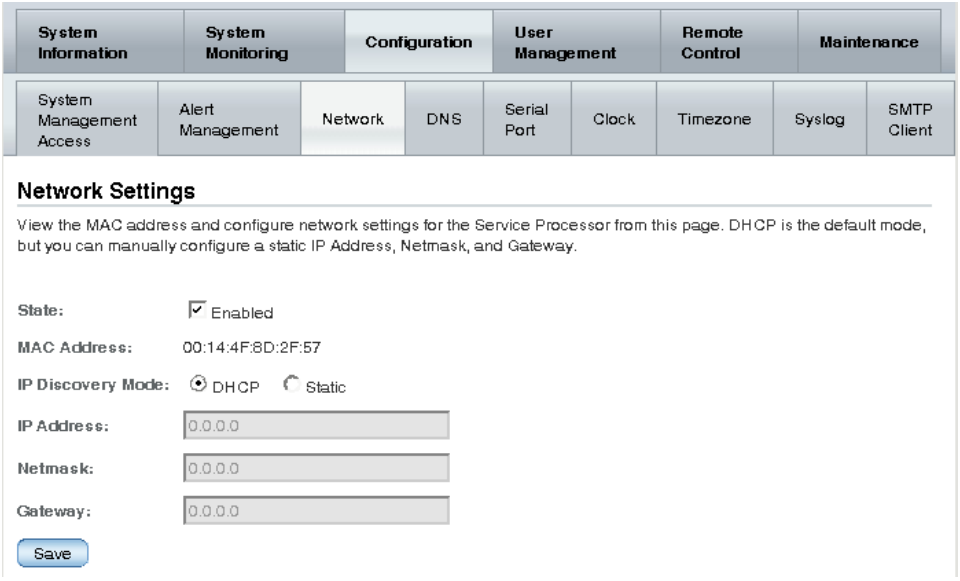
作業を開始する前に

- ネットワーク設定を表示するには、Read Only (o) の役割を有効にする必要があります。ネットワーク設定を構成するには、Admin (a) 役割を有効にする必要があります。

次の手順に従って、ネットワーク設定を表示および構成します。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「Network」を選択します。

   「Network Settings」ページが表示されます。「Network Settings」ページで、MAC アドレスを表示し、サーバのシャーシ監視モジュール (Chassis Monitoring Module、CMM) およびサービスプロセッサ (Service Processor、SP) のネットワークアドレスを設定できます。
3. **DHCP を使用して IP アドレスを自動的に割り当てることも、アドレスを手動で割り当てることを選択することもできます。**
   - IP アドレスを自動的に取得するには、「DHCP」の横にあるラジオボタンをクリックします。次の図を参照してください。



■ 静的 IP アドレスを手動で設定するには、「Network Settings」ページに情報を入力します。次の表の説明を使用してください。

項目	説明
State	ネットワークの状態を有効にするには、チェックボックスをクリックします。
MAC Address	SP の媒体アクセス制御 (Media Access Control、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。MAC アドレスは、SP 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。
IP Discovery Mode	IP アドレス、ネットマスク、およびゲートウェイを手動で割り当てるには、「Static」の横にあるラジオボタンをクリックします。
IP Address	サーバの 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固有の名前です。
Netmask	SP 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	SP のゲートウェイアクセスアドレスを入力します。

4. **「Save」をクリックして設定を有効にします。**

   「Save」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必要がある場合があります。

▼ DNS 設定の表示と構成

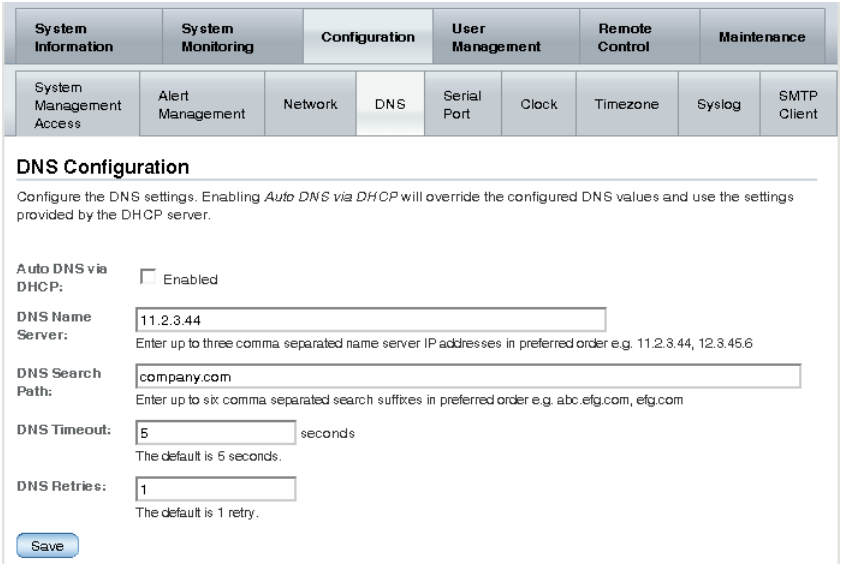
作業を開始する前に

- ドメインネームサービス (Domain Name Service、DNS) を表示するには、Read Only (o) の役割を有効にする必要があります。DNS 設定を構成するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、DNS 設定を表示および構成します。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「DNS」を選択します。

   「DNS Configuration」ページが表示されます。
3. DHCP を使用して DNS ネームサーバおよび検索パスを自動的に割り当てることも、アドレスを手動で割り当てることを選択することもできます。
   - アドレスを自動的に割り当てるには、「Auto DNS via DHCP」の横にあるラジオボタンをクリックします。
   - アドレスを手動で割り当てるには、「DNS Name Server」および「DNS Search Path」テキストボックスに情報を入力します。次の図を参照してください。



▼ シリアルポート設定の表示と構成

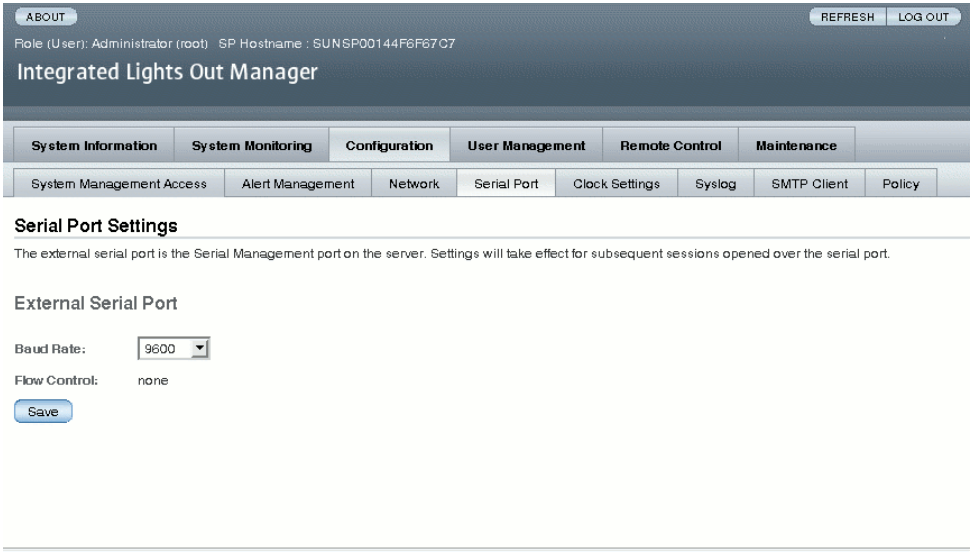
作業を開始する前に

- シリアルポート設定を表示するには、Read Only (o) の役割を有効にする必要があります。シリアルポート設定を構成するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、シリアルポートの設定を表示および構成します。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「Serial Port」を選択します。

   「Serial Port Settings」ページが表示されます。次の図を参照してください。



3. 外部シリアルポートおよび内部ホストシリアルポートのボーレートを表示します。

注 – 内部シリアルポートは SPARC サーバではサポートされていません。

---

4. **内部シリアルポートのボーレートを「Host Serial Port Baud Rate」ドロップダウンリストから選択します。**

   x64 システムの場合、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。

5. **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、サーバの 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。

6. **「Save」をクリックして変更を有効にします。**

▼ HTTP または HTTPS の Web アクセスを有効にする

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。

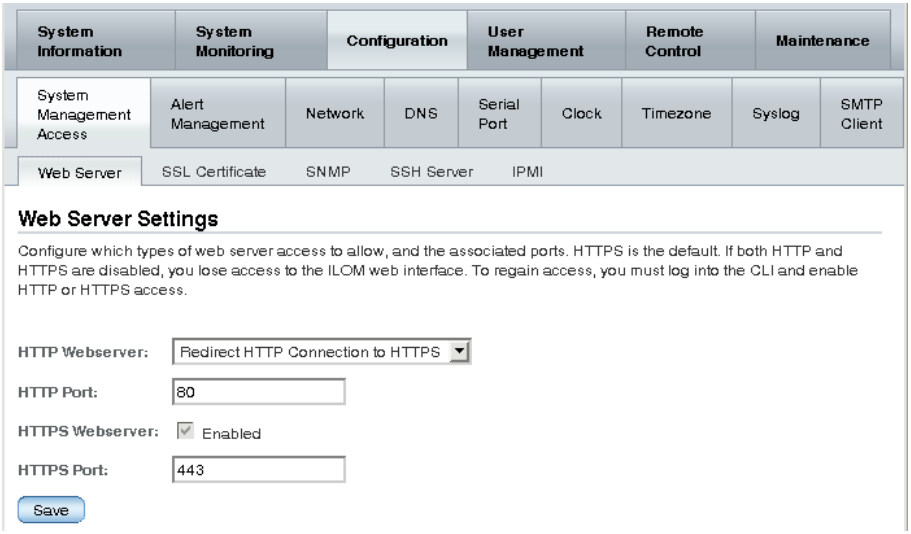
作業を開始する前に

- HTTP および HTTPS の設定を変更するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、HTTP または HTTPS の Web アクセスを有効にします。

1. **ILOM Web インタフェースにログインします。**
2. **「Configuration」-->「System Management Access」-->「Web Server」の順に選択します。**

「Web Server Settings」ページが表示されます。



3. HTTP または HTTPS Web サーバを選択します。
   - **HTTP を有効にする** − ドロップダウンリストから「Enabled」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 接続が自動的に HTTPS にリダイレクトされます。
     - Disabled − HTTP を無効にします。
   - **HTTPS を有効にする** −「HTTPS Web Server」の「Enabled」チェックボックスを選択します。

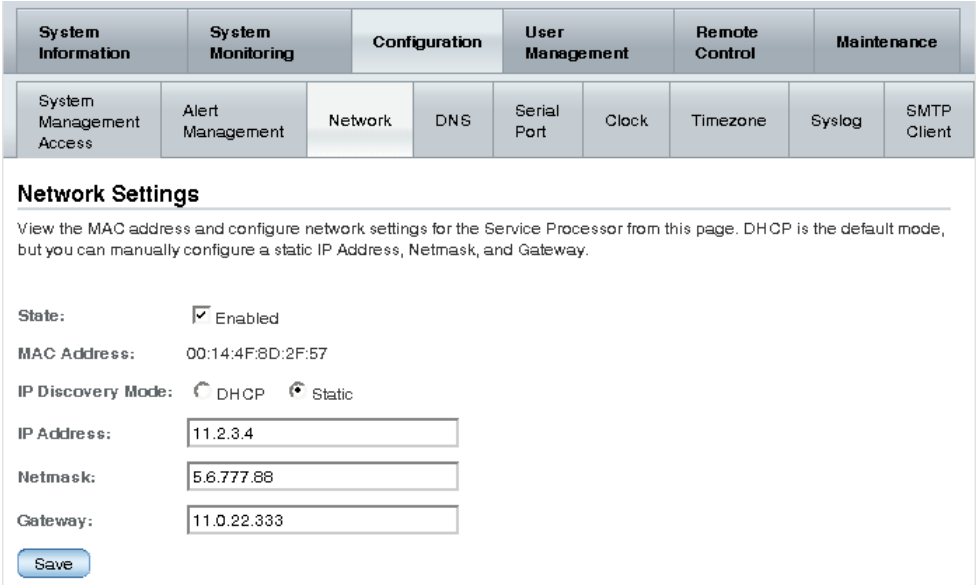
   HTTPS Web サーバはデフォルトで有効になっています。

注 – HTTP を無効にする、または「Redirect HTTP Connection to HTTPS」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。アクセスを復元するには、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』の「HTTP または HTTPS Web アクセスの有効化」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」をクリックして設定を有効にします。
6. 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. 「Configuration」-->「Network」を選択して、「Network Settings」ページにアクセスします。
   b. 「Static IP Discovery Mode」のラジオボタンを選択します。
   c. テキストボックスに IP アドレス、ネットマスク、およびゲートウェイの値を入力します。
   d. 「Save」をクリックして新しい設定を有効にします。

   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。



▼ 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。

作業を開始する前に

- SSL 証明書をアップロードするには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、SSL 証明書をアップロードします。

1. **ILOM Web インタフェースにログインします。**
2. **「Configuration」-->「System Management Access」-->「SSL Certificate」の順に選択します。**

   「SSL Certificate Upload」ページが表示されます。
3. **新しい SSL 証明書のファイル名を入力するか、または「Browse」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」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」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 サーバをリセットする必要があります。

Secure Shell の設定

項目

説明	リンク
Secure Shell の設定	• 28 ページの「SSH の有効化または無効化」 • 28 ページの「新しい SSH 鍵の生成」 • 29 ページの「SSH サーバの再起動」

▼ SSH の有効化または無効化

作業を開始する前に

- Secure Shell (SSH) サーバを再起動するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、SSH を有効または無効にします。

1. **ILOM Web インタフェースにログインします。**
2. **「Configuration」-->「System Management Access」-->「SSH Server」の順に選択します。**

   「SSH Server Settings」ページが表示されます。
3. **SSH サーバを有効にするには、「State」の横にある「Enabled」チェックボックスをクリックします。**
4. **「Save」をクリックして設定を有効にします。**

▼ 新しい SSH 鍵の生成

作業を開始する前に

- 新しい SSH 鍵を生成するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、新しい SSH 鍵を生成します。

1. **ILOM Web インタフェースにログインします。**
2. **「Configuration」-->「System Management Access」-->「SSH Server」の順に選択します。**

   「SSH Server Settings」ページが表示されます。
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。**

   プロンプトが表示されたら、「OK」または「Cancel」をクリックします。

   新しい鍵は、SSH サーバが再起動するまで有効になりません。

▼ SSH サーバの再起動

作業を開始する前に

- SSH サーバを再起動するには、Admin (a) の役割を有効にする必要があります。

注 – SSH サーバの再起動によって、既存のすべての SSH 接続が終了します。

次の手順に従って、SSH サーバを再起動します。

1. **ILOM Web インタフェースにログインします。**
2. **「Configuration」-->「System Management Access」-->「SSH Server」の順に選択します。**

   「SSH Server Settings」ページが表示されます。
3. **「Restart」ボタンをクリックして SSH サーバを再起動します。**

第5章

ユーザーアカウントの管理

項目 説明	リンク
ユーザーアカウントを設定する	• 33 ページの「シングルサインオンの設定」 • 33 ページの「セッションタイムアウトを設定する」 • 34 ページの「ユーザーアカウントの追加と役割の割り当て」 • 36 ページの「ユーザーアカウントの設定」 • 38 ページの「ユーザーアカウントの削除」 • 39 ページの「ユーザーセッションの表示」
SSH ホストキーを設定する	• 39 ページの「SSH 鍵を追加する」 • 42 ページの「SSH 鍵の削除」
Active Directory を設定する	• 43 ページの「Active Directory 設定の表示と構成」 • 47 ページの「Active Directory テーブルの設定」 • 50 ページの「Active Directory 認証および承認のトラブルシューティング」
LDAP を設定する	• 52 ページの「LDAP サーバを設定する」 • 53 ページの「LDAP 用の ILOM 設定」
LDAP/SSL を設定する	• 54 ページの「LDAP/SSL 設定の表示と構成」 • 58 ページの「LDAP/SSL テーブルの設定」 • 61 ページの「LDAP/SSL 認証および承認のトラブルシューティング」
RADIUS を設定する	• 63 ページの「RADIUS を設定する」

関連項目

ILOM	章または節	ガイド
• 概念	• ユーザーアカウントの管理 • ユーザーアカウントの管理のガイドライン	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• ユーザーアカウントの管理	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• SNMP	• ユーザーアカウントの管理	『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

ユーザーアカウントの設定

項目

説明	リンク
ユーザーアカウントを設定する	• 33 ページの「シングルサインオンの設定」 • 33 ページの「セッションタイムアウトを設定する」 • 34 ページの「ユーザーアカウントの追加と役割の割り当て」 • 36 ページの「ユーザーアカウントの設定」 • 38 ページの「ユーザーアカウントの削除」 • 39 ページの「ユーザーセッションの表示」

▼ シングルサインオンの設定

作業を開始する前に

- シングルサインオンを無効または有効にするには、Admin (a) の役割を有効にする必要があります。

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 インタフェースにログインします。**
2. **「User Management」-->「User Accounts」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。**

▼ 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。

作業を開始する前に

- セッションタイムアウトを設定するには、Read Only (o) の役割を有効に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 Web インタフェースにログインします。**
2. **「System Information」-->「Session Time-Out」の順に選択します。**
   「Session Time-Out」ページが表示されます。
3. **ドロップダウンリストから、希望の時間増分を選択します。**
4. **「Apply」ボタンをクリックして変更を保存します。**

▼ ユーザーアカウントの追加と役割の割り当て

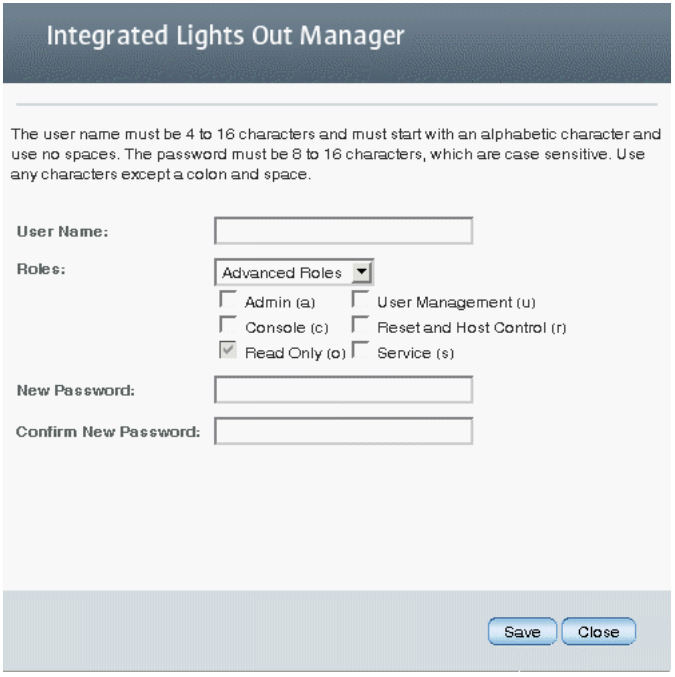
作業を開始する前に

- ユーザーアカウントを追加、変更、または削除するには、Admin (a) の役割を有効にする必要があります。

注 – User Management (u) 役割のあるアカウントのみ、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。ただし、自分のパスワードを変更するために必要な役割は、Read Only (o) のみです。新しいユーザーに User Management (u) の役割が割り当てられている場合、コマンド行インタフェース (command-line interface、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。

次の手順に従って、ユーザーアカウントを追加し、役割を割り当てます。

1. **ILOM Web インタフェースにログインします。**
2. **「User Management」-->「User Accounts」を選択します。**
   「User Account Settings」ページが表示されます。
3. **「Users」テーブルで「Add」をクリックします。**
   「Add User」ダイアログが表示されます。



4. **次の情報を入力します。**

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

   b. **プロファイルを選択します。次のようなオプションがあります。**

   - 新しい ILOM 3.0 のすべてのインストールでは、「`Advanced Role`」を選択できます。「`Advanced Role`」を選択すると、「Admin」(`a`)、「Console」(`c`)、「Read Only」(`o`)、「User Management」(`u`)、「Reset and Host Control」(`r`)、および「Service」(`s`) を選択できるようになります。ユーザーアカウントに割り当てられる役割および権限の説明については、『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』の「ILOM ユーザーアカウントの役割」を参照してください。
   - ILOM 2.0 から ILOM 3.0 にアップグレードするユーザーは、「`Administrator`」または「`Operator`」を選択できます。
   - `None`

   c. **適切な役割を選択します。**

   d. **「Password」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。

   e. **「Confirm 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。**

   f. **新しいユーザーの情報を入力し終わったら、「Save」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。

▼ ユーザーアカウントの設定

ユーザーのパスワードや、ユーザーのネットワーク権限およびシリアル権限を変更することにより、ユーザーアカウントを変更できます。

作業を開始する前に

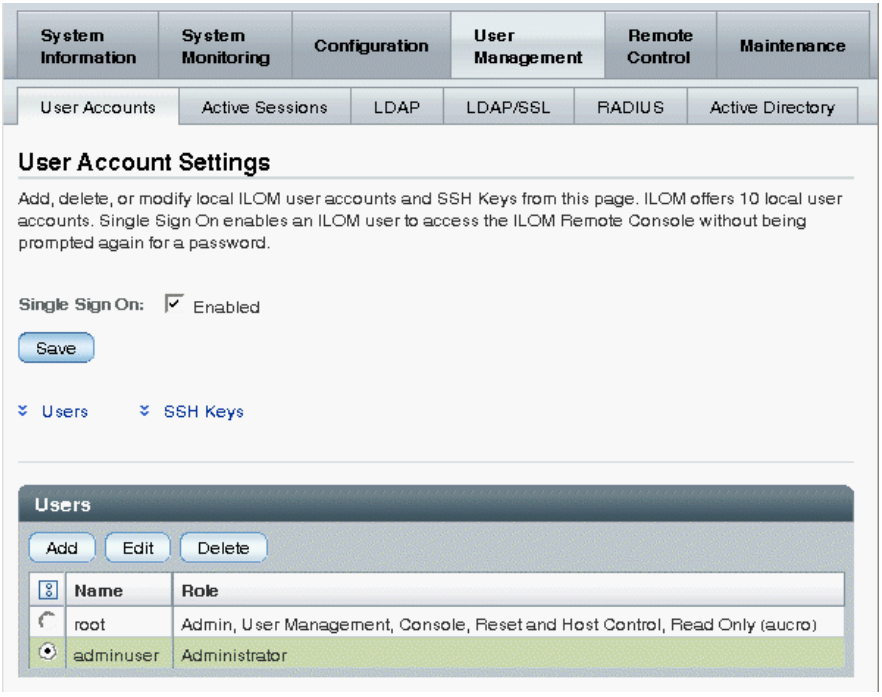
- ユーザーアカウントを追加、変更、または削除するには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、ユーザーアカウントを設定します。

1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「User Accounts」を選択します。

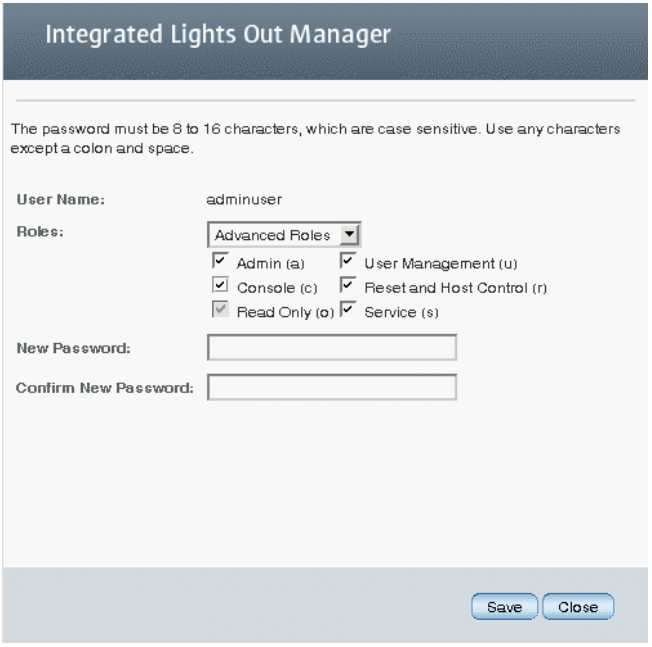
   「User Account Settings」ページが表示されます。
3. 「Users」テーブルで、変更するユーザーアカウントの隣のラジオボタンを選択します。

   次の図では、user1 が選択されています。



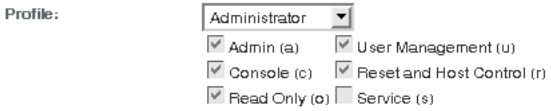
4. 「Edit」をクリックします。

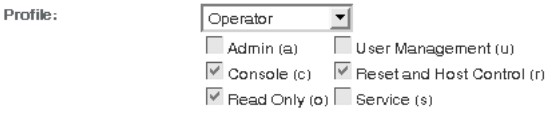
「Edit User」ダイアログが表示されます。次の図を参照してください。



5. プロファイルを変更します。

「Advanced Role」がプロファイルとして選択されている場合、u の役割を持つユーザーは、6 つの使用可能な役割をどれでも選択できます。一方、「Administrator」または「Operator」をプロファイルとして選択した場合は、個々の役割が自動的に選択されます。次の 2 つの図に、「Administrator」および「Operator」を選択したユーザーが使用できるようになる役割を示します。





6. 「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。

7. 「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。

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

   変更が反映された「User Account Settings」ページが再表示されます。

▼ ユーザーアカウントの削除

作業を開始する前に

- ユーザーアカウントを追加、変更、または削除するには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、ユーザーアカウントを削除します。

1. ILOM Web インタフェースにログインします。

2. 「User Management」-->「User Accounts」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。

4. 「Users」テーブルで「Delete」をクリックします。

   確認のダイアログが表示されます。

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

   「User Account Settings」ページが更新され、削除したユーザーアカウントが表示されなくなります。

▼ ユーザーセッションの表示

作業を開始する前に

- ユーザーセッションのリストを表示するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、ユーザーセッションを表示します。

1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「Active Sessions」を選択します。

   「Active Sessions」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。

SSH 鍵の設定

項目

説明	リンク
SSH ホストキーを設定する	• 39 ページの「SSH 鍵を追加する」 • 42 ページの「SSH 鍵の削除」

SSH 鍵を使用してパスワード認証を自動化することができます。次の手順では、SSH 鍵を追加および削除する方法を説明します。

▼ SSH 鍵を追加する

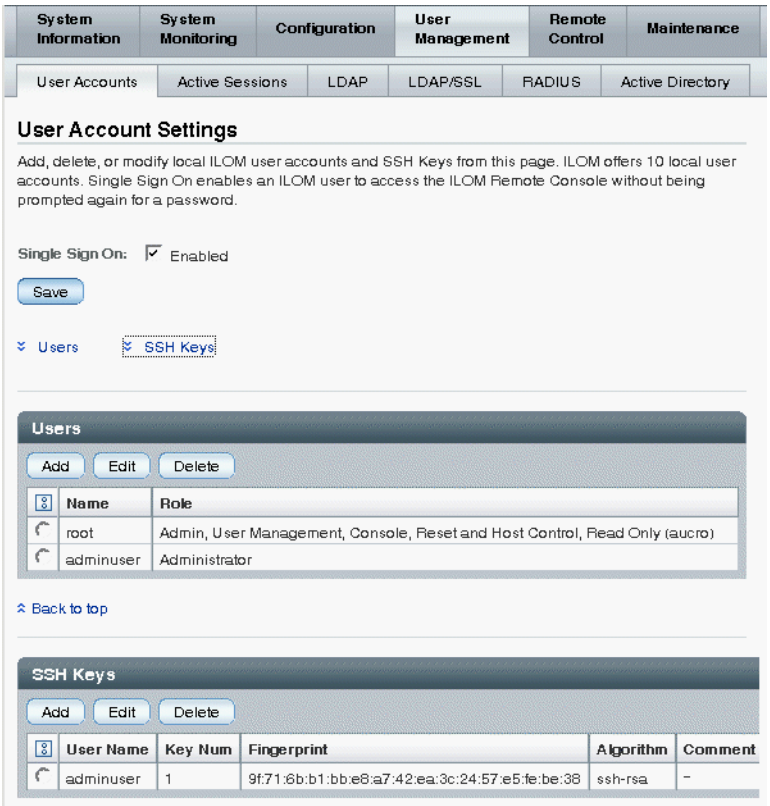
作業を開始する前に

- SSL 鍵を追加するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、SSH 鍵を追加します。

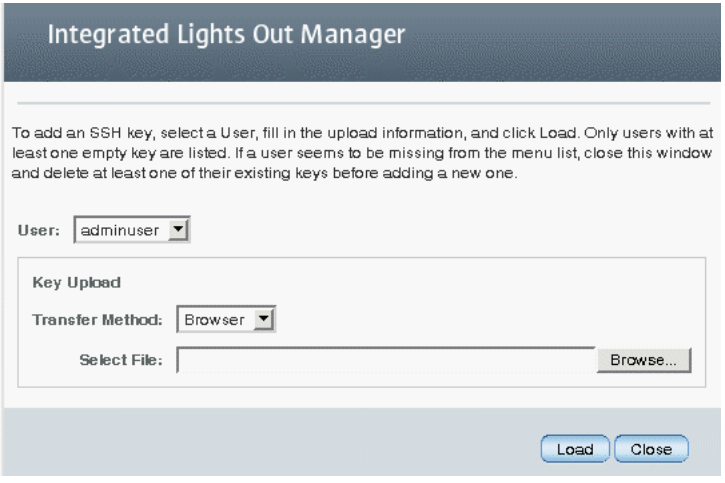
1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「User Accounts」を選択します。

   「User Account Settings」ページが表示されます。



3. ページをスクロールして下部にある「SSH Keys」リストを表示し、「Add」をクリックします。

   SSH 鍵の追加画面が表示されます。



4. 「User」ドロップダウンリストからユーザーアカウントを選択します。
5. 「Transfer Method」ドロップダウンリストから転送方法を選択します。

   次の転送方法を使用できます。

   - Browser
   - TFTP
   - FTP
   - SFTP
   - SCP
   - HTTP
   - HTTPS
6. 「Browser」転送方法を選択した場合は、「Browse」をクリックして SSH 鍵の位置を探します。手順 9 に進みます。
7. 「TFTP」転送方法を選択した場合は、次の図に示すプロンプトが表示されるので、次の情報を入力して、手順 9 に進みます。
   - **Host** – 遠隔ホストの IP アドレスか、DNS を設定している場合は遠隔ホストの名前を入力します。
   - **Filepath** – 設定ファイルの保存先のパスを `directoryPath/filename` 形式で入力します。

8. SCP、FTP、SFTP、HTTP、または HTTPS 転送方法を選択した場合は、次の図に示すプロンプトが表示されるので、次の情報を入力して、手順 9 に進みます。
   - **Host** – 遠隔ホストの IP アドレスか、DNS を設定している場合は遠隔ホストの名前を入力します。
   - **Filepath** – 設定ファイルの保存先のパスを `directoryPath/filename` 形式で入力します。
   - **Username** – リモートシステムでのアカウントのユーザー名を入力します。
   - **Password** – リモートシステムでのアカウントのパスワードを入力します。

9. **選択したユーザーアカウントに SSH 鍵を追加するには、「Load」をクリックします。**

   SSH 鍵がユーザーアカウントに追加されます。

▼ SSH 鍵の削除

作業を開始する前に

- SSL 鍵を削除するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、SSH 鍵を削除します。

1. **ILOM Web インタフェースにログインします。**
2. **「User Management」-->「User Accounts」を選択します。**

   「User Account Settings」ページが表示されます。
3. **ページをスクロールして下部にある「SSH Keys」セクションを表示し、ユーザーを選択して、「Delete」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。
4. **「OK」をクリックします。**

   SSH 鍵が削除されます。

Active Directory の設定

項目

説明	リンク
Active Directory を設定する	• 43 ページの「Active Directory 設定の表示と構成」 • 47 ページの「Active Directory テーブルの設定」 • 50 ページの「Active Directory 認証および承認のトラブルシューティング」

▼ Active Directory 設定の表示と構成

作業を開始する前に

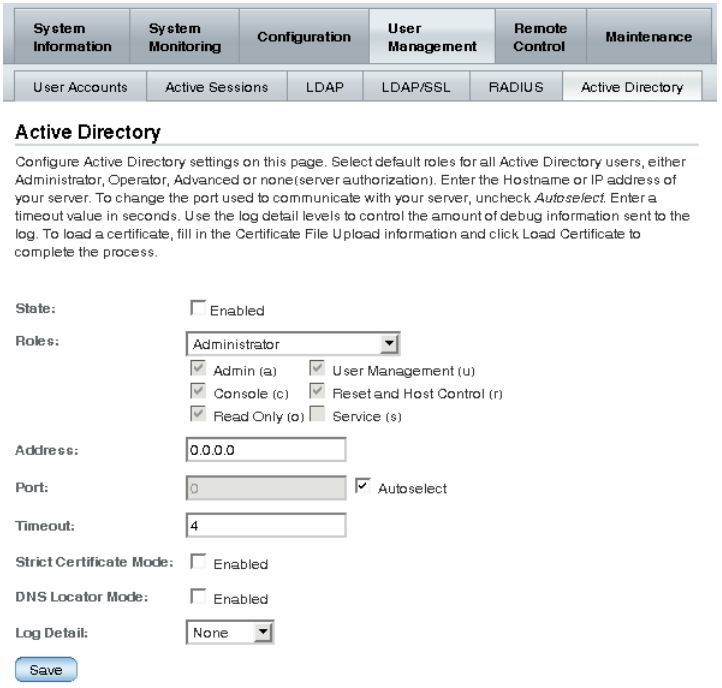
- Active Directory の設定を行うには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、Active Directory 設定を表示および構成します。

1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「Active Directory」を選択します。

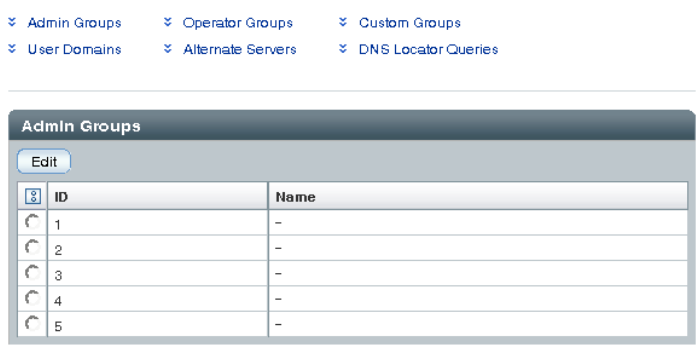
   「Active Directory」ページが表示されます。次の図に示すように、「Active Directory」ページには 3 つのセクションがあります。

   - 一番上のセクション (ターゲットとプロパティー)



- 中央のセクション (主要な証明書情報)

- 一番下のセクション (Active Directory テーブル)



3. **「Active Directory」設定ページの一番上のセクションに表示される Active Directory 設定を構成します。**

   Active Directory の設定については、次の表を参照してください。

プロパティー	デフォルト	説明
State	Disabled	Enabled | Disabled
Roles	(none)	Administrator | Operator | Advanced | なし 認証されたすべての Active Directory ユーザーに付与されるアクセスの役割。このプロパティーには、Administrator や Operator といった従来表記の役割を使用することも、a、u、c、r、o、s といった個々の役割 ID の組み合わせを使用することもできます。たとえば、aucros となっている場合、a は Admin、u は User Management、c は Console、r は Reset and Host Control、o は Read-Only、s は Service を意味します。ここで役割を設定しない場合、役割の決定には Active Directory サーバが使用されます。
Address	0.0.0.0	Active Directory サーバの IP アドレスまたは DNS 名。DNS 名が使用される場合は、DNS が設定済みで機能している必要があります。

プロパティー	デフォルト	説明
Port	0	サーバとの通信に使用するポート。`autoselect` が選択されている場合、ポートは 0 に設定されます。 標準以外の TCP ポートが使用されているという、通常ないような場合に使用できます。
Timeout	4	秒単位のタイムアウト値。 個々のトランザクションが完了するまで待機する秒数です。トランザクション数は設定によって異なる可能性があるため、この値はすべてのトランザクションを合計した時間にはなりません。 このプロパティーにより、サーバが応答しない場合や到達不能な場合に待機する時間を調整することができます。
Strict Certificate Mode	Disabled	Enabled | Disabled 有効になっている場合、認証時にサーバの証明書の内容がデジタル署名によって検証されます。証明書がロードされていないと、「Strict Certificate Mode」を有効にすることができません。
DNS Locator Mode	Disabled	Enabled | Disabled 有効にすると、設定された DNS ロケータクエリーに基づき、Active Directory サーバの検出が試みられます。
Log Detail	none	None | High | Medium | Low イベントログに記録する診断情報の量を指定します。

4. **「Active Directory」設定ページの一番上のセクションにある「Save」をクリックして設定を有効にします。**

5. **「Active Directory」設定ページの中央のセクションにある Active Directory 証明書情報を表示します。**

   Active Directory の証明書の設定については、次の表を参照してください。

プロパティー	表示	説明
Certificate File Status	`certificate not present`	証明書が存在するかどうかを示す読み取り専用インジケータ。
Certificate File Status	`certificate present (details)`	発行者、主題、シリアル番号、有効期間の開始日、有効期間の終了日、およびバージョンについては「details」をクリックしてください。

6. 「Certificate File Upload」セクションで、証明書ファイルをアップロードする転送方法と必要なパラメータを選択します。

注 – このセクションは、「Strict Certificate Mode」を有効にする場合にのみ必要です。「Strict Certificate Mode」が無効になっている場合、データは保護されますが証明書は不要です。

次の表では、転送方法ごとに必要なパラメータを示します。

転送方法	必要なパラメータ
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

7. 「Load Certificate」ボタンまたは「Remove Certificate」ボタンをクリックします。
8. 証明書がロードされている場合は、「details」リンクをクリックして次の情報を表示します。

`Issuer`	証明書を発行した認証局。
`Subject`	証明書の対象のサーバまたはドメイン。
`Valid From`	証明書が有効になる日。
`Valid Until`	証明書が無効になる日。
`Serial Number`	証明書のシリアル番号。
`Version`	証明書のバージョン番号。

▼ Active Directory テーブルの設定

作業を開始する前に

- Active Directory テーブルを設定するには、User Management（u）の役割を有効にする必要があります。

次の手順に従って、Active Directory テーブルを設定します。

1. **ILOM Web インタフェースにログインします。**
2. **「User Management」-->「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、設定するテーブルのカテゴリにアクセスするリンクをクリックします。**
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alternate Servers
   - DNS Locator Queries
4. **個々のテーブルのラジオボタンを選択して、「Edit」をクリックします。**
5. **テーブルに必要なデータを入力します。**
   次の表に、Active Directory データの望ましい形式を示すためのデフォルトデータを示します。
   - **Admin Groups テーブル:**
     Admin Groups テーブルには、Microsoft Active Directory グループの名前が、識別名 (Distinguished Name、DN) 形式、単純名形式、または NT 形式で含まれます。

ID	名前
1	CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=sun,DC=com
2	

- **Operator Groups テーブル:**

  Operator Groups テーブルには、Microsoft Active Directory グループの名前が、識別名 (Distinguished Name、DN) 形式、単純名形式、または NT 形式で含まれます。

ID	名前
1	CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=sun,DC=com
2	

- **Custom Groups テーブル:**

  Custom Groups テーブルには、Microsoft Active Directory グループの名前が、識別名 (Distinguished Name、DN) 形式、単純名形式、または NT 形式で含まれます。エントリに関連付けられている役割も設定されます。

ID	名前	Roles
1	custom_group_1	Admin、User Management、Console、Reset and Host Control、Read Only (aucro)

- **User Domains テーブル:**

  User Domains は、ユーザーの認証に使われる認証ドメインです。ユーザーがログインする際に使用する名前は、特定のドメイン名形式になります。ユーザー認証は、入力されたユーザー名と設定済みのユーザードメインに基づいて試行されます。

  この後の例では、エントリ 1 に表示されているドメインは、ユーザー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、Active Directory が最初のエントリでの認証に失敗した場合に使用する、完全な識別名を示します。

注 – この後の例で、<USERNAME> は、ユーザーのログイン名で置き換えられます。認証時に、ユーザーのログイン名が <USERNAME> に置き換わります。

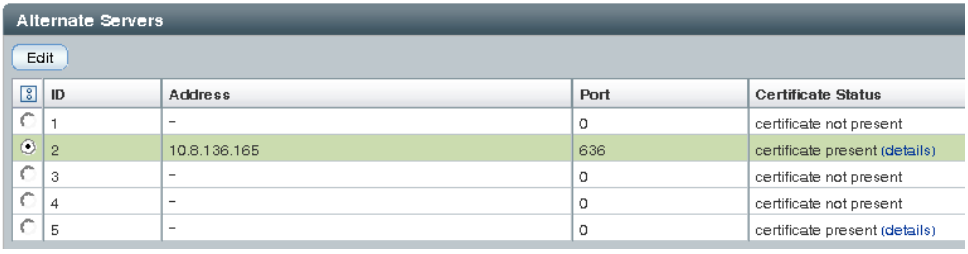
ID	ドメイン
1	<USERNAME>@sales.east.sun.com
2	CN=<USERNAME>,CN=Users,DC=sales,DC=east,DC=sun,DC=com

- **Alternate Servers テーブル:**

  Alternate Servers テーブルは、冗長性および各種サーバからの選択 (分離されたドメインのために必要な場合) を提供します。証明書が指定されていないにもかかわらず必要な場合は、トップレベルの主証明書が使用されます。代替サーバのルールと要件は、トップレベル証明書モードと同じです。各サーバにそれぞれの証明書状態があり、必要に応じてそれぞれの証明書コマンドで証明書を取得します。

ID	Address	Port	証明書の状態
1	-	0	certificate not present
2	10.8.136.165	0	certificate present (details)

次の図に、ID 2 に証明書が存在する Alternate Servers テーブルを示します。



「details」リンクをクリックすると、次の証明書情報が表示されます。

Issuer	証明書を発行した認証局。
Subject	証明書の対象のサーバまたはドメイン。
Valid From	証明書が有効になる日。
Valid Until	証明書が無効になる日。
Serial Number	証明書のシリアル番号。
Version	証明書のバージョン番号。

- **DNS Locator Queries テーブル:**

  DNS Locator Queries テーブルは、認証に使用するホストについて DNS サーバに問い合わせます。

  DNS ロケータサービスクエリーは、名前付き DNS サービスを識別します。ポート ID は、通常、レコードに含まれますが、<PORT:636> 形式を使用してオーバーライドできます。また、認証されるドメイン固有の名前付きサービスは、<DOMAIN> 置換マーカーを使用して指定できます。

名前	ドメイン
1	_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
2	_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>

注 – DNS ロケータクエリーが機能するには、DNS および DNS ロケータモードが有効になっている必要があります。

6. 「Save」をクリックして変更を有効にします。

▼ Active Directory 認証および承認のトラブルシューティング

作業を開始する前に

- 認証イベントおよび承認イベントを表示するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、Active Directory 認証および承認をトラブルシューティングします。

1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「Active Directory」を選択します。

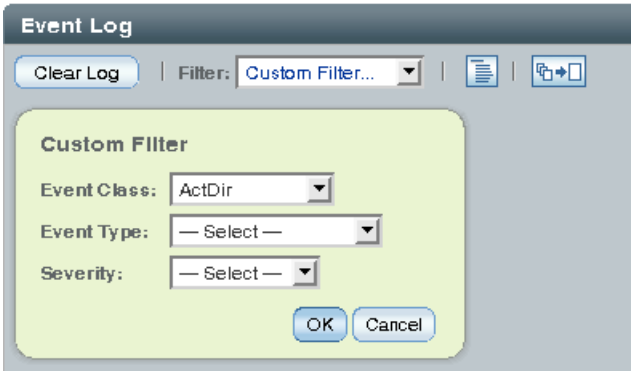
   「Active Directory」ページが表示されます。
3. 「Log Detail」ドロップダウンリストで、記録するイベントログの詳細レベルを選択します。

   「None」、「High」、「Medium」、「Low」、または「Trace」を選択できます。
4. 「Save」をクリックして変更を保存します。

5. 認証を試みてイベントを生成します。次の手順を実行します。

   a. 「System Monitoring」タブから「Event Logs」を選択します。

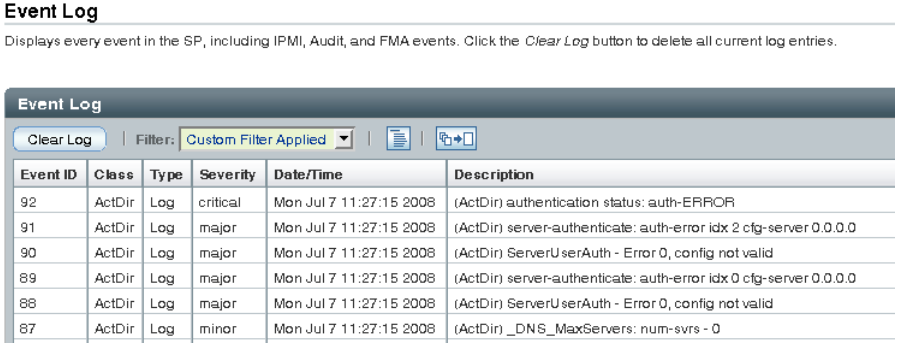
   b. 「Filter」ドロップダウンリストで、「Custom Filter」を選択します。



   c. 「Event Class」ドロップダウンリストで、「ActDir」を選択します。

   d. 「OK」をクリックします。

   すべての Active Directory イベントがイベントログに表示されます。



LDAP (Lightweight Directory Access Protocol) の設定

項目

説明	リンク
LDAP を設定する	• 52 ページの「LDAP サーバを設定する」 • 53 ページの「LDAP 用の ILOM 設定」

▼ LDAP サーバを設定する

作業を開始する前に

- LDAP を設定するには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、LDAP サーバを設定します。

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。**

   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。

   たとえば、次のように入力します。

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

   または

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

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。必要なプロパティー値については、次の表を参照してください。**

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	任意の固有の番号
gidNumber	任意の固有の番号

必須プロパティー	説明
userPassword	パスワード
homeDirectory	任意の値 (ILOM はこのプロパティーを無視します)
loginShell	任意の値 (ILOM はこのプロパティーを無視します)

3. **LDAP サーバを設定して、ILOM のユーザーアカウントにアクセスできるようにします。**

   LDAP サーバが匿名バインドを許可するようにするか、または LDAP サーバにプロキシユーザーを作成します。LDAP サーバは、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 サーバのマニュアルを参照してください。

▼ LDAP 用の ILOM 設定

作業を開始する前に

- LDAP を設定するには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、LDAP 用に ILOM を設定します。

1. **ILOM Web インタフェースにログインします。**
2. **「User Management」-->「LDAP」を選択します。**

   「LDAP Settings」ページが表示されます。

3. **次の値を入力します。**
   - **State** − LDAP ユーザーを認証するには、「Enabled」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。
   - **Address** − LDAP サーバの IP アドレスまたは DNS 名です。
   - **Port** − LDAP サーバのポート番号です。デフォルトのポートは 389 です。
   - **Searchbase** − ユーザーを検索するための LDAP サーバの分岐を入力します。
   - **Bind DN** − LDAP サーバ上の読み取り専用プロキシユーザーの識別名 (Distinguished Name、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** − 読み取り専用ユーザーのパスワードを入力します。

4. 「Save」をクリックして変更を有効にします。

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、ILOM はローカルアカウントを使用して認証を行います。

LDAP/SSL の設定

項目

説明	リンク
LDAP/SSL を設定する	• 54 ページの「LDAP/SSL 設定の表示と構成」 • 58 ページの「LDAP/SSL テーブルの設定」 • 61 ページの「LDAP/SSL 認証および承認のトラブルシューティング」

▼ LDAP/SSL 設定の表示と構成

作業を開始する前に

- LDAP/SSL を設定するには、User Management (u) の役割を有効にする必要があります。

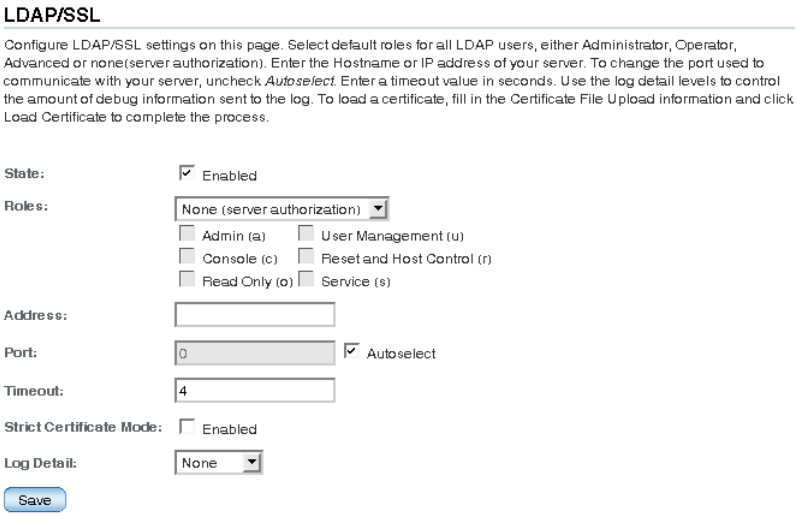
次の手順に従って、LDAP/SSL の設定を表示および構成します。

1. ILOM Web インタフェースにログインします。

2. 「User Management」-->「LDAP/SSL」を選択します。

   「LDAP/SSL」ページが表示されます。「LDAP/SSL」ページには 3 つのセクションがあります。

- 一番上のセクション (ターゲットとプロパティー)



- 中央のセクション (証明書情報)

- 一番下のセクション (LDAP/SSL テーブル)

3. 「LDAP/SSL」設定ページの一番上のセクションに表示される LDAP/SSL 設定を構成します。

LDAP/SSL の設定については、次の表を参照してください。

プロパティー (Web)	デフォルト	説明
State	Disabled	Enabled | Disabled
Roles	(none)	Administrator | Operator | Advanced | (なし) 認証されたすべての LDAP/SSL ユーザーに付与されるアクセスの役割。このプロパティーには、Administrator や Operator といった従来表記の役割を使用することも、a、u、c、r、o、s といった個々の役割 ID の組み合わせを使用することもできます。たとえば、aucros となっている場合、a は Admin、u は User Management、c は Console、r は Reset and Host Control、o は Read-Only、s は Service を意味します。ここで役割を設定しない場合、役割の決定には LDAP/SSL サーバが使用されます。
Address	0.0.0.0	LDAP/SSL サーバの IP アドレスまたは DNS 名。
Port	0	サーバとの通信に使用するポート。autoselect が有効になっている場合、ポートは 0 に設定されます。 標準以外の TCP ポートが使用されているという、通常ないような場合に使用できます。
Timeout	4	秒単位のタイムアウト値。 個々のトランザクションが完了するまで待機する秒数です。トランザクション数は設定によって異なる可能性があるため、この値はすべてのトランザクションを合計した時間にはなりません。 このプロパティーにより、サーバが応答しない場合や到達不能な場合に待機する時間を調整することができます。
Strict Certificate Mode	Disabled	Enabled | Disabled 有効になっている場合、認証時にサーバの証明書の内容がデジタル署名によって検証されます。証明書がロードされていないと、「Strict Certificate Mode」を有効にすることができません。
Log Detail	none	None | High | Medium | Low イベントログに記録する診断情報の量を指定します。

4. 「LDAP/SSL」設定ページの一番上のセクションにある「Save」をクリックして、このセクションで行った変更を保存します。

5. 「LDAP/SSL」設定ページの中央セクションで、LDAP/SSL の証明書情報を確認します。

LDAP/SSL 証明書の設定については、次の表を参照してください。

プロパティー	表示	説明
Certificate File Status	`certificate not present`	証明書が存在するかどうかを示す読み取り専用インジケータ。
Certificate File Status	`certificate present (details)`	発行者、主題、シリアル番号、有効期間の開始日、有効期間の終了日、およびバージョンについては「details」をクリックしてください。

6. 「Certificate File Upload」セクションで、証明書ファイルをアップロードする転送方法を選択します。

注 – このセクションは、「Strict Certificate Mode」を使用にする場合にのみ必要です。「Strict Certificate Mode」が無効になっている場合、データは保護されますが証明書は不要です。

次の表では、転送方法ごとに必要なパラメータを示します。

転送方法	必要なパラメータ
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

7. 「Load Certificate」ボタンまたは「Remove Certificate」ボタンをクリックします。

8. 証明書がロードされている場合は、Web インタフェースで「details」リンクをクリックして次の情報を表示します。

Issuer	証明書を発行した認証局。
Subject	証明書の対象のサーバまたはドメイン。
Valid From	証明書が有効になる日。
Valid Until	証明書が無効になる日。
Serial Number	証明書のシリアル番号。
Version	証明書のバージョン番号。

▼ LDAP/SSL テーブルの設定

作業を開始する前に

- LDAP/SSL を設定するには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、LDAP/SSL テーブルを設定します。

1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「LDAP/SSL」を選択します。
   「LDAP/SSL」ページが表示されます。
3. 「LDAP/SSL」ページの一番下で、設定するテーブルのカテゴリにアクセスするリンクをクリックします。
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alternate Servers
4. 個々のテーブルのラジオボタンを選択して、「Edit」をクリックします。
5. テーブルに必要なデータを入力します。
   次の表に、LDAP/SSL データの望ましい形式を示すためのデフォルトデータを示します。

- **Admin Groups テーブル:**

  Admin Groups テーブルには、LDAP/SSL グループの名前が、識別名 (Distinguished Name、DN) 形式で含まれます。

ID	名前
1	CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=sun,DC=com
2	

- **Operator Groups テーブル:**

  Operator Groups テーブルには、LDAP/SSL グループの名前が、識別名 (Distinguished Name、DN) 形式で含まれます。

ID	名前
1	CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=sun,DC=com
2	

- **Custom Groups テーブル:**

  Custom Groups テーブルには、LDAP/SSL グループの名前が、識別名 (Distinguished Name、DN) 形式、単純名形式、または NT 形式で含まれます。エントリに関連付けられている役割も設定されます。エントリ 1 に表示されている名前は、単純名形式を使用しています。

ID	名前	Roles
1	custom_group_1	Admin, User Management, Console, Reset and Host Control, Read Only (aucro)

- **User Domains テーブル:**

  User Domains は、ユーザーの認証に使われる認証ドメインです。ユーザーがログインする際に使用する名前は、特定のドメイン名形式になります。ユーザー認証は、入力されたユーザー名と設定済みのユーザードメインに基づいて試行されます。

  エントリ 1 は、LDAP/SSL が最初のエントリの認証に失敗した場合に使用する、完全な識別名を示します。

注 – 認証の際、<USERNAME> はユーザーのログイン名に置き替えられます。原則の形式または識別名形式がサポートされます。

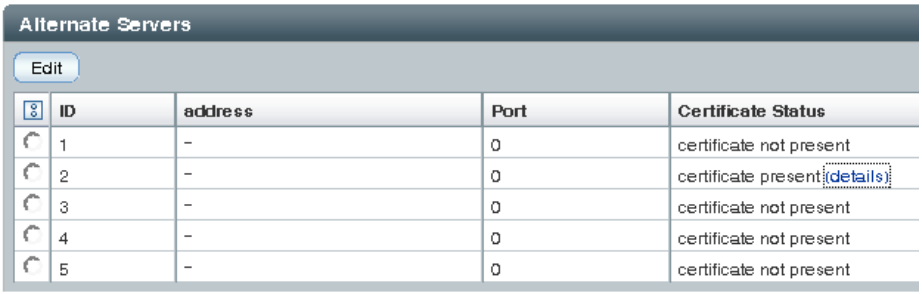
ID	ドメイン
1	UID=<USERNAME>,OU=people,DC=sun,DC=com
2	

- **Alternate Servers テーブル:**

  代替サーバテーブルは、認証に冗長性を提供します。証明書が指定されていないにもかかわらず必要な場合は、トップレベルの主証明書が使用されます。代替サーバのルールと要件は、トップレベル証明書モードと同じです。各サーバにそれぞれの証明書状態があり、必要に応じてそれぞれの証明書コマンドで証明書を取得します。

ID	Address	Port	証明書の状態
1	-	0	certificate not present
2	-	0	certificate not present
3	10.7.143.246	0	certificate present (details)

次の図に、ID 2 に証明書が存在する Alternate Servers テーブルを示します。



「details」リンクをクリックすると、次の情報が表示されます。

Issuer	証明書を発行した認証局。
Subject	証明書の対象のサーバまたはドメイン。
Valid From	証明書が有効になる日。
Valid Until	証明書が無効になる日。
Serial Number	証明書のシリアル番号。
Version	証明書のバージョン番号。

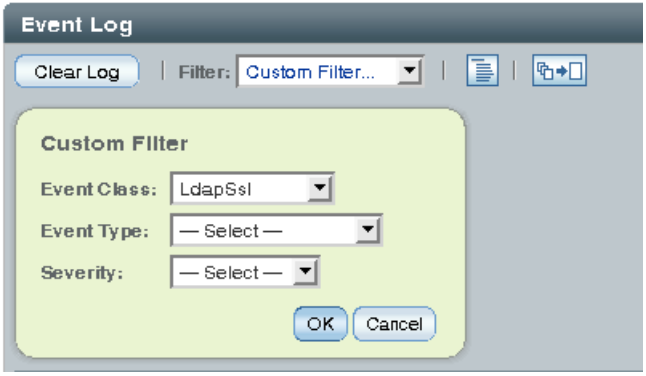
▼ LDAP/SSL 認証および承認のトラブルシューティング

作業を開始する前に

- 認証イベントおよび承認イベントを表示するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、LDAP/SSL の認証と承認をトラブルシューティングします。

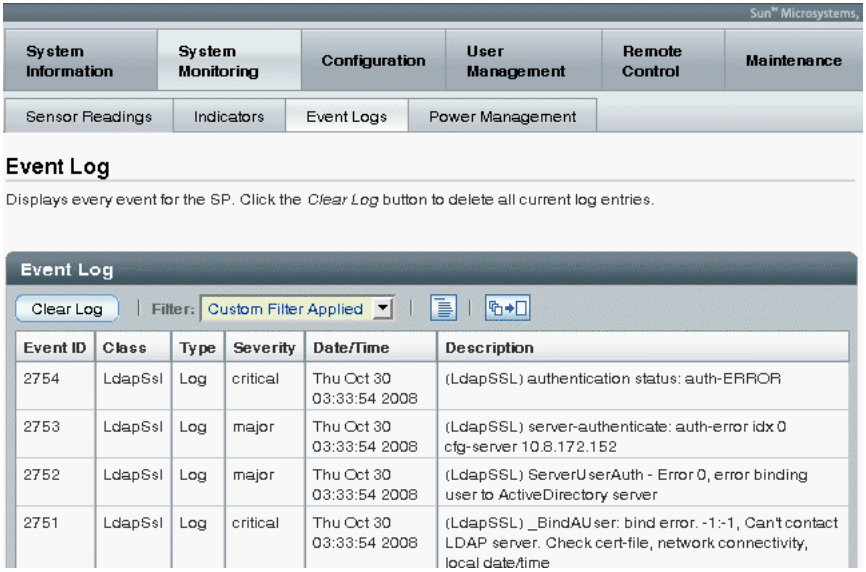
1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「LDAP/SSL」を選択します。
   「LDAP/SSL」ページが表示されます。
3. 「Log Detail」ドロップダウンリストで、記録するイベントログの詳細レベルを選択します。
   「None」、「High」、「Medium」、「Low」、または「Trace」を選択できます。
4. 「Save」をクリックして変更を保存します。
5. 認証を試みてイベントを生成します。
   a. 「System Monitoring」-->「Event Logs」を選択します。
   b. 「Filter」ドロップダウンリストで、「Custom Filter」を選択します。



c. 「Event Class」ドロップダウンリストで、「LdapSsl」を選択します。

d. 「OK」をクリックして変更を有効にします。

すべての LDAP/SSL イベントがイベントログに表示されます。



RADIUS の設定

項目	
説明	リンク
RADIUS を設定する	• 63 ページの「RADIUS を設定する」

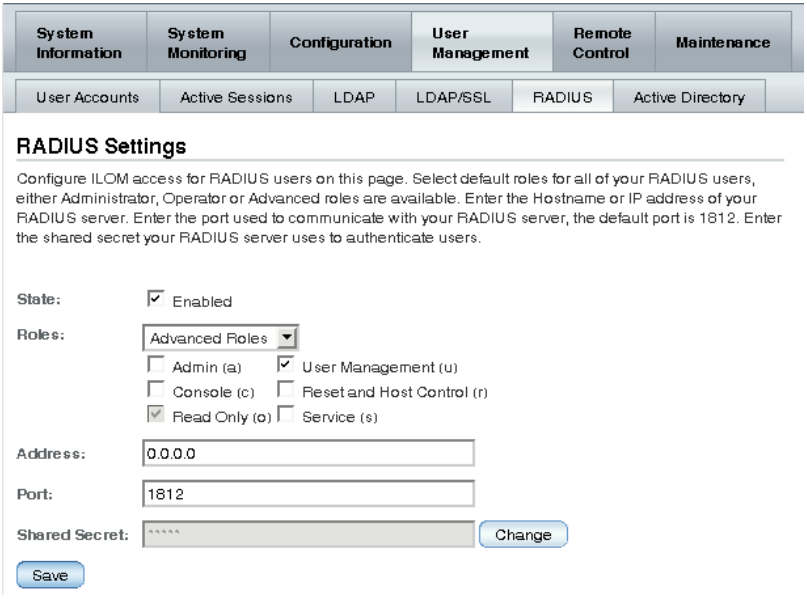
▼ RADIUS を設定する

作業を開始する前に

- RADIUS を設定するには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、RADIUS の設定を行います。

1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「RADIUS」を選択します。
   「RADIUS Settings」ページが表示されます。



3. 設定を完了します。

プロパティー (Web)	デフォルト	説明
State	Disabled	Enabled | Disabled RADIUS クライアントを有効にするか無効にするかを指定します。
Role	Operator	Administrator | Operator | Advanced Roles 認証されたすべての RADIUS ユーザーに付与されるアクセスの役割。このプロパティーは、Administrator や Operator といった従来の表記の役割や、a、u、c、r、o、s といった個々の役割 ID の組み合わせをサポートします。たとえば、aucrs となっている場合、a は Admin、u は User Management、c は Console、r は Reset and Host Control、o は Read Only、s は Service を意味します。
Address	0.0.0.0	RADIUS サーバの IP アドレスまたは DNS 名。DNS 名を使用する場合は、DNS が設定されていて、機能している必要があります。
Port	1812	RADIUS サーバとの通信に使用するポート番号を指定します。デフォルトのポートは 1812 です。
Shared Secret	(none)	機密データを保護しクライアントとサーバの相互認識を可能にするために使われる共有シークレットを指定します。

4. 「Save」をクリックして変更を有効にします。

第6章

システム部品の管理

項目

説明	リンク
システム部品の管理	• 66 ページの「部品情報の表示および変更」 • 68 ページの「部品を取り外す準備」 • 68 ページの「部品をサービスに復帰させる」 • 68 ページの「部品の有効および無効の切り替え」

関連項目

ILOM	章または節	ガイド
• 概念	• 障害管理について	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• システム部品の管理	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

部品情報の表示およびシステム部品の管理

項目

説明	リンク
準備すべき事柄を確認する	• 66 ページの「作業を開始する前に」
システム部品の表示と管理	• 66 ページの「部品情報の表示および変更」 • 68 ページの「部品を取り外す準備」 • 68 ページの「部品をサービスに復帰させる」 • 68 ページの「部品の有効および無効の切り替え」

作業を開始する前に

この節の手順を開始する前に、必ず、次の要件が満たされていることを確認してください。

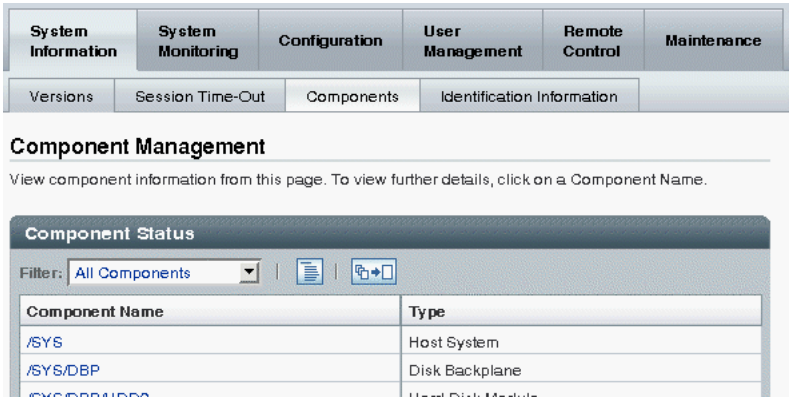
- システム部品を管理するには、Reset and Host Control (r) の役割を有効にする必要があります。

▼ 部品情報の表示および変更

次の手順に従って、部品情報を表示および変更します。

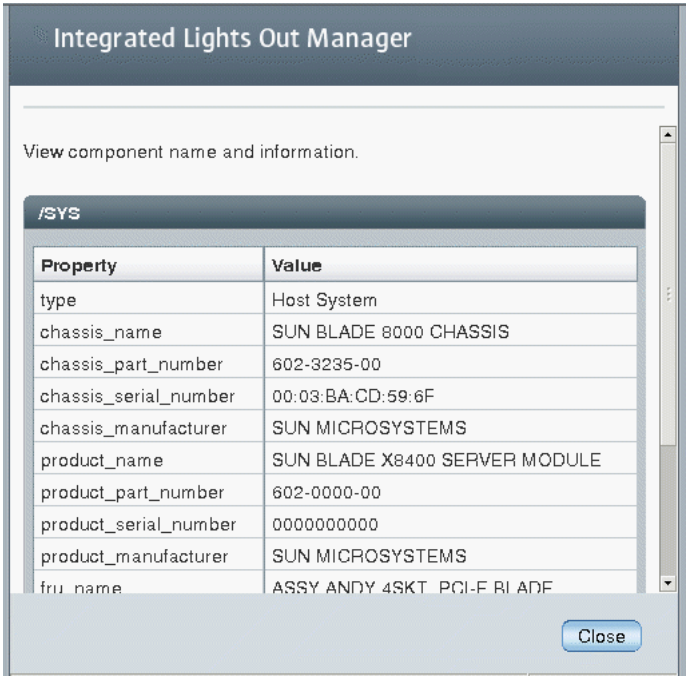
1. ILOM Web インタフェースにログインします。
2. 「System Information」-->「Components」を選択します。

「Component Management」ページが表示されます。



3. **部品で障害が発生している場合、部品名の左横にラジオボタンが表示されます。ラジオボタンをクリックして障害の状態を確認します。ラジオボタンが表示されない場合は、部品名をクリックして状態を確認します。**

   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。次の図を参照してください。



▼ 部品を取り外す準備

次の手順に従って、部品を取り外す準備をします。

1. ILOM Web インタフェースにログインします。
2. 「System Information」-->「Components」を選択します。
   「Component Management」ページが表示されます。
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。

▼ 部品をサービスに復帰させる

次の手順に従って、部品をサービスに復帰させます。

1. ILOM Web インタフェースにログインします。
2. 「System Information」-->「Components」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

次の手順に従って、部品を有効または無効にします。

1. ILOM Web インタフェースにログインします。
2. 「System Information」-->「Components」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」または「Disable」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。

第7章

システム部品の監視

項目	
説明	**リンク**
センサーの測定値を表示する	• 71 ページの「センサー測定値を表示する」
システムインジケータ、クロック、およびタイムゾーンを設定する	• 72 ページの「システムインジケータの設定」 • 72 ページの「クロックの設定」 • 74 ページの「タイムゾーンの設定」
イベントログをフィルタリング、表示、クリア、および設定する	• 74 ページの「イベントログ出力のフィルタリング」 • 76 ページの「ILOM イベントログの表示およびクリア」 • 77 ページの「遠隔 syslog 受信側の IP アドレスを設定する」
障害の状態を表示する	• 78 ページの「障害の状態を表示する」
保守担当者がシステムの問題の診断に使用するデータを収集する	• 79 ページの「システムの問題を診断するための SP データの収集」

関連項目

ILOM	章または節	ガイド
• 概念	• システム監視と警告管理 • システムの問題を診断するための SP データの収集	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• システムセンサー、インジケータ、および ILOM イベントログの監視 • システムの問題を診断するための SP データの収集	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• SNMP	• システムの監視	『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

システムセンサー、インジケータ、および ILOM イベントログの監視

項目

説明	リンク
センサーの測定値を表示する	• 71 ページの「センサー測定値を表示する」
システムインジケータの状態を変更する	• 72 ページの「システムインジケータの設定」
クロック設定を表示および設定する	• 72 ページの「クロックの設定」
タイムゾーンを設定する	• 74 ページの「タイムゾーンの設定」
イベントログデータのフィルタを設定する	• 74 ページの「イベントログ出力のフィルタリング」
イベントログを表示およびクリアする	• 76 ページの「ILOM イベントログの表示およびクリア」

項目	
説明	**リンク**
遠隔 syslog 受信側の IP アドレスを設定する	• 77 ページの「遠隔 syslog 受信側の IP アドレスを設定する」
部品の障害の状態を表示する	• 78 ページの「障害の状態を表示する」
システムの問題を診断するために SP データを収集する	• 79 ページの「システムの問題を診断するための SP データの収集」

▼ センサー測定値を表示する

作業を開始する前に

- インジケータの状態を表示するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、センサー測定値を表示します。

1. **ILOM Web インタフェースにログインします。**
2. **「System Monitoring」-->「Sensors Readings」を選択します。**

   「Sensor Readings」ページが表示されます。

注 – サーバ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。

---

3. **「Sensor Reading」ページで、次の手順を実行します。**

   a. **設定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、サーバ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の設定

作業を開始する前に

- インジケータの状態を設定するには、User Management (u) の役割を有効にする必要があります。

次の手順に従って、システムインジケータの設定を行います。

1. ILOM Web インタフェースにログインします。
2. 「System Monitoring」-->「Indicators」を選択します。
   「Indicators」ページが表示されます。

注 – サーバ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。

---

3. 「Indicators」ページで、次の手順を実行します。
   a. 設定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変更するには、変更す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ます。「Actions」ドロップダウンリストボックスをクリックし、「Turn LED Off」または「Set LED to Fast Blink」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。

▼ クロックの設定

作業を開始する前に

- クロック設定を表示および構成するには、Admin (a) の役割を有効にする必要があります。
- この手順を完了するには、NTP サーバの IP アドレスが必要です。

次の手順に従って、クロックの設定を行います。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「Clock Settings」を選択します。
   「Clock Settings」ページが表示されます。

3. 「Clock Settings」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 SP の日時を手動で設定します。手順 4 を参照してください。
   - ホストサーバ SP の日時を NTP サーバと同期させます。手順 5 を参照してください。
4. ホストサーバ SP の日時を手動で設定するには、次の手順を実行します。
   a. 「Date」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。
   c. 手順 6 に進みます。
5. NTP サーバの IP アドレスを設定して、同期を使用可能にするには、次の手順を実行します。
   a. 「Synchronize Time Using NTP」の隣にある「Enabled」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 サーバの IP アドレスを入力します。
6. 「Save」をクリックして変更を有効にします。

   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、サーバ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。

▼ タイムゾーンの設定

作業を開始する前に

- クロックのタイムゾーン設定を表示および指定するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、タイムゾーンを設定します。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「Timezone」を選択します。

   「Timezone Settings」ページが表示されます。
3. 「Timezone」ドロップダウンリストを使用してタイムゾーンを選択します。

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、サーバ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。

▼ イベントログ出力のフィルタリング

作業を開始する前に

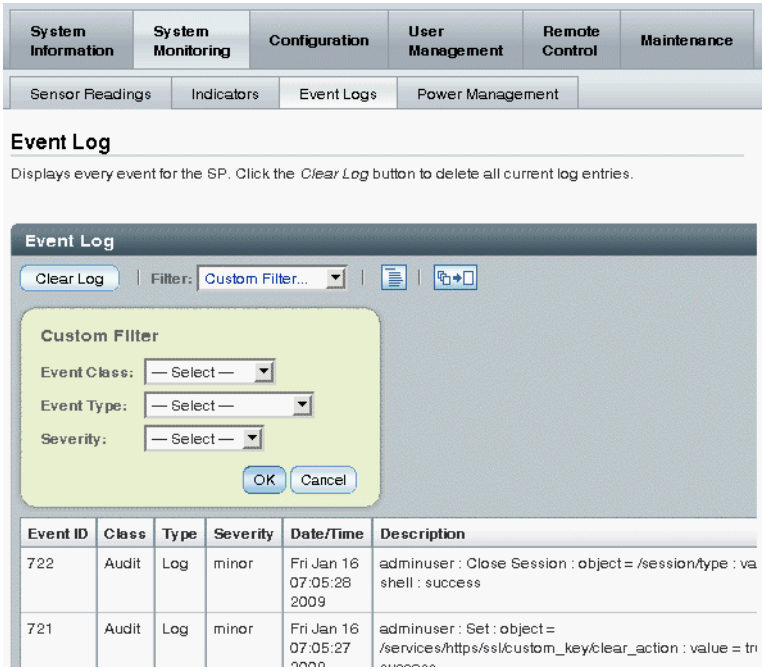
- イベントログ出力をフィルタリングするには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、イベントログ出力をフィルタリングします。

1. ILOM Web インタフェースにログインします。
2. 「System Monitoring」-->「Event Logs」を選択します。

   「Event Log」ページが表示されます。
3. 「Event Log」ページで、次のいずれかの標準フィルタを選択します。
   - All Events
   - Class: Fault
   - Type: Action
   - Severity: Down
   - Severity: Critical

4. または、次の図に示すカスタム出力フィルタのいずれかを選択することもできます。



次の表に、各フィルタに使用できるオプションを示します。

イベントクラス	イベントの種類	Severity
Developer	Log	Debug
Email	Connection	Down
Captive Shell	Send	Critical
Backup	Command Entered	Major
Restore	State	Minor
Reset	Action	
Chassis	Fault	
Audit	Repair	
IPMI	Warning	
Fault		
System		
ActDir		

▼ ILOM イベントログの表示およびクリア

作業を開始する前に

- イベントログを表示またはクリアするには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、ILOM イベントログを表示およびクリアします。

1. **ILOM Web インタフェースにログインします。**
2. **「System Monitoring」-->「Event Logs」を選択します。**

   「Event Log」ページが表示されます。
3. **「Event Logs」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 − 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。 • Fault/Fault − 障害管理の障害。説明には、障害が検出された時刻と疑われる部品が表示されます。 • Fault/Repair − 障害の修復用。説明には部品が表示されます。
Severity	「Debug」、「Down」、「Critical」、「Major」、または「Minor」。
Date/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。
Description	イベントの説明。

- **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」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。

▼ 遠隔 syslog 受信側の IP アドレスを設定する

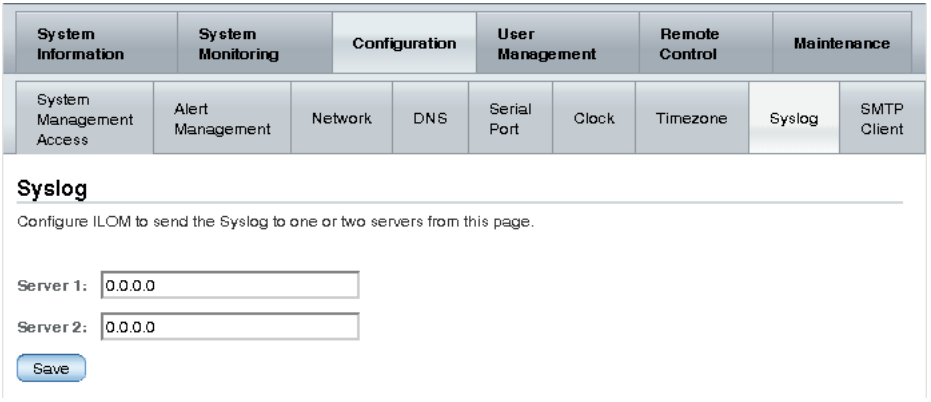
作業を開始する前に

- 遠隔 syslog 受信側の IP アドレスを設定するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、遠隔 syslog 受信側の IP アドレスを設定します。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「Syslog」を選択します。

   「Syslog」ページが表示されます。



3. 「Server 1」および「Server 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。
4. 「Save」をクリックして設定を有効にします。

▼ 障害の状態を表示する

作業を開始する前に

- 障害の状態を表示するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、障害の状態を表示します。

1. **ILOM Web インタフェースにログインします。**
2. **「Fault Management」タブを選択します。**

   「Fault Management」ページには、障害の発生した部品のリストが、ID、FRU、およびタイムスタンプごとに表示されます。障害の発生した部品の ID をクリックすると、障害の発生した部品に関する追加情報にアクセスできます。
3. **または、ILOM Web インタフェースの「Component Management」ページで、部品の障害の状態を識別できます。**

   a. **「Components」タブを選択します。**

   b. **部品の名前をクリックして障害の状態を表示します。**

      次の図のように、部品の状態が個別のウィンドウに表示されます。

View component name and information.

/SYS

Property	Value
type	Host System
ipmi_name	/SYS
fault_state	OK
power_state	Off

システムで提供されている ILOM 障害管理機能の詳細は、サーバ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。

▼ システムの問題を診断するための SP データの収集

作業を開始する前に

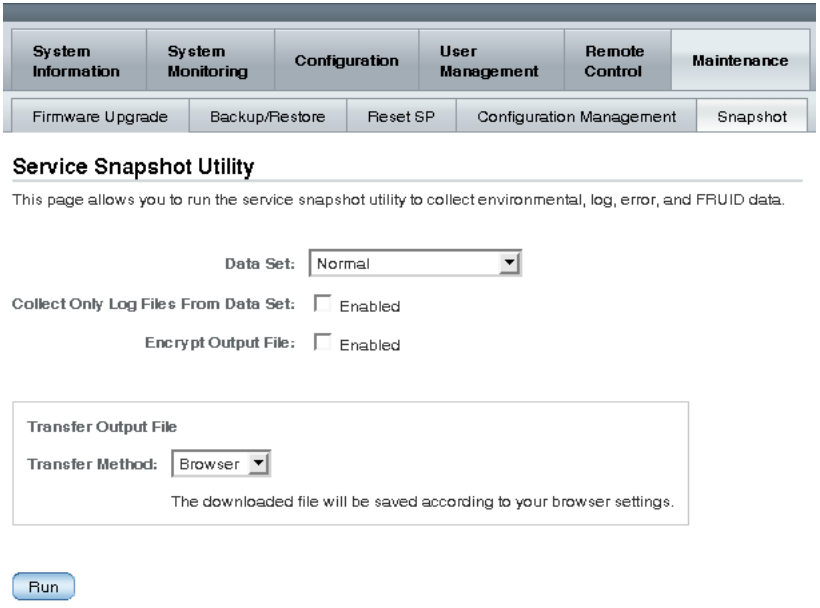
- サービススナップショットユーティリティーを使用して SP データを収集するには、Admin（a）の役割を有効にする必要があります。

注意 – ILOM サービススナップショットユーティリティーの目的は、保守担当者がシステムの問題の診断に使用するデータを収集することです。保守担当者からの依頼がないかぎり、ユーザーはこのユーティリティーを決して実行しないでください。

次の手順に従って、サービススナップショットユーティリティーを実行します。

1. ILOM Web インタフェースにログインします。
2. 「Maintenance」-->「Snapshot」を選択します。

   「Service Snapshot Utility」ページが表示されます。



3. 目的のデータセット (「Normal」、「Full」、または「Custom」) を選択します。
   - **Normal** − ILOM、オペレーティングシステム、およびハードウェアの各情報を収集することを指定します。
   - **Full** − すべてのデータを収集することを指定します。「Full」を選択すると、システムがリセットされる場合があります。
   - **Custom** − 次の 1 つまたは複数のデータセットを選択することができます。
     - ILOM データ
     - ハードウェアデータ
     - 基本 OS データ
     - 診断データ
4. データセットからログファイルだけを収集する場合は、「Enabled」チェックボックスをクリックします。
5. 出力ファイルを暗号化する場合は、「Enabled」チェックボックスをクリックします。
6. 次のいずれかの出力ファイル転送方法を選択します。
   - Browser
   - SFTP
   - FTP
7. 「Run」をクリックします。
   「Save As」ダイアログボックスが表示されます。
8. このダイアログボックスで、ファイルを保存するディレクトリとそのファイル名を指定します。
9. 「OK」をクリックします。
   指定したディレクトリにファイルが保存されます。

第8章

システム警告の管理

項目

説明	リンク
準備すべき事柄を確認する	• 82 ページの「作業を開始する前に」
警告ルールの設定を管理する	• 82 ページの「警告ルールの作成または編集」 • 84 ページの「警告ルールの無効化」
テスト警告を生成して警告の設定が機能していることを確認する	• 84 ページの「テスト警告の生成」
電子メールを使用してシステム警告を受信者に通知する	• 85 ページの「SMTP クライアントの有効化」

関連項目

ILOM	章または節	ガイド
• 概念	• システム監視と警告管理	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• システム警告の管理	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• SNMP	• 警告の管理	『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

警告ルールの設定の管理

項目	
説明	**リンク**
準備すべき事柄を確認する	• 82 ページの「作業を開始する前に」
警告ルールの設定を管理する	• 82 ページの「警告ルールの作成または編集」 • 84 ページの「警告ルールの無効化」 • 84 ページの「テスト警告の生成」

作業を開始する前に

- 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を ILOM で設定する必要があります。送信電子メールサーバ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 ユーザーは SNMP 警告メッセージを復号化できません。
- モジュラーシャーシシステムを使用している場合は、サーバ SP の警告ルール設定を CMM Web インタフェースから管理できます。CMM からサーバ 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 SP (ブレード) を選択してから、ページの右フレームで「Configuration」-->「Alert Management」をクリックします。

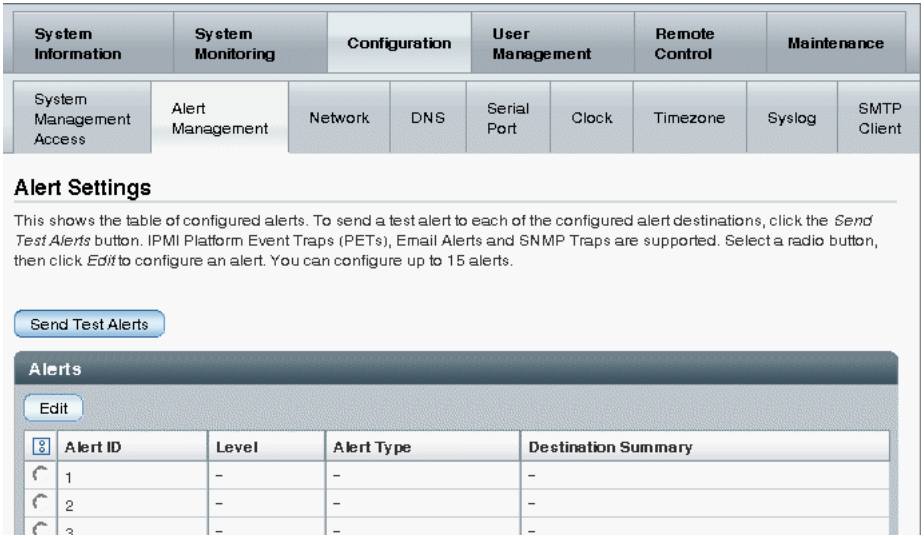
▼ 警告ルールの作成または編集

作業を開始する前に

- 警告ルールを作成または編集するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、警告ルールを設定します。

1. **ILOM Web インタフェースにログインします。**
2. **「Configuration」-->「Alert Management」を選択します。**
   「Alert Settings」ページが表示されます。



3. 「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」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、『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』の「警告管理について」を参照してください。

   d. 「Save」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。

▼ 警告ルールの無効化

作業を開始する前に

- 警告ルールを無効にするには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、警告ルールを無効にします。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「Alert Management」を選択します。
   「Alert Settings」ページが表示されます。
3. 「Alert Settings」ページで、無効に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」を選択します。
   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。
4. このプロパティーダイアログボックスで、「Alert Levels」ドロップダウンリストボックスの「Disabled」を選択します。
5. 「Save」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。

▼ テスト警告の生成

作業を開始する前に

- テスト警告を生成するには、Admin (a) の役割を有効にする必要があります。
- 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。

次の手順に従って、テスト警告を生成します。

1. ILOM Web インタフェースにログインします。
2. 「Configuration」-->「Alert Management」を選択します。
   「Alert Settings」ページが表示されます。
3. 「Alert Settings」ページで、「Send Test Alert」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。

電子メール通知警告用の SMTP クライアントの設定

項目	
説明	リンク
電子メールを使用してシステム警告を受信者に通知する	• 85 ページの「SMTP クライアントの有効化」

▼ SMTP クライアントの有効化

作業を開始する前に

- SMTP クライアントを有効にするには、Admin (a) の役割を有効にする必要があります。
- 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前に、電子メール通知を処理する送信 SMTP 電子メールサーバの IP アドレスとポート番号を確認してください。

次の手順に従って、SMTP クライアントを有効にします。

1. **ILOM Web インタフェースにログインします。**
2. **「Configuration」-->「SMTP Client」を選択します。**
   「SMTP Client」ページが表示されます。
3. **「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 電子メールサーバのポート番号を入力します。

4. **「Save」をクリックして、SMTP 設定を適用します。**

第9章

消費電力の監視

項目

説明	リンク
消費電力インタフェースを監視する	• 88 ページの「システムの消費電力の監視」 • 89 ページの「個々の電源装置の消費電力を監視する」

関連項目

ILOM	章または節	ガイド
• 概念	• 消費電力管理インタフェース	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• 消費電力の管理	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• SNMP	• 消費電力の管理	『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

消費電力インタフェースの監視

項目	
説明	**リンク**
電源装置の消費電力を監視する	• 88 ページの「システムの消費電力の監視」 • 89 ページの「個々の電源装置の消費電力を監視する」

この章では、使用可能な電源管理インタフェースによって消費電力を監視する方法について説明します。消費電力の監視に関する用語は、『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』の「電源監視の用語」の節で定義されています。

注 – この章で説明する消費電力インタフェースは、使用しているプラットフォームによっては、実装されている場合と実装されていない場合があります。実装の詳細については、プラットフォーム固有の ILOM の補足マニュアルまたはプロダクトノートを参照してください。これらの資料は、システムに付属のマニュアルセットに含まれています。

▼ システムの消費電力の監視

作業を開始する前に

- システムの消費電力を表示するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、システムの消費電力を表示します。

1. **ILOM Web インタフェースにログインします。**
2. **「System Monitoring」-->「Power Management」を選択します。**

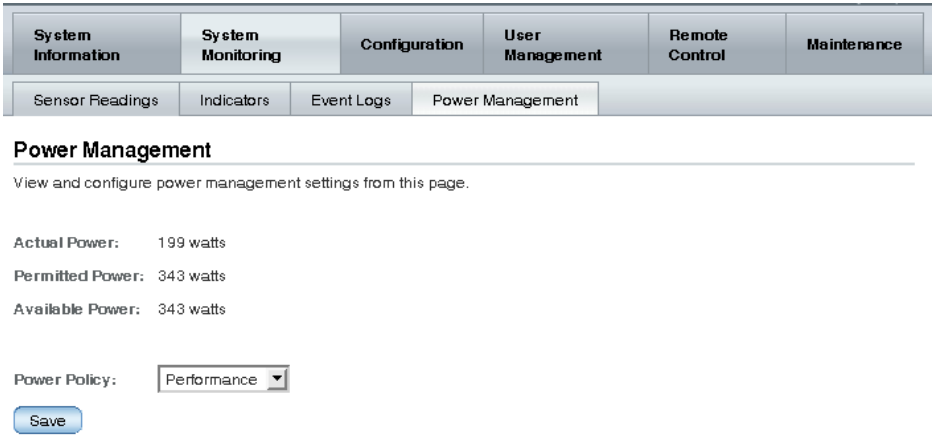
   「Power Management」ページが表示されます。

注 – 電力の監視機能は、この機能のサーバプラットフォームへの実装によって異なります。詳細および手順については、プラットフォーム固有の ILOM 補足マニュアルを参照してください。

---

3. 「Power Management」ページで、実電力、許容電力、および使用可能電力を表示できます。

   これらの電力監視に関する用語については、『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』の「電源監視の用語」を参照してください。



▼ 個々の電源装置の消費電力を監視する

作業を開始する前に

個々の電源の消費電力を監視するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、個々の電源の消費電力を表示します。

- センサーの表示手順については、71 ページの「センサー測定値を表示する」を参照してください。

第 10 章

ILOM 設定のバックアップおよび復元

項目

説明	リンク
ILOM 設定のバックアップ	• 92 ページの「ILOM 設定のバックアップ」
ILOM 設定の復元	• 94 ページの「ILOM 設定を復元する」
ILOM 設定をデフォルト設定にリセットする	• 100 ページの「ILOM 設定をデフォルトにリセットする」

関連項目

ILOM	章または節	ガイド
• 概念	• 設定の管理とファームウェアの更新	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• ILOM 設定のバックアップおよび復元	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

ILOM 設定のバックアップ

項目

説明	リンク
ILOM 設定のバックアップ	• 92 ページの「ILOM 設定のバックアップ」

▼ ILOM 設定のバックアップ

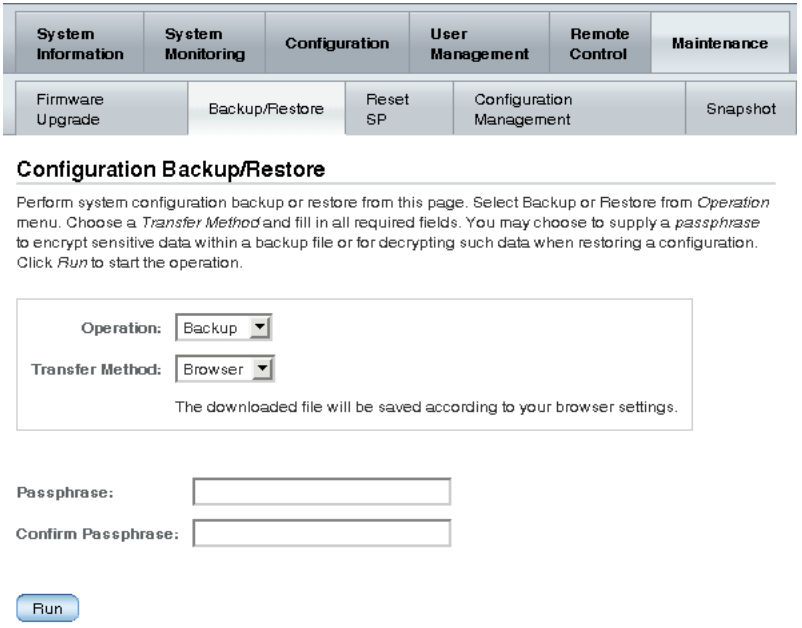
作業を開始する前に

- ILOM 設定をバックアップするには、Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、および Read Only (o) の役割を有効にする必要があります。
- 上記の役割を持たないユーザーアカウントを使用すると、作成される設定バックアップファイルに ILOM SP 設定のすべてのデータが含まれなくなる場合があります。

次の手順に従って、ILOM 設定をバックアップします。

1. ILOM Web インタフェースにログインします。
2. 「Maintenance」-->「Backup/Restore」を選択します。

   「Configuration Backup/Restore」ページが表示されます。



3. 「Operation」ドロップダウンリストから「Backup」を選択します。

4. 「Transfer Method」ドロップダウンリストから転送方法を選択します。

   次の転送方法を使用できます。

   - Browser
   - TFTP
   - FTP
   - SFTP
   - SCP
   - HTTP
   - HTTPS

5. 「Browser」転送方法を選択すると、バックアップファイルはブラウザの設定に従って保存されます。

6. 「TFTP」転送方法を選択すると、次の図に示すプロンプトが表示され、次の情報を入力する必要があります。

   - **Host** – 遠隔ホストの IP アドレスか、DNS を設定している場合は遠隔ホストの名前を入力します。
   - **Filepath** – 設定ファイルの保存先のパスを `directoryPath/filename` 形式で入力します。

7. 「SCP」、「FTP」、「SFTP」、「HTTP」、または「HTTPS」転送方法を選択すると、次の図に示すプロンプトが表示され、次の情報を入力する必要があります。

   - **Host** – 遠隔ホストの IP アドレスか、DNS を設定している場合は遠隔ホストの名前を入力します。
   - **Filepath** – 設定ファイルの保存先のパスを `directoryPath/filename` 形式で入力します。
   - **Username** – リモートシステムでのアカウントのユーザー名を入力します。
   - **Password** – リモートシステムでのアカウントのパスワードを入力します。

8. **パスワード、SSH 鍵、証明書などの機密データをバックアップする場合は、パスフレーズを入力する必要があります。「Passphrase」フィールドにパスフレーズを入力し、「Confirm Passphrase」フィールドにパスフレーズを確認入力します。**

   パスフレーズを入力しないと、機密データはバックアップされません。

9. **バックアップ操作を開始するには、「Run」をクリックします。**

   バックアップ操作が実行されます。

注 – バックアップ操作の実行中は、ILOM SP 上のセッションが一時的に停止します。バックアップ操作が完了すると、セッションは正常動作を再開します。通常、バックアップ操作が完了するには 2 から 3 分かかります。

ILOM 設定の復元

項目	
説明	**リンク**
ILOM 設定の復元	• 94 ページの「ILOM 設定を復元する」 • 97 ページの「バックアップ XML ファイルの編集」

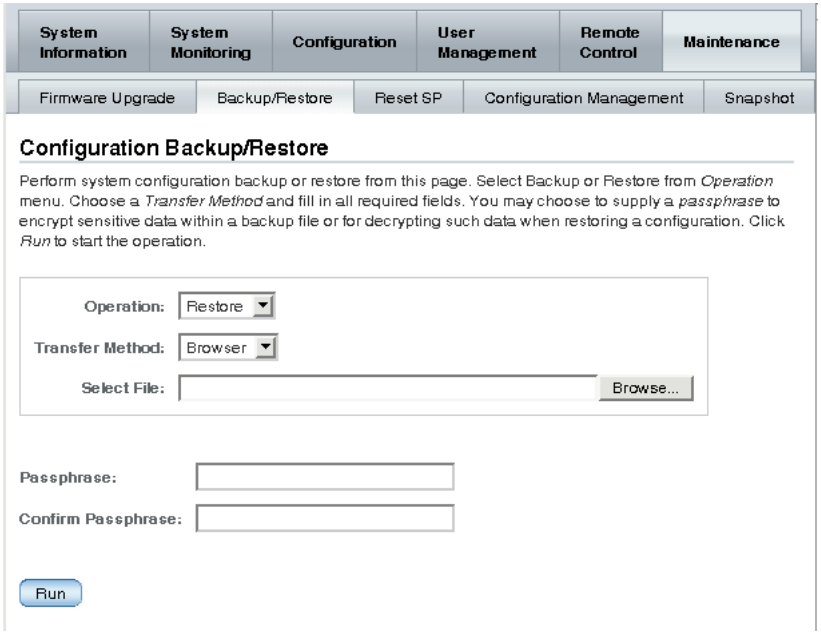
▼ ILOM 設定を復元する

作業を開始する前に

- ILOM 設定を復元するには、Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、および Read Only (o) の役割を有効にする必要があります。
- 上記の役割を持たないユーザーアカウントを使用すると、設定ファイルの一部の情報が復元されない場合があります。復元操作の実行時には、バックアップファイルの作成に使用したユーザーアカウントの権限と同じかそれ以上の権限を持つユーザーアカウントを使用してください。権限が少ないと、バックアップされている設定データの一部が復元されない場合があります。復元されないすべての設定プロパティーは、イベントログに示されます。したがって、イベントログを確認することにより、すべての設定プロパティーが復元されたことを検証できます。

次の手順に従って、ILOM 設定を復元します。

1. ILOM Web インタフェースにログインします。
2. 「Maintenance」-->「Backup/Restore」を選択します。
   「Configuration Backup/Restore」ページが表示されます。
3. 「Operation」ドロップダウンリストから「Restore」を選択します。
   復元操作に使用される「Configuration Backup/Restore」ページが表示されます。



4. 「Transfer Method」ドロップダウンリストから転送方法を選択します。
   次の転送方法を使用できます。
   - Browser
   - TFTP
   - FTP
   - SFTP
   - SCP
   - HTTP
   - HTTPS
5. 「Browser」転送方法を選択する場合は、バックアップファイルのディレクトリパスまたはファイル名を入力するか、「Browse」ボタンをクリックしてバックアップファイルの位置を指定します。

6. **「TFTP」転送方法を選択すると、次の図に示すプロンプトが表示され、次の情報を入力する必要があります。**
   - **Host** − 遠隔ホストの IP アドレスか、DNS を設定している場合は遠隔ホストの名前を入力します。
   - **Filepath** − 設定ファイルの保存先のパスを `directoryPath/filename` 形式で入力します。

7. **「SCP」、「FTP」、「SFTP」、「HTTP」、または「HTTPS」転送方法を選択すると、次の図に示すプロンプトが表示され、次の情報を入力する必要があります。**
   - **Host** − 遠隔ホストの IP アドレスか、DNS を設定している場合は遠隔ホストの名前を入力します。
   - **Filepath** − 次の形式で、設定ファイルのパスを入力します。
     `directoryPath/filename`
   - **Username** − リモートシステムでのアカウントのユーザー名を入力します。
   - **Password** − リモートシステムでのアカウントのパスワードを入力します。

8. **バックアップファイルの作成時にパスフレーズが入力されている場合は、「Passphrase」フィールドにパスフレーズを入力し、「Confirm Passphrase」フィールドにパスフレーズを確認入力します。**
   パスフレーズは、バックアップファイルの作成時に使用したパスフレーズと同じである必要があります。
9. **復元操作を開始するには、「Run」をクリックします。**
   復元操作が実行されます。

注 – 復元操作の実行中は、ILOM SP 上のセッションが一時的に停止します。復元操作が完了すると、セッションは正常動作を再開します。通常、復元操作が完了するには 2 から 3 分かかります。

▼ バックアップ XML ファイルの編集

作業を開始する前に

- バックアップされた XML ファイルを別のシステムで使用する前に、ファイルを編集して、IP アドレスなどの特定のシステムに固有の情報をすべて削除する必要があります。

バックアップされた XML ファイルの例を次に示します。ファイルの内容は、この手順に合わせて省略されています。

```
<SP_config version="3.0">
<entry>
<property>/SP/check_physical_presence</property>
<value>false</value>
</entry>
<entry>
<property>/SP/hostname</property>
<value>labysystem12</value>
</entry>
<entry>
<property>/SP/system_identifier</property>
<value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0, r32722
</value>
</entry>
.
.
.
<entry>
<property>/SP/clock/datetime</property>
<value>Mon May 12 15:31:09 2008</value>
</entry>
.
.
.
<entry>
<property>/SP/config/passphrase</property>
<value encrypted="true">89541176be7c</value>
</entry>
.
.
.
<entry>
<property>/SP/network/pendingipaddress</property>
<value>1.2.3.4</value>
</entry>
.
.
```

```
.
<entry>
<property>/SP/network/commitpending</property>
<value>true</value>
</entry>
.
.
.
<entry>
<property>/SP/services/snmp/sets</property>
<value>enabled</value>
</entry>
.
.
.
<entry>
<property>/SP/users/john/role</property>
<value>aucro</value>
</entry>
<entry>
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
</SP_config>
```

1. **この XML ファイルの例で、次の点を確認します。**
   - パスワードとパスフレーズ以外の設定情報は平文です。
   - ファイルの最初の設定エントリである `check_physical_presence` プロパティーは、`false` に設定されています。デフォルト設定は `true` なので、この設定はデフォルトの ILOM 設定が変更されていることを表しています。
   - `pendingipaddress` と `commitpending` の設定は、各サーバに固有であるため、復元操作でバックアップ XML ファイルを使用する前に削除しなければならない設定の例です。
   - ユーザーアカウントの `john` には、`a`、`u`、`c`、`r`、`o` の役割が設定されています。デフォルトの ILOM 設定ではユーザーアカウントが設定されていないため、このアカウントはデフォルトの ILOM 設定が変更されていることを表しています。
   - SNMPの `sets` プロパティーは、enabled に設定されています。デフォルト設定は disabled です。

2. **平文の設定情報を変更するには、値を変更するか、新しい設定情報を追加します。**

   たとえば、次のように入力します。

   - ユーザー john に割り当てられている役割を変更するには、テキストを次のように変更します。

```
<entry>
<property>/SP/users/john/role</property>
<value>auo</value>
</entry>
<entry>
```

   - 新しいユーザーアカウントを追加し、そのアカウントに a、u、c、r、o の役割を割り当てるには、ユーザー john のエントリのすぐ下に次のテキストを追加します。

```
<entry>
<property>/SP/users/bill/role</property>
<value>aucro</value>
</entry>
<entry>
```

   - パスワードを変更するには、encrypted="true" 設定と暗号化されたパスワード文字列を削除し、パスワードを平文で入力します。たとえば、ユーザー john のパスワードを変更するには、テキストを次のように変更します。

```
<entry>
<property>/SP/users/john/password</property>
<value>newpassword</value>
</entry>
```

3. **バックアップ XML ファイルに変更を加えたら、同じシステムや別のシステムでの復元操作に使用できるようにファイルを保存します。**

ILOM 設定のリセット

項目

説明	リンク
ILOM 設定をデフォルト設定にリセットする	• 100 ページの「ILOM 設定をデフォルトにリセットする」

▼ ILOM 設定をデフォルトにリセットする

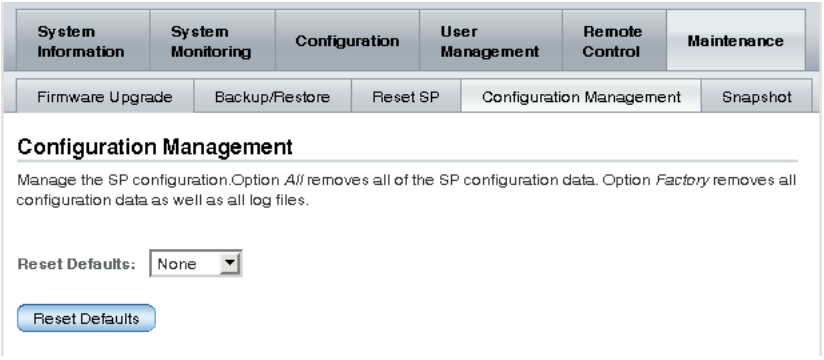
作業を開始する前に

- ILOM 設定をデフォルトにリセットするには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、ILOM 設定をデフォルトにリセットします。

1. ILOM Web インタフェースにログインします。
2. 「Maintenance」-->「Configuration Management」を選択します。

   「Configuration Management」ページが表示されます。



3. 「Reset Defaults」ドロップダウンリストから次のいずれかのオプションを選択して、「Reset Defaults」をクリックします。
   - **All** – ログファイル以外のすべての ILOM 設定データをデフォルト設定にリセットする場合は、「Reset Defaults」ドロップダウンリストから「All」を選択して、「Reset Defaults」をクリックします。ILOM SP が次に再起動するとき、設定がデフォルト設定に復元されます。
   - **Factory** – すべての ILOM 設定データをデフォルト設定にリセットし、ログファイルも消去する場合は、「Reset Defaults」ドロップダウンリストから「Factory」を選択して、「Reset Defaults」をクリックします。ILOM SP が次に再起動するとき、設定がデフォルト設定に復元され、ログファイルが消去されます。
   - **None** – 直前に発行されたデフォルト設定へのリセット操作を取り消すには、「Reset Defaults」ドロップダウンリストから「None」を選択して、「Reset Defaults」をクリックします。ILOM SP の再起動前に「None」オプションが実行された場合のみ、前に発行されたデフォルトへのリセット操作が取り消されます。

第 11 章

ILOM ファームウェアの更新

項目

説明	リンク
準備すべき事柄を確認する	• 102 ページの「作業を開始する前に」
ILOM ファームウェアの更新	• 103 ページの「ILOM ファームウェアバージョンの識別」 • 103 ページの「SPARC ベースのシステムに新しいファームウェアをダウンロードする」 • 103 ページの「ファームウェアイメージの更新」 • 105 ページの「ファームウェア更新時のネットワーク障害から回復する」
ILOM SP のリセット	• 106 ページの「ILOM SP のリセット」

関連項目

ILOM	章または節	ガイド
• 概念	• 設定の管理とファームウェアの更新	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• ILOM ファームウェアの更新	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

ファームウェアの更新

項目

説明	リンク
準備すべき事柄を確認する	• 102 ページの「作業を開始する前に」
ILOM ファームウェアの更新	• 103 ページの「ILOM ファームウェアバージョンの識別」 • 103 ページの「SPARC ベースのシステムに新しいファームウェアをダウンロードする」 • 103 ページの「ファームウェアイメージの更新」 • 105 ページの「ファームウェア更新時のネットワーク障害から回復する」

作業を開始する前に

この節の手順を実行する前に、次の要件を確認してください。

- システム上で現在動作している ILOM のバージョンを識別します。
- プラットフォームの製品 Web サイトから、使用しているサーバまたは CMM のファームウェアイメージをダウンロードします。
- サポートされているプロトコル (TFTP、FTP、HTTP、HTTPS) を使用してファームウェアイメージをサーバにコピーします。CLI で更新する場合は、ローカルサーバにイメージをコピーします。Web インタフェースで更新する場合は、Web ブラウザが動作しているシステムにイメージをコピーします。
- プラットフォームで必要になる場合は、サーバ SP のファームウェアを変更する前に、ホストオペレーティングシステムを停止します。
- Admin (a) 役割のアカウント権限をもつ ILOM ユーザー名とパスワードを取得します。システム上でファームウェアを更新するには、Admin (a) 権限が必要です。
- ファームウェアの更新プロセスの完了には、約 6 分かかります。この間、ほかの ILOM タスクを実行しないでください。ファームウェアの更新が完了すると、システムが再起動します。

▼ ILOM ファームウェアバージョンの識別

作業を開始する前に

- ファームウェアのバージョンを識別するには、Read Only (o) の役割を有効にする必要があります。

次の手順に従って、ファームウェアのバージョンを識別します。

1. ILOM Web インタフェースにログインします。
2. 「User Management」-->「Versions」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。

▼ SPARC ベースのシステムに新しいファームウェアをダウンロードする

1. http://primeserver.fujitsu.com/sparcenterprise/download/firmware/ を参照します。
2. 使用しているサーバ用の最新のファームウェアアップデートを選択します。
3. ファームウェアの使用条件を確認し、「Accept」をクリックします。
4. 「Download」をクリックして zip ファイルパッケージをダウンロードします。
5. zip パッケージを、使用しているネットワークからアクセス可能な TFTP サーバに保存します。
6. zip ファイルパッケージを解凍します。
7. 103 ページの「ファームウェアイメージの更新」に進みます。

▼ ファームウェアイメージの更新

作業を開始する前に

- ILOM ファームウェアを更新するには、Admin (a) の役割を有効にする必要があります。
- プラットフォームで必要になる場合は、サーバ SP のファームウェアを更新する前に、ホストオペレーティングシステムを停止します。
- ホストオペレーティングシステムを正常に停止するには、ILOM Web インタフェースで「`Remote Power Controls`」->「`Graceful Shutdown and Power Off`」オプションを使用するか、ILOM CLI から `stop /SYS` コマンドを発行します。

次の手順に従って、ファームウェアイメージを更新します。

1. ILOM Web インタフェースにログインします。
2. 「Maintenance」-->「Firmware Upgrade」を選択します。

   「Firmware Upgrade」ページが表示されます。
3. 「Firmware Upgrade」ページで、「Enter Upgrade Mode」をクリックします。

   更新プロセスが完了すると、ログインしているほかのユーザーのセッションが切断されることを示す「Upgrade Verification」ダイアログが表示されます。
4. 「Upgrade verification」ダイアログで、「OK」をクリックして続行します。

   「Firmware Upgrade」ページが表示されます。
5. 「Firmware Upgrade」ページで、次の操作を実行します。

   a. 次のいずれかの手順を実行して、イメージの位置を指定します。

      - 「Browse 」をクリックして、インストールするファームウェアイメージの位置を選択します。
      - 使用しているシステムでサポートされている場合は、「Specify URL」をクリックします。ファームウェアイメージの位置を示す URL をテキストボックスに入力します。

   b. 「Upload」ボタンをクリックして、ファイルをアップロードし検証します。

      ファイルがアップロードされ検証されるまで待ちます。

      「Firmware Verification」ページが表示されます。
6. 「Firmware Verification」ページで、次のいずれかのオプションを有効にします。

   - **Preserve Configuration** − ILOM の既存の設定を保存して、更新プロセスの完了後に復元する場合は、このオプションを有効にします。
   - **Delay BIOS upgrade until next server poweroff** − システムが次に再起動するまで BIOS アップグレードを延期する場合は、このオプションを有効にします。

注 – 「Delay BIOS upgrade」オプションは、x64 システム上でファームウェアを ILOM 3.0 以降へ更新する場合にのみ表示されます。

---

7. 「Start Upgrade」をクリックして、アップグレードプロセスを開始するか、「Exit」をクリックしてプロセスを取り消します。

   「Start Upgrade」をクリックすると、アップグレードプロセスが開始され、プロセスの続行を確認するプロンプトが表示されます。

8. **プロンプトで「OK」をクリックして続行します。**

   「Update Status」ページが表示され、更新の進捗状況が表示されます。更新の進捗状況が 100% を示すと、ファームウェアの更新は完了です。

   アップロードが完了すると、システムが自動的に再起動します。

注 – 更新の完了後、ILOM Web インタフェースが正しく再表示されないことがあります。ILOM Web インタフェースで情報が欠落している場合やエラーメッセージが表示される場合は、更新前のバージョンのキャッシュされているページが表示されている可能性があります。ブラウザのキャッシュをクリアしてブラウザを再表示してから、続行してください。

---

9. **SP (または CMM) の ILOM Web インタフェースに再接続します。「System Information」--> 「Version」を選択して、SP または CMM のファームウェアバージョンが、インストールしたファームウェアイメージのバージョンと一致することを確認します。**

注 – ファームウェアを更新する前に ILOM の設定を保存していない場合、ILOM に再接続するには ILOM の初期セットアップ手順を実行する必要があります。

▼ ファームウェア更新時のネットワーク障害から回復する

ローカルファイルを使用して ILOM Web インタフェース経由でファームウェア更新プロセスを実行しているときにネットワーク障害が発生すると、ILOM は自動的にタイムアウトし、システムを再起動します。

次の手順に従って、ファームウェア更新時のネットワーク障害から回復してください。

1. **ネットワークの問題に対処し、解決します。**
2. **ILOM SP に再接続します。**
3. **ファームウェア更新プロセスを再起動します。**

ILOM SP のリセット

項目

説明	リンク
ILOM SP のリセット	• 106 ページの「ILOM SP のリセット」 • 105 ページの「ファームウェア更新時のネットワーク障害から回復する」

▼ ILOM SP のリセット

ILOM サービスプロセッサ (Service Processor、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。

作業を開始する前に

- SP をリセットするには、Reset and Host Control (r) の役割を有効にする必要があります。
- ILOM/BIOS ファームウェアを更新したら、ILOM SP をリセットする必要があります。

次の手順に従って、ILOM/BIOS ファームウェアの更新後に ILOM SP をリセットします。

1. **ILOM SP Web インタフェースにログインします。**
2. **「Maintenance」-->「Reset SP」を選択します。**

   「Reset Service Processor」ページが表示されます。
3. **「Reset SP」ボタンをクリックします。**

   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

遠隔ホストの管理

項目	
説明	**リンク**
準備すべき事柄を確認する	• 108 ページの「遠隔ホストの管理の準備」
ILOM リモートコンソールの初期セットアップの実行	• 110 ページの「ILOM リモートコントロールのビデオリダイレクトの設定」
ILOM リモートコンソールを使用してホストデバイスをリダイレクトする	• 112 ページの「ILOM リモートコンソールの起動」 • 114 ページの「デバイスのリダイレクトを開始、停止、または再起動する」 • 114 ページの「キーボード入力のリダイレクト」 • 115 ページの「キーボードモードとキー送信オプションを制御する」 • 116 ページの「マウス入力のリダイレクト」 • 117 ページの「ストレージメディアのリダイレクト」 • 118 ページの「新規サーバセッションの追加」 • 119 ページの「ILOM リモートコンソールの終了」
リモートサーバモジュールの電源状態の制御	• 119 ページの「遠隔ホストサーバの電源状態を制御する」
SPARC システムのハードウェア問題の診断	• 120 ページの「SPARC システムの診断を設定する」

関連項目

ILOM	章または節	ガイド名
• 概念	• 遠隔ホスト管理オプション	『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』
• CLI	• 遠隔ホストの管理	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』

ILOM 3.0 の各種マニュアルは、http://primeserver.fujitsu.com/sparcenterprise/manual/ から入手できます。

遠隔ホストの管理の準備

ILOM は、ホストの遠隔管理のために、次のような各種オプションを提供します。

- 電源制御
- 診断設定
- Storage Redirection コマンド行インタフェース (Command-Line Interface、CLI)
- ILOM リモートコンソール

次に説明する準備すべき事柄を確認してください。

作業を開始する前に

この章の手順を開始する前に、次の要件が満たされていることを確認してください。

- ILOM リモートコンソールを使用するには、Admin (a) または Console (c) 役割のアカウントを使用する必要があります。
- ILOM リモートコンソールは、ビデオとシリアルコンソールの 2 つのリダイレクト方法をサポートしています。ビデオリダイレクトは、SPARC プロセッサベースの一部のサーバでサポートされています。シリアルコンソールリダイレクトは、すべての SPARC サーバでサポートされています。
- ILOM リモートコンソールを実行するには、JRE 1.5 以降 (Java 5.0 以降) 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。Java Runtime Environment 1.5 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。
- ILOM リモートコンソールは、次の表に示すオペレーティングシステムとブラウザを搭載したローカルクライアントでサポートされています。

オペレーティングシステム	Web ブラウザ
Solaris (9 および 10)	• Mozilla 1.7.5 以降 • Firefox 1.0 以降
Linux (Red Hat、SuSE、Ubuntu)	• Mozilla 1.7.5 以降 • Firefox 1.0 以降 • Opera 6.x 以降
Microsoft Windows (98、2000、XP、Vista)	• Internet Explorer 6.0 以降 • Mozilla 1.7.5 以降 • Firefox 1.0 以降 • Opera 6.x 以降

ILOM リモートコンソールのビデオリダイレクトを有効にするための初期セットアップタスクの実行

項目	
説明	**リンク**
ILOM リモートコンソールの初期セットアップの実行	• 110 ページの「ILOM リモートコントロールのビデオリダイレクトの設定」

注 – この節で説明する初期セットアップ手順はビデオリダイレクトにのみ適用されます。シリアルコンソールリダイレクトのみを使用する場合、この節で説明する初期セットアップタスクは不要です。この初期セットアップの節をスキップして、111 ページの「ILOM リモートコンソールを使用してリダイレクトを起動する」に進むことができます。

▼ ILOM リモートコントロールのビデオリダイレクトの設定

次の手順に従って、ホストサーバの遠隔管理に関する ILOM の設定を構成します。

1. サーバ SP の ILOM Web インタフェースにログインします。
2. 「Remote Control」-->「KVMS」をクリックします。
   「KVMS Settings」ページが表示されます。

注 – 上の図に示されている「Remote Control」第 2 レベルタブのオプションは、サーバによって異なります。同様に、「KVMS Settings」ページの KVMS 設定オプションは、サーバによって異なります。詳細は、この手順の手順 3 に示されているリモートコントロール設定の説明を参照してください。

---

3. 「KVMS Settings」ページのオプションを使用して、遠隔サーバを管理するための次のリモートコントロール設定を指定します。

リモートコントロール設定	適用対象	操作
KVMS の状態	Video redirection	「Enabled」を選択して、管理対象ホストのキーボード、ビデオ、マウス、およびストレージデバイスのリダイレクトを有効にします。選択を解除したままにすると、KVMS デバイスのリダイレクトは無効になります。
マウスモードの設定	Video redirection	次のいずれかのマウスモード設定を選択します。 • **Absolute** − 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」マウスモードを選択します。「Absolute」がデフォルトです。 • **Relative** − Linux オペレーティングシステムを使用している場合は「Relative」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」モードがサポートされているわけではありません。

ILOM リモートコンソールを使用してリダイレクトを起動する

項目

説明	リンク
準備すべき事柄を確認する	• 112 ページの「作業を開始する前に」
ILOM リモートコンソールを使用してリダイレクトを起動する	• 112 ページの「ILOM リモートコンソールの起動」 • 118 ページの「新規サーバセッションの追加」 • 114 ページの「デバイスのリダイレクトを開始、停止、または再起動する」 • 114 ページの「キーボード入力のリダイレクト」 • 115 ページの「キーボードモードとキー送信オプションを制御する」 • 116 ページの「マウス入力のリダイレクト」 • 117 ページの「ストレージメディアのリダイレクト」 • 119 ページの「ILOM リモートコンソールの終了」

作業を開始する前に

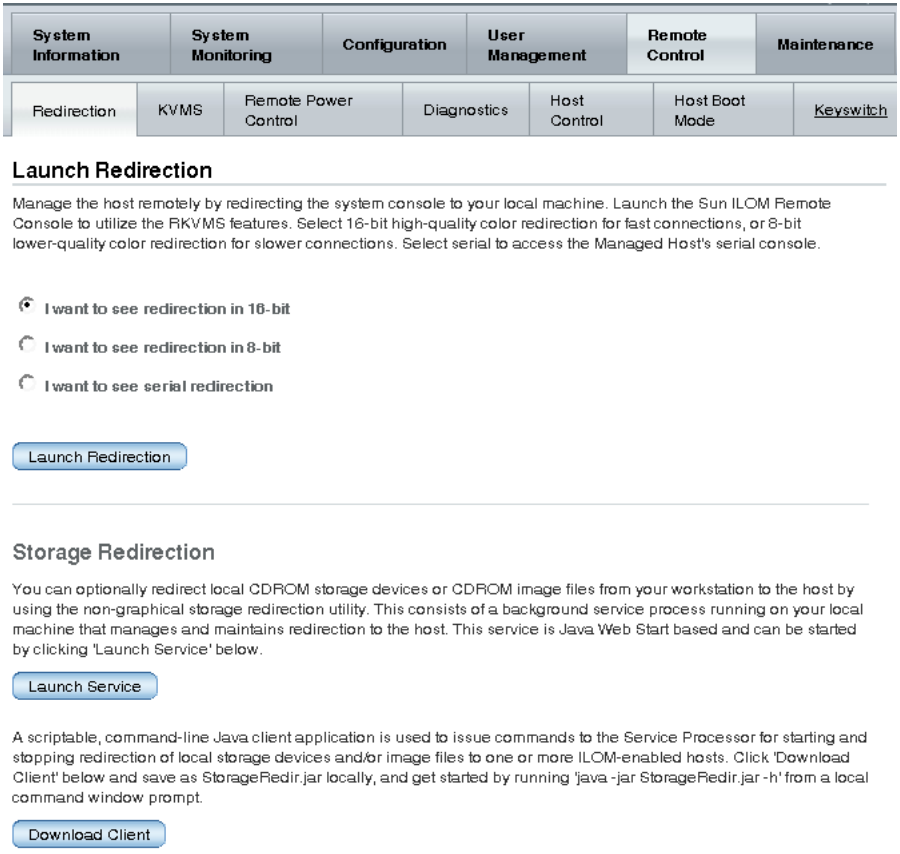
この節の遠隔管理手順を実行する前に、次の要件が満たされている必要があります。

- Java Runtime Environment (1.5 以降) がローカルシステムにインストールされている必要があります。最新の Java Runtime Environment 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。
- Admin (a) または Console (c) 役割のアカウントを使用して ILOM SP Web インタフェースにログインする必要があります。ILOM リモートコンソールを起動するには、Admin 役割または Console 役割のアカウントが必要です。
- ILOM Web インタフェースでリモートコントロール設定を構成済みである必要があります。詳細は、110 ページの「ILOM リモートコントロールのビデオリダイレクトの設定」を参照してください。

▼ ILOM リモートコンソールの起動

1. **サーバ SP の ILOM Web インタフェースにログインします。**
2. **「Remote Control」-->「Redirection」をクリックします。**

   「Launch Redirection」ページが表示されます。



注 – 使用しているプラットフォームによって、「Launch Redirection」ページに表示されるリダイレクトオプションの組み合わせが異なります。複数のオプションが表示されている場合は、このホストを遠隔管理するために使用するリダイレクトの種類を選択します。

---

3. **リダイレクトされたシステムコンソールの表示方法を指定するには、いずれかのラジオボタンをクリックします。**
4. **「Launch Redirection」をクリックします。**
5. **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は、「Run」をクリックして続行します。**

   ILOM リモートコンソールウィンドウが表示されます。

▼ デバイスのリダイレクトを開始、停止、または再起動する

1. ILOM リモートコンソールメニューバーで、「Redirection」をクリックします。
2. 「Redirection」メニューで、次のいずれかのリダイレクトオプションを指定します。

オプション	説明
Start Redirection	「Start Redirection」を選択すると、デバイスのリダイレクションが有効になります。デフォルトでは、「Start Redirection」が有効になっています。
Restart Redirection	「Restart Redirection」を選択すると、デバイスのリダイレクション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ションがまだ確立されている場合に使用します。
Stop Redirection	「Stop Redirection」を選択すると、デバイスのリダイレクションが無効になります。

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」をクリックして続行するか、「No」をクリックして操作を取り消します。**

▼ キーボード入力のリダイレクト

作業を開始する前に

- この手順は、シリアルコンソールリダイレクトにのみ適用されます。
- 複数のユーザーがシステムコンソールに接続できますが、コンソールへの書き込みアクセスを持つことができるのは、一度に 1 人のユーザーだけです (つまり、システムコンソールへのコマンドを入力できるユーザーは 1 人だけです)。ほかのユーザーが入力した文字は無視されます。これは書き込みロックと呼ばれ、その他のユーザーセッションは読み取り専用モードになります。ほかのユーザーがシステムコンソールに現在ログインしていない場合は、キーボードリダイレクトを開始したときに自動的に書き込みロックを得られます。ほかのユーザーがコンソールへの書き込みアクセスを現在持っている場合、それらのセッションの書き込みアクセスを強制的に解除することを要求するプロンプトが表示されます。
- サーバリダイレクトセッションが遠隔ホストサーバ SP に対してアクティブになっている必要があります。詳細は、118 ページの「新規サーバセッションの追加」 を参照してください。
- デバイスのリダイレクトが開始済みである必要があります。詳細は、114 ページの「デバイスのリダイレクトを開始、停止、または再起動する」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のキーボードをリダイレクトします。

1. 「Remote Control」-->「KVMS」を選択します。

   「KVMS Settings」ページが表示されます。

2. 「KVMS Settings」チェックボックスを選択して、キーボードの遠隔管理状態を有効にします。

   KVMS の状態はデフォルトで有効になっています。

▼ キーボードモードとキー送信オプションを制御する

作業を開始する前に

- サーバリダイレクトセッションが遠隔ホストサーバ SP に対してアクティブになっている必要があります。詳細は、118 ページの「新規サーバセッションの追加」を参照してください。
- デバイスのリダイレクトが開始済みである必要があります。詳細は、114 ページの「デバイスのリダイレクトを開始、停止、または再起動する」を参照してください。
- キーボードリダイレクトが有効になっている必要があります。詳細は、114 ページの「キーボード入力のリダイレクト」 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. ILOM リモートコンソールウィンドウで、「Keyboard」メニューをクリックします。
2. 「Keyboard」メニューで、次のキーボード設定を指定します。

オプション	説明
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* *Windows クライアントで使用不可	左側の Alt キーのオンとオフを切り替えるには、「Left Alt Key」を選択します。

Right Alt Key* *Windows クライアントで使用不可	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」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。

注 – シリアルリダイレクト時にこれらのキーボード設定すべてが適用されるわけではありません。

▼ マウス入力のリダイレクト

作業を開始する前に

- マウスリダイレクトは、ビデオリダイレクト設定でのみサポートされます。
- マウス設定を「Absolute」または「Relative」マウスモードに設定します。110 ページの「ILOM リモートコントロールのビデオリダイレクトの設定」を参照してください。
- サーバリダイレクトセッションが遠隔ホストサーバ SP に対してアクティブになっている必要があります。詳細は、118 ページの「新規サーバセッションの追加」 を参照してください。
- デバイスのリダイレクトが開始済みである必要があります。詳細は、114 ページの「デバイスのリダイレクトを開始、停止、または再起動する」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のマウスをリダイレクトします。

1. **「Remote Control」-->「KVMS」を選択します。**

   「KVMS Settings」ページが表示されます。

2. **「KVMS State」チェックボックスを選択して、マウスの遠隔ホスト管理状態を有効にします。**

   「KVMS State」はデフォルトで「Enabled」に設定されています。

▼ ストレージメディアのリダイレクト

作業を開始する前に

- サーバリダイレクトセッションが遠隔ホストサーバ SP に対してアクティブになっている必要があります。詳細は、118 ページの「新規サーバセッションの追加」 を参照してください。
- デバイスのリダイレクトが開始済みである必要があります。詳細は、114 ページの「デバイスのリダイレクトを開始、停止、または再起動する」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、次の操作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、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
```

次の手順に従って、ストレージメディア (CD/DVD または ISO イメージ) をデスクトップからホストサーバにリダイレクトします。

1. ILOM リモートコンソールメニューバーで、「Devices」を選択します。
2. 「Devices」メニューで、次の操作を実行します。
   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。

オプション	説明
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	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	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」を選択します。
Floppy Image	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」を選択します。

注 – フロッピーストレージメディアのリダイレクトは、SPARC システムではサポートされていません。

注 – 配布メディア (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メディアが挿入されていることを確認します。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 イメージが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保存されていることを確認します。

ダイアログが表示され、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ように求められます。

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、次のいずれかの操作を実行します。**

- 「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。
- 「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. **あとでこれらのストレージ設定をホストで再利用するには、「Devices」--> 「Save as Host Default」をクリックします。**

▼ 新規サーバセッションの追加

1. **ILOM リモートコンソールウィンドウで、「Redirection」-->「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、遠隔ホストサーバ 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、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のセッションタブが、ILOM リモートコンソールのタブセットに表示されます。

注 – ログインダイアログでは、新しいセッションをビデオリダイレクト (一部の SPARC システムでサポートされます) とシリアルリダイレクト (現時点ではすべての SPARC システムでサポートされます) のどちらにするかも質問されます。サポートされるリダイレクトの種類の詳細は、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ください。

▼ ILOM リモートコンソールの終了

次の手順に従って、ILOM リモートコンソールを終了し、すべてのリモートサーバセッションを閉じます。

- **ILOM リモートコンソールメニューバーで、「Redirection」-->「Quit」を選択します。**

遠隔ホストの電源状態を制御する

項目

説明	リンク
遠隔ホストサーバの電源状態を制御する	• 119 ページの「遠隔ホストサーバの電源状態を制御する」

▼ 遠隔ホストサーバの電源状態を制御する

作業を開始する前に

- 遠隔ホストサーバの電源状態を制御するには、Admin (a) の役割を有効にする必要があります。

次の手順に従って、遠隔ホストサーバの電源状態を制御します。

1. **サーバ SP の ILOM Web インタフェースにログインします。**
2. **「Remote Power Control」タブをクリックします。**

   「Server Power Control」ページが表示されます。
3. **「Server Power Control」ページから、「Action」メニューで次のいずれかのオプションを選択することにより、ホストサーバの電源状態を遠隔制御できます。**
   - **Reset** – このオプションは、遠隔ホストサーバをただちに再起動します。
   - **Immediate Power Off** – このオプションは、遠隔ホストサーバの電源をただちに切断します。
   - **Graceful Shutdown and Power Off** – このオプションは、遠隔ホストサーバの電源を切る前に OS を正常に停止します。
   - **Power On** (デフォルト) – このオプションは、遠隔ホストサーバの電源を完全に投入します。
   - **Power Cycle** – このオプションは、遠隔ホストサーバの電源をただちに切断し、そのあとで遠隔ホストサーバの電源を完全に投入します。

SPARC システムのハードウェア問題を診断する

項目	
説明	**リンク**
SPARC システムのハードウェア問題の診断	• 120 ページの「SPARC システムの診断を設定する」

▼ SPARC システムの診断を設定する

作業を開始する前に

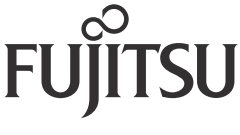
- SPARC プロセッサベースのシステムで診断テストを設定および実行するには、Reset and Host Control (r) の役割を有効にする必要があります。

次の手順に従って、SPARC システムの診断を設定します。

1. **ILOM Web インタフェースにログインします。**
2. **「Remote Control」-->「Diagnostics」を選択します。**
   「Diagnostics」ページが表示されます。
3. **「Trigger」の値を選択します。**
   - **Power On** – 電源投入時に診断を実行します。
   - **User Reset** – ユーザーによるリセット時に診断を実行します。
   - **Error Reset** – エラーによるリセット時に診断を実行します。
4. **各トリガータイプに対する「Verbosity」の値を選択します。**
   - **None** – 診断の実行時には、障害が検出されないかぎり、システムコンソール上に出力は表示されません。
   - **Min** – 診断では、一定限度の量の出力がシステムコンソール上に表示されます (デフォルト値)。
   - **Normal** – 診断では、実行中の各テストの名前や結果など、中程度の量の出力がシステムコンソール上に表示されます。
   - **Debug** – 診断では、テスト中のデバイスや各テストのデバッグ出力など、広範囲のデバッグ出力がシステムコンソール上に表示されます。

5. **各トリガータイプに対する「Level」の値を選択します。**
   - **Min** − システムを検証するための最小限の診断が実行されます。
   - **Max** − システムの健全性を完全に検証するための最大限の診断が実行されます (デフォルト値)。
6. **「Mode」の値を選択します。**
   - **Off** − 診断を実行しません。
   - **Normal** − 診断を実行します (デフォルト値)。
7. **「Save」をクリックして設定を有効にします。**

索引


FUJITSU