FUJITSU

Integrated Lights Out Manager (ILOM) 3.0 概念ガイド

C120-E573-01

FUJITSU

Integrated Lights Out Manager (ILOM) 3.0 概念ガイド

マニュアル番号: C120-E573-01
Part No. 875-4566-10
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 Concepts Guide Manual Code: C120-E573-01EN

目次

はじめに

『Integrated Lights Out Manager (ILOM) 3.0 概念ガイド』には、ILOM をサポートする ラック搭載型サーバやその他のプラットフォームに共通する ILOM の機能が記載されています。ILOM で管理するサーバプラットフォームに関係なく、さまざまなユーザーインタフェースを使用して、これらの ILOM 機能にアクセスし、ILOM タスクを実行することができます。

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「設定の管理とファームウェアの更新」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

ILOM 概要

項目

説明	リンク
ILOM の特長と機能について学習する	• 2 ページの「ILOM とは」 • 2 ページの「ILOM の機能」 • 3 ページの「ILOM の特長と機能」 • 4 ページの「ILOM 3.0 の新機能」 • 5 ページの「ILOM ユーザーアカウントの役割」 • 7 ページの「ILOM のインタフェース」 • 8 ページの「サーバと CMM 上の ILOM」 • 9 ページの「ILOM への初回のログイン」 • 9 ページの「`root` および `default` ユーザーアカウント」 • 10 ページの「インベントリと部品の管理」

関連項目

ILOM	章または節	ガイド
• CLI	• CLI の概要	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• Web インタフェース	• Web インタフェースの概要	『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。

ILOM とは

Integrated Lights Out Manager (ILOM) は、サーバの管理と監視に使用できる高度なサービスプロセッサハードウェアおよびソフトウェアを提供します。ILOM 専用のハードウェアとソフトウェアは、一部のサーバプラットフォームにプリインストールされています。ILOMは、データセンターに不可欠な管理ツールであり、すでにシステムにインストールされているほかのデータセンター管理ツールと統合して使用できます。

ILOM の機能

ILOM を使用すると、オペレーティングシステムの状態とは独立にサーバをアクティブに管理および監視し、信頼性の高い Lights Out Management （LOM) システムを実現できます。ILOM を使用すると、次のことを予防保守的に実行できます。

- ハードウェアのエラーと障害を発生時に認識します。
- サーバの電源状態を遠隔から制御します。
- ホストのグラフィカルコンソールまたはグラフィカルでないコンソールを表示します。
- システム上のセンサーとインジケータの現在の状態を表示します。
- システムのハードウェア構成を確認します。
- IPMI PET 警告、SNMP トラップ警告、または電子メール警告によって、事前にシステムイベントに関して生成された警告を受け取ります。

ILOM サービスプロセッサ (Service Processor、SP) は、組み込まれているオペレーティングシステムで動作し、専用の Ethernet ポートを利用して、帯域外管理機能を実現します。さらに、サーバのホストオペレーティングシステム (Solaris、Linux、および Windows) から ILOM にアクセスできます。ILOM を使用すると、キーボード、モニター、およびマウスをローカルで接続して使用するのと同じように、サーバを遠隔から管理できます。

サーバ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。完全な機能を備えたブラウザベースの Web インタフェースと、それと同等なコマンド行インタフェース (Command-Line Interface、CLI) を利用できます。さらに、業界標準の SNMP インタフェースと IPMI インタフェースも利用できます。

ILOM の特長と機能

ILOM は、ILOM2.x ファームウェア と ILOM3.x ファームウェアのどちらを使用している場合でも、サーバシステムの監視と管理を支援する完全な機能とプロトコルを提供します。

表 1-1 ILOM の特長と機能

ILOM の特長	可能な操作
専用のサービスプロセッサとリソース	• システムリソースを消費することなく、サーバを管理します • サーバ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サーバの管理を続行します
簡略な ILOM 初期設定	• 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 を介して、IP アドレスなど SP を手動で設定します
ファームウェア更新をダウンロード可能	• ブラウザベースの Web インタフェースを通じて、ファームウェア更新をダウンロードします
ハードウェアのリモート監視	• システム状態とイベントログを監視します • 電源装置、ファン、ディスク、CPU、メモリー、マザーボードなど、顧客交換可能ユニット (Customer-Replaceable Unit、CRU) と現場交換可能ユニット (Field-Replaceable Unit、FRU) を監視します • 環境 (部品の温度) を監視します • 電圧や電力などのセンサーを監視します • インジケータ (LED) を監視します
ハードウェアと FRU のインベントリと存在	• インストールされている CRU と FRU およびそのステータスを識別します • パーツ番号、バージョン、および製品シリアル番号を識別します • NIC カードの MAC アドレスを識別します
遠隔アクセス	• シリアルポートや LAN を通じて、システムのシリアルコンソールをリダイレクトします • 一部の SPARC システムでのキーボード、ビデオ、マウス (KVM) へのアクセス • OS のグラフィカルコンソールを遠隔クライアントのブラウザへリダイレクトします • 遠隔の CD/DVD またはフロッピーを遠隔ストレージとしてシステムに接続します
システム電源制御と監視	• ローカルまたは遠隔から、システムの電源を投入または切断します • 緊急停止用に強制的に電源を切断するか、ホストのオペレーティングシステムを正常に停止してから電源を切断します

表 1-1　ILOM の特長と機能 (続き)

ILOM の特長	可能な操作
ユーザーアカウントの設定と管理	• ローカルユーザーアカウントを設定します • LDAP、LDAP/SSL、RADIUS、および Active Directory を使用して、ユーザーアカウントを認証します
エラーと障害の管理	• システムの BIOS、POST、およびセンサーメッセージを監視します • すべての「サービス」のデータにつ • いて、一貫した方法でイベントを記録します • SP ログ、syslog、および遠隔ログホストで報告されるハードウェアとシステムに関連するエラーおよび ECC メモリーエラーを監視します
SNMP トラップ警告、IPMI PET 警告、遠隔 syslog 警告、電子メール警告などのシステム警告	• 業界標準の SNMP コマンドと 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。

ILOM 3.0 の新機能

ILOM 3.0 は、改善されたセキュリティー、改善されたユーザビリティー、およびデータセンター環境との容易な統合など、ILOM 2.x では利用できなかった多くの新しい特徴と機能で強化されています。表 1-2 に、ILOM 3.0 の新機能を示します。

表 1-2　ILOM 3.0 の新機能

カテゴリ	機能
一般的な機能	
	DNS のサポート
	タイムゾーンのサポート
	設定のバックアップと復元
	出荷時のデフォルトの復元
	LDAP と LDAP/SSL のサポートの強化
	Java ベースの遠隔ストレージ CLI
	電源管理機能
	新しい SSH キーを生成する機能

表 1-2　ILOM 3.0 の新機能 (続き)

カテゴリ	機能
スケーラビリティーとユーザビリティー	
	ハードウェア監視情報に対する、CLI および Web インタフェースでユーザー設定可能なフィルタリング
	ホスト名を使用した、LDAP、Active Directory、LDAP/SSL のようなほかのサービスへの名前によるアクセス
セキュリティー	
	より詳細なユーザー役割
	定義済みの `root` アカウントと `default` アカウント
	ユーザー SSH キー認証
	ネットワーク管理ポートを無効にしてシリアルポートのみを使用する機能
	IPMI、SSH、KVMS などの個々のサービスを無効にしてポートを閉じる機能
保守性	
	システム問題を診断するためのデータ収集ユーティリティー

ILOM ユーザーアカウントの役割

ILOM 3.0 では、ユーザー権限を制御するために、ユーザーの役割が実装されています。ただし、下位互換性のために、ILOM 2.x 方式のユーザーアカウント (管理者権限またはオペレータ権限) もサポートされています。

ILOM 3.0 ユーザーアカウントの役割

ILOM 3.0 では、ユーザーアカウントに、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。表 1-3 で、ILOM 3.0 ユーザーアカウントに割り当てることができる役割について説明します。

表 1-3 ILOM 3.0 ユーザーアカウントの役割

役割	定義	権限
a	Admin	Admin (a) 役割が割り当てられたユーザーは、ILOM 設定変数の状態を表示および変更することができます。Admin 役割が割り当てられたユーザーは、User Management、Console、および Reset and Host Control の役割を持つユーザーのタスクを除き、すべての ILOM 機能を実行できます。
u	User Management	User Management (u) 役割が割り当てられたユーザーは、ユーザーアカウントの作成および削除、ユーザーパスワードの変更、ほかのユーザーに割り当てられた役割の変更、および `default` ユーザーアカウントに対する物理アクセス要件の有効化または無効化を実行できます。また、この役割では、LDAP、LDAP/SSL、RADIUS、および Active Directory を設定することもできます。
c	Console	Console (c) 役割が割り当てられたユーザーは、ILOM リモートコンソールおよび SP コンソールにアクセスし、ILOM コンソール設定変数の状態を表示および変更できます。
r	Reset and Host Control	Reset and Host Control (r) 役割が割り当てられたユーザーは、電源制御、リセット、ホットプラグ操作、コンポーネントの有効化と無効化、障害管理など、システムを操作することができます。この役割は、ILOM 2.0 のオペレータ権限を持つユーザーにほぼ対応しています。
o	Read Only	Read Only (o) 役割が割り当てられたユーザーは、ILOM設定変数の状態を表示できますが、変更できません。また、この役割を割り当てられたユーザーは、自分のユーザーアカウントのパスワードとセッションタイムアウト設定を変更できます。
s	Service	Service (s) 役割が割り当てられたユーザーは、オンサイトサービスが必要な場合に保守担当者を補助することができます。

ILOM 2.x ユーザーアカウントのサポート

下位互換性のために、ILOM 3.0 は ILOM 2.x の ユーザーアカウントをサポートしており、ILOM 2.x の Administrator 権限または Operator 権限を持つユーザーは、それらの権限に対応する ILOM 3.0 の役割を付与されます。表 1-4 に、Administrator 権限と Operator 権限を持つユーザーに割り当てられる役割を示します。

表 1-4 ILOM 2.x ユーザーアカウントに付与される ILOM 3.0 の役割

2.x のユーザー権限	付与される ILOM 3.0 のユーザー役割
Administrator	Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、および Read Only (o)
Operator	Console (c)、Reset and Host Control (r)、および Read Only (o) **注 –** Operator 権限を持つユーザーに付与される承認レベルを 2.x の権限と一致させるため、この場合に付与されるConsole (c) 役割は、ILOM リモートコンソール (JavaRConsole) にアクセスできないように変更されます。

ILOM のインタフェース

ILOM のすべての機能にアクセスするには、ブラウザベースの Web インタフェース、コマンド行インタフェース、または業界標準のプロトコルを使用できます。ILOM のインタフェースの詳細は、『ILOM 3.0 手順ガイド』の「概要」の章を参照してください。

ILOM は、機能にアクセスするための、複数のインタフェースをサポートしています。ブラウザベースの Web インタフェース、コマンド行インタフェース、または業界標準のプロトコルを使用できます。

- **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。
- **コマンド行インタフェース (Command-Line Interface、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 DMTF 形式の CLI とスクリプトプロトコルに準拠しています。ILOM は、CLI へのセキュリティー保護されたアクセスのために、SSH v2.0 および v3.0 をサポートしています。CLI を使用すると、既存のスクリプトを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できます。
- **リモートコンソール** – ILOM リモートコンソール (JavaRConsole) を使用すると、SPARC サーバ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。

- **Intelligent Platform Management Interface (IPMI)** – IPMI v1.5 または 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、およびサーバコンソールのリダイレクトを行うことができます。
- **簡易ネットワーク管理プロトコル (Simple Network Management Protocol、SNMP) インタフェース** – ILOM は、第三者のアプリケーション用に SNMP v3.0 インタフェースも提供しています。ILOM 3.0 では、次のような MIB をサポートしています。
  - SUN-PLATFORM-MIB
  - SUN-ILOM-CONTROL-MIB
  - SUN-HW-TRAP-MIB
  - SUN-ILOM-PET-MIB
  - SNMP-FRAMEWORK-MIB (9RFC2271.txt)
  - SNMP-MPD-MIB (RFC2572)
  - SNMPv2-MIB (RFC1907) のシステムグループと SNMP グループ
  - ENTITY-MIB (RFC2737) の entPhysicalTable

ILOM でサポートされ使用される SNMP MIB の完全なリストについては、『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』を参照してください。

サーバと CMM 上の ILOM

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、モジュラーシャーシシステムを使用している場合にはシャーシ監視モジュール (Chassis Monitoring Module、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** – ラック搭載型サーバの SP やサーバモジュールの SP と直接通信すると、個々のサーバの操作を管理することができます。この方法は、サーバモジュールまたはラック搭載型サーバの障害追跡や、データセンター内の特定のサーバ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** – モジュラーシャーシシステムを使用している場合、CMM からシステムを管理すると、ILOM を使用して、モジュラーシャーシシステム全体のコンポーネントを設定して管理したり、個々のサーバモジュールまでドリルダウンして管理したりすることができます。

ILOM への初回のログイン

はじめて ILOM 3.0 にログインする場合、root ユーザーアカウントを使用します。この root ユーザーアカウントについては、ILOM 2.x から ILOM 3.0 への移行で変更はありません。

ILOM のログインとログアウトの詳細と手順については、次のガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

root および default ユーザーアカウント

ILOM 3.0 では、root ユーザーアカウントと default ユーザーアカウントの 2 つのアカウントが事前構成されています。はじめて ILOM にログインするときは、root アカウントを使用します。この root ユーザーアカウントについては、ILOM 2.x から ILOM 3.0 への移行で変更はありません。同じ方法で、root ユーザーアカウントを使用してログインできます。default ユーザーアカウントは、パスワードの復旧に使用するための、ILOM 3.0 の新機能です。

root ユーザーアカウント

root ユーザーアカウントは持続的であり、root アカウントを削除しないかぎり、すべてのインタフェース (Web インタフェース、CLI、SSH、シリアルコンソール、および IPMI) で使用できます。root 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) が提供されます。

ILOM にログインするには、次に示す root アカウントのユーザー名とパスワードを使用します。

ユーザー名: **root**

パスワード: **changeme**

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、システムに取り付けられている各サービスプロセッサ (Service Processor、SP) またはシャーシ監視モジュール (Chassis Monitoring Module、CMM) で、root のパスワード (changeme) を変更します。あるいは、root アカウントを削除して、システムアクセスのセキュリティーを保護することもできます。ただし、root アカウントを削除する前に、新しいユーザーアカウントを設定するか、ディレクトリサービスを設定して、ILOM にログインできるようにする必要があります。

default ユーザーアカウント

default ユーザーアカウントは、パスワードを復旧するために使用します。default ユーザーアカウントはシリアルコンソールでのみ使用できます。default ユーザーアカウントを使用するには、物理的にサーバの前にいることを証明する必要があります。default ユーザーアカウントは、変更または削除できません。

ILOM にログインするための別のユーザーアカウントを設定する前に root アカウントを削除した場合は、代替手段として default アカウントを使用してログインし、root アカウントを再作成できます。root ユーザーアカウントを再作成するには、通常の ILOM ユーザーコマンドを使用して新しいアカウントを作成します。ユーザーアカウントを作成する方法については、『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』の Web インタフェース節または CLI 節の「ユーザーアカウントの追加と権限の割り当て」を参照してください。

パスワードを復旧するには、次のユーザー名とパスワードを使用して、default アカウントを使用してログインします。

ユーザー名: **default**

パスワード: **defaultpassword**

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、部品の取り外しと取り付けおよび部品の有効化と無効化に備えることもできます。これらのタスクを実行する方法については、『ILOM 3.0 手順ガイド』を参照してください。

第2章

ILOM のネットワーク設定

項目

説明	リンク
ILOM のネットワーク管理と接続方法について学習する	• 12 ページの「ILOM のネットワーク管理」
ILOM のネットワーク通信設定とネットワークポート割り当てについて学習する	• 15 ページの「ILOM の通信設定」 • 14 ページの「ネットワークポートの割り当て」

関連項目

ILOM	章または節	ガイド
• 概要	• ILOM への接続 • Web インタフェースを使用した ILOM 初期セットアップ手順 • CLI 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 に対するログインおよびログアウト • 通信設定 • 動的 DNS の設定例	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• Web インタフェース	• ILOM に対するログインおよびログアウト • 通信設定	『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 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。

ILOM のネットワーク管理

サーバまたはシャーシ監視モジュール (Chassis Monitoring Module、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。

専用のネットワーク管理ポートを使用すると、ILOM でサーバプラットフォームを適切に管理することができます。ネットワーク管理ポートを使用すると、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。

ネットワーク管理ポートに接続する方法については、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。

動的 DNS を使用すると、新しく取り付けられた ILOM に対し、システムのシリアル番号に基づいてホスト名と IP アドレスを自動的に割り当てることができます。動的 DNS の概要と設定手順については、付録 A を参照してください。

ILOM の接続方法

ILOM に接続する方法は、サーバ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 2-1 ILOM の接続方法

接続方法	ラック搭載型	ブレード	サポートされているインタフェース	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 のホスト名または IP アドレスが既知である必要があります。
シリアル接続	はい	はい	CLI のみ	シリアル管理ポートに直接接続します。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。

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。

初期設定ワークシート

表 2-2 のワークシートで、ILOM との通信をはじめて確立するために必要な情報を説明します。

表 2-2 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
管理接続-シリアル	任意 – ネットワークを設定するために *DHCP* を使用する場合 必須 – ネットワーク設定が静的である場合、またはネットワークを使用しない場合	SP または CMM とのネットワークを設定するために DHCP サーバを利用しない場合は、サーバまたは 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。 ネットワークを使用しない場合、またはネットワークを設定するために DHCP を使用しない場合は、サーバまたは 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または CMM に接続する方法については、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。
管理接続-Ethernet	任意	サーバまたは CMM の Ethernet ネットワーク管理ポートにローカルエリアネットワークを接続します。接続手順については、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。 DHCP を使用してネットワーク設定を取得するか、静的なネットワーク設定を行うかを決定します。
SP ホスト名の割り当て	任意	わかりやすいホスト名をサーバ SP に割り当てることができます。詳細は、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』または『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』を参照してください。
システム識別子の割り当て	任意	システム識別子 (わかりやすい名前) をサーバに割り当てることができます。詳細は、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』または『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』を参照してください。
動的 DNS の設定	任意	動的 DNS を設定すると、ホスト名を使用してサーバ SP にアクセスできます。動的 DNS の設定手順については、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』を参照してください。

ネットワークポートの割り当て

表 2-3 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。

表 2-3 ILOM のネットワークポート

ポート	プロトコル	用途
一般的なネットワークポート		
80	HTTP over TCP	Web (ユーザー設定可能)
443	HTTPS over TCP	Web (ユーザー設定可能)
22	SSH over TCP	SSH − Secure Shell
69	TFTP over UDP	TFTP − Trivial File Transfer Protocol (送信)
123	NTP over UDP	NTP − Network Time Protocol (送信)
161	SNMP over UDP	SNMP − Simple Network Management Protocol (ユーザー設定可能)
162	IPMI over UDP	IPMI − Platform Event Trap (PET) (送信)
389	LDAP over UDP/TCP	LDAP − Lightweight Directory Access Protocol (送信、ユーザー設定可能)
514	Syslog over UDP	Syslog − (送信)
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 (送信、ユーザー設定可能)
SP ネットワークポート		
5120	TCP	ILOM リモートコンソール: CD
5123	TCP	ILOM リモートコンソール: フロッピーディスク
5121	TCP	ILOM リモートコンソール: キーボードおよびマウス
7578	TCP	ILOM リモートコンソール: ビデオ
CMM ネットワークポート		
8000 - 8023	HTTP over TCP	ILOM ドリルダウン (ブレード)
8400 - 8423	HTTPS over TCP	ILOM ドリルダウン (ブレード)
8200 - 8219	HTTP over TCP	ILOM ドリルダウン (NEM)
8600 - 8619	HTTPS over TCP	ILOM ドリルダウン (NEM)

ILOM の通信設定

ILOM の CLI インタフェース、Web インタフェース、または SNMP を使用して、ネットワーク、シリアルポート、Web、Secure Shell (SSH) 設定などのILOM の通信設定を管理できます。ILOM を使用すると、システムのホスト名、IP アドレス、DNS 設定、およびシリアルポート設定を表示し、設定することができます。また、HTTP または HTTPS による Web アクセスや SSH を有効または無効にすることができます。

ILOM の通信設定を管理するための情報と手順については、次のいずれかのガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

第3章

ユーザーアカウント管理

項目

説明	リンク
ユーザーアカウントと役割の管理について学習する	• 18 ページの「ユーザーアカウントの管理のガイドライン」 • 19 ページの「ユーザーアカウントの役割と権限」
シングルサインオンについて学習する	• 20 ページの「シングルサインオン」
SSH 認証について学習する	• 20 ページの「SSH ホストキーベース認証」
Active Directory について学習する	• 21 ページの「Active Directory」
LDAP について学習する	• 22 ページの「Lightweight Directory Access Protocol」 • 23 ページの「LDAP/SSL」
RADIUS について学習する	• 23 ページの「RADIUS」

関連項目

ILOM	章または節	ガイド
• 概要	• Web インタフェースを使用した ILOM 初期セットアップ手順 • CLI 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	• 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』
• Web インタフェース	• ユーザーアカウントの管理	『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

関連項目

ILOM	章または節	ガイド
• SNMP および IPMI ホスト	• SNMP を使用したユーザーアカウントの管理 • SNMP コマンドリファレンス	『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います。
- アカウントのユーザー名は 8 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。
- ユーザーアカウントにはそれぞれ 1 つまたは複数の詳細な役割が割り当てられ、それによってユーザーアカウントの権限が決定されます。ユーザーアカウントに割り当てられた役割によっては、ILOM Web インタフェース、コマンド行インタフェース (Command-Line Interface、CLI)、または SNMP を使用して、アカウント情報を表示し、さまざまな管理機能を実行することができます。
- ローカルアカウントを設定するか、Active Directory、LDAP、LDAP/SSL、RADIUS などのリモート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。

ユーザーアカウントを管理するための情報と手順については、次のいずれかのガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

ユーザーアカウントの役割と権限

ILOM 3.0 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。ILOM Web インタフェースまたは CLI を使用すると、ユーザーアカウントを管理できます。表 3-1 に、ILOM アカウントに割り当てられた役割を示します。

表 3-1 ILOM 3.0 ユーザーアカウントの役割

役割	定義	権限
a	Admin	Admin (a) 役割が割り当てられたユーザーは、ILOM 設定変数の状態を表示および変更することができます。Admin 役割が割り当てられたユーザーは、User Management、Console、および Reset and Host Control の役割を持つユーザーのタスクを除き、すべての ILOM 機能を実行できます。
u	User Management	User Management (u) 役割が割り当てられたユーザーは、ユーザーアカウントの作成および削除、ユーザーパスワードの変更、ほかのユーザーに割り当てられた役割の変更、および `default` ユーザーアカウントに対する物理アクセス要件の有効化または無効化を実行できます。また、この役割では、LDAP、LDAP/SSL、RADIUS、および Active Directory を設定することもできます。
c	Console	Console (c) 役割が割り当てられたユーザーは、ILOM リモートコンソールおよび SP コンソールにアクセスし、ILOM コンソール設定変数の状態を表示および変更できます。
r	Reset and Host Control	Reset and Host Control (r) 役割が割り当てられたユーザーは、電源制御、リセット、ホットプラグ操作、コンポーネントの有効化と無効化、障害管理など、システムを操作することができます。この役割は、ILOM 2.0 の Operator 権限を持つユーザーにほぼ対応しています。
o	Read Only	Read Only (o) 役割が割り当てられたユーザーは、ILOM 設定変数の状態を表示できますが、変更できません。また、この役割を割り当てられたユーザーは、自分のユーザーアカウントのパスワードとセッションタイムアウト設定を変更できます。
s	Service	Service (s) 役割が割り当てられたユーザーは、オンサイトサービスが必要な場合に保守担当者を補助することができます。

シングルサインオン

シングルサインオン (Single Sign On、SSO) は、ILOM に 1 回ログインするだけで資格を確立できるので、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ことができる、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、SSO 認証サービスを無効にすることを検討してください。

SSH ホストキーベース認証

従来は、SSH キーベース認証で、パスワード認証の自動化が行われていました。SSH キーベースの認証機能が実装される以前は、SSH を使用して ILOM SP にログインするユーザーは、対話式にパスワードを入力する必要がありました。自動パスワード認証機能は、同様の更新が必要なシステムが多数ある場合に非常に便利です。

SSH キーベース認証が提供する主な機能は、次のとおりです。

- アーカイブや分析のためにサービスプロセッサ (Service Processor、SP) のログファイルを自動的にコピーするスクリプトを書くことができます。
- ネットワーク経由の SSH 接続で遠隔システムから自動的または定期的に SP コマンドを実行するスクリプトを書くことができます。

SSH キーベース認証を使用すると、ユーザーの操作を必要とせず、パスワードが書き込まれていないスクリプトを使用して、上記の両方の操作を行うことができます。

SSH キーの使用と処理については、ILOM を使用して、生成したキーを SP 上の各ユーザーアカウントに追加することができます。

SSH キーの追加と削除に関する詳細と手順については、次のいずれかのガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

Active Directory

ILOM では、Microsoft Windows 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。LDAP ディレクトリサービスの実装と同様、Active Directory はユーザー資格の認証に使用できます。

注 – サービスプロセッサ (Service Processor、SP) では、安全なチャネルを使用した Active Directory サーバとの通信が想定されています。セキュリティーを確保するため、プロトコルネゴシエーションでプライベートチャネルをセットアップできるように、SP のユーザー認証プロセス中に提供できる証明書が Active Directory サーバにロードされている必要があります。

ユーザーの認証と承認

Active Directory は、ユーザー資格の認証とネットワークリソースへのユーザーのアクセスレベルの承認を提供します。Active Directory は、ユーザーがシステムリソースにアクセスする前に、認証を使用してユーザーの属性を検証します。Active Directory は、ネットワークリソースへのユーザーのアクセス権を制御するために、承認を使用してユーザーに特定のアクセス権限を付与します。ユーザーのアクセスレベルは、特定のインターネット名で識別されるホストのグループであるネットワークドメイン内のユーザーのグループメンバーシップに基づいて、サーバから設定され、学習されます。ユーザーは、複数のグループに所属できます。Active Directory は、ユーザーのドメインが設定された順序でユーザーを認証します。

ユーザーの承認レベル

いったん認証が終わると、ユーザーの承認レベルを次の方法で決定することができます。

- もっとも単純な場合、Operator、Administrator、またはAdvanced Roles のユーザーの承認 (19 ページの「ユーザーアカウントの役割と権限」を参照) は、SP の Active Directory 設定を通じて直接学習されます。アクセスレベルと承認レベルは、`defaultrole` プロパティーで指定します。Active Directory データベースでのユーザーの設定では、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` は、管理者、オペレータ、または詳細な役割設定のいずれか `a/u/c/r/o/s` 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、Administrator、Operator、または Advanced Roles に関連した権限が割り当てられます。

- また、サーバに問い合わせることで、より統合された方法を使用できます。設定の際には、アクセスレベルの決定に使用する、Active Directory サーバの対応するグループ名を使用して、SP の Administrator Group テーブル、Operator Group テーブル、または Custom Group テーブルを設定する必要があります。Administrator を指定するために、最大 5 つの Active Directory グループを入力でき、Operator 権限を割り当てるために、さらに 5 つ使用できます。また、Advanced Roles を含むカスタムグループに最大 5 つのグループを割り当てることができます (19 ページの「ユーザーアカウントの役割と権限」を参照)。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、Administrator、Operator、または Advanced Roles のいずれかの適切なアクセスレベルが識別されます。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。複数のグループに割り当てられたユーザーには、すべての権限の和が与えられます。

Active Directory 設定の構成に関する詳細と手順については、次のいずれかのガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

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、次の Web サイトを参照してください。

http://www.openldap.org/

LDAP 設定の構成に関する詳細と手順については、次のいずれかのガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

LDAP/SSL

LDAP/SSL は、Secure Socket Layer (SSL) テクノロジを使用して強化されたセキュリティーを LDAP ユーザーに提供します。SP で LDAP/SSL を設定するには、主サーバ、ポート番号、証明書モードのような基本的なデータや、代替サーバ、イベントレベル、または重要度レベルのような省略可能データを入力する必要があります。ILOM Web インタフェース、CLI、または SNMP の LDAP/SSL 設定ページを使用して、このデータを入力することができます。

LDAP/SSL 設定の構成に関する詳細と手順については、次のいずれかのガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

RADIUS

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 サーバは、複数の RADIUS サーバやその他の種類の認証サーバと一緒に動作できます。

RADIUS は、クライアントサーバモデルに基づいています。RADIUS サーバ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モデルでは、クライアントが RADIUS サーバに Access-Request クエリーを送信します。サーバ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のそれぞれで共有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 設定の構成に関する詳細と手順については、次のいずれかのガイドを参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

第4章

システム監視と警告管理

項目

説明	リンク
ILOM のシステム監視機能について学習する	• 26 ページの「システム監視」 • 26 ページの「センサー測定値」 • 27 ページの「システムインジケータ」 • 28 ページの「障害管理」 • 28 ページの「ILOM イベントログ」 • 29 ページの「syslog 情報」 • 30 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」
ILOM のシステム警告の管理について学習する	• 30 ページの「警告管理」 • 34 ページの「CLI からの警告管理」 • 35 ページの「Web インタフェースからの警告管理」 • 36 ページの「SNMP ホストからの警告管理」

関連項目

ILOM に関する項目	節	ガイド
• CLI	• システム部品の監視 • システム部品の監視	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• Web インタフェース	• システム部品の監視 • システム部品の監視	『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
• IPMI および SNMP ホスト	• システム部品の監視 • システム部品の監視	『Integrated Lights Out Manager (ILOM) 3.0 IPMI および SNMP 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。

システム監視

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ひと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。

- システムコンポーネントの温度、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表示します。詳細は、26 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、27 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、28 ページの「ILOM イベントログ」を参照してください。
- Syslog 情報を送信して、ILOM 内の複数インスタンスからのイベントを組み合わせて表示します。詳細は、29 ページの「syslog 情報」を参照してください。
- 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します。詳細は、30 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」を参照してください。

センサー測定値

ILOM を使用するすべての サーバ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。

センサー測定値は、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、次のいずれかのガイドの「センサー測定値の表示」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

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、サーバ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 (Field-Replacement Unit、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。詳細は、次のいずれかのガイドの「システムインジケータの表示および管理」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

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。

- **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。ILOM を使用するほとんどのサーバ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 (Field-Replacement Unit、FRU) が保守を必要としている。

障害管理

ILOM を使用するほとんどのサーバ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、サーバ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、使用しているサーバプラットフォームのマニュアルを参照してください。

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、次のいずれかのガイドの「障害状態の表示」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

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、サーバ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ついては、使用しているサーバプラットフォームのマニュアルを参照してください。

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。

ILOM では、ホストサーバの 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。

CLI、Web、または SNMP ホストからのイベントログとタイムスタンプの管理

CLI、Web インタフェース、または SNMP ホストから、ILOM のイベントログとタイムスタンプを表示および管理できます。詳細は、次のガイドの「クロック設定の構成」および「イベントログ出力のフィルタリング」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

syslog 情報

syslog は多くの環境で使用されている標準ログユーティリティーです。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、次のいずれかのガイドの「遠隔 Syslog 受信側の IP アドレスの設定」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

システムの問題を診断するための SP データの収集

ILOM サービススナップショットユーティリティーを使用すると、SP のスナップショットをいつでも即時に生成できます。このユーティリティーは ILOM CLI と ILOM Web インタフェースのどちらからでも実行できます。

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。

ILOM サービススナップショットユーティリティーは、サービスプロセッサ (Service Processor、SP) 状態データを収集します。このユーティリティーは、ログファイルを収集し、各種コマンドを実行してその出力を収集し、この収集データをユーザーが定義した場所にダウンロードファイルとして送信します。

システムの問題を診断するために SP データを収集する方法の詳細は、次のいずれかのガイドの「システムの問題を診断するための SP データの収集」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

警告管理

ILOM では、IPMI PET 警告、SNMP トラップ警告、および電子メール通知警告の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、サーバの ILOM SP から実行できます。

ILOM を使用する各サーバ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。指定した警告の宛先は警告メッセージ (IPMI PET または SNMP) の受信をサポートしている必要があります。警告の宛先が警告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デコードできません。

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、29 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

ILOM を使用するすべてのサーバ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。

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次のプロパティー値を用意しています。

- Alert Type
- Alert Level
- Alert Destination
- Alert Destination Port
- Email Custom Sender
- Email Message Prefix
- Email Class Filter
- Email Type Filter
- SNMP Version (*SNMP* トラップ警告のみ)
- SNMP Community Name or User Name (*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 4-1 を参照してください。

表 4-1 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
Alert Type	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、CMM を除く ILOM を使用するすべてのサーバ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デコードできません。 • **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とブレードサーバ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 電子メールサーバの名前を最初に ILOM で設定する必要があります。
Alert Destination	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。
Alert Destination Port	任意	警告の宛先ポートは、警告の種類が SNMP トラップである場合のみ適用されます。宛先ポートプロパティーは、SNMP トラップ警告が送信される UDP ポートを指定します。

表 4-1 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
Alert Level	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 Minor です。 • **Minor**。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。 • **Major**。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。 • **Critical**。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。 • **Down**。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。 • **Disabled**。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で、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、「Minor」、「Major」、「*Critical*」、または「Down」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」オプションを選択する必要があります。
Email Custom Sender	任意	電子メールのカスタム送信者プロパティーは、警告の種類が電子メール警告である場合のみ適用されます。`email_custom_sender` プロパティーを使用すると、「from」アドレスの形式を上書きすることができます。*<IPADDRESS>* または *<HOSTNAME>* のどちらかの置換文字列を使用して、たとえば alert@[*<IPADDRESS>*] のように指定できます。このプロパティーを設定すると、この値が SMPT カスタム送信者情報を上書きします。
Email Message Prefix	任意	電子メールメッセージのプレフィックスプロパティーは、警告の種類が電子メール警告である場合のみ適用されます。`email_message_prefix` プロパティーを使用すると、メッセージの内容に情報を付加することができます。
Event Class Filter	任意	イベントのクラスフィルタプロパティーは、警告の種類が電子メール警告である場合のみ適用されます。デフォルト設定では、すべての ILOM イベントが電子メール警告として送信されます。`event_class_filter` プロパティーを使用すると、選択したイベントクラスを除くすべての情報を除外することができます。"" (空の二重引用符) を使用すると、フィルタをクリアし、すべてのクラスに関する情報を送信することができます。

表 4-1　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
Event Type Filter	任意	イベントの種類フィルタプロパティーは、警告の種類が電子メール警告である場合のみ適用されます。`event_type_filter` プロパティーを使用すると、イベントの種類を除くすべての情報を除外することができます。"" (空の二重引用符) を使用すると、フィルタをクリアし、すべてのイベントの種類に関する情報を送信することができます。
SNMP Version	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 Community Name or User Name	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 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。 **注 –** 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 トラップ警告をデコードできません。ILOM での SNMP ユーザーの定義に関する詳細は、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』、または『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』を参照してください。

CLI からの警告管理

ILOM の警告ルール設定は、コマンド行インタフェース (Command-Line Interface、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。

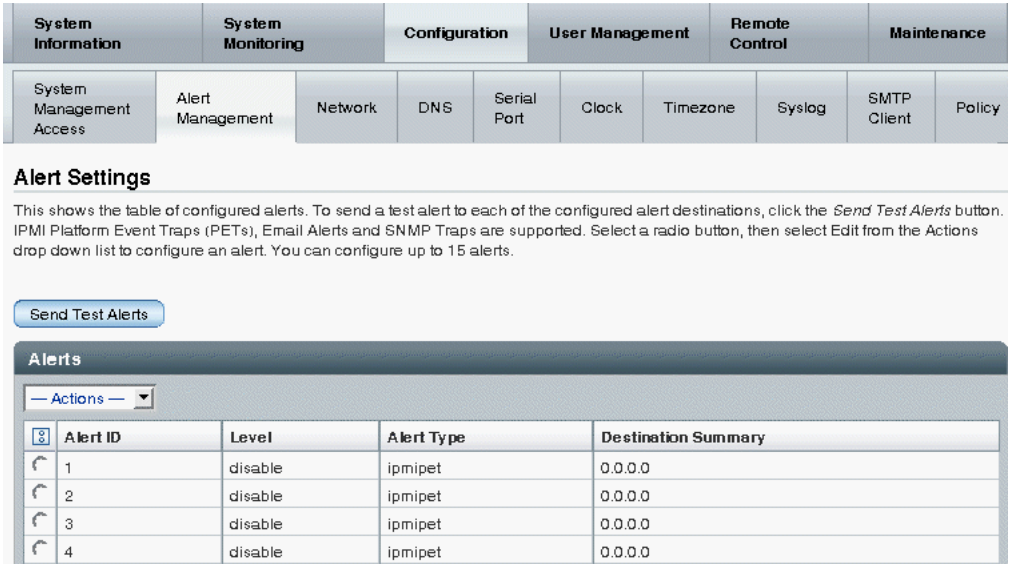
ILOM CLI を使用して警告を管理する方法の詳細は、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』の「システム警告の管理」を参照してください。

Web インタフェースからの警告管理

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 」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 4-1　「Alert Settings」ページ



ILOM Web インタフェースを使用して警告を管理する方法の詳細は、『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』の「システム警告の管理」を参照してください。

SNMP ホストからの警告管理

`get` および `set` コマンドを使用すると、SNMP ホストを使用して警告ルール設定を表示および設定することができます。

SNMP を使用して ILOM 設定を表示および設定する前に、SNMP を設定する必要があります。SNMP を使用してシステム警告を管理する方法の詳細は、『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』の「システム警告の管理」を参照してください。

第5章

電源監視および管理インタフェース

項目

説明	リンク
ILOM の電源監視および消費電力インタフェースについて学習する	• 38 ページの「電源監視インタフェース」
消費電力の監視に関連する用語と電力ポリシー機能について学習する	• 38 ページの「電源監視の用語」 • 39 ページの「電力ポリシー」

関連項目

ILOM	章または節	ガイド
• CLI	• 消費電力の監視	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• Web インタフェース	• 消費電力の監視	『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
• IPMI と SNMP ホスト	• 消費電力の監視	『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。

電源監視インタフェース

電源監視インタフェースを使用すると、リアルタイムに消費電力を監視できます。リアルタイムの監視では、サービスプロセッサ (Service Processor、SP) または個々の電源装置をいつでもポーリングすることができ、電力が使用された時点から 1 秒以内の正確さで「ライブの」データを取り出してレポートできます。

電源監視の用語

報告される消費電力には、入力電力と出力電力が含まれます。入力電力は、外部の供給元からシステムの電源装置に供給される電力です。出力電力は、電源装置からシステムコンポーネントに供給される電力量です。

ラック搭載型サーバの場合、合計消費電力は、サーバが消費する入力電力です。サーバモジュール (ブレード) の場合、合計消費電力は、ブレードのみが消費する入力電力です。共有コンポーネントが消費する電力は含まれません。シャーシ監視モジュール (Chassis Monitoring Module、CMM) の場合、合計消費電力は、シャーシ全体またはシェルフ全体が消費する入力電力です。

また、ハードウェア構成の最大電力、使用可能電力、および許容電力を監視することもできます。

ハードウェア構成の最大電力は、システムのハードウェア構成で任意の時点にシステムが消費できる最大入力電力です。したがって、ハードウェア構成の最大電力は、各プロセッサ、I/O モジュール、メモリーモジュール、ファンなどが消費できる最大電力の合計です。

注 – ハードウェア構成の最大電力メトリックは、すべてのシステムでサポートされているわけではありません。詳細は、使用しているプラットフォーム固有の ILOM 補足マニュアルまたは製品ノートを参照してください。

使用可能電力は、システム内の電源装置が外部の供給元から取り込み可能な最大電力です。通常、この値は、ハードウェア構成の最大電力より大きくなります。ブレードの使用可能電力は、シャーシによって制御されます。シャーシは、常に一定の電力がブレードで使用できるようにします。ブレードは、シャーシが供給する使用可能電力の範囲内にあることを保証できない場合、電源が入りません。

システムによっては、ソフトウェアの設定により、最大消費電力がハードウェア構成の最大電力より低いことを保証できる場合があります。この低いことが保証された最大消費電力は、「許容電力」と呼ばれます。ラック搭載型サーバの場合、許容電力は、サーバが任意の時点での消費を保証している最大入力電力です。ブレードの場合、許容電力は、ブレードが消費を保証している最大電力です。共有コンポーネントの電力負荷は含まれません。CMM の場合、許容電力は、シャーシ全体 (すべてのブレード、NEM、ファンなど) が任意の時点で消費する最大入力電力です。ソフトウェアによる電力制限が無効の場合、許容電力は、ハードウェア構成の最大電力になります。

電力ポリシー

電力ポリシー設定は、システムの電力使用を任意の時点で管理します。「Performance」および「Elastic」の 2 つの電力ポリシーがサポートされています。

- **Performance** − システムは使用可能電力をすべて使用できます。
- **Elastic** − システムの電力使用を現在の利用レベルに適合させます。たとえば、作業負荷が変動した場合でも、相対利用率が常に 70% で保持されるように、システムコンポーネントに供給する電力を増減します。

注 – 電力ポリシー機能は、すべてのプラットフォームでサポートされているわけではありません。使用しているプラットフォームで実装されている電力ポリシー機能については、プラットフォーム固有の ILOM 補足マニュアルまたは製品ノートを参照してください。

CLI、Web インタフェース、IPMI、または SNMP ホストから、ILOM の電源監視インタフェースにアクセスできます。電源監視インタフェースを使用する方法の詳細は、次のいずれかのガイドの「消費電力の監視」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 SNMP および IPMI 手順ガイド』

第6章

設定の管理とファームウェアの更新

項目

説明	リンク
ILOM の設定管理機能について	• 42 ページの「設定管理作業」 • 43 ページの「バックアップ操作と復元操作」 • 44 ページの「デフォルトにリセットする機能」
ILOM のファームウェア更新操作について	• 45 ページの「ILOM ファームウェアの更新」 • 45 ページの「ILOM バージョン情報の識別」 • 46 ページの「ファームウェア更新のプロセス」 • 46 ページの「設定保持オプション」 • 47 ページの「更新セッションでネットワーク障害が発生した場合のトラブルシューティング」

関連項目

ILOM	章または節	ガイド
• CLI	• ILOM 設定のバックアップおよび復元 • ILOM ファームウェアの更新	『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
• Web インタフェース	• ILOM 設定のバックアップおよび復元 • ILOM ファームウェアの更新	『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 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。

設定管理作業

次のような設定管理作業を実行できます。

- リモートシステム上の XML ファイルに ILOM 設定をバックアップします。
- バックアップファイルを使用して、バックアップした設定に ILOM を復元します。
- バックアップファイルを使用して、バックアップした設定をほかの ILOM SP にインストールします。
- ILOM 設定をデフォルト設定にリセットします。

バックアップおよび復元機能とデフォルトにリセットする機能は、次のように組み合わせて使用することができます。

- ILOM 設定をバックアップ XML ファイルに保存し、ILOM 設定をデフォルト設定にリセットし、コマンド行インタフェース (Command-Line Interface、CLI) または Web インタフェースを使用して新しい ILOM 設定を作成します。
- ILOM 設定をデフォルト設定にリセットし、既知の良好な ILOM 設定バックアップファイルを使用して ILOM 設定を復元します。
- CLI または Web インタフェースを使用して新しい ILOM 設定を作成し、ILOM 設定をバックアップ XML ファイルに保存し、XML ファイルを編集して特定のシステムに固有の設定を削除し、復元操作を実行して、ほかのシステムでバックアップファイルを読み込みます。

これらの機能について、典型的な使用例を次に説明します。

- ILOM の設定を変更したところ、正常に動作しなくなったため、既知の良好な設定を復元して ILOM を回復します。この場合、最初に ILOM 設定をデフォルト設定にリセットし、次に既知の良好な設定を使用して復元操作を実行します。
- バックアップおよび復元機能を使用して、ILOM の設定をほかのシステムに複製します。この場合、標準の ILOM 設定を作成し、その設定をバックアップし、バックアップ XML ファイルを編集して特定のシステムに固有の設定 (たとえば IP アドレス) を削除し、次に復元操作を実行してほかのシステムへ設定を複製します。
- 最小限の ILOM 設定を作成しましたが、完了するためには、多くのユーザーを設定する必要があります (ILOM は、最大 10 個のローカルユーザーアカウントをサポートしています)。同じユーザーを含む設定をすでにバックアップしている場合は、XML ファイルを編集してユーザー情報のみが含まれるようにしてから復元操作を実行すれば、オーバーレイする設定をそのユーザーアカウントを含む設定のみに限定することができます。もう 1 つの方法として、Active Directory のような大規模ネットワーク設定を再利用することもできます。

Web インタフェースまたは CLI を使用して、ILOM で設定管理作業を実行できます。これらの作業の詳細は、次の項を参照してください。

- 43 ページの「バックアップ操作と復元操作」
- 44 ページの「デフォルトにリセットする機能」

バックアップ操作と復元操作

ILOM は、バックアップと復元の 2 つの操作をサポートしています。

- バックアップ操作では、現在の ILOM 設定データを XML ファイルに収集し、そのファイルを遠隔システムに転送します。
- 復元操作では、XML バックアップファイルを取り出し、そのファイルを使用して ILOM SP をバックアップした設定に復元します。

したがって、バックアップ操作と復元操作を使用すると、ILOM 設定をバックアップ XML ファイルに保存し、あとでバックアップファイルを同じシステムに復元することができます。さらに、ほかのシステムのバックアップ XML ファイルを使用する場合は、XML ファイルを編集して IP アドレスのような固有の設定を削除または変更することができます。バックアップ XML ファイルは読み取り可能であり、手動で編集できます。

注意 – 編集したバックアップ XML ファイルを同じシステムに復元する場合は、ILOM 設定をデフォルト設定にリセットする必要があります。リセットしない場合、復元した設定は、現在の設定に単にオーバーレイされます。編集したバックアップ XML ファイルを、すでに ILOM 設定があるほかのシステムに復元する場合、現在の設定に重ね合わせる場合を除き、ILOM 設定を消去する必要があります。現在の ILOM 設定を消去するには、ILOM 設定をデフォルト設定にリセットする必要があります。手順については、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』または『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』の「ILOM 設定をデフォルト設定にリセットする」を参照してください。

システムで設定できるすべての情報をバックアップすることができます。バックアップ XML ファイルに含まれる設定の内容は、バックアップ操作の実行に使用するユーザーアカウントに割り当てられている権限で決定されます。セキュリティー上の理由から、復元操作の実行に使用するユーザーアカウントの権限が、バックアップファイルの作成に使用したアカウントの権限より少ない場合は、一部の設定が復元されない場合があります。権限不足のために復元されない構成プロパティーごとに、ログエントリが作成されます。したがって、イベントログを確認することにより、すべての構成プロパティーが復元されたことを検証できます。

また、権限が限定されたユーザーアカウントを使用して、バックアップ XML ファイルに含まれる情報量を制限することもできます。たとえば、Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、および Read Only (o) の役割が割り当てられたアカウントは、すべての権限を持ち、もっとも完全な設定バックアップファイルを作成します。そのため、バックアップ操作と復元操作を実行するときは、a、u、c、r、o の役割が割り当てられたユーザーアカウントを使用することをお勧めします。

設定のバックアップ操作と復元操作では、ホストオペレーティングシステムの電源状態は変更されません。ただし、バックアップまたは復元操作が完了するまで、ILOM SP 上のすべてのセッションが一時的に停止します。通常、バックアップまたは復元操作には 2 - 3 分かかり、そのあとで、ログインしていたすべてのセッションが正常に動作を再開します。

バックアップ操作と復元操作を実行し、バックアップ XML ファイルを編集する手順については、次のガイドの「ILOM 設定のバックアップおよび復元」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

デフォルトにリセットする機能

ILOM でデフォルトにリセットする機能を使用すると、ILOM 設定をデフォルト設定にリセットすることができます。この機能を使用する場合、次の 3 つのオプションがあります。

- **All** − 既存の ILOM 設定ファイルを消去する場合は、このオプションを選択します。ILOM SP が再起動すると、SP のファームウェアに含まれている設定ファイルが代わりに使用されます。
- **Factory** − 既存の設定ファイルと内部ログファイルを消去する場合は、このオプションを選択します。ILOM SP が再起動すると、SP のファームウェアに含まれている設定ファイルが代わりに使用され、内部ログファイルが消去されます。
- **None** − 以前実行したリセット操作を取り消す場合は、このオプションを選択します。以前実行したリセット操作を取り消すには、ILOM SP が再起動する前に、None オプションを使用してリセット操作を開始する必要があります。

注 – ILOM 設定のリセットを実行する場合、ILOM SP が再起動するまでリセットされた設定は有効になりません。

ILOM 設定をデフォルト設定にリセットする手順については、次のガイドの「ILOM 設定をデフォルト設定にリセットする」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

ILOM ファームウェアの更新

すべての ILOM ファームウェアリリースは、使用しているサーバプラットフォーム用の公式ダウンロードページからダウンロードできます。

通常、新しいバージョンのファームウェアは、新しい機能と製品の品質向上を提供します。常に最新の改善点を適用するためには、システムのファームウェアを利用可能な最新のファームウェアリリースで更新することを強くお勧めします。

システムのファームウェアを前のリリースに更新することは、お勧めしません。ただし、システムで前のバージョンのファームウェアを実行する必要がある場合は、ダウンロードできる任意のファームウェアリリースでファームウェアを更新することができます。

使用しているサーバ用のダウンロードページの URL を確認するには、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。

ILOM バージョン情報の識別

ILOM のファームウェアを更新する前に、サーバ SP または CMM で動作している ILOM ファームウェアのバージョンを識別する必要があります。

システム (サーバ SP または CMM) 上に ILOM 2.x がインストールされていて、新しい ILOM 2.x バージョンへ更新する場合は、『Integrated Lights Out Manager 2.0 ユーザーズガイド』で ILOM 2.x 用のファームウェア更新手順を参照してください。

ILOM3.x へ更新する場合は、次のいずれかのガイドで ILOM ファームウェアを更新する手順を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 入門ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

ファームウェア更新のプロセス

サーバまたは CMM にインストールされているファームウェアバージョンを更新するには、次の手順に従います。

1. 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 用のファームウェアイメージをダウンロードします。
2. サポートされているプロトコル (FTP、TFTP、HTTP、HTTPS) を使用して、サーバにイメージをコピーします。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。
3. 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。
4. Admin (a) 役割のアカウントを使用して、ILOM にログインします。
5. ILOM の CLI または Web インタフェースを使用して、サーバ SP (または CMM) にファームウェアイメージをロードします。
6. 任意で、現在の設定を ILOM に保持します。詳細は、46 ページの「設定保持オプション」を参照してください。
7. システムの再起動後に、適切なファームウェアバージョンがインストールされていることを検証します。

設定保持オプション

新しいファームウェアリリースへ更新するときに、「Preserve Configuration」オプションが有効な場合、既存の設定が ILOM に保存され、更新プロセスが完了すると、設定が復元されます。

注 – 「configuration」という用語は、ユーザーが ILOM で設定する設定値を指します。この設定には、ユーザー管理設定、SP のネットワーク設定、シリアルポート設定、警告管理設定、リモート管理設定などがあります。

前のファームウェアリリースへ更新する場合、ILOM がそのリリース用に保持されている設定を検出すると、「Preserve Configuration」オプションが有効であれば、更新プロセスが完了したあとで前のリリース用の設定が元に戻されます。

例: システムファームウェアを 3.0 から 2.0 へ更新する場合、更新プロセス中に「Preserve Configuration」が有効であれば、ILOM は次のように動作します。

- 2.0 設定のスナップショットがシステム上に保持されているかどうかを確認します。
- スナップショットを検出した場合、更新プロセスが完了したあとで、2.0 設定のスナップショットを復元します。

ただし、この例で、2.0 設定のスナップショットを検出できない場合、ILOM は 2.0 設定を復元しません。更新プロセスが完了すると、設定内容はシステムのデフォルトに戻されます。

更新セッションでネットワーク障害が発生した場合のトラブルシューティング

ILOM の Web インタフェースまたは CLI を使用して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した場合、ILOM は再起動しません。システムを再起動しないでください。次の手順を実行して更新を続行します。

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. 更新プロセスを再起動します。

第7章

遠隔ホスト管理オプション

項目	
説明	**リンク**
リモート管理オプションを識別する	• 50 ページの「リモート管理オプション」
リモートサーバの電源状態の制御について学習する	• 50 ページの「電源制御」 • 51 ページの「ILOM CLI – リモート電源コマンド」 • 51 ページの「ILOM Web インタフェース – リモート電源制御」
診断テストについて学習する	• 52 ページの「SPARC システムの診断」
ローカルシステム上のCLIから遠隔ホストサーバへのストレージメディアのリダイレクトについて学習する	• 52 ページの「Storage Redirection CLI」 • 53 ページの「初回のアクセス」 • 53 ページの「Storage Redirection CLI のアーキテクチャー」 • 54 ページの「デフォルトのネットワーク通信ポート」
ローカルシステム上の Web インタフェースから遠隔ホストサーバへのデバイス (キーボード、ビデオディスプレイ、マウス、ストレージ) のリダイレクトについて学習する	• 55 ページの「ILOM リモートコンソール」 • 56 ページの「1 台構成および複数台構成の遠隔ホストサーバ管理ビュー」 • 57 ページの「インストール要件」 • 58 ページの「ネットワーク通信ポートとプロトコル」 • 58 ページの「サインイン認証情報の要求」 • 59 ページの「CD とフロッピーディスクのリダイレクション操作のシナリオ」

関連項目

ILOM	章または節	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』
• Web インタフェース	• 遠隔ホストの管理	『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 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。

リモート管理オプション

ILOM 3.0 の ILOM には、次のリモート管理オプションがあります。

- 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 (グラフィカルインタフェース)

これらのリモート管理オプションについての情報を次に示します。

電源制御

ILOM のリモート電源制御オプションは、ILOM を使用するすべての サーバに対して ILOM CLI または Web インタフェースから使用できます。このオプションを使用すると、遠隔ホストサーバの電源状態を制御できます。

ILOM CLI − リモート電源コマンド

コマンドウィンドウまたは端末から、次のコマンドを発行して、ホストサーバの電源状態を遠隔から制御できます。

- **start**。遠隔ホストサーバの電源を完全に投入するには、start コマンドを使用します。

  例: -> start /SYS

- **stop**。遠隔ホストサーバの電源を切断する前に OS を正常に停止するには、stop コマンドを使用します。

  例: -> stop /SYS

- **stop -f**。遠隔ホストサーバの電源をただちに切断するには、stop -f コマンドを使用します。

  例: -> stop -f /SYS

- **Reset**。遠隔ホストサーバをただちに再起動するには、reset コマンドを使用します。

  例: -> reset /SYS

ホストサーバとの接続または ILOM CLI からのコマンドの発行については、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』を参照してください。

ILOM Web インタフェース − リモート電源制御

ホストサーバの電源状態を遠隔から制御するには、ILOM Web インタフェースの「Remote Control」-->「Remote Power Control」タブを選択します。次のオプションを使用できます。

- **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。
- **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。

SPARC システムの診断

ILOM の診断設定オプションは、サーバの一部で使用できます。このオプションは、ILOM Web インタフェースの「Remote Control」-->「Diagnostics」タブから、または CLI を使用してアクセスできます。サーバプラットフォームがこれらの診断オプションをサポートしているかどうかについては、使用しているプラットフォームの ILOM 補足マニュアルを参照してください。

- **SPARC システムの診断設定**

  ILOM を使用する SPARC システムでは、診断モードを有効にし、診断のトリガー、レベル、および診断出力の詳細度を指定できます。

ILOM の診断オプションを使用する手順の詳細については、次のガイドの「SPARC システムハードウェア問題の診断」を参照してください。

- 『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』
- 『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』

Storage Redirection CLI

ILOM のStorage Redirection CLI 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。ただし、Storage Redirection CLI は、ILOM 2.0 を実行するサーバ SP やシャーシ監視モジュール (Chassis Monitoring Module、CMM) ではサポートされていません。また、ILOM 3.0 を実行する CMM でもサポートされていません。

Storage Redirection CLI を使用すると、ローカルクライアント上のストレージデバイス (CD/DVD または ISO イメージ) が、遠隔ホストサーバに直接接続されているように動作します。たとえば、リダイレクト機能を使用して、次の操作をローカルで実行できます。

- ILOM リモートコンソールアプリケーションを起動せずに、ストレージデバイスまたはイメージをデスクトップから遠隔 SP ホストへ直接マウントします。
- `/SP/console` を使用したテキストベースのコンソール通信のために、メディアをリダイレクトします。
- 複数の SP ホストサーバでストレージリダイレクトを開始および停止するためのスクリプトを作成します。

注 – Storage Redirection CLI は、遠隔メディア制御に限定されています。遠隔ホストサーバ上のほかのデバイス (キーボード、ビデオディスプレイ、マウスなど) を遠隔から管理する必要がある場合は、ILOM リモートコンソールを使用する必要があります。ILOM リモートコンソールの詳細については、55 ページの「ILOM リモートコンソール」を参照してください。

Storage Redirection CLI を使用する手順については、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』の「遠隔ホストの管理」を参照してください。

初回のアクセス

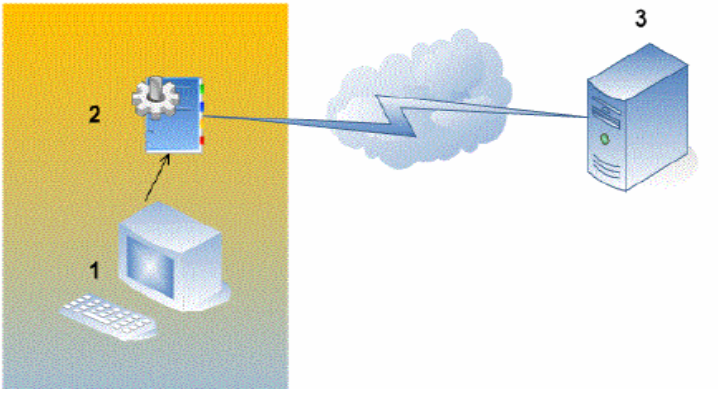
はじめて Storage Redirection CLI にアクセスするときは、ILOM Web インタフェースにサインインし、サービスとクライアントをインストールする必要があります。サービスとクライアントをシステムにインストールしたら、コマンドウィンドウまたは端末から直接サービスを開始し、Storage Redirection CLI を起動することができます。

注 – あるいは、ILOM Web インタフェースから直接サービスを開始することもできます。サービスをインストールせずに ILOM Web インタフェースからサービスを開始する場合は、コマンドウィンドウまたは端末から Storage Redirection CLI を起動する前に、ILOM Web インタフェースにアクセスしてサービスを開始する必要があります。サービスをインストールまたは開始する方法の詳細については、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』の「遠隔ホストの管理」を参照してください。

Storage Redirection CLI のアーキテクチャー

Storage Redirection CLI は、Java Web Start サービスおよびスクリプト可能な Java コマンド行クライアントから構成されます。サービスの開始とクライアントのインストールは、ILOM Web インタフェースから実行する必要があります。Storage Redirection サービスは、ローカルクライアントのバックグラウンドで動作し、ローカルクライアントと遠隔ホストサーバ間の接続を確立します。接続が確立されると、コマンドウィンドウまたは端末から Storage Redirection CLI をローカルで起動できます。Storage Redirection CLI を使用すると、ストレージリダイレクトを開始および停止するために、サービスへコマンドを発行することができます。

図 7-1　Storage Redirection のサービスとクライアント



図の説明

1	Storage Redirection コマンド行クライアントを実行するローカルクライアント
2	ローカルクライアントで動作する Storage Redirection サービス
3	遠隔ホストサーバ

注 – Storage Redirection サービスは、ローカルシステムで一度に 1 つのインスタンスのみ実行できます。ただし、ローカルのコマンドウィンドウまたは端末から Storage Redirection コマンド (`-jar StorageRedir.jar`) を発行すると、複数の Storage Redirection CLI を起動できます。

デフォルトのネットワーク通信ポート

Storage Redirection CLI で使用されるデフォルトのネットワーク通信ポートは、2121 です。このデフォルトのソケットポートを使用すると、Storage Redirection CLI がネットワーク経由で遠隔ホストサーバの SP と通信することができます。デフォルトのネットワークポートを変更する必要がある場合は、`Jnlpgenerator-cli` ファイルを編集して、デフォルトのポート番号 (2121) を手動で上書きする必要があります。

`Jnlpgenerator-cli` ファイルで参照されているネットワークポート番号を編集する方法の詳細については、『Integrated Lights Out Manager (ILOM) 3.0 CLI 手順ガイド』の「デフォルトの Storage Redirect ポート番号 (2121) の変更」を参照してください。

ILOM リモートコンソール

ILOM リモートコンソールは、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。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。ILOM リモートコンソールを使用する場合、遠隔ホストサーバ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、ISO イメージ)

ILOM 遠隔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、リダイレクト機能を使用して、次の操作を実行できます。

- 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上の GUI ベースのプログラムにアクセスし、実行します。
- サーバの機能をローカルクライアントから遠隔で設定します。
- サーバ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。
- サーバ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から実行可能な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。

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、SPARC プロセッサベースのすべての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使用してホストデバイスをリダイレクトする手順については、『Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』の「遠隔ホストの管理」を参照してください。

1 台構成および複数台構成の遠隔ホストサーバ管理ビュー

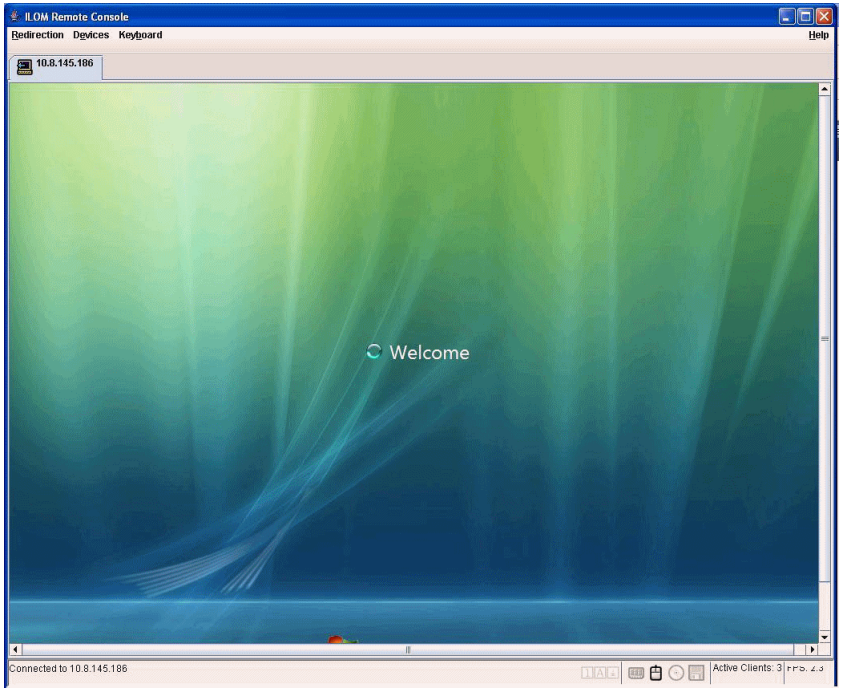
ILOM リモートコンソールは、1 台構成および複数台構成のリモートサーバ管理ビューをサポートしています。

1 台構成および複数台構成のサーバ管理ビューは、現在 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。

- **1 台構成のリモートサーバ管理ビュー** – 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。

  1 台構成のリモートサーバ管理ビューは、任意のサーバ SP の IP アドレスに接続する場合にサポートされます。

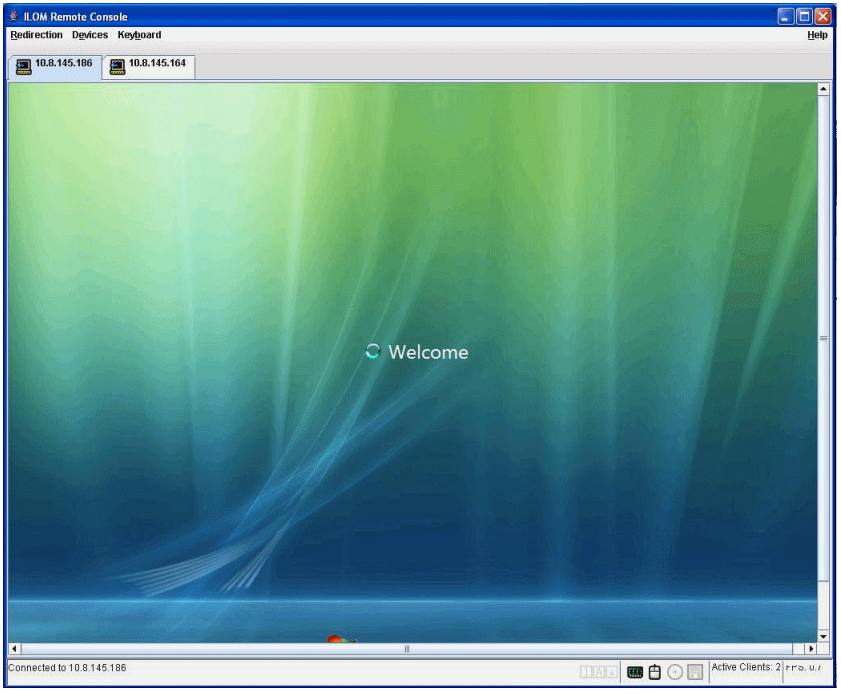
図 7-2 1 台構成のサーバ管理ビュー



- **複数台構成のリモートサーバ管理ビュー** – ILOM リモートコンソールを起動して、複数の遠隔ホストサーバビューを管理できます。

  複数台構成のリモートサーバ管理ビューは、(1) 別の遠隔ホストサーバを管理する新しい ILOM リモートコントロールセッションを追加する場合、(2) シャーシ監視モジュール (Chassis Monitoring Module、CMM) に関連付けられた IP アドレスに接続する場合のいずれかでサポートされます。

図 7-3　　複数台構成のサーバ管理ビュー



インストール要件

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。これらは 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、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。

さらに、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。

表 7-1 サポートされているオペレーティングシステムと 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 1.7.5 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

ネットワーク通信ポートとプロトコル

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、遠隔ホストサーバの SP と通信します。

表 7-2 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

サインイン認証情報の要求

ILOM Web インタフェースから ILOM リモートコンソールを起動するには、Admin (a) 役割または Console (c) 役割のアカウントを使用してサインインする必要があります。そのあとは、リダイレクトの開始、リダイレクトの停止、またはリダイレクトの再起動のいずれかを実行するたびに、Admin 役割または Console 役割のアカウントで入り直す必要があります。

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、Admin (a) または Console (c) 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、20 ページの「シングルサインオン」を参照してください。

CD とフロッピーディスクのリダイレクション操作のシナリオ

表 7-3 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 7-3 DVD ドライブとフロッピーディスクドライブを使用した遠隔コンソールの操作

事例	状態	遠隔ホストから見た DVD	遠隔ホストから確認できるフロッピーディスク
1	遠隔コンソールアプリケーションが起動していない、または遠隔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ションが開始されていない	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と、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	遠隔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と、遠隔クライアントは状態メッセージを送信します。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 (ドライブをダブルクリックした場合など)、遠隔クライアントは状態メッセージを送信します。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	遠隔コンソールアプリケーションがメディアがない状態で起動し、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があることを示す状態メッセージを送信し、さらにメディアの変更を知らせます。	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があることを示す状態メッセージを送信し、さらにメディアの変更を知らせます。
4	遠隔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	遠隔コンソールアプリケーションが、メディアがある状態で起動し、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、メディアがないことを示す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、メディアがないことを示す状態メッセージを受け取ります。
6	遠隔コンソールアプリケーションが、イメージリダイレクションで起動している	事例 3 と同じ。	事例 3 と同じ。

表 7-3 DVD ドライブとフロッピーディスクドライブを使用した遠隔コンソールの操作 (続き)

事例	状態	遠隔ホストから見た DVD	遠隔ホストから確認できるフロッピーディスク
7	遠隔コンソールアプリケーションがイメージを使用して起動したが、リダイレクションは停止している (これは ISO のリダイレクションを停止する唯一の方法)	ドライバは、DVD のリダイレクションが停止していることを認識しているため、次のホストのクエリー時にメディアなしの状態を送信します。	ドライバは、DVD のリダイレクションが停止していることを認識しているため、次のフロッピーディスクのクエリー時にメディアなしの状態を送信します。
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機構があります。通信がないために、ソフトウェアがキープアライブ障害を検出し、クライアントからの応答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機構があります。ソフトウェアは、応答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

動的 DNS の設定例

この付録では、典型的なインフラストラクチャーで動的ドメインネームサービス (Dynamic Domain Name Service、DDNS) を設定する方法について説明します。ここに示す手順と設定例は、ILOM やサービスプロセッサ (Service Processor、SP) に影響しません。

この付録では、次の項目について説明します。

動的 DNS の概要

DDNS を設定すると、新しい ILOM システムの接続時にホスト名と IP アドレスが自動的に割り当てられます。したがって、DDNS を設定すると、クライアントは、ホスト名または IP アドレスを使用して、ネットワークに追加された ILOM SP にアクセスできます。

ILOM システムでは、出荷時のデフォルトでは、動的ホスト構成プロトコル (Dynamic Host Configuration Protocol、DHCP) が有効になっているので、DHCP を使用して SP のネットワークインタフェースを設定できます。DDNS を使用すると、DHCP をさらに活用して、ネットワークに追加され DHCP を使用して設定された ILOM システムのホスト名を DNS サーバが自動的に認識できます。

注 – ILOM 3.0 リリースで追加されたドメインネームサービス (Domain Name Service、DNS) のサポートにより、ILOM のコマンド行インタフェース (Command-Line Interface、CLI) やほかのユーザーインタフェースで、NTP サーバ、ロギングサーバ、およびファームウェアアップグレードサーバのようなホストをホスト名または IP アドレスで参照することができます。この付録で説明する DDNS サポートにより、SP を手動で設定せずにホスト名で参照することができます。

ILOM システムには、接頭辞、ハイフン、および ILOM SP 製品シリアル番号から構成される既知のホスト名が割り当てられます。ラック搭載型システムとサーバモジュールの場合、ホスト名は、接頭辞 SUNSP と製品シリアル番号から構成されます。複数のシャーシ監視モジュール (Chassis Monitoring Module、CMM) があるサーバシャーシの場合、各 CMM のホスト名は、接頭辞 SUNCMM*n* と製品シリアル番号から構成されます。*n* は、0 または 1 です。たとえば、製品シリアル番号が 0641AMA007 である場合、ラック搭載型システムまたはサーバモジュールのホスト名は、SUNSP-0641AMA007 になります。2 つの CMM があるサーバシャーシの場合、CMM のホスト名は、SUNCMM0-0641AMA007 および SUNCMM1-0641AMA007 になります。

DDNS を設定すると、SP、DHCP、DNS 間のトランザクションが自動的に実行され、新しいホスト名および対応する IP アドレスが DNS データベースに追加されます。各トランザクションは、次の段階から構成されます。

1. ILOM が、適切な接頭辞と製品シリアル番号を使用して SP のホスト名を作成し、ILOM SP が、DHCP 要求の一環としてホスト名を DHCP サーバへ送信します。
2. DHCP サーバは、要求を受信すると、使用できるアドレスのプールから IP アドレスを ILOM SP に割り当てます。
3. 次に、DHCP サーバは、新しく設定された ILOM SP のホスト名と IP アドレスを通知するために、DNS サーバへ更新を送信します。
4. DNS サーバは、新しい情報でデータベースを更新し、SP、DHCP、DNS 間のトランザクションが完了します。

割り当てられたホスト名に対して SP、DHCP、DNS 間のトランザクションが完了すると、クライアントはそのホスト名を使用して DNS 要求を行うことができ、DNS は割り当てられた IP アドレスを返します。

特定の ILOM SP のホスト名を決定するには、SP の外側に記載されている製品シリアル番号を調べ、前述のように適切な接頭辞と製品シリアル番号を組み合わせます。また、DNS ゾーン更新メッセージのサーバログを確認して、ホスト名を調べることもできます。

注 – CLI を使用すると、SP ホスト名をデフォルト以外の名前に変更することができます。ただし、ホスト名をデフォルト以外の名前に変更すると、クライアントは、そのホスト名を使用して DNS を使用する SP を参照する必要があります。

DHCP リースの更新によって IP アドレスが変化すると、DNS 情報が更新され、DHCP リースを解放すると、DNS 情報が削除されます。

注 – DDNS がサポートされる以前にホスト名が割り当てられている ILOM SP、または DDNS および MAC アドレスベースのホスト名を使用して設定されている ILOM SP では、すでに設定されているホスト名がそのまま有効になります。

動的 DNS の設定例

この節では、DDNS DNS の設定を行う方法の例について説明します。ここで提供する手順とサンプルファイルにサイト固有の変更を行うことで、使用している DDNS を設定できます。

注 – DDNS を設定する方法は、サイトで使用しているインフラストラクチャーによって異なります。Solaris、Linux、および Windows オペレーティングシステムはすべて、DDNS 機能を提供するサーバソリューションをサポートしています。この設定例では、サーバのオペレーティングシステム環境として Debian r4.0 を使用しています。

この節では、次の項目について説明します。

前提条件

この設定例は、次の前提条件に基づいています。

- SP が存在するネットワーク上に、DNS と DHCP の両方を処理する 1 台のサーバがある。
- SP のネットワークアドレスは 192.168.1.0。
- DHCP/DNS サーバのアドレスは 192.168.1.2。
- 192.168.1.100 から 192.168.1.199 の IP アドレスが、SP およびほかのクライアントにアドレスを提供するためのプールとして使用される。
- ドメイン名は `example.com`。
- DNS 設定や DHCP 設定がまだ存在しない。すでに設定されている場合は、次のファイルをガイドラインとして使用し、既存の設定を更新する。

▼ DHCP サーバと DNS サーバの設定と起動

サーバを設定するには、次の手順に従います。

1. **Debian ディストリビューションから、`bind9` および `dhcp3-server` パッケージをインストールします。**

   `dnsutils` パッケージをインストールすると、`dig`、`nslookup`、およびほかの有用なツールにアクセスできます。

2. **`dnssec-keygen` を使用して、DHCP サーバと DNS サーバ間で共有され、DNS データへのアクセスを制御するキーを生成します。**

3. **次のような DNS 設定ファイルを `/etc/bind/named.conf` という名前で作成します。**

```
options {
  directory "/var/cache/bind";
  auth-nxdomain no;    # conform to RFC1035
  listen-on-v6 { any; };
};
// prime the server with knowledge of the root servers
zone "." {
  type hint;
  file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones,
// and for broadcast zones as per RFC 1912
zone "localhost" {
  type master;
  file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
  type master;
  file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
  type master;
  file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
  type master;
  file "/etc/bind/db.255";
};
// additions to named.conf to support DDNS updates from dhcp server
key server.example.com {
  algorithm HMAC-MD5;
  secret "your-key-from-step-2-here"
};
```

```
zone "example.com" {
  type master;
  file "/etc/bind/db.example.com";
  allow-update { key server.example.com; };
};
zone "1.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.example.rev";
  allow-update { key server.example.com; };
};
```

4. **ローカルネットワーク用に、空のゾーンファイルを追加します。**

   空のゾーンファイルの名前は、/etc/bind/db.example.com および /etc/bind/db.example.rev とします。

   ディストリビューションに付属する db.empty ファイルをコピーするだけで十分です。このファイルは、DNS サーバによって自動的に更新されます。

5. **次のような** /etc/dhcp3/dhcpd.conf **ファイルを作成します。**

```
ddns-update-style interim;
ddns-updates      on;
server-identifier server;
ddns-domainname   "example.com.";
ignore client-updates;
key server.example.com {
  algorithm hmac-md5;
  secret your-key-from-step-2-here;
}
zone example.com. {
  primary 127.0.0.1;
  key server.example.com;
}
zone 1.168.192.in-addr.arpa. {
  primary 127.0.0.1;
  key server.example.com;
}
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.100 192.168.1.199;
  option domain-name-servers 192.168.1.2;
}
```

6. **上記のステップ 1 から 5 を完了したら、`/etc/init.d` スクリプトを実行して、DNS サーバと DHCP サーバを起動します。**

   いったんサーバが稼働すると、DHCPのために構成された新しいILOMのSPは、電源投入時にホスト名で自動的にアクセスできるようになります。必要に応じて、ログファイル、`dig`、`nslookup`、およびほかのユーティリティーを使用してデバッグします。

参照先

この例で使用した、Linux の DHCP サーバと DNS サーバの詳細は、次の Internet Systems Consortium の Web サイトを参照してください。http://www.isc.org/

付録B

用語集

A

access control list, ACL (アクセス制御リスト)
サーバ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。

Active Directory
Microsoft Windows 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。Active Directory は、ユーザー資格の認証とネットワークリソースへのユーザーのアクセスレベルの承認を提供します。

actual power (実電力)
システム内のすべての電源装置で消費される電力の量。

address (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.fujitsu.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。

address resolution (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。

Address Resolution Protocol, ARP (アドレス解決プロトコル)
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。

Administrator (管理者)
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。

agent (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。

alert (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。

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。

authentication (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) を使ってサーバを常に認証します。

authenticated user (認証済みユーザー) 正しく認証され、特定のシステムリソースへのアクセス権限を付与されたユーザー。

authorization (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。

available power (使用可能電力) ラック搭載型サーバの場合、使用可能電力は、電源装置が供給できる電力すべての合計です。サーバモジュールの場合、使用可能電力は、シャーシがサーバモジュールに供給する用意のある電力の量です。

B

bandwidth (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。

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持するために自立的に動作できます。

baud rate (ボーレート) たとえば端末とサーバの間といったデバイス間で送信される情報の速度。

bind (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 サーバに接続する際に行われます。

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。

blade modular system (ブレードモジュールシステム)
: 複数のサーバモジュールを保持するシャーシ。

blade server module (ブレードサーバモジュール)
: シャーシに挿入できるサーバモジュール (ブレード)。モジュラーシステムとも呼ばれます。

boot loader (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。

C

cache (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。

certificate (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。

Certificate Authority, CA (認証局)
: 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。

chassis monitoring module, CMM (シャーシ監視モジュール) 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 (Service Processor、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。

client (クライアント) クライアント/サーバモデルにおいて、ネットワーク上のサーバ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。

command-line interface, CLI (コマンド行インタフェース) 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。

console 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。

Coordinated Universal Time, UTC (協定世界時) 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 サーバが使用します。

core file (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。

critical event (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。

customer-replaceable unit, CRU (顧客交換可能ユニット) 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。

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、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。

digital signature (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。

Digital Signature Algorithm, DSA (デジタル署名アルゴリズム)
: 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。

デジタル署名アルゴリズム, DMA (ダイレクトメモリーアクセス)
: 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。

directory server (ディレクトリサーバ)
: 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。

Distinguished Name, DN (識別名)
: 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。

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。

domain (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。

domain name (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「fujitsu.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。

Domain Name Server, DNS (ドメインネームサーバ)
: ドメインにおいて通常はホスト名を管理するサーバ。DNS サーバは「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。

Domain Name System, DNS (ドメインネームシステム)
: 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.fujitsu.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 サーバから受け取ります。

Dynamic Domain Name Service, DDNS (動的ドメインネームサービス)
: ドメインネームサーバ (DNS) が、ドメイン名に関連付けられた動的または静的 IP アドレスを常に認識できるようにするサービス。

Dynamic Host Configuration Protocol, DHCP (動的ホスト構成プロトコル)
: DHCP サーバが、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。

E

enhanced parallel port, EPP (拡張パラレルポート)
: 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。

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。

event (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いません。

external serial port (外部シリアルポート)
: サーバの RJ-45 シリアルポート。

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。

F

failover (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。

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。

Fault Management Architecture, FMA (障害管理アーキテクチャー) ハードウェアやソフトウェアに障害が発生してもコンピュータが機能し続けるようにするアーキテクチャー。

field-replaceable unit, FRU (現場交換可能ユニット) 顧客サイトで交換可能なシステム部品。

file system (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。

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。

firewall (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。

firmware (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。

fully qualified domain name, FQDN (完全修飾ドメイン名) 「www.fujitsu.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、ホストサーバ名 (www) や、第 1 レベル (.com) および第 2 レベル (.fujitsu) 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。

G

gateway (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。

Gigabit Ethernet (ギガビット Ethernet) — 最大 1000 Mbps でデータを転送する Ethernet 技術。

graphical user interface, GUI (グラフィカルユーザーインタフェース) — 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。

H

host (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。

host ID (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。

host name (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。

hot-plug (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。

hot-swap (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。

Hypertext Transfer Protocol, HTTP (ハイパーテキスト転送プロトコル)
: 遠隔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への要求およびサーバ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。

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

ILOM Remote Console (ILOM リモートコンソール)
: デバイス (キーボード、マウス、ビデオディスプレイ、ストレージメディア) をデスクトップから遠隔ホストサーバへリダイレクトするグラフィカルユーザーインタフェース。

in-band system management (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、サーバがきちんと機能している場合のみ使用可能な、サーバ管理機能。

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。

internal serial port (内部シリアルポート)
: ホストサーバと 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。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。

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。

Internet Protocol, IP (インターネットプロトコル)　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。

Internet Protocol, IP (インターネットプロトコル) 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。

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 Remote Console (Java リモートコンソール)　動作中のアプリケーションにユーザーがアクセスするための、Java で書かれたコンソール。

Java(TM) Web Start application (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

kernel (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。

Keyboard Controller Style (KCS) interface (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。

keyboard, video, mouse, storage, KVMS (キーボード、ビデオ、マウス、ストレージ) 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。

L

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。

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。

Lightweight Directory Access Protocol (LDAP) server (LDAP サーバ) 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。

local area network, LAN (構内通信網) 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。

local host (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。

M

major event (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。

Management Information Base, MIB (管理情報ベース) 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。

man pages (マニュアルページ) オンライン UNIX ドキュメント。

media access control (MAC) address (媒体アクセス制御アドレス) 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。

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。

minor event (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。

N

namespace (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。

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。

network interface card, NIC (ネットワークインタフェースカード)
ワークステーションやサーバ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。

network management station, NMS (ネットワーク管理ステーション)
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。

network mask (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。

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 サーバのミリ秒に同期します。

node (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。

nonvolatile memory (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。

O

object identifier, OID (オブジェクト識別子)
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。

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。

Operator (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。

out-of-band (OOB) system management (帯域外システム管理)
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が正常に機能していない時に使用可能なサーバ管理機能。

P

parity (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。

PC-Check コンピュータハードウェアで診断テストを実行するアプリケーション。

permissions (権限) 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。

permitted power (許容電力) 特定の時点でサーバが使用を許可する最大電力。

physical address (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。

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。

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。

port (ポート) TCP/IP 接続が確立される場所 (ソケット)。Web サーバは従来からポート 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プログラムを指定できます。サーバ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。

port number (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。

power cycling (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。

Power Monitoring

interface (電源監視インタフェース)
: サービスプロセッサ (service processor、SP) または個々の電源装置について、使用可能電力、実電力、および許容電力を含むリアルタイムの消費電力を、電力が使用された時点から 1 分以内という正確さで監視できるインタフェース。

power-on self-test, POST (電源投入時自己診断)
: 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。

PXE
: 業界標準クライアント/サーバインタフェースで、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 (operating system、OS) をサーバ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。

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。

protocol (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。

proxy (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。

public key encryption (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。

R

real-time clock, RTC (リアルタイムクロック)
: 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。

reboot (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。

redirection (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。

RADIUS
: サーバ上のデータベースの情報を使用してユーザーを認証し、承認されたユーザーにリソースへのアクセス権限を付与するプロトコル。

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。

remote procedure call, RPC (遠隔手続き呼び出し)
: クライアントシステムがリモートサーバ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。

remote system (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。

reset (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。

role (役割)
: ユーザーのアクセス権を決定するユーザーアカウントの属性。

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。

root directory (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。

router (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。

RSA algorithm (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

schema (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。

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。

sensor data record, SDR (センサーデータレコード) 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。

serial console (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。

serial port (シリアルポート) コマンド行インタフェース (CLI) や、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を可能にするポート。

server certificate (サーバ証明書) 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。

Server Message Block (SMB) protocol (サーバメッセージブロックプロトコル) 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プログラムのファイルの読み書きおよびサーバ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。

service processor, SP (サービスプロセッサ)
: 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持するために自立的に動作できます。

session time-out (セッションタイムアウト)
: サーバがユーザーセッションを無効化するまでの一定の時間。

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、ホストやルーター、Web サーバ、またはネットワーク上のその他のサーバなどの、SNMP が動作しているいずれのデバイスも含まれます。

Single Sign On, SSO (シングルサインオン)
: 資格を 1 回入力するだけで複数のアプリケーションにアクセスできる認証形式。

Snapshot utility (スナップショットユーティリティー)
: サーバプロセッサ (server processor、SP) の状態に関するデータを収集するアプリケーション。保守担当者がこのデータを診断用に使用します。

subnet (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。

subnet mask (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。

superuser (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。

syslog
: ログメッセージをサーバへ送信するためのプロトコル。

system event log, SEL (システムイベントログ)
: 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。

system identifier (システム識別子)
: ホストシステムを識別するテキスト文字列。この文字列は、SUN-HW-TRAP-MIB で生成される SNMP トラップに変数バインディングとして含まれます。システム識別子は任意の文字列に設定できますが、一般にホストシステムの識別に使用できるようにします。ホストシステムを識別するには、その位置を記述するか、ホスト上のオペレーティングシステムが使用するホスト名を参考にします。

T

Telnet
: あるホストのユーザーが遠隔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。遠隔ホストにログインしているあるホストの Telnet ユーザーは、その遠隔ホストの通常の端末ユーザーのように対話できます。

threshold (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。

time-out (タイムアウト)
: サーバが、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。

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。

trap (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。

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

Uniform Resource Identifier, URI (ユニフォームリソース識別子)	インターネットまたはイントラネット上のリソースを識別する固有の文字列。
Universal Serial Bus, USB (ユニバーサルシリアルバス)	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。
user account (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。
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。
user privilege levels (ユーザーの権限レベル)	ユーザーが実行できる操作とアクセスできるリソースを指定するユーザーの属性。
user identification, userid (ユーザー ID)	システムのユーザーを識別する固有の文字列。
user identification number, UID number (ユーザー ID 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。
user name (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。

W

web server
(Web サーバ)

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、サーバサイドプログラムを実行します。

wide area network, WAN
(広域通信網)

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。

X

X.509 certificate
(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。

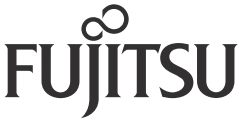
X Window System
(X ウィンドウシステム)

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。

索引

り

れ


FUJITSU