User Guide - 日本語

FUJITSU

Rack Management Unit (RMU)

Hardware, Firmware, Software Interfaces

2010/3

DIN EN ISO 9001:2000 に準拠した認証を取得

高い品質とお客様の使いやすさが常に確保されるように、このマニュアルは、DIN EN ISO 9001:2000 基準の要件に準拠した品質管理システムの規定を満たすように作成されました。

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

著作権および商標

お届けまでの日数は在庫状況によって異なります。技術的修正の権利を有します。

使用されているハードウェア名とソフトウェア名は、各メーカーの商標名および商標です。

Microsoft、Windows、Windows Server、および Hyper V は、米国およびその他の国における Microsoft Corporation の商標または登録商標です。

Intel および Xeon は、米国 Intel Corporation またはその関連会社の米国およびその他の国における登録商標または商標です。

目次

1 はじめに

ラックサーバのラック管理ユニット (RMU) を用いると、サーバの集中換気システムの無故障稼動に寄与するコンポーネント、すなわちファン、圧力センサ、温度センサを監視、制御することができます。

ラックサーバシステムの集中冷却システムは 2 個の集中ファンを搭載しています。これらのファンが低圧チャンバから空気を排出して、サーバを通り抜ける空気流を発生させます。

自立型コンポーネントとして、RMU は独自のオペレーティングシステム、独自の Web サーバ、別個のユーザー管理、それに独立の警告 (アラート) 管理機能を備えています。ラックサーバがスタンバイモードのときでも RMU はパワーオンのままです。

1.1 本書のコンセプトとターゲットグループ

本書をお読みになれば、集中冷却ラックサーバシステムの監視・制御用に設計されたラック管理ユニット (RMU) について詳しくお知りいただけます。

本書は次の事項について説明します。

- 第 2 章 ラック管理ユニット "

  この章では RMU のハードウェア、ファームウェア、およびテクニカルデータの概要を紹介します。

- 第 3 章 : "RMU を用いたラックサーバ管理 "

  この章では、RMU を使用して、サーバの集中換気システムの無故障運転に寄与するラックサーバシステムのコンポーネントをどのように監視・制御できるかを説明します。

- 第 4 章 : " RMU のユーザー管理 "

  この章では RMU のユーザー管理について詳しく説明します。RMU は 2 種類のユーザー管理を区別します。

  – RMU 内部ローカルユーザー管理。

  – RMU のグローバルユーザー管理は、次のディレクトリサービスをサポートします。Microsoft ActiveDirectory, Novell eDirectory、および Open LDAP.

- 第 5 章 : "RMU Web インターフェース "

  この章では RMU Web インターフェースの機能を説明します。Web インターフェースを使用すれば、すべてのシステム情報とセンサーから得られるファン速度、電圧などのデータにアクセスすることができます。RMU Web インターフェースからは RMU 設定値の設定もできます。

- 第 6 章 : "RMU シリアルポートインターフェース (リモートマネージャ)"

  この章では、リモートマネージャとして知られる RMU の Telnet ベースインターフェースについて説明します。RMU は SSH (**セキュアシェル**) 上のセキュリティ保護された接続をサポートします。リモートマネージャインターフェースは Telnet および SSH 接続と同じものです。リモートマネージャは RMU Web インターフェースでも、Telnet/SSH クライアントでも呼び出すことができます。

本書は、システム管理者およびネットワーク管理者、ハードウェアおよびソフトウェアの十分な知識を持ったサービススタッフを対象としています。

1.2 文書

PRIMERGY のマニュアルは、PDF フォーマットのものが ServerView Suite DVD 2 にあります。ServerView Suite DVD 2 はサーバに付属しています。ServerView Suite DVDs をもうお持ちでない場合は、注文番号 U15000-C289 で最新のバージョンを入手することができます (日本市場向け注文番号は、サーバ設定者の URL を参照してください。
http://primeserver.fujitsu.com/primergy/system.html.

マニュアルの PDF ファイルはインターネットから無料でダウンロードすることもできます。インターネットで入手可能なオンライン文書を記載した概観ページは、次の URL (EMEA 市場向け) で見ることができます。
http://manuals.ts.fujitsu.com.

PRIMERGY サーバ文書は、インダストリースタンダードサーバ (PC サーバ) のナビゲーション機能を用いてアクセスできます。日本市場向けは次の URL を使用してください。*http://primeserver.fujitsu.com/primergy/manual.html*.

1.3 本文中の記号

本書で使用している記号には、次の意味があります。

 **注意**	この記号は、人的傷害、データ損失、機材破損の危険性を示しています。
	この記号は、重要な情報やヒントを強調しています。
►	この記号は、操作を続行するために行わなければならない手順を示しています。
斜体	コマンド、ファイル名、およびパス名は、*斜体* で表記されています。
固定フォント	システム出力は、固定フォントで表記されています。
太字の固定フォント	キーボードから入力する必要のあるコマンドは、太字の固定フォントで表記されています。
<abc>	山カッコは、実数値に置き換えられる変数を囲っています。
[パラメータ]	大括弧は、オプション（任意指定）パラメータとオプションを示すために使用されます。
Key symbols	キーは、キーボード上の該当するキーを表しています。また、大文字を入力する必要がある場合は、シフトキーも表示されています。 例：大文字 A の場合、SHIFT - A 2 つのキーを同時に押す必要がある場合は、それぞれのキー記号の間にハイフンが表示されています。

表 1: 本書の表記

本書内での引用箇所を示す場合は、参照するセクションの章名もしくは節名およびページ番号で示しています。

2 ラック管理ユニット (RMU)

本章では次の事項について説明しています。

– ラック管理ユニットの表示ランプ、制御機能、コネクタ

– RMU ファームウェアと RMU ファームウェア更新法の概要

– RMU を使用したラックサーバ管理

2.1 ラック管理ユニット (RMU) - ハードウェア

ラック管理ユニット (RMU) は、ラックサーバシステムとその全コンポーネントを冷却する 2 個の大型ファンを自律的に制御、監視します。これにより低また外部データセンター管理施設に圧チャンバ内を一定の低圧に維持し、騒音レベルと電力損を最小限に抑え、報告を行います。

図 1: ラック管理ユニット (RMU)

特徴

- 両システムファンの制御および監視
- 圧力測定
- 2 個の温度センサのサポート
- 3 個の汎用入力
- アラーム出力
- リモート識別出力
- ホットプラグ対応 FRU ユニット
- リセットボタン
- 状態表示ランプ
- シリアルポート
- LAN インターフェース

2.1.1 フロントパネル

周囲圧力センサおよびコネクタ

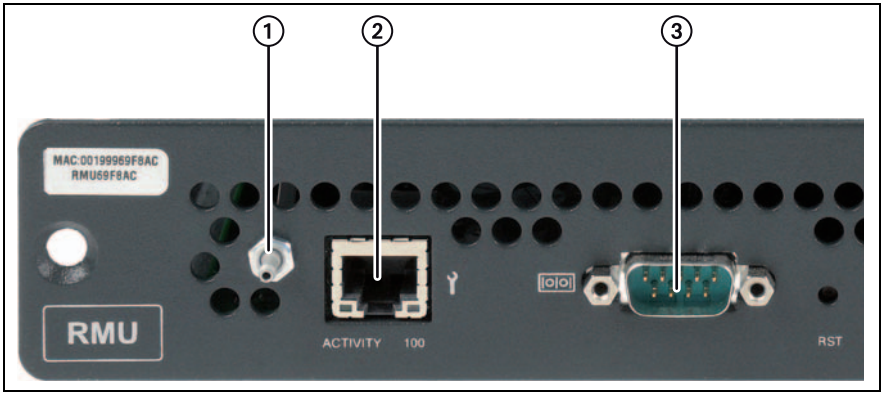


図 2: RMU フロントパネル - コネクタ

1	圧力センサ (周囲圧力の測定点)	2	10/100 Mbit LAN コネクタ
		3	Telnet/SSH ベース・リモートマネージャインターフェース用 COM1 シリアルコネクタ

フロント表示ランプおよびコントロール

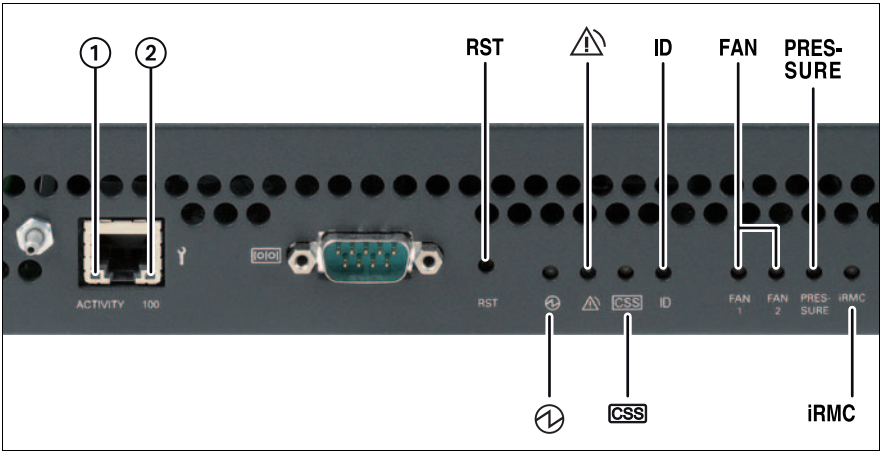


図 3: RMU フロントパネル - 表示ランプおよびコントロール

1 / 2	**1 監視用 LAN アクセス表示ランプ 2 監視用 LAN 転送速度表示ランプ**	
	緑 ON / 緑 ON	100 Mbps
	OFF / 緑 ON	10 Mbps
	OFF / OFF	電源オフ

RST	**リセットボタン**
	リセットボタンを押すと RMU は再起動します。

	電源オン表示ランプ (緑)	
	緑 ON	RMU は電源に接続されている。

	**グローバルエラー表示ランプ (オレンジ)**	
	オレンジ ON	故障の予兆を検出したときに点灯します .
	オレンジ 点滅	故障・異常を検出したときに点滅します .
	i	停電後に重大なイベントがまだ残っている場合、表示ランプは再起動後に点灯します. 表示されたエラーについて、システムイベントログ (SEL) で詳しく知ることができます。

CSS	**CSS ランプ (未対応)**
	利用可能な CSS コンポーネントはなし。

ID	ID 表示ランプ (青)	
	青 ON	システムが RMUWeb インターフェースでの識別のために選ばれているときは青に点灯。

ファン 1 **ファン 2**	ファン故障表示ランプ (黄色)	
	黄色 ON	ファン 1 / 2 故障の予兆、または故障 ファン 1 / 2 は直ちに取り替える必要あり。.

圧力	空気圧表示ランプ (オレンジ)	
	オレンジ ON	故障の予兆、または エラー 圧力レベルは正常範囲外。ファンがフル稼動しても低圧が実現できない。
	i	圧力表示ランプは必ずグローバルエラー表示ランプと一緒に点灯します。

iRMC	iRMC 表示ランプ (緑)	
	緑 FLASHING	RMU 内部サーバ管理コントローラ（iRMC S2）は正しく動作しています。
	緑 ON 又は OFF	iRMC S2 は停止しています。

2.1.2 リアパネル

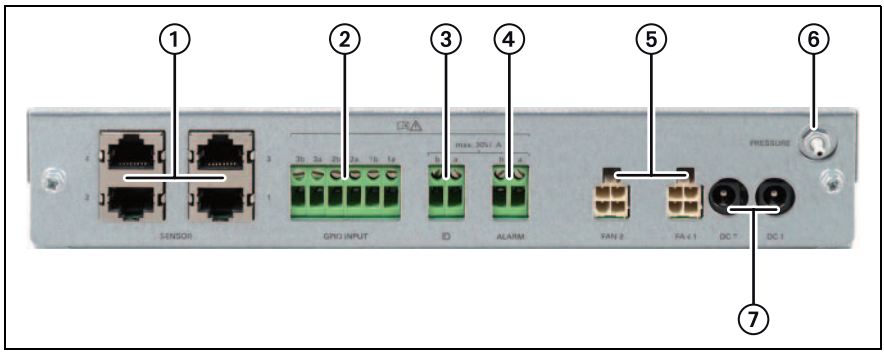


図 4: RMU リアパネルコネクタ

1	4x RJ45 コネクタ センサ 1 = 排気温度センサまたはセンサ 2-4 は不使用	4	2 ピンねじ込み端子 (ステータス用リレー接点)
		5	2x 4 ピン・ミニフィット 4.2 mm ファンコネクタ
2	6 ピンねじ込み端子 (3 個の外部接点); 外部接点で端子 a<、b 間を接続。	6	圧力センサ (圧力チャンバ低圧の測定点)
3	2 ピンねじ込み端子 (ID 用リレー接点)	7	2x PSU コネクタ 2.5 mm, 5 V / 2 A

2.2 ラック管理ユニット (RMU) - ファームウェア

RMU は、万一のファームウェア故障の場合にフォールバック機構となるように、2 種類の異なるファームウェアイメージを使用します。

2 種類のファームウェアイメージは 16-MB EEPROM (**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory) に格納されています。

– ファームウェアイメージ 1 (low FW イメージ)
– ファームウェアイメージ 2 (high FW イメージ)

RMU のファームウェアは EEPROM では実行されず、起動時に SRAM メモリにロードされ、そこで実行されます。したがって、オンラインつまり Windows もしくは Linux といったサーバのオペレーティングシステムの実行中に、動作中のファームウェアと動作していないファームウェアの両方をアップデートすることができます。

動作中の RMU ファームウェアおよび EEPROM に関する情報は、RMUWeb インターフェース、*RMU ファームウェアアップデートのページにあります* (164 ページを参照)。

2.2.1 RMU ファームウェア - 概要

アクティブおよびパッシブファームウェアイメージ

常時 2 種類のファームウェアイメージのうちのどちらかが動作しています。どちらのファームウェアイメージが実行されるかは、いわゆるファームウェアセレクタが決定します (21 ページ参照)。

RMU EEPROM - の構造

RMU の EEPROM には、ファームウェアイメージ 1 用の領域とファームウェアイメージ 2 用の領域とがあります。

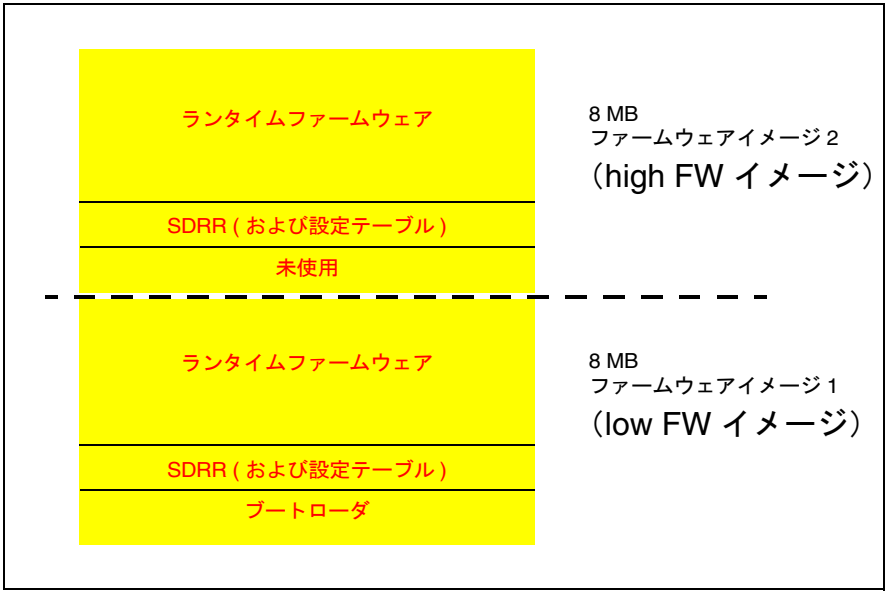


図 5: RMU EEPROM - の構造

– ブートローダ

  ブートローダは、動作中のファームウェアイメージの状態確認を行います。ファームウェアエラーを発見すると、ファームウェアセレクタにもう一方のファームウェアイメージを設定します。

– SDRR (Sensor Data Record Repository)

  SDRR 内の SDR（Sensor Data Records）には、管理対象サーバのセンサ情報が格納されています。また、SDRR は SDR にアクセスするためのインターフェースとしての役割も果たします。

– ランタイムファームウェア

  ランタイムファームウェアは RMU のファームウェアの実行可能部分です。

この 3 つの領域の各々について、ファームウェアのアップデートが行えます。

ファームウェアセレクタ

ファームウェアセレクタが、実行する RMU ファームウェアを指定します。RMU が再設定および再起動されるたびに、ファームウェアセレクタが評価され、対応するファームウェへのブランチを処理します。

ファームウェアセレクタには、次の値があります。:

0 ファームウェアバージョン最も新しいファームウェアイメージ

1 ファームウェアイメージ 1

2 ファームウェアイメージ 2

3 ファームウェアバージョンが最も古いファームウェアイメージ

4 更新時期が最も新しいファームウェアイメージ

5 更新時期が最も古いファームウェアイメージ

どんな形の更新イメージを用いるかによって、更新後のファームウェアセレクタの設定は異なります。

ファームウェアセレクタのクエリと明示的設定は、RMUWeb インターフェースの RMU 情報ページで行うことができます (146 ページ参照)。

2.2.2 RMU ファームウェアの更新

RMU ファームウェアの更新は、RMU Web インターフェースの RMU 更新ページで行います (164 ページ の「RMU アップデート」の項を参照).

最新バージョンのファームウェアは Fujitsu Technology Solutions Web サーバのダウンロードセクションから手動でダウンロードすることができます。

ファームウェアを更新する前に、最新バージョンのファームウェアの注意書き（特に Readme ファイル）をしっかりとお読みください。

更新したファームウェアを起動するには、RMU を再起動する必要があります。

注意 !

ファームウェアを更新するときは、ランタイムファームウェアおよび SDR（Sensor Data Record、20 ページ を参照) が同一ファームウェアリリースのものである場合にのみファームウェアの正常な動作が保証されます。ご注意ください。

2.3 ラック管理ユニット (RMU) - テクニカルデータ

電気的データ

電源電圧 (DC 入力)	5V +/- 5%
現在の電力消費量 (最大)	0.65 A / 3.25 W

規制および規格への適合

製品の安全性と人間工学	
グローバル	IEC 60950-1/2
ヨーロッパ	EN 60950-1/2
米国 / カナダ	UL/CSA 60950-1/2
台湾	CNS 14336
中国	GB 4943

電磁両立性	
ヨーロッパ	EN 55022 EN 55024 EN 61000-3-2/ EN 61000-3-3
米国 / カナダ	FCC Class A 47CFR part 15 Class A / ICES-003
オーストラリア / ニュージーランド	AS / NZS 3548 Class A
台湾	CNS 13438
中国	GB 9245 / GB 17625
日本	VCCI Class A / Jeida

適合宣言	
ヨーロッパ (CE)	89/336/EEC(EMV);73/23 EEC(LVD)
北米	FCC class A

承認	
グローバル	CB
米国 / カナダ	CSAUS / CSAC

寸法および重量

幅	255 mm
奥行	171 mm
高さ	45 mm / 1 HU
重量	1.18 kg

搭載

RMU は必ずシャシスロット内に搭載してください。

重要！

フロントカバーから周囲空気が (集中換気により) 常に滞りなく吸い込まれるようにしなければなりません。

周囲条件

注意！

稼動中決して結露が生じないようにすること。

環境クラス 3K2 環境クラス 2K2	DIN IEC 721 section 3-3 DIN IEC 721 section 3-2
温度 : 稼動時 (3K2) 輸送時 (2K2)	 10°C ... 35°C -25°C ... 60°C
湿度	10% .. 85% RH 結露なし 稼動中決して結露が生じないこと。

3 RMU を使用するラックサーバ管理

ラックサーバのラック管理ユニット (RMU) を用いて、サーバの集中換気システムの無故障稼動に寄与するコンポーネントを監視、制御することができます。

RMU には、集中換気システムの監視用と設定用の 2 つのインターフェースがあります。

– RMU Web インターフェース (137 ページを参照)

– RMU シリアルポートインターフェース (231 ページを参照)。

RMU は自動的・自律的に集中換気ファン (ファン 1 およびファン 2) の速度を制御し、また広範な監視機能を遂行します。

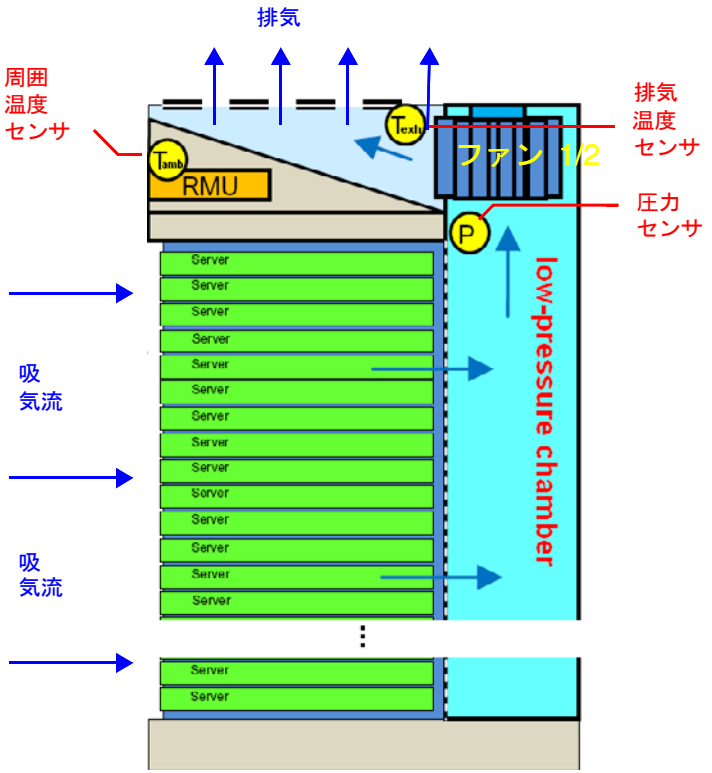
本章では次の事項について説明します。

– RMU による自律的ファン速度制御と、制御に関連する設定。

– RMU の有する監視機能

3.1 ファン速度制御

RMU は、ラックの全コンポーネントの間接冷却を行う 2 個の集中ファンを制御、監視するように設計されています。そのためにファンは低圧チャンバから空気を排出して空気流を発生させ、この空気流が個々のサーバを通り抜けながら冷却します (図 6 を参照)。



1.) 空気を排出することにより、ファン 1 とファン 2 はチャンバ内に低圧を発生さ。

2.) 低圧チャンバと周囲圧力との差が
サーバを通り抜ける空気流を発生させます。

3.) 測定値 (周囲 / 排気温度、圧力) と
ユーザーの設定値とにしたがい、RMU はファン 1 とファン 2 の速度を制御して適切な空気流を維持します。

図 6: 空気流の発生によるラックコンポーネントの冷却

RMU は次の目標にしたがい自律的にファン 1 とファン 2 を制御します。

– 消費電力と騒音レベル の最小化

– 常時のファン監視によりファンの誤作動をただちに検出することができます。

– 冗長ファン (ファン 1 およびファン 2) がフェイルオーバー保護を提供します。一方のファンが故障すると、RMU は自動的に他方のファンをスピードアップさせて、適切な空気流を確実に維持します。

RMU は自律的にファン速度を制御

RMU は次の諸点を考慮しながら自動的にファン速度を制御します。

– ファンの最大速度時の冷却能力は周囲温度を 35° C として設計されています。周囲温度が低いときは小さいファン速度 ですみます。

– 使用負荷が小さいときは、RMU はファンを可能な限り減速させることにより電力消費を最小にします。

– ファン 1 とファン 2 は排気流のなかにあり、使用温度範囲を超えてはいけません。そのため、排気温度が警告レベルに達すると、RMU はファンを加速させます。

自律的 RMU ファン速度制御アルゴリズムのカスタマイズ

RMU はまた、内蔵ファン速度制御アルゴリズムをカスタマイズしてユーザーの特殊なニーズに適合させることも可能です。ラックサーバシステムが高負荷で作動しているか、低負荷で動作しているかにより、消費電力最小化の戦略は、適切なファン速度の点で違ってきます。

– ラックサーバシステムが高負荷で稼動している場合

  ファン速度を上げると個々のサーバの温度が低下し、それにより、システム全体の消費電力が減少します (半導体の熱挙動による)。

– ラックサーバシステムが低負荷で稼動している場合

  ファン速度を上げるとシステム全体の消費電力は増大します。個々のサーバはすでに低い温度をそのまま維持し、ファンの電力消費が増大するからです。

圧力プロファイル

ラックサーバシステムの集中換気を最適化するため、RMU では 3 通りの圧力プロファイル、すなわち*低*、*中*、*高*からひとつを選択することができます。周囲温度と排気温度の測定値に応じて、各圧力プロファイルは、周囲温度と RMU が設定する低圧チャンバ内の圧力との差を定めます。適切な圧力プロファイルの指定は RMU Web インターフェースを用いて行います (173 ページ の「圧力情報 - 圧力センサのチェック」の項を参照)。

各圧力プロファイルについて、の表 2 は、周囲温度、排気温度と、MRU の設定する結果の圧力差との相互関係を示します。

圧力プロファイル	下の場合の設定圧力差	
	周囲温度 < 32° C かつ排気温度 < 45° c	周囲温度 > 35° C かつ排気温度 > 50° C
低	0.036 kPa	0.062 kPa
中 (デフォルト設定)	0.050 kPa	0.076 kPa
高	0.080 kPa	0.090 kPa

表 2: 圧力プロファイル

周囲温度や排気温度が次の範囲にある場合、RMU は線形内挿法を用いて設定圧力差を計算します。

$32^{o}C \leq$ 周囲温度 $\leq 35^{o}C$

$45^{o}C \leq$ 排気温度 $\leq 50^{o}C$

3.2 監視機能

RMU は常時、次のコンポーネントとセンサの状態を RMU Web インターフェースで報告します (169 ページ の「センサ - センサの状態のチェック」の項を参照 :

- ファン速度
- ファンの故障予兆検出
- 電圧
- 圧力
- 圧力漏れの状態
- 温度
- 汎用入出力 (GPIO)

ファン速度監視

RMU はファン 1 とファン 2 のファン速度を監視します。どちらかのファンが致命的な下限値まで減速すると、RMU は警告を生成します。

致命的な下限値は 840rpm です。

ファンの故障予兆検出

生産工程の途中で各ファンの最高速度が登録されます。ファンを交換するときは、ファン速度を再度登録する必要があります。登録された値は 100% の速度と見なされます。日々の最高速度測定が登録値の 70% を超えると、RMU は警告を生成します。

電圧監視

RMU はラックサーバのコンポーネントに割り当てられた電圧センサの状態を報告します。電圧が致命的なレベルを超えるたびに、RMU は対応するシステムイベントログ (SEL) イベントと警告を生成します。

圧力監視

RMU は低圧チャンバ内の圧力を監視します。圧力が設定値を超過すると、RMU はシステムイベントログ (SEL) イベントを生成し、圧力 LED を点灯させます。

表 3 に、致命的な値と非致命的な (警告) 値に関する情報を示します。

	致命的		非致命的		範囲		非致命的		致命的	
圧力 (単位 kPa)	デアサーション	アサート	デアサート	アサート	最小	最大	デアサート	アサート	デアサート	アサート
センサ	0.006	0.000	0.016	0.010	0.030	0.120	0.150	0.156	0.200	0.206

表 3: 圧力監視

圧力漏れの状態

圧力の測定値にもとづき、内部 MRU コントローラは所要の圧力に達するまでファンの速度を上げます。所要の圧力に到達できない (漏れなどにより) と、コントローラは最高速度までファンを加速します。それでも圧力が 20 秒以上 0.080 kPa 未満にとどまる場合は、RMU システムイベントログ (SEL) イベントを生成し、圧力 LED を点灯させます。

温度監視

RMU は温度を監視し、次のようなことが生じるとシステムイベントログ (SEL) イベントを生成します。

– 温度が非致命的 (警告) または致命的な上限アサートレベルを超える。

– 温度が警告または致命的レベルを下回る。ヒステリシスは通常 1° C です。

表 4 に、致命的な値と非致命的な (警告) 値に関する情報を示します。

温度 (単位 °C)	下限				動作範囲		上限			
	致命的		非致命的				非致命的		致命的	
	デアサート	アサート	デアサート	アサート	最低	最大	デアサート	アサート	デアサート	アサート
周囲	2	1	6	5	5	35	36	37	41	42
排気	2	1	6	5	5	55	51	52	56	57

表 4: 温度監視

非致命的 (警告) および致命的温度の値は、RMU Web インターフェースを使用して表 4 の動作範囲欄に定めた範囲内で変更することができます (171 ページ の「温度 - 温度センサのチェック」の項を参照)。

– 致命的な限度値がアサートされると、グローバルエラー LED が点灯します。

– 致命的な限度値がデアサートされると、グローバルエラー LED が消灯します。

汎用入出力 (GPIO) 監視

RMU はリアパネルの 6 ピン端子 (3 個の外部接点) (18 ページを参照) を通じて受け取る GPIO 入力の監視をサポートします。RMU はその必要がある状況では適切な警告を生成します。

4 RMU のユーザー管理

RMU のユーザー管理には 2 種類のことなるユーザー ID を使用します。

– ローカルユーザー ID は RMU の不揮発性記憶装置に保存され、RMU のユーザーインターフェース経由で管理されます。

– グローバルユーザー ID はディレクトリサービスの集中データストアに保存され、ディレクトリサービスのインターフェース経由で管理されます。

  グローバル RMU ユーザー管理では、現在以下のディレクトリサービスがサポートされます。

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP

本章では以下の事項について説明します。

– RMU のユーザー管理の概念
– ユーザー 許可
– RMU 上のローカルユーザー管理
– 個別のディレクトリサービスを使用するグローバルユーザー管理

4.1 RMU のユーザー管理の概念

RMU のユーザー管理は、ローカルとグローバルのユーザー ID を並列に管理することができます。

ユーザーがいずれかの RMU のインターフェースにログインするために入力する認証データ（ユーザー名、パスワード）を検証する際には、RMU は以下のように処理します (合わせて 35 ページ の図 7 も参照してください)。

1. RMU はユーザー名とパスワードを内部に保存されたユーザー ID と照合します。
   - ユーザーは、RMU 認証に成功すれば（ユーザー名とパスワードが有効）ログインすることができます。
   - 認証に失敗した場合には、RMU はステップ 2 の検証手順を継続します。
2. RMU はユーザー名とパスワードを使用して、LDAP 経由でディレクトリサービスの認証を受け、LDAP クエリによってユーザーの権限を判断してユーザーに RMU を操作する権限があるかどうかを確認します。

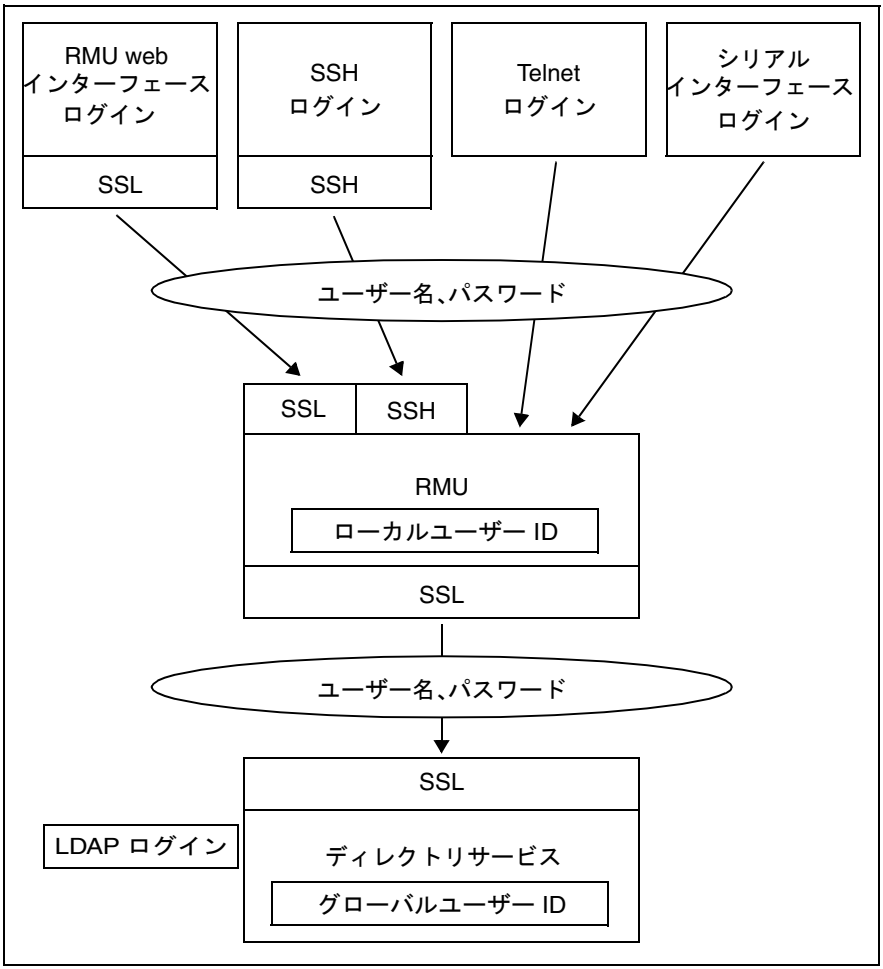


図 7: RMU 経由のログイン認証

RMU とディレクトリサービスの間の LDAP 接続には、オプションの SSL を使用することを推奨します。SSL で保護された RMU とディレクトリサービスの間の LDAP 接続では安全なデータ交換が保証されますが、特にユーザー名とパスワードのデータの送信が安全にできます。

RMU Web インターフェース経由の SSL ログインが必要になるのは、LDAP が有効な場合のみです (*LDAP 有効化オプション*、214 ページも参照)。

4.2 ユーザー許可

RMU は以下の 2 つの相互補完的なユーザー許可を区別します。

– チャネル (接続経路) 別特権（LAN ／シリアルの許可グループへの割り当てによる)

– RMU 独自の機能によるアクセス許可

個々の RMU 機能を使用するために必要な特権と許可は次の下記のページに説明があります。

– RMU-Web インターフェースに関しては、137 ページを参照。

– リモートマネージャに関しては、231 ページを参照。

チャネル別特権（LAN ／シリアルの許可グループ)

RMU は各々のユーザー ID を次の 4 つの LAN ／シリアル接続許可グループのうちのひとつに割り当てます。

– User (ユーザー)
– Operator (オペレーター)
– Administrator (管理者)
– OEM

RMU はこれらの許可を、チャンネル固有を基本にして割り当てますので、ユーザーは、RMU に LAN のインターフェースを経由して接続したか、シリアルインターフェースを経由して接続したかにより、別々に許可を取得することができます。

与えられる許可の範囲は、「User」（最も低い許可レベル）から 「Operator」、「Administrator」、「OEM」（最も高い許可レベル）の順に大きくなります。

許可グループは IPMI 特権レベルに対応しています。特定の許可（たとえば、「Power Management」）はこれらのグループまたは特権レベルに関連づけられます。

RMU 独自の機能による許可

チャネル別の許可に加えて、ユーザーに次の許可を個別に割り当てることもできます。

– ユーザーカウントの設定ローカルユーザー ID を設定する許可

– **RMU 設定の設定**
RMU 設定を設定する許可

初期設定のユーザー ID

RMU のファームウェアには、RMU 用のすべての許可を持つデフォルトの管理者 ID が用意されています。

管理者 ID:	admin
パスワード	admin

ローカルユーザーの場合には管理者 ID もパスワードも大文字小文字を区別します。

最初にログインした時になるべく早く新しい管理者アカウントを作成して、デフォルトの管理者アカウントを削除するか、少なくともパスワードを変更しておくことを強く推奨します (202 ページ の「RMU ユーザー - RMU 上のローカルユーザー管理」の項を参照してください)。

4.3 ローカルユーザー管理

RMU には独自のローカルユーザー管理方法があります。最大 16 人のユーザーをパスワード付きで設定し、それぞれが属するユーザーグループによってさまざまな権限を割り当てることができます。ユーザー ID は、RMU の不揮発性メモリに保存されます。ローカルユーザー管理は RMU Web インターフェースを使用して行うことができます。

4.3.1 RMU Web インターフェースを使用したローカルユーザー管理

RMU 上のユーザー管理には 「Configure User Accounts」許可が必要です。

設定されたユーザーのリストは Web インターフェースの下に見ることができます。新しいユーザーの設定、既存ユーザーの設定変更、または、ユーザーのリストからの削除が可能です。

- RMU Web インターフェースを起動します (138 ページ の「RMU Web インターフェースへの ログイン」の項を参照してください)。

設定されたユーザーのリスト表示

- ナビゲーション領域で「ユーザー管理」-「RMU ユーザー」(ユーザー管理 - RMU User) 機能をクリックします。

  「ユーザー管理」ページが開いて設定されたユーザーのリストが表示されます (201 ページを参照してください)。ここで、ユーザーの削除と新しいユーザーの設定ができます。

新しいユーザーの設定

- *「ユーザー管理」ページで、［ユーザーの新規作成］(New User)) ボタンをクリックします。*

  「新しいユーザーの設定」(New User Configuration) ページが開きます。このページで新しいユーザーの基本設定を設定することができます。このページについては 203 ページ の「新規ユーザー設定 - 新規ユーザーの設定」に説明があります。

ユーザー設定の変更

- 「ユーザー管理」ページで、設定されたパラメータを変更したいユーザーのユーザー名をクリックします。

  「ユーザー名の設定」(> <><<>>*User “<name>” Configuration*) ページが開いて選択されたユーザーの設定値を表示します。このページで新しいユーザーの設定パラメータを変更することができます。このページについては、204 ページ の「ユーザー名の設定 - ユーザー設定 (詳細)」に説明があります。

ユーザーの削除

- 「ユーザー管理」ページで、削除するユーザーと同じ行にある［削除］(Delete) ボタンをクリックします。

4.3.2 ローカル RMU ユーザーの SSHv2 公開鍵認証

ユーザー名とパスワードによる認証方法に加えて、RMU は SSHv2 に基づくローカルユーザーの公開鍵と秘密鍵のペアを使用する公開鍵認証もサポートしています。SSHv2 公開鍵認証を実装するには、RMU ユーザーの SSHv2 鍵を RMU にアップロードし、RMU ユーザーは <、たとえば、PuTTY プログラムまたは OpenSSH クライアントプログラムの「ssh」などでその秘密鍵を使用します。

RMU はは以下の種類の公開鍵をサポートしています。

– SSH DSS (最低要件)
– SSH RSA (推奨)

アップロードする公開 SSHv2 鍵は、RFC4716 フォーマットでも OpenSSH フォーマットでも使用可能です (52 ページを参照してください)。

公開鍵認証

RMU の公開鍵認証は、おおむね以下のように処理されます。

RMU にログインしたいユーザーが鍵のペアを作成します。

– 秘密鍵は読み取り保護され、ユーザーのコンピュータ内に保存されます。

– ユーザー（または管理者）は公開鍵を RMU にアップロードします。

設定が正しければ、ユーザーはパスワードの入力をしなくても非常に安全に RMU にログインすることができるようになります。ユーザーの責任は秘密鍵の機密保護のみです。

秘密鍵の認証には以下の手続きが必要です。この手続きはこれ以降の節にも説明があります。

1. 「PuTTYgen」または「ssh-keygen」プログラムを使用して SSHv2 の公開鍵と秘密鍵を作成して、別々のファイルに保存します (41 ページを参照してください)。
2. ファイルから SSHv2 鍵を RMU にアップロードします (45 ページを参照してください)。
3. 「PuTTY」または「ssh」プログラムを RMU への SSHv2 アクセス用に設定します (47 ページを参照してください)。

4.3.2.1 SSHv2 の公開鍵と秘密鍵の作成

SSHv2 の公開鍵と秘密鍵を以下のように作成することができます。

– プログラム「PuTTYgen」を使用する。

– または、– OpenSSH クライアントプログラム、「ssh-keygen」を使用する。

PuTTYgen を使用する SSHv2 の公開鍵と秘密鍵の作成

以下の通り進めます。

► ユーザーの Windows 機で PuTTYgen を起動します。

PuTTYgen が起動すると以下の画面が表示されます。

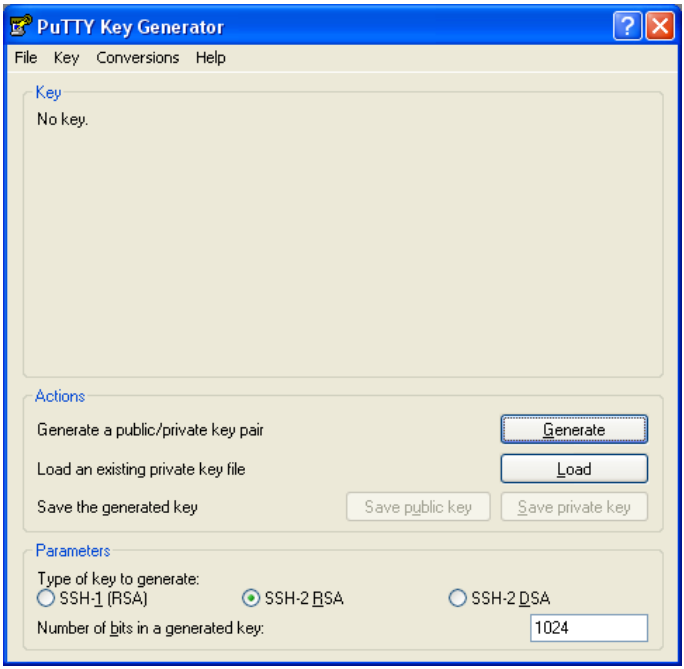


図 8: PuTTYgen: SSHv2 の新しい公開鍵と秘密鍵の作成

► 「Parameters」の項目で SSH-2RSA 鍵タイプを選択し［Generate］をクリックすると鍵の生成が開始されます。

鍵生成の進行状況は「Key」のペインに表示されます (42 ページ の図 9 を参照してください)。

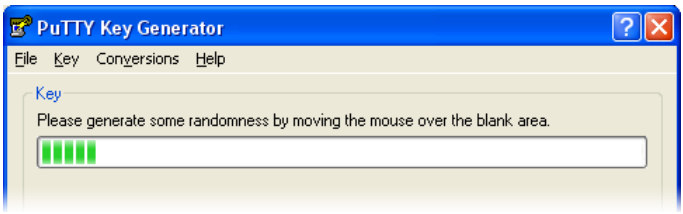


図 9: PuTTYgen: 新しい鍵のペアの作成 (プログレスバー)。

- 進行表示部の空白部分でマウスポインタを動かすと、作成される鍵のランダム性がより増大します。

鍵が生成されると PuTTYgen が鍵と公開 SSHv2 鍵の指紋を表示します。

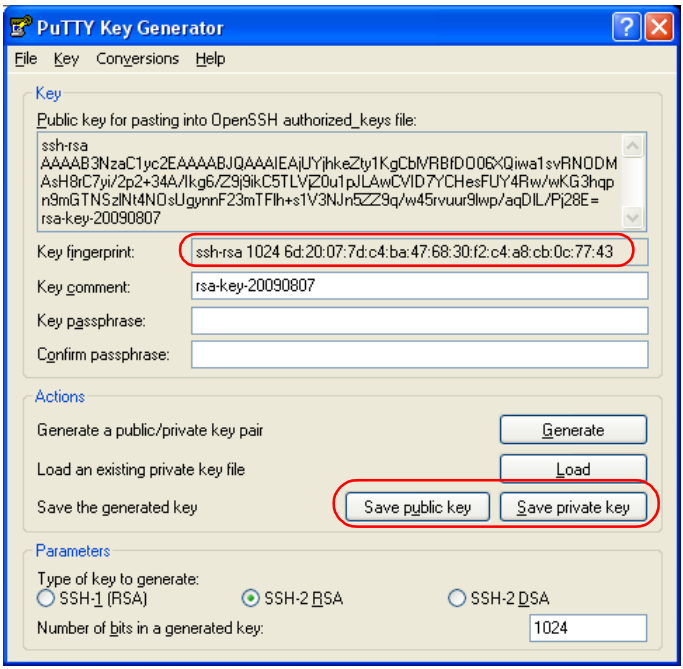


図 10: PuTTYgen: 新しい秘密 SSHv2 鍵の作成 (プログレスバー)。

- ［Save public key］ボタンをクリックして、SSHv2 鍵をファイルに保存してください。このファイルから RMU に公開鍵をアップロードすることができます (45 ページを参照してください)。
- ［Save private key］をクリックして、PuTTY に使用する秘密 SSHv2 鍵を保存します (47 ページを参照してください)>。

ssh-keygen を使用する SSHv2 の公開鍵と秘密鍵の作成

使用している Linux の版にプリインストールされていない場合には、*http://www.openssh.org* から OpenSSH を入手できます。

OpenSSH 用オペランドの詳しい説明は *http://www.openssh.org/manual.html* 上の OpenSSH ユーザーガイドにあります。

以下の通り進めます。

- 「ssh-keygen」を呼び出して RSA 鍵のペアを生成させます。

```
ssh-keygen -t rsa
```

ssh-keygen は鍵生成処理の進行のログを作成します。「ssh-keygen」はユーザーに秘密鍵を保存するファイル名と秘密鍵のパスフレーズを問い合わせます。「ssh-keygen」は生成された SSHv2 の秘密鍵と公開鍵を別々のファイルに保存し、公開鍵の指紋を表示します。

例：「ssh -keygen」による RSA 鍵ペアの生成

```
$HOME/benutzer1 ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key
($HOME/benutzer1/.ssh/id_rsa):                    (1)
Enter passphrase (empty for no passphrase):       (2)
Enter same passphrase again:                      (2)
Your identification has been saved in
$HOME/benutzer1/.ssh/id_rsa.                      (3)
Your public key has been saved in
$HOME/benutzer1/.ssh/id_rsa.pub.                  (4)
The key fingerprint is:
ee:99:d7:ac:8f:8e:c7:2f:2c:9b:81:80:3f:84:28:7d   (5)
                                  benutzer1@mycomp
```

解説

1. 「ssh-keygen」が SSHv2 鍵を保存するファイル名を要求します。[Enter] が押下されてファイル名なしの入力が確認されると「ssh-keygen」はデフォルト名の「id_rsa」を使用します。
2. 「ssh-keygen」が秘密鍵の暗号化に使用するパスフレーズの入力（および確認）を要求します。[Enter] が押下されてパスフレーズなしの入力が確認されると、「ssh-keygen」はパスフレーズを使用しません。
3. *「ssh-keygen」は、新しく生成された秘密 SSHv2 鍵が「/.ssh/id_rsa」ファイルに保存されたことを知らせます。*
4. *「ssh-keygen」は、新しく生成された公開 SSHv2 鍵が「/.ssh/id_rsa.pub」ファイルに保存されたことを知らせます。*
5. *「ssh-keygen」は公開 SSHv2 鍵の指紋と公開鍵が属するローカルのログインを表示します。*

4.3.2.2 SSHv2 鍵のファイルから RMU へのロード

以下の通り進めます。

- RMU の Web インターフェースから、RMU ユーザー管理 (RMU User Management) ページの要求される一覧画面の詳細なビュー（この例では user3 ）を開きます 。

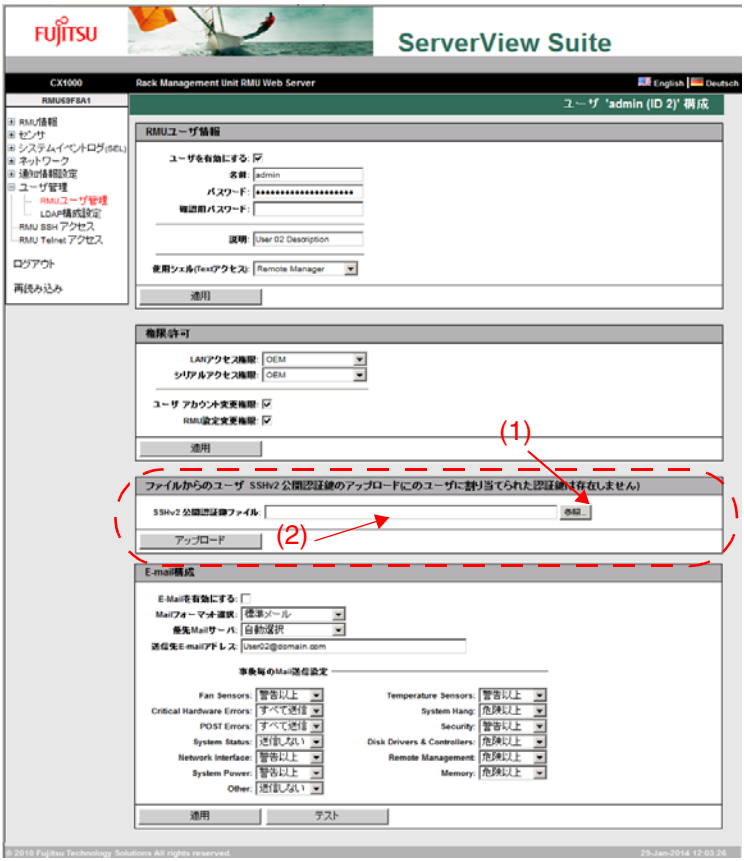


図 11: RMU Web インターフェース : 公開 SSHv2 鍵の RMU - へのロード

- 「ファイルからのユーザー SSHv2 公開鍵アップロード」(User SSHv2 public key upload from file) グループの中の［参照］(Browse) ボタン (1) をクリックして、必要な公開鍵 (2) のあるファイルまで進みます。

- ［アップロード］(Upload) ボタンをクリックして公開鍵を RMU にロードします。

  鍵が正常にアップロードされると、RMU は「ファイルからのユーザー SSHv2 公開鍵アップロード」グループの中に鍵の指紋を表示します。

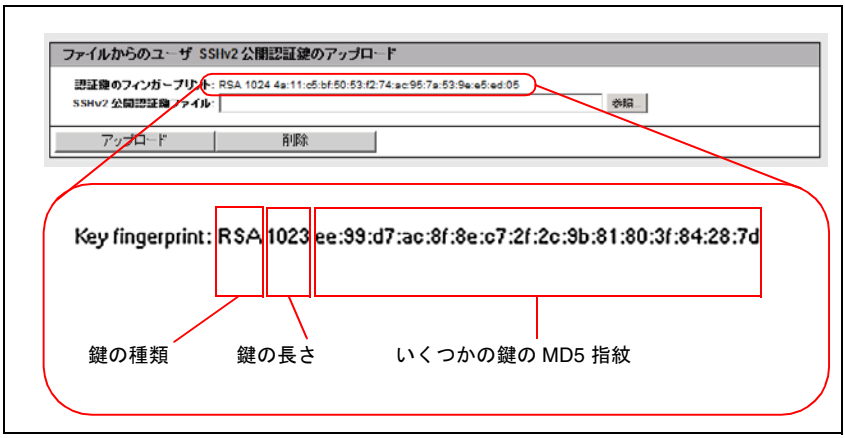


図 12: 鍵指紋の表示

セキュリティのため、ここに表示された鍵指紋が PuTTYgen (42 ページ の図 10 を参照) の *「鍵指紋」(Key fingerprint)* に表示された指紋と一致していることを確認してください。

4.3.2.3 PuTTY と OpenSSH クライアントが公開 SSHv2 鍵を使用するための設定

公開 SSHv2 鍵を使用する PuTTY の設定

PuTTY プログラムでは、RMU への公開鍵認証接続のセットアップと、自身のユーザー名または自動ログイン機能によるログインが可能になります。
PuTTY は、事前に生成された公開／秘密 SSHv2 鍵のペアに基づいて、自動的に認証プロトコルを処理します。

以下の通り進めます。

- ユーザーの Windows 機で PuTTY を起動します。

  PuTTY が起動すると以下の画面が表示されます。

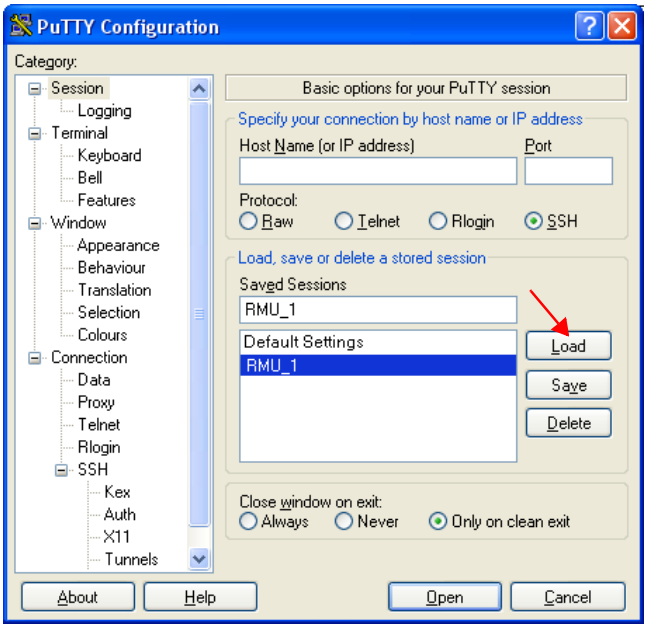


図 13: PuTTY: SSH セッションの選択とロード

- SSHv2 鍵を使用したい RMU に、保存されている SSH セッションを選択するか新しい SSH セッションを作成します。

► ［Load］をクリックして選択した SSH セッションをロードします。

その結果、次のウィンドウが開かれます。

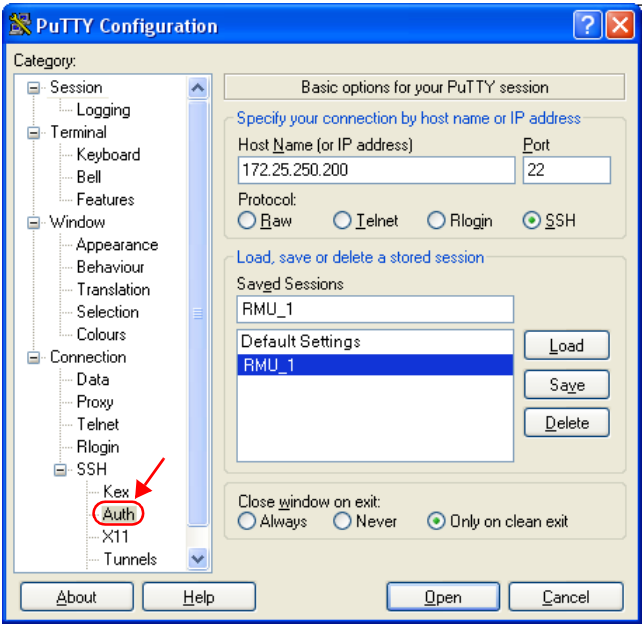


図 14: PuTTY: SSH セッションのロード

► 「*SSH - Auth*」を選択して、SSH 認証のオプションを設定します。

次のウィンドウが開きます (49 ページ の図 15 を参照してください)。

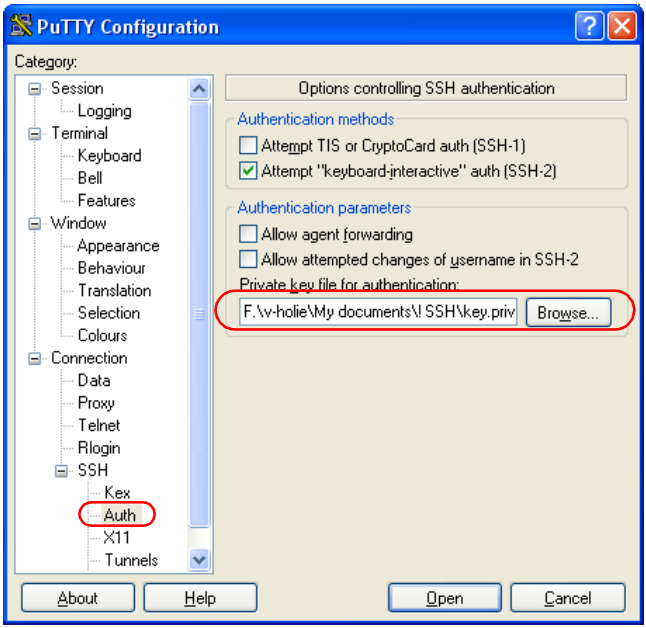


図 15: SSH 認証のオプションの設定

► RMU で使用したい秘密鍵が入ったファイルを選択します。

注意

この時点では必要なのは秘密鍵 (42 ページを参照) であり、RMU にロードされた公開鍵ではありません。

「*Connection - Data*」の下で、RMU に自動ログインするユーザー名を追加指定できます。

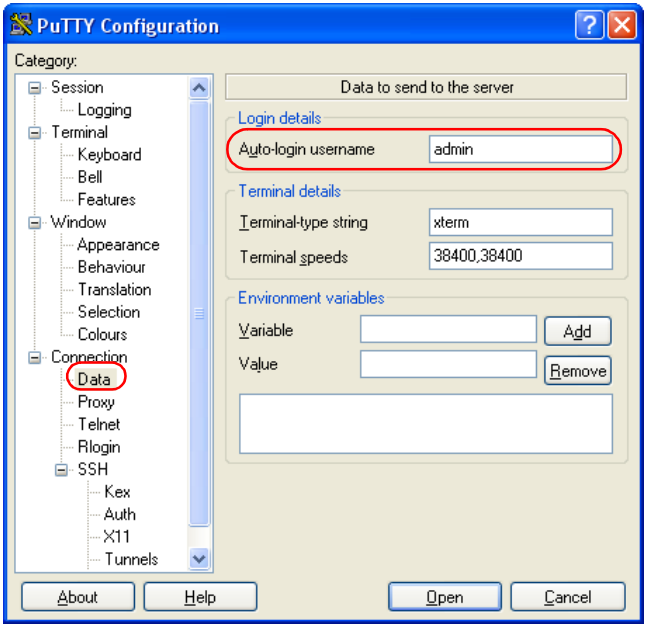


図 16: PuTTY: RMU に自動ログインするユーザー名の指定

公開 SSHv2 鍵に使用する OpenSSH クライアントプログラム ssh の設定

OpenSSH クライアントプログラム「ssh」を使用して SSHv2 で保護された RMU への接続を確立します。現在のローカルログインのままでも、別のログインでもログインすることができます。

ログインは、RMU 上のローカルログインとして設定され、関連する SSHv2 鍵は RMU にロードされていなければなりません。

「*ssh*」は以下のソースから順番に設定オプションを読み込みます。

1. 「*ssh*」を呼び出すときに使用したコマンドライン引数
2. ユーザー毎の設定ファイル (*$HOME/.ssh/config*)

   このファイルにはセキュリティ上重要な情報は含まれていませんが、読取り／書込み許可はオーナーにのみ与えるべきです。ほかのどのユーザーもアクセスを拒否すべきです。

3. システム全体の設定ファイル (*/etc/ssh/ssh_config*)

   以下の場合には、このファイルに設定パラメータのデフォルト値が書き込まれます。

   – ユーザー毎の設定ファイルがない 。

   – または、– ユーザー毎の設定ファイルに関連するパラメータが指定されていない。

最初に取得された値が各々のオプションに適用されます。

「*ssh* 」の設定とそのオペランドに関する詳細な情報は以下のサイトの OpenSSH のページから得ることができます。

http://www.openssh.org/manual.html

以下の通り進めます。

▶ 「*ssh*」を起動して、SSHv2 認証により RMU にログインします。

```
ssh -l [<user>] <RMU>
```

または

```
ssh [<user>@]<RMU>
```

<user>
RMU へのログインに使用したいユーザー名。< user> を指定しない場合は、ssh は、RMU にログインしようとしているローカルコンピュータ上のログインユーザー名をそのまま使用します。

<RMU>
ユーザーがログインしようとしている RMU 名または RMU の IP アドレス

例 : RMU 上の SSHv2 認証ログイン

次の *ssh-* コールでは、43 ページ の「例 : 「ssh -keygen」による RSA 鍵ペアの生成」で説明した通り「ssh-keygen」が公開／秘密 RSA 鍵のペアの生成に用いられたものと見なされます。また、公開鍵 *User1/.ssh/id_rsa.pub* は、RMU ユーザー「user4 」のために RMU にロードされていると見なされます (45 ページを参照してください)。

ユーザーは自身のローカルコンピュータから、「$HOME/User1 」の下でログインユーザー「user4 」を使用して、以下のように RMU "RMU_1" にログインすることができます。

```
ssh user4@RMU_1
```

4.3.2.4 例 : 公開 SSHv2 鍵

同じ公開 SSHv2 鍵を、RFC4716 フォーマットと OpenSSH フォーマットの双方で以下に示します。

RFC4716 フォーマットの公開 SSHv2 鍵

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090401"
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH フォーマットの公開 SSHv2 鍵

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+F
pGJ2iw== rsa-key-20090401
```

4.4 RMU - のグローバルユーザー管理

RMU のグローバルユーザー ID は、LDAP ディレクトリサービスを利用して集中管理されます。

RMU ユーザー管理では、現在次のディレクトリサービスがサポートされます。

– Microsoft® Active Directory
– Novell® eDirectory
– OpenLDAP

この節では次の事項に関して説明します。

– RMU のグローバルユーザー管理の概要
– LDAP ディレクトリサービスを使用する RMU のグローバルユーザー管理の概念
– ディレクトリサービスによるグローバル RMU ユーザー管理の設定 (ディレクトリサービス中で Ldap v1 / LDAP v2 に特化した許可構造の生成)>。
– Microsoft Active Directory によるグローバル RMU ユーザー管理
– Novell eDirectory によるグローバル RMU ユーザー管理
– OpenLDAP によるグローバル RMU ユーザー管理

本節で説明される、ディレクトリサービスのためにユーザーが実行する作業とは別に、グローバルユーザー管理には、RMU 上でローカルの LDAP 設定を設定する必要があります >。

ローカル LDAP 設定は RMU Web インターフェースで設定することができます (213 ページを参照してください)。

4.4.1 概要

RMU のグローバルユーザー ID は、ディレクトリサービスのディレクトリにすべてのプラットフォームの分が集中保管されています。これにより、集中サーバによるユーザー ID 管理が可能となっています。そのため、ネットワークでこのサーバに接続されているすべての RMU で、ユーザー ID を使用することができます。

そのうえ、RMU のディレクトリサービスを使用することにより、管理対象サーバのオペレーティングシステムに使用されるものと同じユーザー ID を RMU へのログインにも使用することが可能です。

グローバルユーザー管理は現在、IPMI-over-LAN 経由ログイン 機能ではサポートされません。

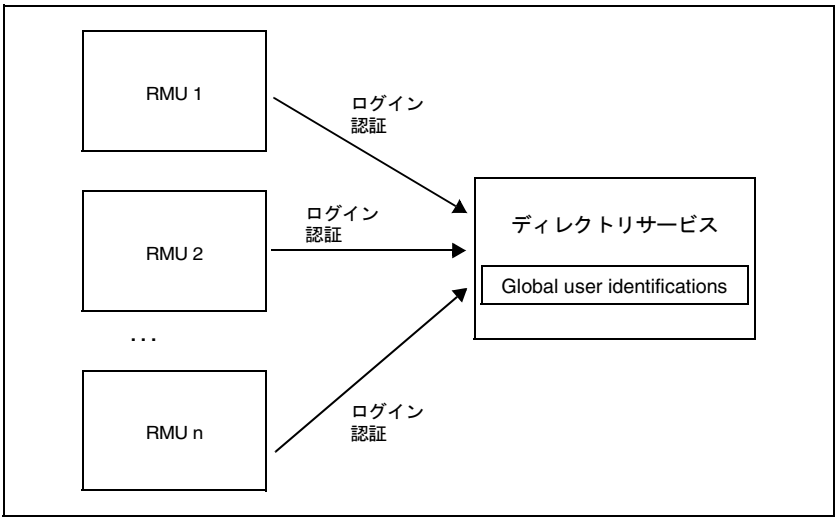


図 17: 複数の RMU によるグローバルユーザー ID の共用

個々の RMU と集中ディレクトリサービスの間の通信は TCP/IP プロトコル LDAP （Lightweight Directory Access Protocol）経由で実行されます。LDAP によって、最も頻繁に使用され、ユーザー管理に最も適しているディレクトリサービスにアクセスすることができます。LDAP 経由の通信はオプションで SSL によるセキュリティ確保が可能です。

4.4.2 LDAP ディレクトリサービス経由の RMU ユーザー管理 (概念)

以下に説明するディレクトリサービスに基づくグローバル RMU ユーザー管理の概念は、Microsoft Active Directory、Novell eDirectory および OpenLDAP に等しく適用されます。図は、Microsoft Active Directory のユーザーインターフェースにある *Active Directory Users and Computers* コンソールの例に基づいています。

次の文字は、LDAP での検索文字列用メタキャラクタとして指定されています。*, \, &, (,), |, !, =, <, >, ~, :

したがって、ユーザーはこれらの文字を相対識別名（RDN）の要素として使用することはできません。

4.4.2.1 許可グループとロールを使用するグローバル RMU ユーザー管理

LDAP ディレクトリサーバ経由の グローバル RMU ユーザー管理には、標準のディレクトリサーバのスキーマを拡張する必要はありません。その代わりに、ディレクトリサーバ に関連するすべての情報は、ユーザー許可（特権）も含めて、追加 LDAP グループと組織単位（OU）を経由して提供されます。これらの OU は、LDAP ディレクトリサーバのドメイン内の別々の OU で結合されたものです (58 ページ の図 19 を参照してください)。

RMU ユーザーは、組織単位（OU）SVS で宣言されるロール（ユーザーロール）が割り当てられるか、または OU iRMCgroups のグループのメンバーとなることにより、特権を得ることができます。

OU *SVS* とストラクチャ *iRMCgroups* の両方がディレクトリサービスで定義されている場合には、ユーザーのログインデータはまず SVS のエントリと照合され、ユーザー認証されます。一致するエントリが見つからない場合には、i*RMCgroups* のエントリとの一致を検索します。いずれの場合も最初に一致したエントリが適用されます。

ユーザーロール (略称 ロール)

による許可の割り当て

RMU 上のグローバルユーザー管理では、許可の割り当てをユーザーロールにより管理します。この場合は、各ロールは、RMU 上で有効なタスクに基づく許可プロファイルを個々に定義します。

各々のユーザーには複数のロールを割り当てることができますので、そのユーザーの許可は、割り当てられたロールすべての許可の合計により定義されます。

図 18 は、*Administrator*、*Maintenance*、および *Observer*

の各ロールによるユーザー許可の、ロールに基づく割り当ての概念を図解したものです。

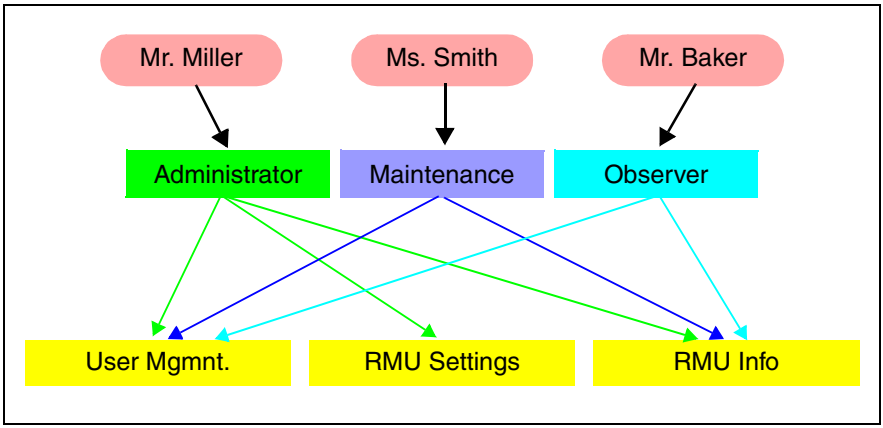


図 18: ロールに基づくユーザー許可の割り当て

ユーザーロールの概念には、以下のような重要な利点があります。

– 各々のユーザーまたはユーザーグループに、個別に許可を割り当てる必要がない。その代わりに、許可はユーザーロールに従って割り当てられる。

– 許可のストラクチャが変更になった場合にユーザーロールによる許可を適合させるのみでよい。

4.4.2.2 組織単位 (OU) SVS と iRMCgroups

RMU (および iRMC と iRMC S2) のファームウェアは現在 2 種類の LDAP ストラクチャをサポートしています。

– RMU および iRMC S2 ファームウェアバージョン 3.77 A 以上は、OU SVS に保存されている LDAP v2 ストラクチャをサポートします。

  LDAP v2 ストラクチャは将来的な機能拡張を考慮して導入されました。

– iRMC S2 < ファームウェアバージョン < <<<<<<<3.77A 未満と iRMC は、OU *iRMCgroups* に保存されている LDAP v1 ストラクチャをサポートします。

そのため、以下のように推奨します。

– サーバーパークが RMU のラックサーバと iRMC S2 の PRIMERGY サーバだけで構成されている場合は、ディレクトリサーバ上のグローバルユーザー管理には、LDAP v2 ストラクチャのみを使用してください。(この場合はすべての iRMC S2 に 3.77A 以降のバージョンがインストールされていることを確認してください)。

– RMU のラックサーバと iRMC のサーバの両方を運用している場合には、グローバルユーザー管理のため、ディレクトリサーバは LDAP v1 ストラクチャと LDAP v2 ストラクチャの両方を必要とします。

ソフトウェアツール *SVS_LdapDeployer* (67 ページを参照) を使用して、LDAP v1 および LDAP v2 ストラクチャを生成し、並存する LDAP v1 および LDAP v2 ストラクチャを維持管理します。

iRMCgroups と *SVS* OU のストラクチャは以下の通りです。

– *iRMCgroups* には *Departments* と *Shell* の OU が含まれています。
  – *Departments* にはユーザー特権のためのグループが含まれています。
  – *Shell* にはユーザーシェルのためのグループが含まれています。

– *SVS* には、*Declarations*、*Departments* および *User Settings* の OU が含まれています。
  – *Declarations* には、定義されたロールのリストと定義済みの RMU ユーザー許可のリストが含まれています (36 ページ の「ユーザー許可」の項を参照してください)。
  – *Departments* にはユーザー特権のためのグループが含まれています。
  – *User Settings* には、メールフォーマット（警告メールに使用します）などのユーザーまたはユーザーグループ固有の詳細情報と、ユーザーシェルのためのグループが含まれています。

たとえば、Microsoft Active Directory の場合には、RMU ユーザーのエントリは標準 OU である Users に納められています。ただし、RMU ユーザーは標準ユーザーとはことなり、OU *SVS* または OU *iRMCgroups* のひとつまたは複数のグループのメンバにもなっています。

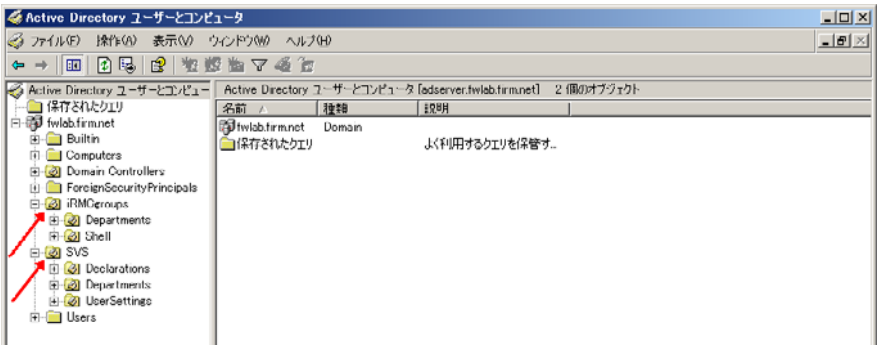


図 19: ドメイン fwlab.firm.net にある SVS および iRMCgroups の OU

RMU 用のユーザーエントリは基本ドメインの配下のどのポイントにも配置できます。許可グループも基本ドメインの配下のどのポイントにも配置できます。

4.4.2.3 多部門サーバ間のアクセス許可 (Cross-server, global user permissions

大規模な企業では、RMU によって管理されるラックサーバが複数の部門 (departments) に 割り当てられるのが普通です。その上、管理対象サーバの管理者権限も多くの場合部門独自の基準で割り当てられます。

部門は「Departments」という OU 内で結合されます

OU *Departments* は、RMU によって管理されるラックサーバを結合し、いくつかのグループを形成します。これらの OU は、同じユーザー ID と許可が適用される部門に対応します。たとえば、60 ページ の図 20 では、*DeptX*、*DeptY* および *Others* という 部門になります。

Others というエントリは任意ですが推奨します。*Others は、他の部門に属していないこれらのサーバすべてを包含する既定の部門名です。*Departments の下にリストされる部門（OU）の数に関しては、制限はありません。

RMU でディレクトリサービスを RMU Web インターフェース経由 (213 ページを参照) で設定する場合には、当の RMU を運用する管理対象サーバが属する部門の名前を指定します。LDAP ディレクトリにその名前の部門がない場合には、Others 部門にある許可を使用します。

60 ページ の図 20 は、*Active Directory Users and Computers* (Active directory ユーザとコンピュータ) を基本としたこのタイプの組織構造の例を表します。

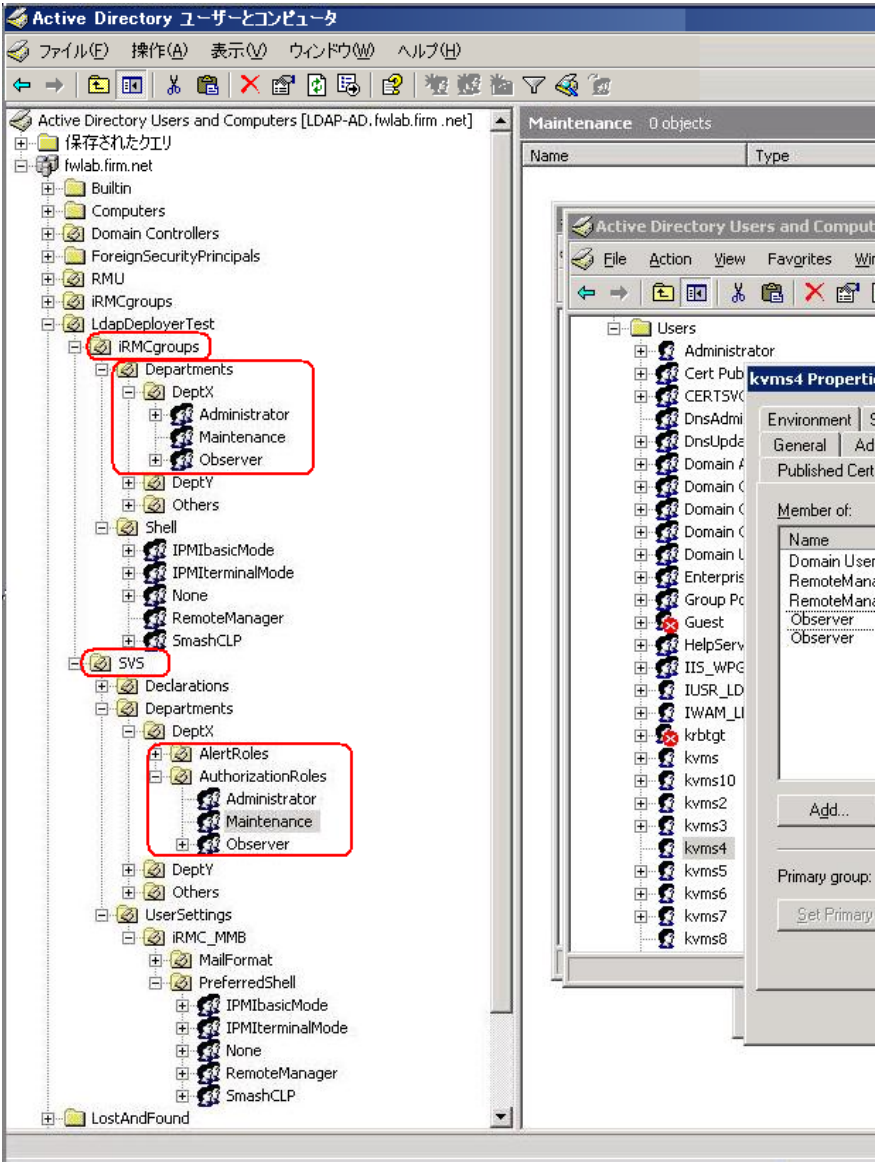


図 20: ドメイン fwlab.firm.net の組織構造

4.4.2.4 iRMCgroups: 許可プロファイルは許可グループにより定義される

関連する許可グループ（セキュリティグループ）は各部門の直下にリストされます (60 ページ の図 20) 。許可グループの数に関しては、制限はありません。許可グループの名前は必要に応じて選ぶことができますが、採用しているディレクトリサービスにより課される特定の構文要件を守らなければなりません。各々の許可グループは、当の許可グループに所属するすべてのユーザーに当てはまる特有の許可プロファイルを定義します。

注意！

ユーザーが同一部門内の複数の許可グループに同時に所属することのないよう確認してください。（ユーザーが同一部門で複数の許可グループに所属している場合には、必ず LDAP クエリから返される最初の結果が適用されます。）

グローバル RMU ユーザー管理の許可グループには、チャンネル (接続経路) 別許可グループも含まれます (36 ページを参照してください)。個々のユーザー許可に関する詳細情報は、36 ページ の「ユーザー許可」の項 を参照してください。

たとえば、Active Directory Users and Computers の階層ツリー (62 ページ の図 21 を参照) である部門（例 : DeptX ） をクリックすると、この部門に定義された許可グループ（セキュリティグループ）が表示部 (この例では DeptX) にリストされます。

表示されたセキュリティグループ (2) の中からひとつをクリックして、そのセキュリティグループ (この例では *Maintenance*) の Properties ダイアログを開くことができます。対応する許可は *Notes* の下に、次の構文を用いてリストされます。

注意！

Notes フィールドの下のユーザープロファイルは決して変更しないこと。変更するとログインできなくなります。ロールは *SVS_LdapDeployer* を用いてのみ変更が可能です (67 ページを参照してください)。

```
LAN: OEM | Administrator | Operator | User | None
Serial: OEM | Administrator | Operator | User | None
UserAccounts: On | Off
RMUsettings: On | Off
```

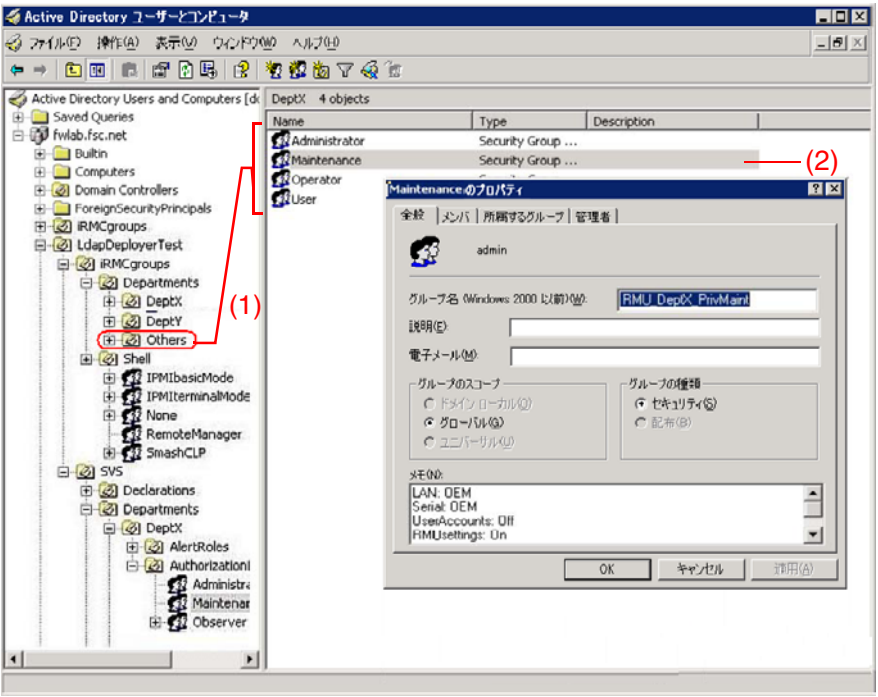


図 21: Maintenance セキュリティグループの Properties ダイアログ

動作シェル (preferred shel) の設定 I

LDAP サーバでは、ユーザーアクセス許可のみではなく、ユーザーの動作シェルも指定することができます。許可の割り当てとはことなり、動作シェルの定義は完全にユーザー特定のものであり、部門には依存しません。

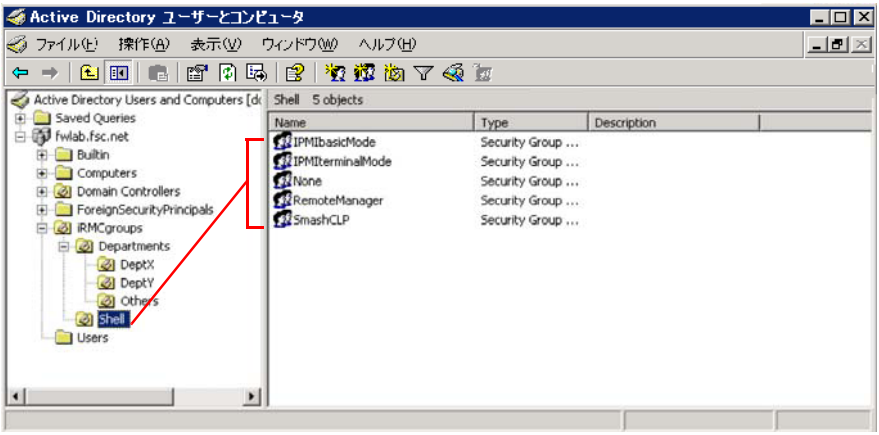


図 22: 動作シェルの定義

以下のグループから選択できます。

– *IPMIterminalMode*

– *None*

– *RemoteManager* (231 ページを参照)

– *SmashCLP* (246 ページを参照)

ユーザーは単一のシェルグループにのみ所属すべきです。複数のシェルグループに所属するユーザーは、自動的にそれらのグループの中で最も優先度が高いグループに割り当てられます。優先度の順位は上のリストの通りです（優先度は上から下に行くにしたがって低くなります）。

シェルグループに属さないユーザーはいずれもデフォルトとして *Remote Manager* グループに割り当てられます。

4.4.2.5 SVS: 許可プロファイルはロールにより定義される

要求される関連ユーザーロール（認証ロール）は各部門の直下にリストされます (60 ページ の図 20)。ここにリストされるロールはすべて *Declarations* の OU で定義しなければなりません。それ以外にロールの数に関する制限はありません。ロールの名前は必要に応じて選ぶことができますが、採用しているディレクトリサービスにより課される特定の構文要件を守らなければなりません。各認証ロールは、RMU 上の処理のためにタスクに基づく許可プロファイルを個々に定義します。

認証ロールと同様に警告ロールもリストされます。各々の警告ロールは Email で警告するための具体的な警告プロファイルを定義しています (127 ページ の「グローバル RMU ユーザー宛て Email 警告の設定」の項を参照してください)。

ユーザーロールの表示

Active Directory Users and Computers のストラクチャツリー (図 23 を参照) で *SVS* の下のある部門 (例 : *DeptX*) を選択し (1) 、対応するノード *DeptX – Authorization Roles* を展開すると、その部門 (この例では *DeptX*) に定義されたユーザーロールが表示されます (2)。

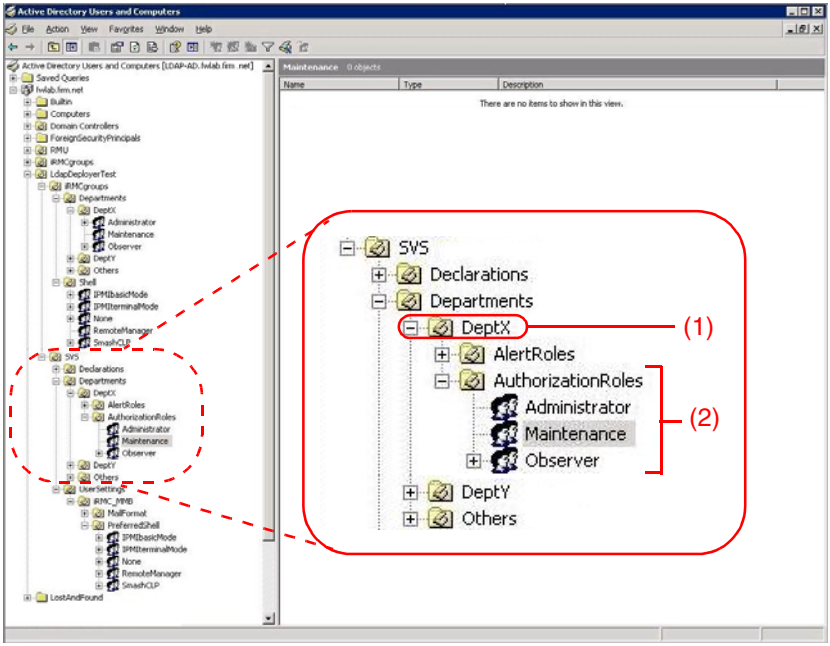


図 23: “Users and Computers” スナップイン中のユーザーロールの表示

ユーザーが割り当てられている許可グループの表示

Active Directory Users and Computers のストラクチャツリー (図 24 を参照) で Users の配下にあるユーザー (例 : *Obs1*) を選択し (1)、コンテキストメニューから *PropertiesMembers* を選択してこのユーザーの Properties ダイアログボックスを開くと、ユーザーが所属する許可グループ – (この例では *Obs1*) が *Members* タブの中に表示されます (2)。

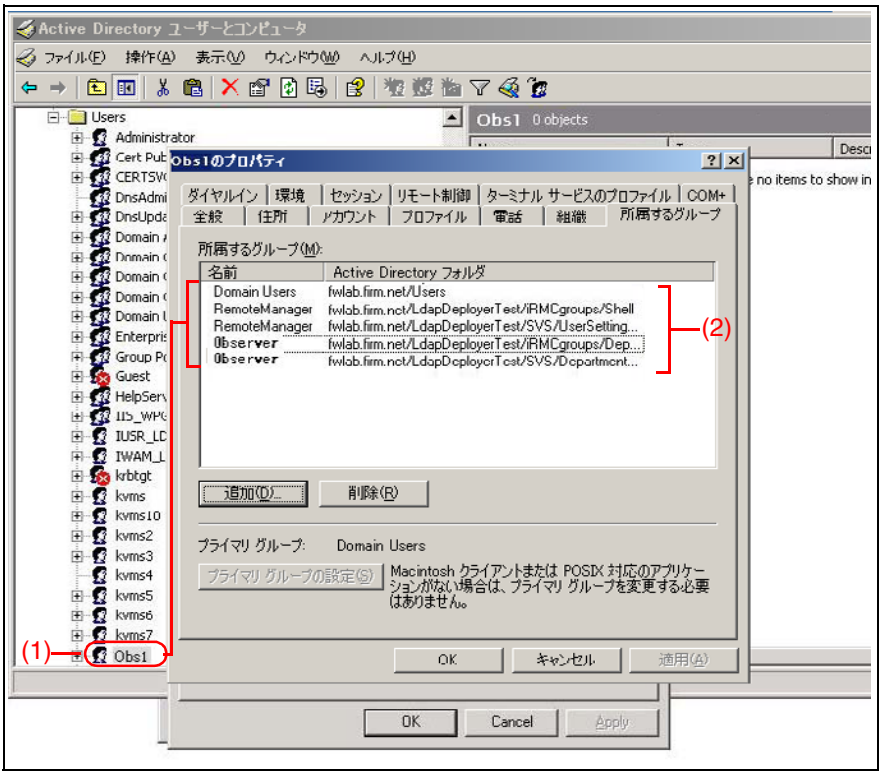


図 24: ユーザー Obs 1 - の Properties ダイアログボックス 1

4.4.3 SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除

ディレクトリサービスを使用してグローバル RMU ユーザー管理を操作できるようにするために、LDAP ディレクトリサービスの中に SVS と iRMCgroups のストラクチャ (OU) を作成する必要があります。

SVS および *iRMCgroups* ストラクチャの生成または変更には *SVS_LdapDeployer* を使用します。
SVS_LdapDeployer は Java アーカイブ (*SVS_LdapDeployer.jar*) で、*http://support.ts.fujitsu.com/com/support/downloads.html*.

からダウンロードできます。

本節では次の事項について説明します。

– *の設定ファイル*

– *SVS_LdapDeployer*

– のコマンドとオプション

– 一般的な使用例

4.4.3.1 設定ファイル (XML file)

SVS_LdapDeployer は XML 設定ファイルに基づいて LDAP ストラクチャを生成します。この入力ファイルには、*ストラクチャ SVS か iRMCgroups* または双方の XML 構文によるストラクチャ情報が入っています。

設定ファイルの構文は、サンプル設定ファイル *Generic_Settings.xml* および *Generic_InitialDeploy.xml* に説明があります。これらのファイルは *http://support.ts.fujitsu.com/com/support/downloads.html* から、*jar* アーカイブ *SVS_LdapDeployer.jar* と併せてダウンロードできます。

ディレクトリサーバ接続のための有効な接続データは、かならず入力ファイルの Settings> の下に入力しなければなりません。

サーバにアクセスするための認証データをオプションで入力することもできます。あるいは、*SVS_LdapDeloyer のコマンドラインでその認証データを指定することもできます。*

SVS_LdapDeployer を呼び出すときに設定ファイルまたはコマンドラインで認証データを指定しないと、*SVS_LdapDeployer* から認証データをランタイムで入力するように督促されます。

4.4.3.2 SVS_LdapDeployer の起動

SVS_LdapDeployer は以下の手順で起動してください。:

- Java アーカイブ (*jar* アーカイブ) *SVS_LdapDeployer.jar* をディレクトリサーバ上のフォルダに保存します。
- ディレクトリサーバのコマンドインターフェースを開きます。
- *jar* アーカイブ *SVS_LdapDeployer.jar* が保存されているフォルダに移動します。
- 次の構文を用いて *SVS_LdapDeployer* を呼び出します。

```
java -jar SVS_LdapDeployer.jar <command> <file>
                                                [<option>...]
```

SVS_LdapDeployer の稼動中に実行されるさまざまなステップに関する情報が知らされます。詳細な情報は *log.txt* ファイルで見ることができます。このファイルは SVS_LdapDeployer 稼働時に毎回実行フォルダの中に作られます。

< コマンド >
実行するアクションを指定 します。

以下のコマンドが利用できます。

-deploy
グローバル RMU ユーザー管理の LDAP ストラクチャをディレクトリサーバの中に作成します (70 ページ を参照してください)。

-delete
グローバル RMU ユーザー管理に用いた LDAP ストラクチャをディレクトリサーバから削除します (72 ページ を参照してください)。

-import
既存の LDAP v1 ストラクチャから 同等の LDAP v2 ストラクチャを作成します (70 ページ を参照してください)。

-synchronize
LDAP v2 に何らかの変更を行うと、その変更を反映して既存の LDAP v1 ストラクチャを同じように変更します (70 ページ を参照してください)。

<file>

SVS_LdapDeploy が入力ファイルとして用いる設定ファイル (*.xml*)。この設定ファイルには、ストラクチャ *SVS* か *iRMCgroups* または双方の *XML* 構文によるストラクチャ情報が入っています。

設定ファイルの構文は、サンプル設定ファイル *Generic_Settings.xml* および *Generic_InitialDeploy.xml* に説明があります。これらのファイルは *jar* アーカイブ *SVS_LdapDeployer.jar* と一緒に提供されます。

<option> [<option> ...]

指定されたコマンドの実行を制御するオプション 。

以下の数節では、*SVS_LdapDeployer* で使用できる個々のコマンドを関連するオプションと合わせて詳しく解説します。

SVS_LdapDeployer は、すべてのグループが含まれる必要なサブツリーを生成しますが、ユーザーとグループの関連付けはしません。

ユーザーエントリは、ディレクトリサービスで OU *SVS* か *iRMCgroups* または双方を生成した後、採用しているディレクトリサービスの適切なツールを使用して作成し、グループに割り当てます。

4.4.3.3 -deploy: LDAP ストラクチャの作成または変更

-deploy コマンドを使用して、ディレクトリサーバ上に新しい LDAP ストラクチャを作成したり、既存の LDAP ストラクチャに新しいエントリを追加したりすることができます。

既存の LDAP ストラクチャからエントリを削除する場合は、先ず *-delete* (72 ページ を参照) を使用して LDAP ストラクチャ自体を削除し、次に適切に修正した設定ファイルを使用して LDAP ストラクチャを再作成する必要があります。

構文

```
-deploy <file> [-structure {v1 | v2 | both}]
      [ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

設定データを含む XML ファイル。

設定ファイルの <Data> 部にはストラクチャを最初に生成するため、または展開するために必要なロールと部門がすべて含まれなければなりません。

-structure v1 | -structure v2 | -structure both

LDAP v1 ストラクチャか LDAP v2 ストラクチャ、または LDAP v1 および LDAP v2 ストラクチャを作成します。

-username <user>

ディレクトリサーバにログインするためのユーザー名

-password <password>

ユーザー <user のパスワード。

-store_pwd

-deploy が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルト設定では、ランダムに生成された鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保管してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザーもアクセスできる場合は、オプション *-kloc* および *-kpwd* を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。<password> が指定されない場合は、最新のランタイム環境のスナップショットを基にしてパスワードが自動的に生成されます。

4.4.3.4 -delete: LDAP ストラクチャの削除

-delete コマンドを用いて、ディレクトリサーバから LDAP ストラクチャを削除することができます。

Syntax:

```
-delete <file> [-structure {v1 | v2 | both}]
      [ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

削除するストラクチャを指定する XML ファイル。

-structure v1 | -structure v2 | -structure both

LDAP v1 ストラクチャか LDAP v2 ストラクチャ、または LDAP v1 および LDAP v2 ストラクチャを削除します。

-username <user>

ディレクトリサーバにログインするためのユーザー名

-password <password>

ユーザー <user のパスワード

-stor_pwd

-delete が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルト設定では、ランダムに生成された鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保管してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザーもアクセスできる場合は、オプション *-kloc* および *-kpwd* を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。
password> が指定されない場合は、最新のランタイム環境のスナップショットを基にしてパスワードが自動的に生成されます。

4.4.3.5 -import: LDAP v1 ストラクチャの LDAP v2 ストラクチャへのインポート

The *-import* コマンドを使用すると、既存の LDAP v1 ストラクチャから、同等の LDAP v2 ストラクチャをディレクトリサーバ上に生成させることができます。

Syntax:

```
-import <file>[ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

インポートするストラクチャを指定する XML ファイル。

-username <user>

ディレクトリサーバにログインするためのユーザー名

-password <password>

ユーザー <user のパスワード。

-stor_pwd

-import が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルト設定では、ランダムに生成された鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保管してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザーもアクセスできる場合は、オプション *-kloc* および *-kpwd* を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。password> が指定されない場合は、最新のランタイム環境のスナップショットを基にしてパスワードが自動的に生成されます。

4.4.3.6 -synchronize: SLDAP v2 ストラクチャに行った変更に LDAP v 1 ストラクチャを同期させて変更

LDAP v2 ストラクチャと LDAP v1 ストラクチャが混在する設定では、*-synchronize* コマンドを使用すると LDAP v2 上で行った変更を既存の LDAP v1 ストラクチャに同期させて変更することができます。

変更は必ず LDAP v2 ストラクチャ上で行うこと！

構文

```
-import <file>[ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

インポートするストラクチャを指定する XML ファイル。

-username <user>

ディレクトリサーバにログインするためのユーザー名

-password <password>

ユーザー <user のパスワード。

-stor_pwd

-synchronize が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルト設定では、ランダムに生成された鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保管してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザーもアクセスできる場合は、オプション *-kloc* および *-kpwd* を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は *SVS_LdapDeployer* が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。password> が指定されない場合は、最新のランタイム環境のスナップショットを基にしてパスワードが自動的に生成されます。

4.4.4 一般的な使用例

SVS_LdapDeployer の一般的な使用例を以下に説明します。

4.4.4.1 LDAP v1 ストラクチャと LDAP v2 ストラクチャが併存する初期設定の 実行

RMU のグローバルユーザー管理を初めて設定しようとする場合は、これを行うために LDAP v1 と LDAP v2 の両方のストラクチャが必要となります。

推奨する方法

1. LDAP v1 と LDAP v2 ストラクチャの部門の定義 (*iRMCgroups* と *SVS*) を生成します。

   ```
   java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
        -structure both
   ```

2. 今後変更を行う場合は LDAP v2 ストラクチャ上のみで行い、*-synchronize* コマンドを使用してその変更を LDAP v1 ストラクチャに転送してください (74 ページ を参照してください)。:

   ```
   java -jar SVS_LdapDeployer.jar -synchronize mySettings.xml
   ```

4.4.4.2 ILDAP v1 ストラクチャの LDAP v2 ストラクチャへのインポート

LDAP v1 に基づき iRMC や iRMC S2 のグローバルユーザー管理をすでに運用しており、今後、LDAP v2 ストラクチャを使用してさらに RMU のグローバルユーザー管理も実行したい。

推奨する方法

1. 既存の LDAP v1 ストラクチャ (*iRMCgroups*) を LDAP v2 ストラクチャ (*SVS*) にインポート (変換) します。両方のストラクチャが並存することになります。

   ```
   java -jar SVS_LdapDeployer.jar -import mySettings.xml
   ```

   このステートメントにより、部門の定義とユーザーの許可グループへの割り当ては、既存の LDAP v1 ストラクチャから新しい LDAP v2 ストラクチャにコピーされます。

2. 今後変更を行う場合は LDAP v2 ストラクチャ上のみで行い、*-synchronize* コマンドを使用してその変更を LDAP v1 ストラクチャに転送してください (74 ページ を参照)。

   ```
   java -jar SVS_LdapDeployer.jar -synchronize mySettings.xml
   ```

4.4.4.3 LDAP v2 ストラクチャの再生成と展開

LDAP v2 ストラクチャを再生成するか、既存の LDAP v2 ストラクチャを展開したい。

推奨する方法

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure -structure v2
```

または

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
```

4.4.4.4 LDAP v2 ストラクチャの再生成と認証データの督促 および保存

LDAP v2 ストラクチャを再生成したい。認証データはコマンドラインを用いて作成、保存されます。

推奨する方法

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -store_pwd -username admin -password admin
```

ログインデータを保存した後には、ユーザー名およびとパスワードを指定せずに *SVS_LdapDeployer* を使用してディレクトリサーバに接続することができます。その際、使用可能な数値が XML 設定ファイルに保管されている場合には *SVS_LdapDeployer* はその数値を使用します。*SVS_LdapDeployer* が保存されたパスワードを使用できるのは、暗号化されたパスワードを解読できる場合のみです。そのため、SVS_LdapDeployer は、*-store_pwd* (71 ページ を参照) を用いた前の呼び出しで適用したのと同じランタイム環境で実行する必要があります。このコンテキストで「同じランタイム環境」とは、「同じコンピュータを使用する同じユーザー」または「鍵が保管保存されているフォルダにアクセスする許可を持つユーザー (*-kloc* オプション、71 ページ を参照)」を意味します。

今後 SVS_LdapDeployer を呼び出すときは、すでに保存してあるユーザーアカウントを使用することもできます。さらに、データをコマンドラインに明確に指定することにより、または SVS_LdapDeployer がそうするように求めるときには、他の認証データを一時的に使用することもできます。

4.4.5 Microsoft Active Directory による RMU ユーザー管理

本節では、RMU ユーザー管理を Microsoft Active Directory に統合する方法を説明します。

前提条件

LDAP v1 か LDAP v2 ストラクチャ、または双方が Active Directory サービスですでに生成されていること (67 ページ の「SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除」の項 を参照してください)。

RMU ユーザー管理を Microsoft Active Directory に統合するには、以下の手順を実行しなければなりません。

1. RMU のユーザーを Active Directory の RMU ユーザーグループに割り当てる。
2. Active Directory サーバで RMU LDAP/SSL アクセスを設定する。

4.4.5.1 Active Directory サーバ上の RMU LDAP/SSL アクセスの設定

RMU-LDAP の統合には、OpenSSL プロジェクトに基づき Eric Young 氏が開発した SSL 実装を使用します。SSL copyright の複製を 135 ページ に掲げます。

RMU が SSL 経由で LDAP を使用できるためには、RSA 証明書が必要です。

LDAP アクセスを設定する手順は以下の通りです。

1. 企業 CA (Enterprise CA) をインストールする。
2. ドメインコントローラ用の RSA 証明書を生成する。
3. サーバに RSA 証明書をインストールする。

企業 CA のインストール

CA は「証明書の認証局」です。企業 CA (企業の認証局) はドメインコントローラ自体または別のサーバにインストールすることができます。

CA をドメインコントローラに直接インストールする方が、別のサーバにインストールするよりも必要な手順が少ないので簡単です。

企業 CA をドメインコントローラ以外のサーバにインストールする方法を、以下に説明します。

企業 CA のインストールと設定を成功させるには、Active Directory 環境とインストール済みの IIS (**I**nternet **I**nformation **S**ervices) が必要です。

企業 CA のインストールは以下の手順で行います。

- Windows のスタートメニューで、次のように進みます。

  Start - Control Panel - Software - Add/Remove Windows Components

- Windows コンポーネントのウィザードで、Components の項の *Certificate Services* を選びます。
- *Certificate Services* をダブルクリックし、*Certificate Services Web Enrollment Support* と *Certificate Services CA* のオプションが選択されていることを確認します。
- *Enterprise root CA* を選びます。
- オプション *Use custom settings to generate the key pair and CA certificate* (カスタム設定を用いて鍵ペアと CA 証明書を生成) を選択します。

- *Microsoft Base DSS Cryptographic Provider* を選択して 長さ 1024 バイトの DSA 証明書を作成します。
- 公開認証局証明書 (CA 証明書) をエクスポートします。

  これは次の手順で行います。

  - Windows のプロンプトウィンドウで *mmc* と入力して、Management Console を起動させます。
  - ローカルコンピュータ証明書用のスナップインを追加します。
  - *Certificates (Local Computer) - Trusted Root Certification Authorities - Certificates* へと進み、ダブルクリックします。
  - 新規に作成された認証局からの証明書をダブルクリックします。
  - 証明書ウィンドウの *Details* タブをクリックします。
  - *Copy to File* をクリックします。
  - 認証局証明書のファイル名を選び、*Finish* をクリックします。
- 公開認証局証明書をドメインコントローラ上の証明書ディレクトリ *Trusted Root Certification Authorities* にロードします。

  これは次の手順で行います。

  - 認証局証明書を収めたファイルをドメインコントローラに転送します。
  - Windows Explorer で、新規に作成された認証局からの証明書を開きます。
  - *Install Certificate* をクリックします。
  - *Place all certificates in the following store* の下の *Browse* をクリックし、*Trusted Root Certification Authorities* を選びます。
  - Windows のプロンプトウィンドウで *mmc* と入力して、Management Console を起動させます。
  - ローカルコンピュータ証明書のスナップインを追加します。
  - 現在のユーザーの証明書のスナップインを追加します。
  - 認証局証明書 (CA 証明書) を、現在のユーザーの Trusted Root Certification Authorities ディレクトリからローカルコンピュータの *Trusted Root Certification Authorities* にコピーします。

ドメインコントローラ証明書の作成

ドメインコントローラの RSA 証明書の作成は、以下の手順で行います。

- *下記の内容の request.inf* という名前のファイルを作成します。

```
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic
Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
; this is for Server Authentication
```

- ファイル *request.inf* で、“Subject=” の下の指定を、用いているドメインコントローラの名前に合わせます。たとえば、
  `Subject = ÅgCN=domino.fwlab.firm.netÅh.`
- Windows のプロンプトウィンドウに次のコマンドを入力します。
  certreq -new request.inf request.req
- 認証局ブラウザに次の URL を入力します。
  http://localhost/certsrv
- *Request a Certificate* をクリックします。
- *advanced certificate request* をクリックします。
- *Submit a certificate request* をクリックします。
- ファイル *request.req* の内容を *Saved Request* ウィンドウにコピーします。
- *Web Server* 証明書のテンプレートを選択します。
- 証明書をダウンロードし、保存します (たとえば、ファイル *request.cer* に)。

- Windows のプロンプトウィンドウに次のコマンドを入力します。
  certreq -accept request.cer
- 証明書を秘密鍵付きでエクスポートします。

  これは次の手順で行います。

  - Windows のプロンプトウィンドウで *mmc* と入力して、Management Console を起動させます。
  - ローカルコンピュータ証明書のスナップインを追加します。
  - *Certificates (Local Computer) - Personal Certificates - Certificates* へと進みます。
  - 新規サーバ認証局証明書をクリックします。
  - 証明書ウィンドウの *Details* タブをクリックします。
  - *Copy to File* をクリックします。
  - *Yes, export the private key* を選択します。
  - パスワードを割り当てます。
  - 証明書のファイル名を選び、*Finish* をクリックします。

ドメインコントローラ証明書のサーバへのインストール

ドメインコントローラ証明書のサーバへのインストールは、次の手順で行います。

- 作成されたばかりのドメインコントローラ証明書のファイルをドメインコントローラにコピーします。
- ドメインコントローラ証明書をダブルクリックします。
- *Install Certificate* をクリックします。
- 証明書をエクスポートするときに割り当てたパスワードを使用します。
- *Place all certificates in the following store* の下の *Browse* をクリックし、*Personal Certificates* を選びます。
- Windows のプロンプトウィンドウで *mmc* と入力して、Management Console を起動させます。
- ローカルコンピュータ証明書のスナップインを追加します。
- 現在のユーザーの証明書のスナップインを追加します。
- ドメインコントローラ証明書を現在のユーザーの *Personal Certificates* ディレクトリからローカルコンピュータの *Personal Certificates* ディレクトリにコピーします。

4.4.5.2 RMU ユーザーのロール (許可グループ) への割り当て

次のいずれかの方法で、RMU ユーザーを RMU 許可グループに割り当てることができます。

– ユーザーエントリに基づき
– または、ロールエントリ / グループエントリに基づき

以下の例では、LDAP v2 ストラクチャを使用して、OU SVS のロールエントリに基づく割り当てを説明しています。 LDAP v1 ストラクチャの場合は、グループエントリは OU iRMCgroups に保存されています。
.

ユーザーエントリに基づく割り当て手順もよく似ています。

Active Directory にユーザーを「マニュアルで」入力する必要があります。

以下の通り進めます。

► スナップイン *Active Directory Users and Computers を開きます。*

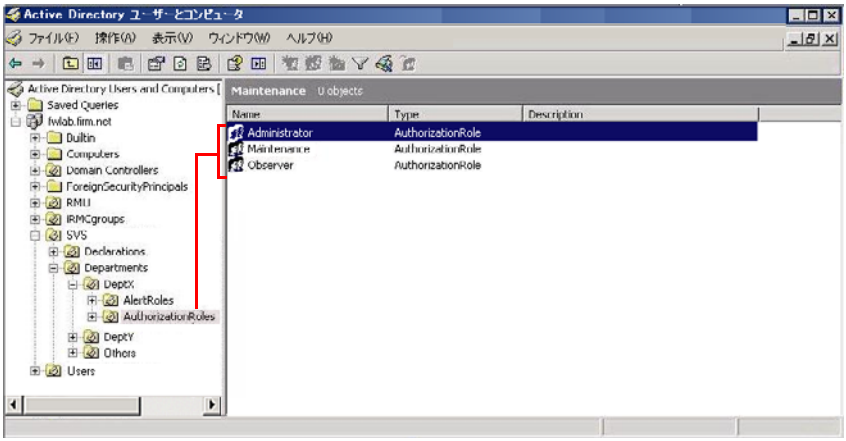


図 25: Active Directory Users and Computers のスナップイン

► 許可グループ (この例では Administrator).

Administrator Properties ダイアログが開きます (85 ページ の図 26 を参照)。

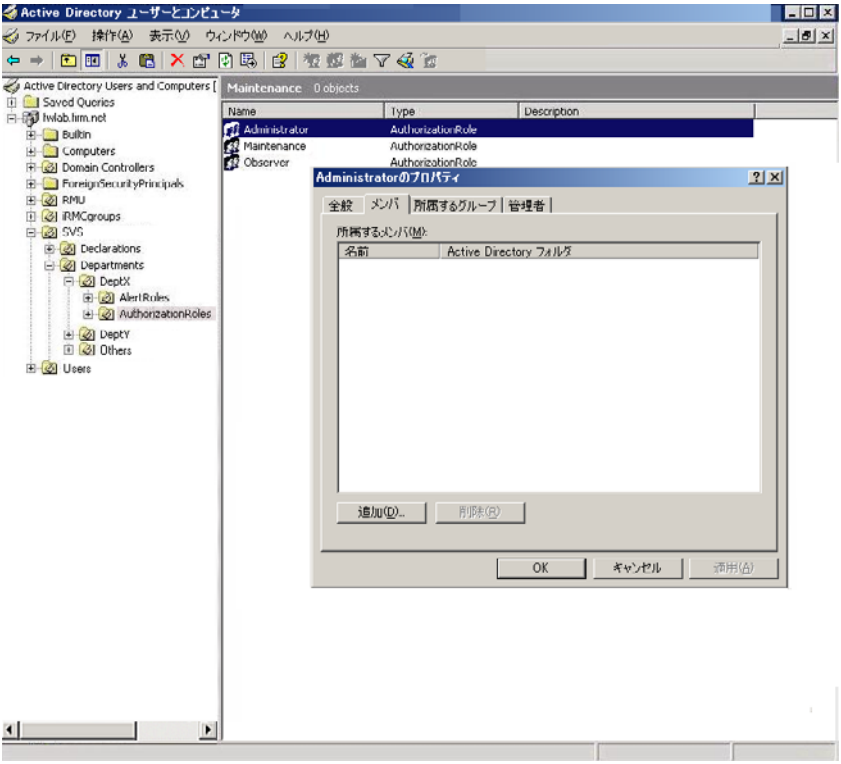


図 26: Administrator Properties ダイアログ

- *Members* タブを選びます。
- *Add...* ボタンをクリックします。

  Select Users, Contacts, or Computers ダイアログが開きます (86 ページ の 図 27 を参照)。

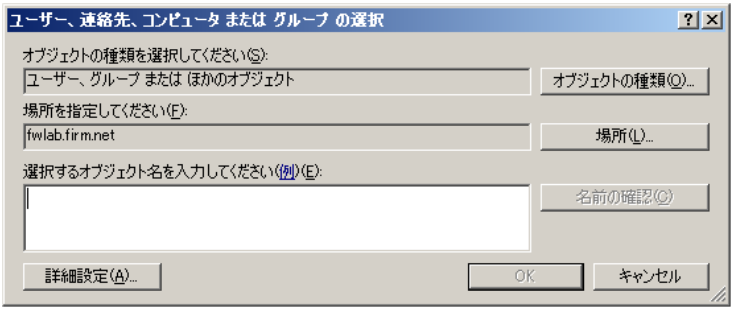


図 27: Select Users, Contacts, or Computers ダイアログ

► *Locations...* ボタンをクリックします。

Locations ダイアログが開きます。

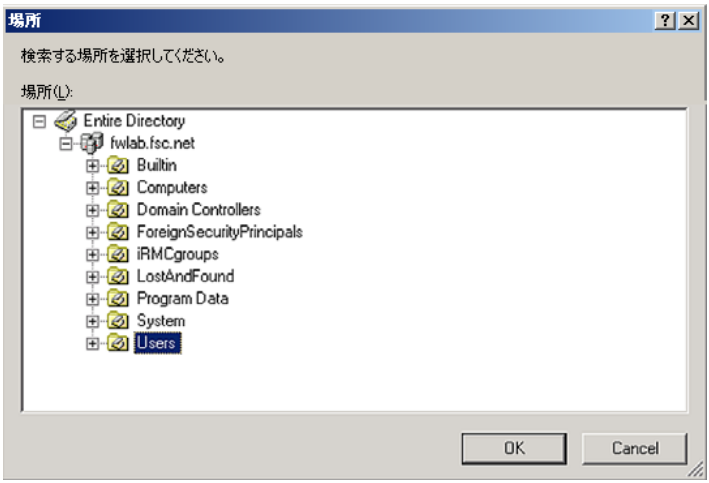


図 28: Locations ダ イアログ

► 該当するユーザーを含むコンテナ (OU) を選択します。(デフォルト時には OU *Users となります。*). *OK* をクリックして確定します。

Select Users, Contacts, or Computers ダイアログが開きます (87 ページ の 図 29 を参照)。

ユーザーをディレクトリ内の別の場所に入力することも可能です。

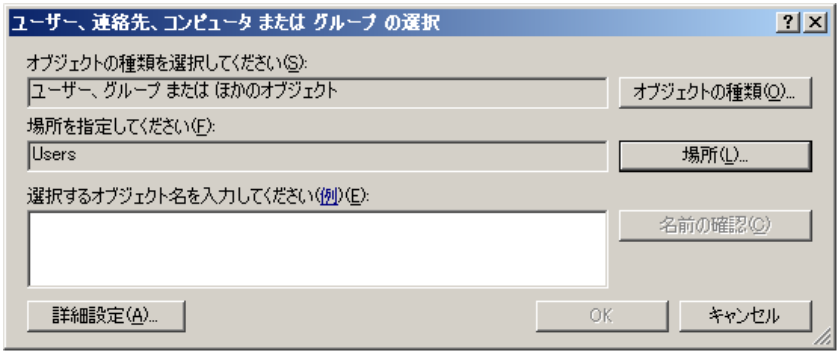


図 29: Select Users, Contacts, or Computers ダイアログ

► *Advanced...* ボタンをクリックします。

Select Users, Contacts, or Computers 展開ダイアログが開きます (88 ページ の図 30 を参照)。

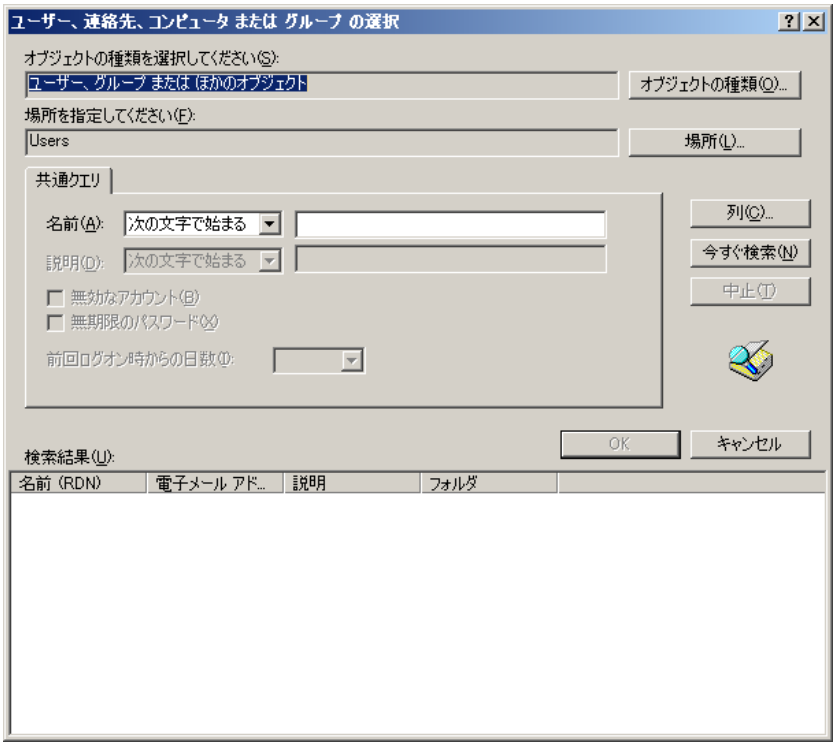


図 30: Select Users, Contacts, or Computers ダイアログ - 検索

► *Find Now* ボタンをクリックすると、ドメイン内のすべてのユーザーが表示されます。

Search results 欄、表示部で検索結果を見ることができます (89 ページ の 図 31 を参照)。

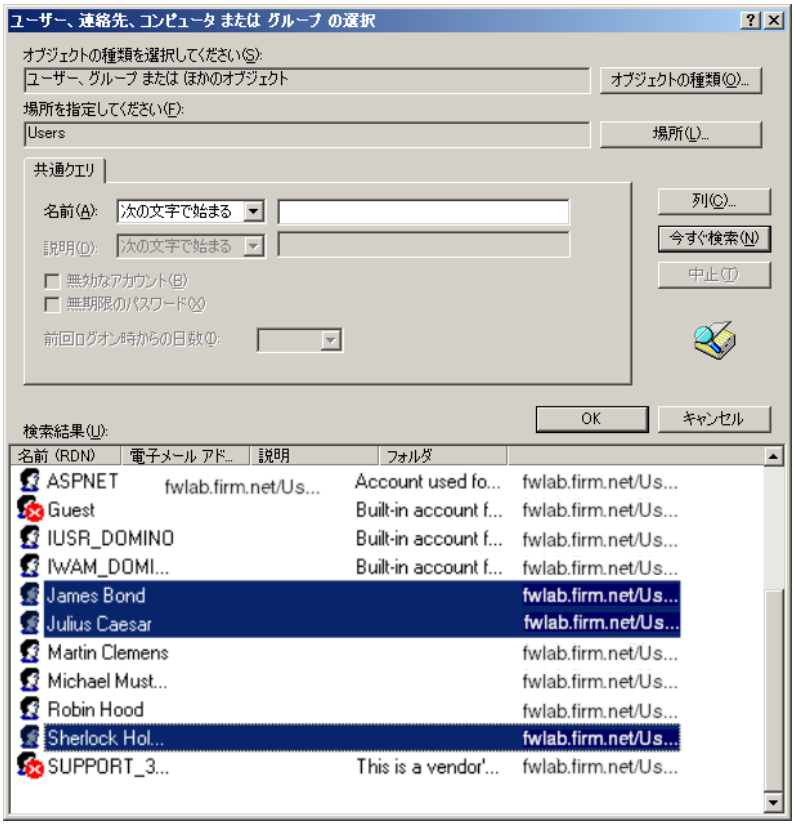


図 31: Select Users, Contacts, or Computers ダイアログ - 検索結果の表示

► グループに追加するユーザーを選択し、*OK* をクリックして確定します。
選択したユーザーが表示されます (90 ページ の図 32 を参照)。

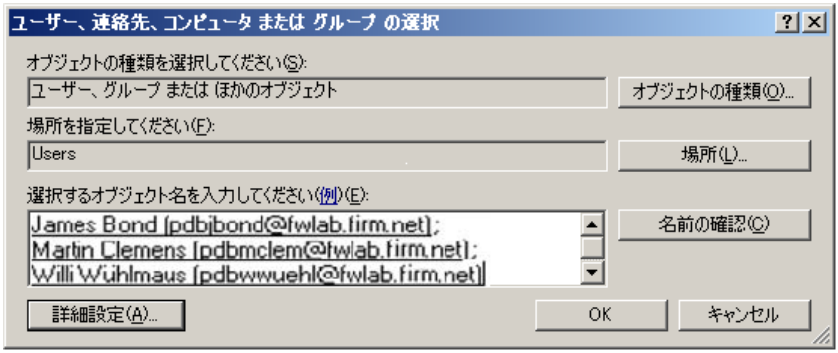


図 32: Select Users, Contacts, or Computers ダイアログ - 検索結果の確認

► *OK* をクリックして確定します。

4.4.6 Novell eDirectory による RMU ユーザー管理

本節では次の事項について説明します。

– Novell eDirectory システムのコンポーネントとシステム要件

– Novell eDirectory のインストール の設定

– Novell eDirectory への統合

– RMU ユーザー管理の Novell eDirectory

– Novell eDirectory 管理のためのヒント

以下に Novell eDirectory のインストールと設定を詳しく説明します。eDirectory についての広範な知識は必要ありません。すでに Novell eDirectory に習熟しているユーザーは、初めの 3 つの節を飛ばして 105 ページ の「RMU ユーザー管理の Novell eDirectory への統合」の項 に進んでさしつかえありません。

4.4.6.1 ソフトウェアコンポーネントとシステム要件

下記の指定のバージョンかそれ以降のコンポーネントを使用してください。

Novell eDirectory (以前の NDS) は次のソフトウェアコンポーネントで構成されています。

– eDirectory 8.8: *20060526_0800_Linux_88-SP1_FINAL.tar.gz*

– eDirectory 8.8: *eDir_88_iMan26_Plugins.npm*

– iManager: *SuSE 用は iMan_26_linux_64.tgz*、その他は *iMan_26_linux_32.tgz*

– ConsoleOne: *c1_136f-linux.tar.gz*

Novell eDirectory をインストールし運用するには、以下のシステム要件が満たされる必要があります。

– OpenSSL を必ずインストールすること。

  OpenSSL がインストール済みでない場合は、

  ► まず l OpenSSL をインストールしてから、Novell eDirectory のインストールを開始してください。

– 512 MB の空き RAM 容量

4.4.6.2 Novell eDirectory のインストール

Novell eDirectory をインストールするには、下記のコンポーネントをインストールする必要があります。

– eDirectory Server および管理ユーティリティ

– iManager (管理ユーティリティ)

– ConsoleOne (管理ユーティリティ)

Novell eDirectory インストールの前提条件

– Linux サーバ OS のフルインストールと稼動。

– ファイヤーウォールを以下のポートに接続可能な設定にします。
8080, 8443, 9009, 81, 389, 636.

OpenSuSE では、ファイル */etc/sysconfig/SuSEfirewall2* のなかでこの設定を行います。

► ファイル */etc/sysconfig/SuSEfirewall2* に、エントリ *FW_SERVICES_EXT_TCP* を次のように追加します。

```
FW_SERVICES_EXT_TCP="8080 8443 9009 81 389 636"
```

– eDirectory インストールガイドに従ってシステムにマルチキャストルーティングの設定を行います。

SuSE Linux の場合は以下の通り進めてください。

► ファイル */etc/sysconfig/network/ifroute-eth0* を作成するか、（作成済みの場合は）開いてください。

► */etc/sysconfig/network/ifroute-eth0* に以下の行を追加します。

```
224.0.0.0  0.0.0.0  240.0.0.0  eth0
```

この操作で *eth0* がシステムコンフィグレーションに取り込まれます。

eDirectory Server、eDirectory ユーティリティ、iManager および ConsoleOne インストールの前提条件

- インストールを実行するにはルート権限が必要です。
- 以下の手順でインストールを実行する前に、必要なすべてのファイルをディレクトリ (たとえば */home/eDirectory*) にコピーしておく必要があります。必要なファイルは以下のとおりです。

  20060526_0800_Linux_88-SP1_FINAL.tar.gz
  iMan_26_linux_64.tgz
  c1_136f-linux.tar.gz

eDirectory Server と管理ユーティリティのインストール

以下の通り進めます。

- ルート権限（スーパーユーザー）でログインします。
- インストールに必要なファイルが入っているディレクトリに移動します (この例では */home/eDirectory*)。

  ```
  cd /home/eDirectory
  ```

- *20060526_0800_Linux_88-SP1_FINAL.tar.gz* アーカイブを解凍します。

  ```
  tar -xzvf 20060526_0800_Linux_88-SP1_FINAL.tar.gz
  ```

  解凍すると、*/home/eDirectory* に *eDirectory* という新しいサブディレクトリが作られます。

eDirectory Server のインストール

- このディレクトリ *eDirectory* のサブディレクトリ setup に進みます。

  ```
  cd eDirectory/setup
  ```

- インストール用スクリプト *./nds-install* を呼び出します。

  ```
  ./nds-install
  ```

- “y” をキーインして EULA を承認し、Enter キーで確定します。
- どのプログラムをインストールするか尋ねられたら

  install the Novell eDirectory server に “1” を入力し、Enter キーで確定します。

  これで、eDirectory パッケージがインストールされます。

Novell eDirectory Server がインストールできたら、eDirectory までのパス名を環境変数で更新し、これらの変数をエクスポートする必要があります。

- この操作を行うには、設定ファイル (この例では : */etc/bash.bashrc*) を開き、以下の各行を指定された順序で「# End of ...」の前に入力します。

```
export PATH/opt/novell/eDirectory/bin:/opt/novell/eDirectory/
       sbin:$PATH

export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/
       opt/novell/eDirectory/lib/nds-modules:/opt/novell/
       lib:$LD_LIBRARY_PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
       man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
       locale:$TEXTDOMAINDIR
```

- ターミナルを閉じ、新しいターミナルを立ち上げて環境変数をエクスポートします。

eDirectory 管理ユーティリティのインストール

- ディレクトリ *eDirectory* のサブディレクトリ setup に進みます。

```
cd eDirectory/setup
```

- インストール用スクリプトを呼び出します。

```
./nds-install
```

- “y” をキーインして EULA を承認し、Enter キーで確定します []。
- どのプログラムをインストールするか尋ねられたら

  install the Novell eDirectory administration utilities に “2” を入力し、Enter キーで確定します。

  これで、eDirectory 管理ユーティリティがインストールされます。

iManager のインストールと起動

Novell eDirectory のインストールには iManager を使用することを推奨します。SLES10 または OpenSuSE にインポートする場合は、アーカイブ **_64.tgz* を使用します。

以下の通り進めます。

- ルート権限（スーパーユーザー）でログインします。
- ディレクトリ */home/eDirectory* に進みます。

  ```
  cd /home/eDirectory
  ```

- アーカイブ *iMan_26_linux_64.tgz* を解凍します。

  ```
  tar -xzvf iMan_26_linux_64.tgz
  ```

  解凍すると、*/home/eDirectory* に *iManager* という新しいサブディレクトリが作られます。

- *iManager* の *installs* サブディレクトリに進みます。

  ```
  cd iManager/installs/linux
  ```

- インストール用スクリプトを呼び出します。

  ```
  ./iManagerInstallLinux.bin
  ```

- インストール時のメッセージを出力する言語を選択します。
- クリックを繰り返し、EULA を承認します。
- iManager のインストールは *1- Novell iManager 2.6, Tomcat, JVM* を選びます。
- プラグインダウンロードは *1- Yes* を選びます。
- ダウンロードにデフォルトのパスを使うには Enter を押します。

  インストールプログラムがインターネット上でダウンロードするサイトを検索します。この処理には数分かかることがあります。次に、どのプラグインをインストールしたいかを尋ねられます。

  - すべてのプラグインをダウンロードするには *All* を選択します。
  - 自環境で使用可能なプラグインをインストールするには *1- Yes* を選択します。

- ダウンロードにデフォルトのパスを使うには Enter を押します。
- Apache を自動設定（オプション）させるには *2- No* を選択します。
- Tomcat 用のデフォルトポート (8080) を承認します。

- Tomcat 用のデフォルト SSL ポート (8443) を承認します。
- Tomcat 用のデフォルト JK コネクタポート (9009) を承認します。
- 適切な管理権限を持つ管理ユーザーの ID (たとえば “root.fts”) を入力してください。
- 適切な管理権限を持つ管理ユーザーの ツリー名 (たとえば “fwlab”) を入力してください。
- 表示されているエントリの要約を *1-OK...* を押して承認し、インストールを終了させます。

Novell iManager へのログイン

インストールが終わると、以下の URL からウェブブラウザ経由で iManager にログインできます。

https://<IP address of the eDirectory server>:8443/nps

Novell のブラウザには Microsoft Internet Explorer または Mozilla Firefox を推奨します。Mozilla Firefox であれば、一度にすべてのコンテキストメニューのポップアップウィンドウを表示させないようにすることもできます

ConsoleOne のインストールと起動

ConsoleOne は Novell eDirectory のもうひとつの管理ツールです。

ConsoleOne を以下のようにインストールしてください。

- ルート権限（スーパーユーザー）で eDirectory Server にログインします。
- ディレクトリ */home/eDirectory* に進みます。

  ```
  cd /home/eDirectory
  ```

- ConsoleOne のアーカイブ *c1_136f-linux.tar.gz* を解凍します。

  ```
  tar -xzvf c1_136f-linux.tar.gz
  ```

  解凍すると、*/home/eDirectory* に *Linux* という新しいサブディレクトリが作られます。

- ディレクトリ *Linux* に進みます。

  ```
  cd Linux
  ```

- インストール用スクリプト *c1-install を呼び出します。*

  ```
  ./c1-install
  ```

- インストールのメッセージを出力する言語を選択します。
- “8” を入力してすべてのスナップインをインストールしてください。

ConsoleOne にはインストール済みの Java ランタイム環境へのパスが必要です。対応するパス名を環境変数 *C1_JRE_HOME.* にエクスポートすることができます。ただし、パス名をシステム全体にエクスポートするためには、*bash* プロファイルの変更が必要です。

ConsoleOne を操作するためには、原則として ID *superuser Root* をエクスポートできるレベルのルート権限が要求されます。パス名をシステム全体にエクスポートする方法は以下に紹介する通りです。すなわち、通常のユーザーでもルート権限があれば ConsoleOne を操作することができます。

以下の通り進めます。

- 編集する設定ファイルを開きます (この例では */etc/bash.bashrc*)。
- 設定ファイルの “# End of ...” の前に次の行を入力します。

```
export C1_JRE_HOME=/opt/novell/j2sdk1.4.2_05/jre
```

eDirectory と同時にインストールされた java ランタイム環境をここで使用します。一方、eDirectory Server 上にインストールされたいずれかの Java ランタイム環境のパス名を指定することもできます。

ConsoleOne はローカルの設定ファイル hosts.nds または SLP サービスとマルチキャストを経由して使用可能なツリー階層を取得します。

以下のように、ユーザーのツリー階層を設定ファイルに挿入してください。

- 設定用ディレクトリに進みます。

```
cd /etc
```

- ファイル *hosts.nds* がまだ存在しない場合には作成してください。
- ファイル *hosts.nds* を開いて以下の行を挿入します。

```
#Syntax: TREENAME.FQDN:PORT
MY_Tree.mycomputer.mydomain:81
```

ConsoleOne の起動

ConsoleOne はシステムプロンプトから以下のコマンドを使用して起動できます。

```
/usr/ConsoleOne/bin/ConsoleOne
```

4.4.6.3 Novell eDirectory の設定

以下の手順を実行して Novell eDirectory を設定してください。

1. NDS ツリーの作成
2. eDirectory の LDAP 用設定
3. LDAP Browser を経由した eDirectory への試験アクセス .

NDS ツリーの作成

ndsmanage ユーティリティを使用して NDS（Network Directory Service）を作成します。この作業を行うために、ndtmanage には以下の情報が必要です。

TREE NAME (ツリー名)
新しい NDS ツリーのネットワーク用の一意の名前、たとえば *MY_TREE*。

Server Name (サーバ名
eDirectory の *server* クラスのインスタンス名。*Server Name* には、LDAP サーバが稼働している PRIMERGY サーバの名前、たとえば、*lin36-root-0* を指定してください。

Server Context (サーバコンテキスト)
server オブジェクトを格納するコンテナの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、*dc=organization.dc=mycompany*。

Admin User (Admin ユーザー)
管理を実行する許可を持つユーザーの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、*cn=admin.dc=organization.dc=mycompany*

NCP Poert (NCP ポート)
ポート 81 を指定してください。

Instance Location (インスタンスのロケーション)
パスを指定してください。*/home/root/instance0*

Confuguration File (設定ファイル)
次のファイルを指定してください。*/home/root /instance0/ndsconf*

Password for admin user (Admin ユーザー用パスワード)
管理者のパスワードをここに入力してください。

次の手順で NDS ツリーを設定します。

- コマンドボックスを開きます。
- ディレクトリ */home/eDirectory* に移動します。
- コマンド ndsmanage を入力してユーティリティ ndsmanage を起動します。

  ```
  ndsmanage
  ```

- “c” を入力して、クラス *server* の新しいインスタンスを生成します。
- “y” を入力して設定作業を続けます。
- “y” 入力して新しいツリーを作成します。

  次に、ndsmanage から、*順番に TREE NAME, Server Name, Server Context* などの値が尋ねられます (99 ページ を参照)。

  入力が完了すると、NDS ツリーが ndsmanage によって設定されます。
- NDS ツリーの設定が終わったら、PRIMERGY サーバを再起動させて、設定の実効化、すなわち、NDS ツリーの再作成を行います。

eDirectory の LDAP 用設定

eDirectory を LDAP 用に設定する手順は次の通りです。

– Role Based Services (RBS) のインストール

– プラグインモジュールの設定

– Role Based Services (RBS) の設定

– eDirectory の SSL/TLS サポートあり / なしでの設定

以下の手順で個々の作業を完了させます。

- 管理者 ID (*Admin*) を使用してウェブブラウザ経由で iManager にログインします。

*Role Based Services (RBS) の*インストール

iManager Configuration Wizard を使用して RBS をインストールします。

以下の通り進めます。

- iManager で、*Configure* タブを選択します (desk アイコンをクリックしてください)。
- *Configure* タブで、*次の通り選択します。*
  Role Based Services - RBS Configuration
- RBS Configuration ウィザードを起動させます。
- 管理を行うコンテナに *RBS2* を割り当てます。(上の例では“mycompany”となります。)

プラグインモジュールのインストール

以下の通り進めます。

- iManager で、*Configure* タブを選択します (desk アイコンをクリックしてください)。
- *Configure* タブで、次の通り選択します。
  Plug-in installation - Available Novell Plug-in Modules
- *Available Novell Plug-in Modules* ページにリストされたモジュールから、eDirectory 専用のパッケージ *eDir_88_iMan26_Plugins.npm* を 選択します。
- *Install* をクリックします。

Role Based Services (RBS) の設定

- *Available Novell Plug-in Modules* ページで、LDAP 統合に必要なすべてのモジュールを選択してください。よくわからない場合は、すべてのモジュールを選択します。
- *Install* をクリックします。

eDirectory の SSL/TLS で セキュリティ保護されたアクセスの設定

eDirectory のインストール中には、臨時の証明書が生成されますので、eDirectory へのアクセスは初期設定でも SSL/TLS によりセキュリティ保護されます。ただし、RMU のファームウェアは RSA/MD5 証明書を使用するように設定されているので、SSL/TLS セキュリティ保護された eDirectory 経由のグローバル RMU ユーザー管理には 1024 バイト長の RSA/MD5 証明書が必要です。

1024 バイト長の RSA/MD5 証明書は ConsoleOne を使用して以下のように作成します >。

- 管理者 ID (*Admin*) を使用して LDAP サーバにログインし、ConsoleOne を起動してください。
- コーポレートストラクチャのルートディレクトリに移動してください。(たとえば、*treename/mycompany/myorganisation*).
- *New Object - NDSPKI key material - custom* を選択して、クラス *NDSPKI:Key Material* の新しいオブジェクトを作成します。
- その後に表示されるダイアログで、以下の値を指定してください。

  1. 1024 bits
  2. SSL or TLS
  3. signature RSA/MD5

  必要なタイプの新しい署名が作成されます。

新たに作成した証明書を SSL セキュリティ保護された LDAP 接続のために有効化するには、iManager で以下の作業を実行します。

- ウェブブラウザから iManager を起動します。
- 有効な認証データで iManager にログインします。
- *LDAP - LDAP Options - LDAP Server - Connection* の順に選択します。

  Connection タブには、システム上でインストールされたすべての証明書を表示するドロップダウンリストがあります。
- ドロップダウンリストから必要な証明書を選択します。

eDirectory の SSL- セキュリティ保護されないアクセスの設定

eDirectory のデフォルト設定では匿名ログインやセキュリティ保護されないチャンネルを経由する平文表示のパスワードは無効となります。このため、eDirectory サーバにウェブブラウザでログインするには SSL 接続経由とするほかには方法がありません。

LDAP を SSL なしで使用したい場合は、以下の手順を実行しなければなりません。

1. SSL セキュリティ保護されない LDAP 接続の確立
2. バインド制限の緩和
3. LDAP 設定の再ロード

以下の通り進めます。

1. SSL セキュリティ保護されない LDAP 接続の確立
   - ウェブブラウザから iManager を起動します。
   - 有効な認証データを使用して iManager にログインします。
   - *Roles and Tasks* ビューを選択します。
   - *LDAP - LDAP Options - LDAP Server - Connection* の順に選択します。
   - *Connection* タブで、次のオプションを無効にします。
     Require TLS for all Operations.
   - *LDAP - LDAP Options - LDAP Group - General* の順に選択します。
   - *General* タブで、次のオプションを無効にします。
     Require TLS for Simple Binds with password.
2. バインド制限の緩和
   - 有効な認証データを使用して iManager にログインします。
   - オブジェクトツリーで、*LDAP Server* オブジェクトに進みます。
   - マウスで *LDAP Server* オブジェクトをクリックしてハイライトさせ、関連するコンテキストメニューから Modify Object を選択します。
   - 右側のコンテントフレームで、*Other* シートを開きます。
   - *Valued Attributes* の下から、*ldapBindRestrictions* を選びます。
   - *Edit* ボタンをクリックします。
   - 値を “0” に設定します。
   - *OK* をクリックします。
   - *Other* シートで、*Apply* ボタンをクリックします。

3. LDAP 設定の再ロード

   ► ConsoleOne を起動させ、eDirectory にログインします。

   ► ウィンドウの左側にある *Base DN* オブジェクト (たとえば *Mycompany*) をクリックします。*すると*、*LDAP server* オブジェクトがウィンドウの右側に表示されます。

   ► 右クリックして LDAP Server オブジェクトをハイライトさせ、関連するコンテキストメニューから Properties... を選択します。

   ► *General* タブで、*Refresh NLDAP Server Now* をクリックします。.

eDirectory への LDAP Browser 経由のアクセス試験

以上 1 から 3 までの手順に成功したら、LDAP Browser ユーティリティを使用して eDirectory への接続が確立できなければなりません。Jarek Gavor 氏の LDAP Browser (121 ページを参照) を使用して、以下のようにこの接続の試験をします。

► 管理者 ID (この例では *admin*) を使用して SSL 接続経由で eDirectory にログインできるか試してみます。

ログインに失敗した場合は、以下のようにしてください。

► SSL が有効かどうか確かめます (102 ページ を参照してください)。

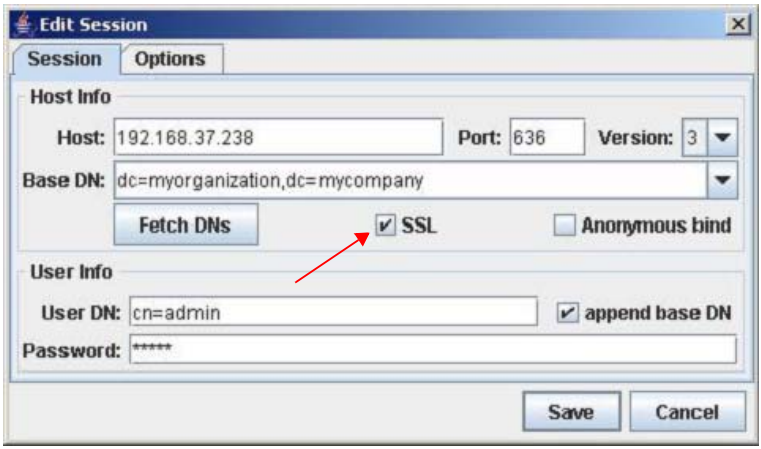


図 33: LDAP 経由の eDirectory アクセス試験 SSL 有効時

► 有効な管理者 ID（この例では *admin*）を使用して、SSL- セキュリティ設定のない接続経由で eDirectory にログインできるか試してみます。

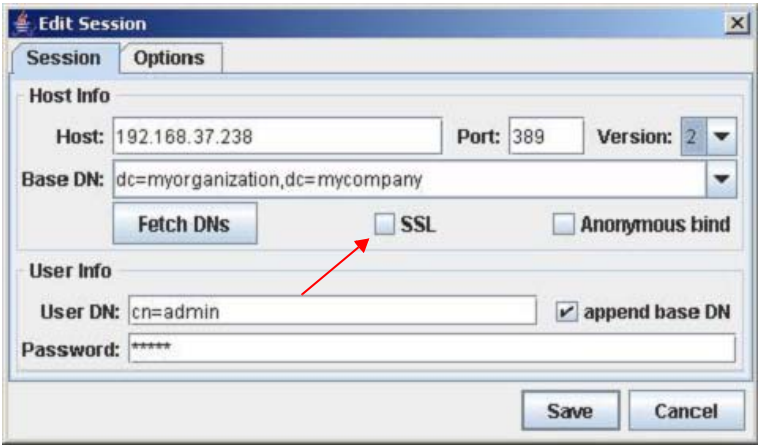


図 34: LDAP 経由の eDirectory アクセス試験 : SSL 無効時

► 再度ログインに失敗したら :
バインド制限を緩和します (102 ページ を参照)。

4.4.6.4 RMU ユーザー管理の Novell eDirectory への統合

前提条件

LDAP v1 ストラクチャか LDAP v2 ストラクチャ、または両方が eDirectory ディレクトリサービスですでに生成されていること (67 ページ の「SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除」の項 を参照)。

以下の手順を実行して、RMU ユーザー管理を Novell eDirectory に統合します。

– RMU プリンシパルユーザーの生成

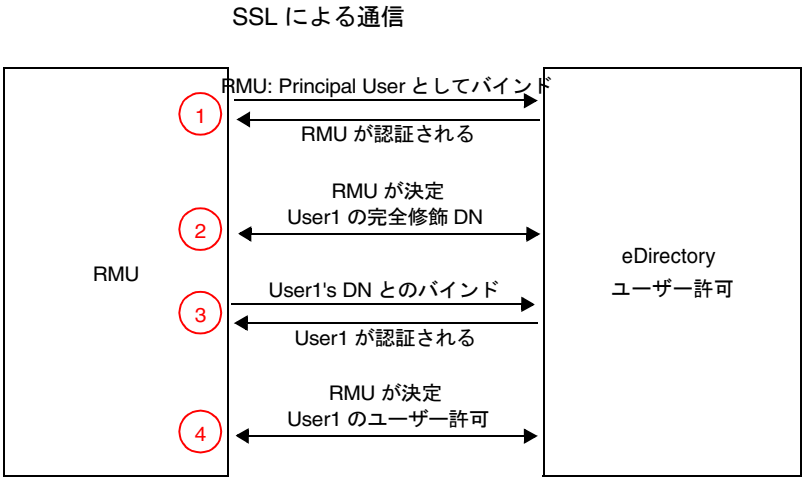
– eDirectory の RMU グループとユーザー許可の宣言

– ユーザーの許可グループへの割り当て

eDirectory の RMU ユーザーのための LDAP 認証プロセス

グローバル RMU ユーザーが RMU にログインする際の認証は、定義済みのプロセスに従って処理されます (34 ページを参照してください)。106 ページ の図 35 はこの認証プロセスを、Novell eDirector のグローバル RMU ユーザー管理に関して図解したものです。

対応するログイン情報による接続とログインの確立を、BIND 操作と呼びます。



1) RMU は、“Principal User” という定義済みの既知の許可データ (RMU 設定) を使用して eDirectory サーバにログインし、バインドのバインドの成功。

2) RMU は eDirectory サーバに、“cn=User1” でユーザーの完全修飾識別名 (DN) を与えるよう求めます。eDirectory が DN を決定します。定義済みサブツリー (RMU 設定) から。

3) RMU はユーザー User1 の完全修飾 DN で eDirectory サーバにログインしバインドの成功を待ちます。

4) RMU は eDirectory サーバに、... のユーザー許可を与えるよう求めます。ユーザーUser1.

図 35: グローバル RMU の許可の認証ダイアグラム

「プリンシパルユーザー」の許可データと DN を含むサブツリーは、RMU の Web インターフェースの Directory Service Configuration ページで設定します (213 ページ を参照してください)。

ユーザーの CN は、検索対象ツリー内で一意でなければなりません。

RMU 用のプリンシパルユーザーの作成

RMU 用のプリンシプルユーザーを以下の通り作成します。

- 有効な認証データで iManager にログイン します。
- *Roles and Tasks* を選択します。
- *Users - Create User* を選択します。
- 表示されたテンプレートに必要な明細事項を記入します。

  プリンシパルユーザーの識別名（DN）とパスワードは RMU 設定の際に指定したものと一致していなければなりません (213 ページ の「ディレクトリサービス設定 (LDAP) - RMU」の項 を参照してください)。

  ユーザーの *Context:* はツリーのどの位置にあっても構いません。

- 以下のサブツリーにプリンシパルユーザーの検索許可を割り当てます。
  - サブツリー (OU) *iRMCgroups* または *SVS*
  - ユーザーを含むサブツリー (OU) (たとえば *people*)

RMU グループとユーザーへのユーザー許可の割り当て

デフォルト設定では、eDirectory のオブジェクトには、LDAP ツリー内の非常に限定されたクエリと検索の許可しかありません。ひとつまたは複数のサブツリーのすべての属性をオブジェクトがクエリできるようにするには、このオブジェクトに対応する許可を割り当てる必要があります。

許可は個々のオブジェクト（すなわち個々のユーザー）に割り当てることもできますし、*iRMCgroups* / *SVS* または *people* のような同じ組織単位（OU）のなかで照合されるオブジェクトのグループに割り当てることもできます。この場合は、OU に割り当てられ、「引き継がれた」と識別された許可は、このグループのオブジェクトに自動的に認定されます。

RMU ユーザー管理を Novell eDirectory に統合するには、次のオブジェクト（トラスティ）に検索の許可を割り当てる必要があります。

- *Principal User*
- RMU ユーザーを含むサブツリー

以下にこの操作を詳しく説明します。

すべての属性に関するオブジェクト検索許可を割り当てるプロセスは以下の通りです。

- ウェブブラウザから iManager を起動します。
- 有効な認証データを使用して iManager にログインします。
- IiManager で、*Roles and Tasks* ボタンをクリックします。
- メニューツリーストラクチャで、*Rights - Rights to Other Objects* を選択します。

  Rights to Other Objects のページが表示されます。
- *Trustee Name* の下で、許可を与えるオブジェクトの名前を (109 ページ の図 36 *iRMCgroups.sbrd4* および *SVS.sbdr4* で) 指定します。
- *Context to Search From* の下で、eDirectory サブツリー (*iRMCgroups* / *SVS*) を指定します。iManager はこのサブツリーから、トラスティ *Users* が現在読み取り許可を持っているすべてのオブジェクトを検索することになります。
- *OK* をクリックします。

  進捗ディスプレイが検索の状況を表示します。検索作業か終了すると、*Rights to Other Objects* のページが検索結果と合わせて表示されます (109 ページ の図 36 を参照してください)。

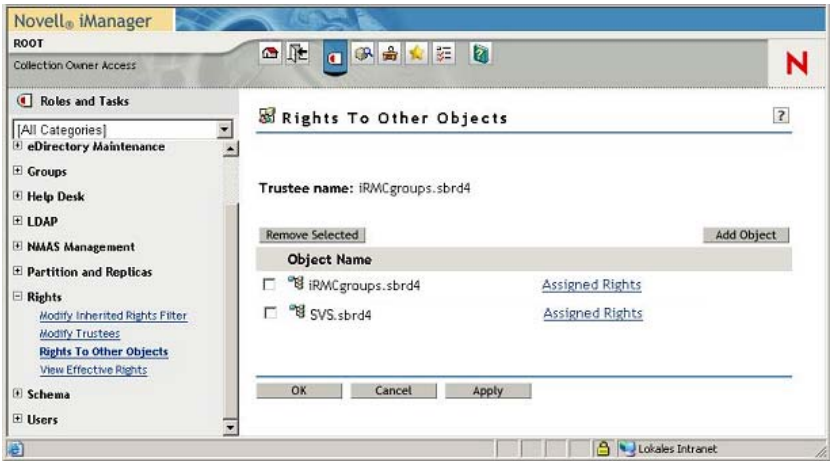


図 36: iManager - Roles and Tasks - Rights To Other Objects

Object Name の下になにもオブジェクトが表示されない場合は、トラスティには指定されたコンテキストの範囲内に許可はありません。

► 必要に応じてトラスティに追加の許可を割り当ててください。

  ► *Add Object* をクリックします。

  ► オブジェクトセレクタボタンを使用して、トラスティに許可を割り当てたいオブジェクトを選択します。

  ► *Assigned Rights* をクリックします。

  プロパティ *[All Attributes Rights]* が表示されない場合は :

    ► *Add Property* をクリックします。

    Add Property ウィンドウが表示されます (110 ページ の図 37 を参照)。

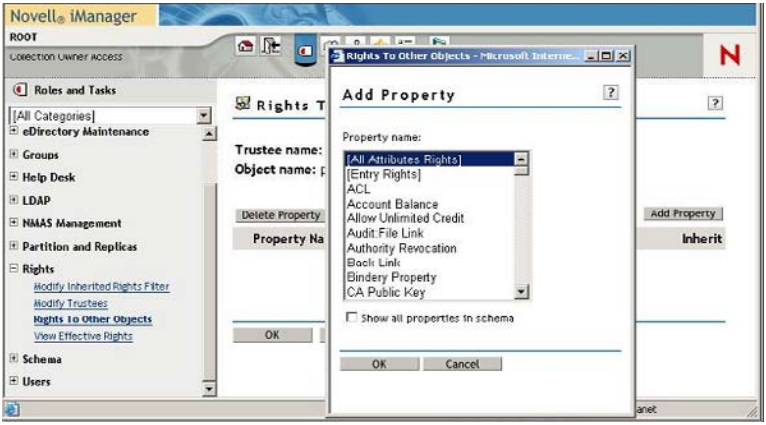


図 37: iManager - Roles and Tasks - Rights To Other Objects - Add Property

► プロパティ *[All Attributes Rights]* をハイライトさせ、*OK* をクリックして追加します。

► プロパティ *[All Attributes Rights]* に対し、オプション *Compare*、*Read*、*Inherit* を有効にし、*OK* をクリックして確定します。

この操作によって、ユーザーまたはユーザーグループに、選択されたオブジェクトのサブツリーの属性をすべてクエリする権限が与えられます。

► *Apply* をクリックして設定を有効にしてください。

4.4.6.5 RMU ユーザーの許可グループへの割り当て

RMU ユーザーを (たとえば OU *people* から) 次のいずれの方法でも RMU 許可グループに割り当てる事ができます。

– ユーザーエントリから開始 (ユーザーエントリの数がごく少い場合はこの方が適当)
– または、ロールエントリ / グループエントリから開始 (ユーザーエントリの数が多い場合はこの方が適当)。

次の例は RMU ユーザーを OU *people* から許可グループに割り当てる方法を示します。割り当てをロールエントリ／グループエントリから開始する方法を説明しています。

ユーザーエントリから開始する割り当てる方法もほぼ同じです。

eDirectory 内のグループにユーザーを「マニュアル」で入力する必要があります。

以下の通り進めます。

- ウェブブラウザから iManager を起動します。
- 有効な認証データを使用して iManager にログインします。
- *Roles and Tasks* を選択します。
- *Groups - Modify Group* を選択します。

  Modify Group のページが表示されます。
- RMU ユーザーを割り当てたいすべての許可グループについて次の作業を実行します。
  - オブジェクトセレクタボタン を使用して、RMU ユーザーを追加したい許可グループを選択します。 
    – LDAP v1 ストラクチャの例 (112 ページ の図 38 を参照) では、この操作は : *Administrator.DeptX.Departments.iRMCgroups.sbrd4*.
    – LDAP v2 ストラクチャの例 (112 ページ の図 39 を参照) では、この操作は : *Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4*.
  - *Members* タブを選択します。

    Modify Group ページの *Members* タブが表示されます。

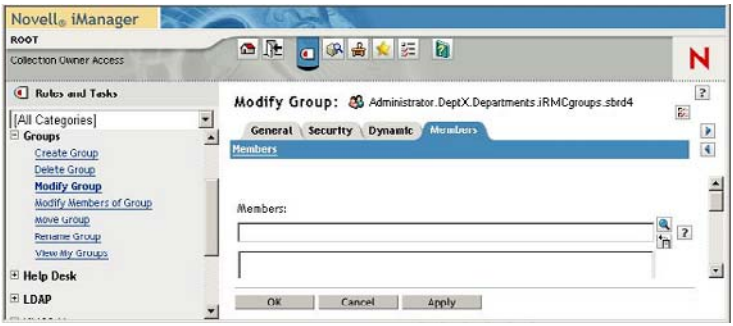


図 38: iManager - Roles and Tasks - Modify Group - “Members”タブ (LDAP v1)

図 39: iManager - Roles and Tasks - Modify Group - “Members”タブ (LDAP v2)

- RMU グループに割り当てたい OU *people* のすべてのユーザーについて <、次の作業を実行します。
  - オブジェクトセレクタボタン  をクリックします。

    Object Selector (Browser) ウィンドウが開きます (113 ページ の図 40 を参照)。

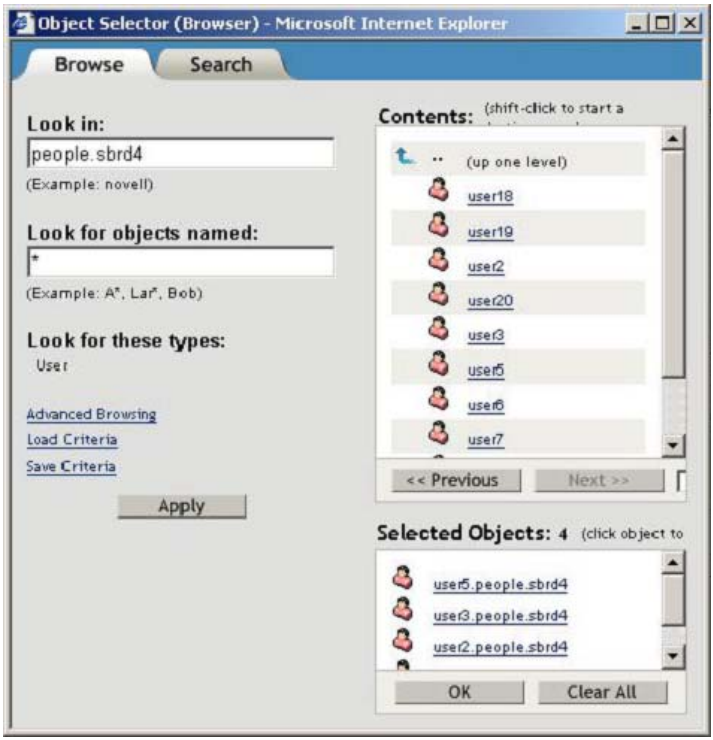


図 40: RMU グループへのユーザーの割り当て - ユーザーの選択

► *Object Selector (Browser)* ウィンドウで、OU *people* の中の必要なユーザーを選択し、OK をクリックして確定します。

選択されたユーザーは *Modify Group* page ページの Members タブの表示部にリストされています (114 ページ の図 41 を参照)。

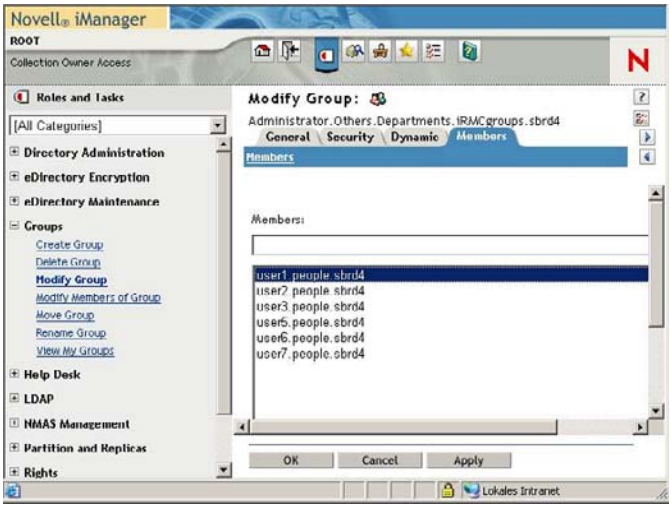


図 41: 選択された RMU ユーザーの “Members LDAP v1” タブでの表示

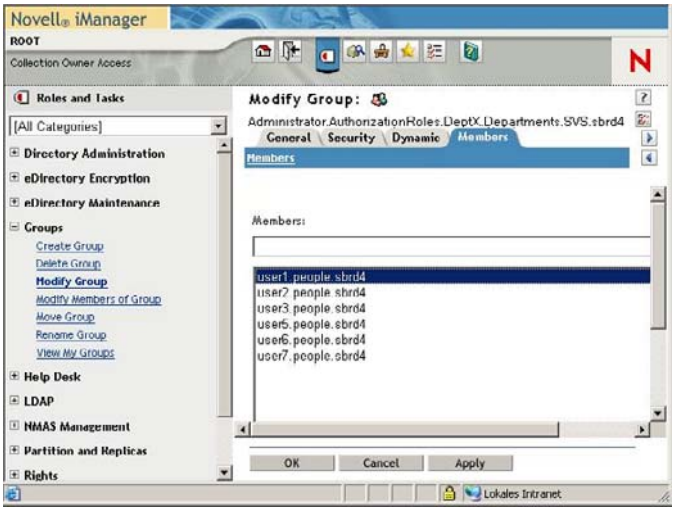


図 42: 選択された RMU ユーザーの “Members LDAP v2” タブでの表示

► 選択されたユーザーを RMU グループ (この例では ... *.iRMCgroups.sbdr4* または ... *.SVS.sbdr4*) に追加するため、*Apply* または *OK* で確定してください。

4.4.6.6 Novell eDirectory 管理のためのヒント

NDS デーモンの再 起動

次の手順で NDS デーモンを再起動します。

- コマンドボックスを開きます。
- ルート許可でログインします。
- 次のコマンドを実行します。

```
rcndsd restart
```

nldap デーモンの再起動に失敗し、理由が分からない場合は、

- *nldap* デーモンを「マニュアル」で起動します。

```
/etc/init.d/nldap restart
```

iManager から応答がない場合は

- iManager を再起動してください。

```
/etc/init.d/novell-tomcat4 restart
```

NLDAP サーバの設定の再ロード

以下の通り進めます。

- ConsoleOne を起動して eDirectory ログインします。

  ConsoleOne を初めて立ち上げる場合は、ツリーが設定されていません。

  以下の手順でツリーを設定してください。

  - *My World* の下のノード *NDS* を選択します。
  - メニューバーで、*File - Authenticate* を選択します。
  - 次のログイン用認証データを入力します。
    1. ログイン名 : root
    2. パスワード : <password>
    3. ツリー : MY_TREE
    4. コンテキスト : mycompany

- ウィンドウの左側部分で、*Base DN* オブジェクト (*Mycompany*) をクリックします。

  すると、*LDAP Server* オブジェクトがウィンドウの右側に表示されます。

- *LDAP Server* オブジェクトを右クリックし、コンテキストメニューで *Properties...* を選択します。

- *General* タブで、*Refresh NLDAP Server Now* ボタンをクリックします。

NDS メッセージトレースの設定

nds デーモンは、デバッグおよびログメッセージを生成し、このメッセージは *ndstrace* ツールを使用してトレースすることができます。以下に説明する設定の目的は、ndstrace からの出力をファイルにリダイレクトし、他のターミナルでこのファイルの内容を表示させることです。後者の作業には *screen* ツールを使用します。

以下の手順を推奨します。

- コマンドボックス (たとえば *bash*) を開きます。

ndstrace の設定

- eDirectory のディレクトリ */home/eDirectory* に移動します。

  ```
  cd /home/eDirectory
  ```

- コマンド `screen` で *screen* を起動します。

- コマンド ndstrace で *ndstrace* を起動します。

- 有効化したいモジュールを選択します。

  たとえば、イベントが発生した時間を表示したい場合は、次のように入力します。`dstrace TIME`.

  是非次のように入力して、モジュール *LDAP* および *TIME* を有効化することをお勧めします。

  ```
  dstrace LDAP TIME
  ```

- *quit* を入力して *ndstrace* を終了します。

  これで *ndstrace* の設定は終了しました。

別のターミナルでのメッセージの出力

- *ndstrace* を起動して、メッセージ出力をリダイレクトします。

  ```
  ndstrace -l >ndstrace.log
  ```

- 次の連結キーを使用して別のターミナルを開きます。
  Ctrl + a, Ctrl + c

- ログ記録を開始させます。

  ```
  tail -f ./ndstrace.log
  ```

- 仮想ターミナル間の切り替えには、次の連結キーを使用します。Ctrl + a, Ctrl + 0.
  (ターミナルには 0 から 9 まで番号が付されます。)

4.4.7 OpenLDAP による RMU ユーザー管理

本節では次の事項について説明します。

– OpenLDAP (Linux) のインストール
– SSL 証明書の作成
– OpenLDAP の設定
– RMU ユーザー管理の OpenLDAP への統合
– OpenLDAP 管理のヒント

4.4.7.1 OpenLDAP のインストール

OpenLDAP をインストールする前に、ファイヤーウォールをポート 389 と 636 に接続できるように設定する必要があります。

OpenSuSE の場合は以下の通り進めます。

► ファイル */etc/sysconfig/SuSEfirewall2* で、オプション *FW_SERVICES_EXT_TCP* を次のように拡張します。

```
FW_SERVICES_EXT_TCP=Åg389 636Åh
```

配布媒体から取得したパッケージ *OpenSSL* および *OpenLDAP2* をインストールするときは、セットアップツール YaST を使用してください。

4.4.7.2 SSL 証明書の作成

次のプロパティを持つ証明書を作成する必要があります。

– 鍵の長さ : 1024 ビット
– md5RSAEnc

鍵ペアと署名入り証明書（自己署名または外部 CA の署名）の作成には OpenSSL を使用します。より詳しい情報は OpenSSL のホームページ、http://www.openssl.org を参照してください。

CA の設定とテスト証明書の作成の説明書は以下のリンクから入手してください。

– *http://www.akadia.com/services/ssh_test_certificate.html*
– *http://www.freebsdmadeeasy.com/tutorials/web-server/apache-ssl-certs.php*
– *http://www.flatmtn.com/computer/Linux-SSLCertificates.html*
– *http://www.tc.umn.edu/~brams006/selfsign.html*

証明書の作成に続いて、以下の 3 個の PEM ファイルを入手してください。

– ルート証明書 *root.cer.pem*

– サーバ証明書 *server.cer.pem*

– 秘密鍵 *server.key.pem*

秘密鍵は決してパスフレーズで暗号化しないでください。*server.key.pem*. ファイルには、LDAP デーモン（ldap）読み取り許可のみが割り当てられるためです。

次のコマンドを使用してパスフレーズを削除してください。

```
openssl rsa -in server.enc.key.pem -out server.key.pem
```

4.4.7.3 OpenLDAP の設定

次の手順で OpenLDAP を設定し てください。

- Yast セットアップツールを起動させ、*LDAP-Server-Configuration* を選択します。
- *Global Settings/Allow Settings* の下で、*LDAPv2-Bind* の設定を有効にします。
- *Global Settings/TLS Settings* を選択します。
  - *TLS* 設定を有効にします。
  - インストール時に作成されたファイルのパスを宣言してください (118 ページ の「OpenLDAP のインストール」の項 を参照してください)。
  - ファイルシステムの証明書と秘密鍵を読み取ることができるのはLDAP サービスのみであることを確認してください。

    openldap は *uid/guid=ldap* の下で実行されるので、確認は以下の方法で行うことができます。

    – 証明書と秘密鍵を含むファイルのオーナーを "ldap" に設定する、または、

    – LDAP デーモン ldap の読み取り許可を証明書と秘密鍵が入ったファイルに割り当てる。

► *Databases* を選択して新しいデータベースを作成します。

YaST で作成した設定が全体的に機能しない場合には、次のファイルに下記の必須エントリが存在しているかを確認してください。
/etc/openldap/slapd.conf:

```
allow bind_v2
TLSCACertificateFile /path/to/ca-certificate.pem
TLSCertificateFile /path/to/certificate.pem
TLSCertificateKeyFile /path/to/privat.key.pem
```

YaST で作成した SSL の設定が機能しない場合には、次の設定ファイルに下記のエントリが存在しているかを確認してください。
/etc/sysconfig/openldap:

```
OPENLDAP_START_LDAPS=ÅgyesÅh
```

4.4.7.4 RMU ユーザー管理の OpenLDAP への統合

前提条件

LDAP v1 ストラクチャか LDAP v2 ストラクチャ、または両方が OpenLDAP ディレクトリサービスのなかに生成済みであること (67 ページ の「SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除」の項 を参照してください)。

RMU ユーザー管理の OpenLDAP への統合は以下の手順からなります。

– RMU プリンシパルユーザーの生成

– 新規 RMU ユーザーの作成と許可グループへの割り当て

プリンシパルユーザー (ObjectClass: *Person*) の生成には、LDAP ブラウザ、たとえば Jarek Gawor 氏が作成した LDAP Browser\Editor などを使用します (121 ページ を参照してください)。

Jarek Gawor 氏作成の LDAP Browser\Editor

Jarek Gawor 氏作成の LDAP Browser\Editor は、グラフィカルユーザーインターフェースによる使いやすいものです。

このツールはインターネットでダウンロードできます。

以下の手順で **LDAP Browser\Editor** をインストールしてください。

- 圧縮アーカイブ *Browser281.zip* を任意のインストール用ディレクトリで解凍します。
- JAVA ランタイム環境用の環境変数 *JAVA_HOME* をインストール用ディレクトリに設定してください。たとえば、

```
JAVA_HOME=C:\Program Files\Jave\jdk1.5.0_06
```

プリンシパルユーザーの生成

プリンシパルユーザー (ObjectClass: *Person*) の生成には、LDAP ブラウザ、たとえば Jarek Gawor 氏が作成した LDAP Browser\Editor などを使用します (121 ページ を参照してください)。

以下に、Jarek Gawor 氏の LDAP Browser\Editor を用いてプリンシパルユーザーを作成する方法を説明します。

以下の通り進めます。

- LDAP ブラウザを起動します。
- 有効な認証データを使用して OpenLDAP ディレクトリサービスにログインします。
- プリンシパルユーザーを作成するサブツリー（サブグループ）を選択します。プリンシパルユーザーはサブツリー内のどこにでも作成できます。
- *Edit* メニューを開きます。
- *Add Entry* を選択します。
- *Person* を選択します。
- 識別名 *DN* を編集します。

  プリンシパルユーザーの識別名（DN）とパスワードは RMU 設定の際に指定したものと一致していなければなりません (213 ページ の「ディレクトリサービス設定 (LDAP) - RMU」の項 を参照してください)。
- *Set* をクリックしてパスワードを入力します。
- 苗字 *SN* を入力します。
- *Apply* をクリックします。

新規 RMU ユーザーの作成と許可グループへの割り当て

新規ユーザー (ObjectClass *Person*) の作成とユーザーの許可グループへの割り当てには、LDAP ブラウザ、たとえば Jarek Gawor 氏が作成した LDAP Browser\Editor などを使用します (121 ページ を参照してください)。

以下に、Jarek Gawor 氏の LDAP Browser\Editor を用いて新規の RMU ユーザーを作成し、そのユーザーを許可グループに割り当てる方法を説明します。

以下の通り進めます。

- LDAP ブラウザを起動します。
- 有効な認証データを使用して OpenLDAP ディレクトリサービスにログインします。
- 新規ユーザーを作成します。

  この作業は次のように行います。

  - 新規ユーザーを作成するサブツリー（サブグループ）を選択してください。新規ユーザーはサブツリー内のどこにでも作成できます
  - *Edit* メニューを開きます。
  - *Add Entry* を選択します。
  - *Person* を選択します。
  - 識別名 *DN* を編集します。
  - *Set* をクリックしてパスワードを入力します。
  - 苗字 *SN* を入力します。
  - *Apply* をクリックします。

► 今作成したユーザーを許可グループに割り当てます。

この作業は以下のように行います。

► ユーザーが所属することになる *iRMCgroups* または *SVS* サブツリー (サブグループ) を選択します。すなわち

– LDAP v1 の場合は :
```
cn=Observer,ou=YourDepartment,ou=Departments,ou=
iRMCgroups,
dc=myorganisation,dc=mycompany
```

– LDAP v2 の場合は :
```
cn=Observer,ou=YourDepartment,ou=Departments,ou=SVS,
dc=myorganisation,dc=mycompany
```

► *Edit* メニューを開きます。

► *Add Attribute* を選択します。

► 属性名として “Member” を指定します。値にはここで作成したユーザーの完全修飾 DN を指定してください。すなわち、

```
cn=Observer,ou=YourDepartment,ou=Departments,
ou=iRMCgroups,dc=myorganization,dc=mycompany
```

または

```
cn=Observer,ou=YourDepartment,ou=Departments,ou=SVS,
dc=myorganisation,dc=mycompany
```

4.4.7.5 OpenLDAP 管理のヒント

LDAP サービスの再起動

次の手順で LDAP サービスを再起動します。

- コマンドボックスを開きます。
- ルート権限でログインします。
- 次のコマンドを入力します。

```
rcldap çƒãNìÆ
```

メッセージログ作製

LDAP デーモンは Syslog プロトコルを使用してメッセージログを作成します。

ログ化されたメッセージは、ファイル */etc/openldap/slapd.conf* でログレベルが 0 以外に設定されている場合にのみ表示されます。

各レベルの説明は下記を参照してください。

http://www.zytrax.com/books/ldap/ch6/#loglevel

126 ページ の表 5 に、ログレベルとその意味の概要を記載しています。

ログレベル	意味
-1	全面的なデバッグ実行
0	デバッグ実行なし
1	ログファンクションコール
2	試験パケットの取扱い
4	ヘビートレースデバッグ実行
8	接続管理
16	送信 / 受信パケット表示
32	フィルタ処理の検索
64	設定ファイル処理
128	アクセス制御リスト処理
256	接続／操作／イベントのステータスログ作成
512	送信済みエントリのステータスログ作成
1024	シェルバックエンドによる出力通信
2048	エントリパースの出力結果

表 5: OpenLDAP - ログレベル

4.4.8 グローバル RMU ユーザー宛て Email 警告の設定

グローバル RMU ユーザー宛の Email 警告は、グローバル RMU ユーザー管理システムに組み込まれています。すなわち、1 台のディレクトリサーバを使用して、email 警告をすべてのプラットフォーム向けに集中的に設定し操作することができます。適切に設定されたグローバルユーザー ID は、ネットワーク上でディレクトリサーバに接続されたすべての RMU から Email 警告を受け取ることができます。

前提条件

email 警告のためには下記の要件が満たされなければなりません。

- プリンシパルユーザーが RMU Web インターフェースで設定され、LDAP ツリー内で検索する権限を付与されていること (213 ページ の「ディレクトリサービス設定 (LDAP) - RMU」の項 を参照してください)。
- *Directory Service Configuration* ページ (213 ページ を参照) で LDAP 設定を設定する際、email 警告が *Directory Service Email Alert Configuration* の下で有効にされていること。

4.4.8.1 グローバル email 警告

ディレクトリサーバ経由のグローバル Email 警告には警告ロールが必要です。この警告ロールは管理ロールに加えて *SVS_LdapDeployer* の設定ファイル (67 ページ を参照) で定義されます。

警告グループ (警告ロール) の表示

警告ロールは、選ばれた警告タイプ（たとえば、温度のしきい値を超えた、など）をまとめてグループ化しますが、各警告タイプに重大度 (たとえば . “致命的”) が割り当てられています。ユーザーを特定の警告グループに割り当てると、ユーザーが Email で受け取る警告のタイプと重大度が指定されます。

警告ロールの構文はサンプル設定ファイル *Generic_Settings.xml* と *Generic_InitialDeploy.xml* に具体的に解説されています。これらのファイルは *jar* アーカイブ *SVS_LdapDeployer.jar* に付属しています。

警告タイプの表示

以下の警告タイプがサポートされます。

警告タイプ 1	原因
FanSens	冷却ファンセンサ
Temperat	温度センサ
HWError	致命的なハードウェア故障
Security	セキュリティ
SysHang	システムのハング
POSTErr	POST エラー
SysStat	システムの状態
DDCtrl	ディスクドライブとコントローラ
NetInterf	ネットワークインターフェース
RemMgmt	リモートマネジメント
SysPwr	電源管理
Memory	メモリ
Others	その他

表 6: 警告タイプ

各々の警告タイプには以下の重大度のいずれかが割り当てられます。*警告 Warning*、*致命的 Critical* 、*すべて All*、*（なし none）*

優先メールサーバ

グローバル Email 警告には、優先メールサーバに関して Automatic 設定が適用されます。Email を即時に送ることができない場合、たとえば 1 番目のメールサーバが使用不可能な場合には、Email は 2 番目のメールサーバに送られます。

サポートされるメールフォーマット

以下の email フォーマットがサポートされます。

- 標準
- Fixed Subject
- ITS- フォーマット
- 富士通 REMCS フォーマット

標準以外のメールフォーマットを使用する場合は、対応するメールフォーマットグループにユーザーを追加しなければなりません。

LDAP email テーブル

email 警告が設定され (131 ページ を参照)、オプション *LDAP Email Alert Enable* (213 ページ を参照) が選択されている場合は、RMU は警告が発せられると以下のユーザーに email を送信します。

- 適切に設定されたすべてのローカル RMU ユーザー
- この警告のための LDAP email テーブルに登録されているすべての RMU ユーザー

LDAP Email テーブルは、RMU が初回に起動されたときに、RMU ファームウェアにより最初に作成され、定期的に更新されます。LDAP Email テーブルのサイズは、最大 64 の LDAP 警告ロールと、Email 警告の送信先に設定されている最大 64 のグローバル RMU ユーザーに限定されています。

グローバル Email 警告には Email 配布リストの使用を推奨します。

LDAP ディレクトリサーバは、Email 警告の目的で、以下の情報を Email テーブルから取得します。

- email 警告の送信先に設定されているグローバル RMU ユーザーのリスト
- 各グローバル RMU ユーザーについて
  - 警告タイプ毎に設定された警告のリスト（タイプと重大度）
  - 要求されるメールフォーマット

LDAP email テーブルは以下の情況で更新されます。

- RMU が初回に起動されるか再起動されるとき。
- LDAP の設定が変更されるとき。
- 定期的 (任意)。更新の間隔は、RMU Web インターフェースでの LDAP 設定の一部として (LDAP Alert Table Refresh オプションの下で) 指定します (213 ページ の「ディレクトリサービス設定 (LDAP) - RMU」の項 , および *LDAP Alert Table Refresh* オプションを参照してください)。

ディレクトリサーバ上のグローバル Email 警告の設定

この節ではディレクトリサーバ上に LDAP Email 警告を設定する方法を説明します。

設定は RMU についても行う必要があります。これらの設定は RMU Web インターフェースで行います (213 ページ の「ディレクトリサービス設定 (LDAP) - RMU」の項 を参照してください)。

以下の通り進めます。

- ディレクトリサービスで、Email 警告が送信されるべきユーザーの Email アドレスを入力します。

  Email アドレス設定に使用する方法は、採用しているディレクトリサービス (Active Directory、eDirectory または OpenLDAP) によって異なります。

- 警告ロールを定義する設定ファイルを作成します。
- この設定ファイルを使用して SVS_LdapDeployer を起動し、対応する LDAP v2 ストラクチャ (*SVS*) をディレクトリサーバ上に生成させます (68 ページ and 77 ページ を参照してください)。

4.4.8.2 警告ロールの表示

LDAP v2 ストラクチャが生成されると、新たに作成された OU SVS が 表示されます。たとえば、Active Directory では、Declarations の配下にコンポーネント Alert Roles および Alert Types と一緒に、また DeptX の配下にコンポーネント Alert Roles と一緒に表示されます (図 43 を参照してください)。

– Declarations の配下では、*Alert Roles* にすべての定義された警告ロールが表示され、*Alert Types* の下にすべての警告タイプが表示されます (1)。

– DeptX の配下では、Alert Roles の下に OU DeptX において有効なすべての警告ロールが表示されます (2)。

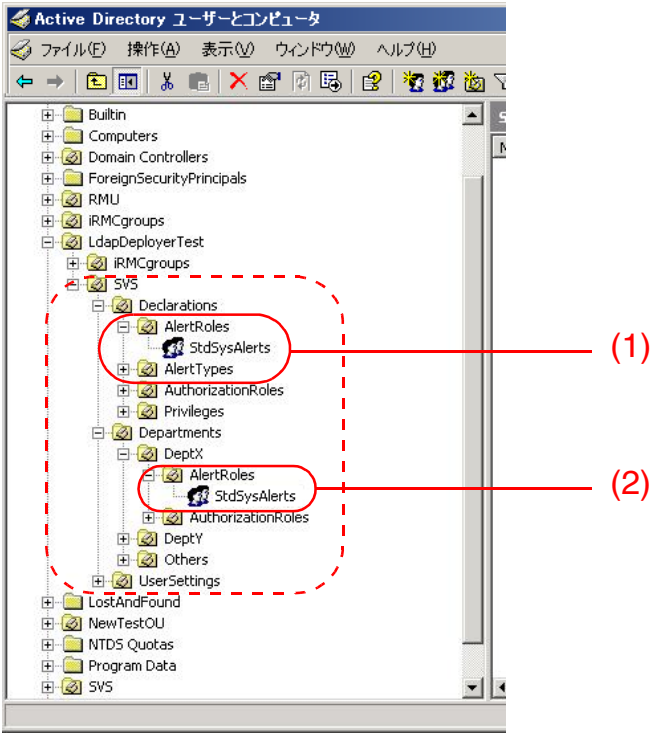


図 43: OU SVS と警告ロール

個々の警告ロールのユーザーに Email が確実に送信されるようにするため、RMU の対応する部門を設定する必要があります (図 43: *DeptX* で) (217 ページ を参照してください)。

Active Directory Users and Computers のストラクチャツリー (図 44 を参照) *SVS - Departments - DeptX - Alert Roles* の下で警告ロール (たとえば *StdSysAlerts*) を選択し (1)、次にコンテキストメニューから *PropertiesMembers* を選んでこの警告ロールの *Properties* ダイアログボックスを開くと、その警告ロール (この例では *StdSysAlerts*) に属するすべてのユーザーが *Members* タブに表示されます (2)。

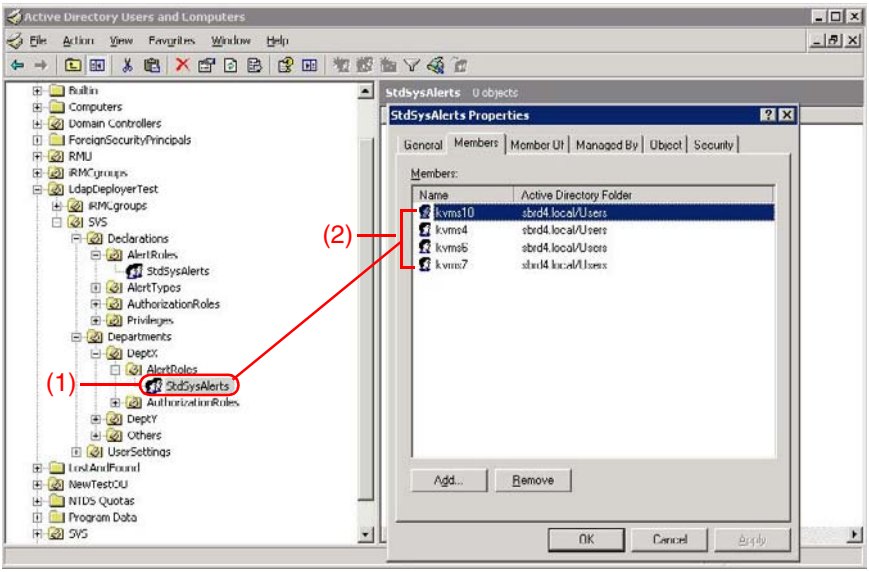


図 44: 警告ロール “StdSysAlert に割り当てられたユーザー

4.4.8.3 RMU ユーザーの警告ロールへの割り当て

RMU ユーザーの警告ロールへの割り当ては次の方法で行うことができます。

– ユーザーエントリに基づいて、または
– ロールエントリに基づいて

異なるさまざまなディレクトリサービス (Microsoft Active Directory、Novell eDirectory および OpenLDAP) がありますが、RMU ユーザーの RMU 警告ロールへの割り当ては、RMU ユーザーが RMU 権限ロール (Authorization roles) に割り当てられるのと同じ方法で、同じツールを使用して行われます。

たとえば、Active Directory の場合は – 、*Active Directory Users and -Computers* スナップイン (133 ページ の図 44 を参照) の *Properties* ダイアログボックスで Add... をクリックして、割り当てを行うことができます。

4.4.9 SSL copyright

RMU--LDAP の統合には、OpenSSL プロジェクトに基づき Eric Young 氏が開発した SSL 実装を使用しています。

```
/* ====================================================================
 * Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

5 RMU Web インターフェース

RMU はそれ自身のオペレーティングシステムを持つだけでなく、Web サーバとしても動作して、それ自身のインターフェースを提供します。 RMU Web インターフェースのメニューおよびダイアログボックスとして、ドイツ語表記と英語表記、日本語表記のいずれかを選択することができます。

RMU Web インターフェースから値を入力すると、いつでもツールチップ形式のアシストが受けられます。

以下に説明するソフトウェアは Independent JPEG Group の成果に一部基づいています。

5.1 RMU Web インターフェースへの ログイン

RMU Web インターフェースが開くと、*RMU 情報 (RMU Information)* ページが現われます (146 ページ を参照してください)。

► リモート管理端末で Web ブラウザを開き、RMU の (設定済みの) DNS 名 (191 ページ を参照) かまたは IP アドレスを入力してください。

RMU のディレクトリサービスへの LDAP アクセスが設定されているかどうかで、現われるログイン画面が異なります (*LDAP enabled* オプション、214 ページ を参照)。

ログイン画面がまったく現われない場合は、LAN 接続をチェックしてください。

– RMU のディレクトリサービスへの LDAP アクセスが設定されておらず (*LDAP enabled* オプションが有効になっていない)、*Always use SSL Login* オプション (214 ページ を参照) も有効になっていない場合。

図 45: RMU Web インターフェースのログイン画面 (LDAP アクセスが設定されておらず、“Always use SSL login” オプションが選択されていない)

► デフォルトの管理者アカウントのデータを入力してください。

ユーザー名 : admin

パスワード: admin

ユーザー名もパスワードも大文字、小文字を区別します。

セキュリティ上の理由から、一度ログインした後は、新しい管理者アカウントを作成してデフォルトの管理者アカウントを削除するか、少なくともパスワードを変更するようにお勧めします (204 ページ の「ユーザー名の設定 - ユーザー設定 (詳細)」を参照してください)。

► *OK* をクリックして入力を確定してください。

– RMU のディレクトリサービスへの LDAP アクセスが設定されている (*LDAP enabled* オプションが有効になっている) か、*Always use SSL Login* オプションが有効になっている場合。

図 46: RMU Web インターフェースのログイン画面 (LDAP アクセスが設定されている)

ユーザー名とパスワードは、送信されるとき常に SSL で保護されています。*Secure (SSL)* オプションを有効にすると、Web ブラウザと RMU の間の通信はすべて HTTPS 経由で行われます。

► デフォルトの管理者アカウントのデータを入力してください。

ユーザー名: admin
パスワード: admin

セキュリティ上の理由から、一度ログインした後は、新しい管理者アカウントを作成してデフォルトの管理者アカウントを削除するか、少なくともパスワードを変更するようにお勧めします (204 ページ の「ユーザー名の設定 - ユーザー設定 (詳細)」を参照してください)。

► *Login* をクリックして入力を確定してください。

5.2 必要なユーザー許可

表 7 に、RMU Web インターフェースの個々のファンクションを使用するために必要な許可の概要を示します。

RMU Web インターフェースのファンクション	IPMI 特権レベルで許可				必要な許可	
	OEM	管理者	オペレーター	ユーザー	ユーザーアカウントの設定	RMU 設定の構成
System Overview (システム概要) ページのオープン	X	X	X	X		
識別灯のオン / オフ	X	X	X	X		
Asset Tag Configuration (資産管理情報)						X
RMU Information (RMU 情報) ページのオープン	X	X	X	X		
Reboot RMU (RMU の再起動)。	X	X				
RMU の時計の手動調整						X
Set *Miscellaneous RMU Options* (RMU その他のオプション) の設定						X
Open and edit *Certificate Upload* (証明書の更新) ページのオープンおよび編集						X
Open and edit *Generate a self signed RSA Certificate* (自己署名入り RSA 証明書) ページのオープンおよび編集						X
RMU Firmware Update (RMU ファームウェアの更新) ページのオープン	X	X	X	X		
RMU TFTP Firmware Update (RMU TFTP ファームウェアの更新) ページのオープンおよび編集						X
ファームウェアセレクタの設定	X	X				X
Firmware update via Upload from file (ファイルからのアップロードによるファームウェアの更新)						X
RMU TFTP Einstellungen						X
Open and edit the *Fans* (ファン) ページのオープンおよび編集						X

表 7: RMU Web インターフェースを使用する許可

RMU Web インターフェースのファンクション	IPMI 特権レベルで許可				必要な許可	
	OEM	管理者	オペレーター	ユーザー	ユーザーアカウントの設定	RMU 設定の構成
ファンテストの無効化 (*Fan Test* グループ)						X
Set *Fan Check Time* (ファンチェック時刻) の設定 (*Fan Test* グループ)						X
Temperature (温度) ページのオープン	X	X	X	X		
Define 警告 / 致命的レベルの定義						X
Voltages (電圧) ページのオープン	X	X	X	X		
Open *Pressure Information* (圧力情報) ページのオープン	X	X	X	X		
圧力プロファイルの設定						X
Contact/Switch Configuration (接点 / スイッチ設定) ページのオープン	X	X	X	X		
接点 / スイッチ設定の構成						X
Power Supply (電源装置) ページのオープン	X	X	X	X		
Component Status (コンポーネントの状態) ページのオープン	X	X	X	X		
System Event Log Content (システムイベントログ内容) ページのオープン	X	X	X	X		
システムイベントログ (SEL) の消去	X	X	X			
Save event log (イベントログの保存)	X	X	X	X		
SEL エントリ表示のための重大度の定義	X	X	X	X		
System Event Log Configuration (システムイベントログ設定) ページのオープン	X	X	X	X		X
System Event Log Configuration (システムイベントログ設定) ページのオープン						X
Network Interface (ネットワークインターフェース) ページのオープンおよび編集						X

表 7: RMU Web インターフェースを使用する許可

RMU Web インターフェースのファンクション	IPMI 特権レベルで許可				必要な許可	
	OEM	管理者	オペレーター	ユーザー	ユーザーアカウントの設定	RMU 設定の構成
Ports and Netw. Services (ポート番号とネットワークサービス設定) ページのオープンおよび編集						X
DHCP Configuration (DHCP 設定) ページのオープンおよび編集						X
DNS Settings (DNS 設定) ページのオープンおよび 編集						X
SNMP TRAP Alerting (SNMP TRAP 警告) ページのオープンおよび 編集						X
Email Alerting (Email 警告) ページのオープンおよび 編集						X
RMU User (RMU ユーザー) ページのオープンおよび 編集					X	
Directory Service Config. (ディレクトリサービス設定) ページのオープンおよび 編集						X
RMU Telnet/SSH Access (RMU Telnet/SSH アクセス) の起動	X	X	X	X		
SSH ログイン / Telnet ログイン	X	X	X	X		

表 7: RMU Web インターフェースを使用する許可

5.3 ユーザーインターフェース画面

RMU Web インターフェースの画面を以下に示します。

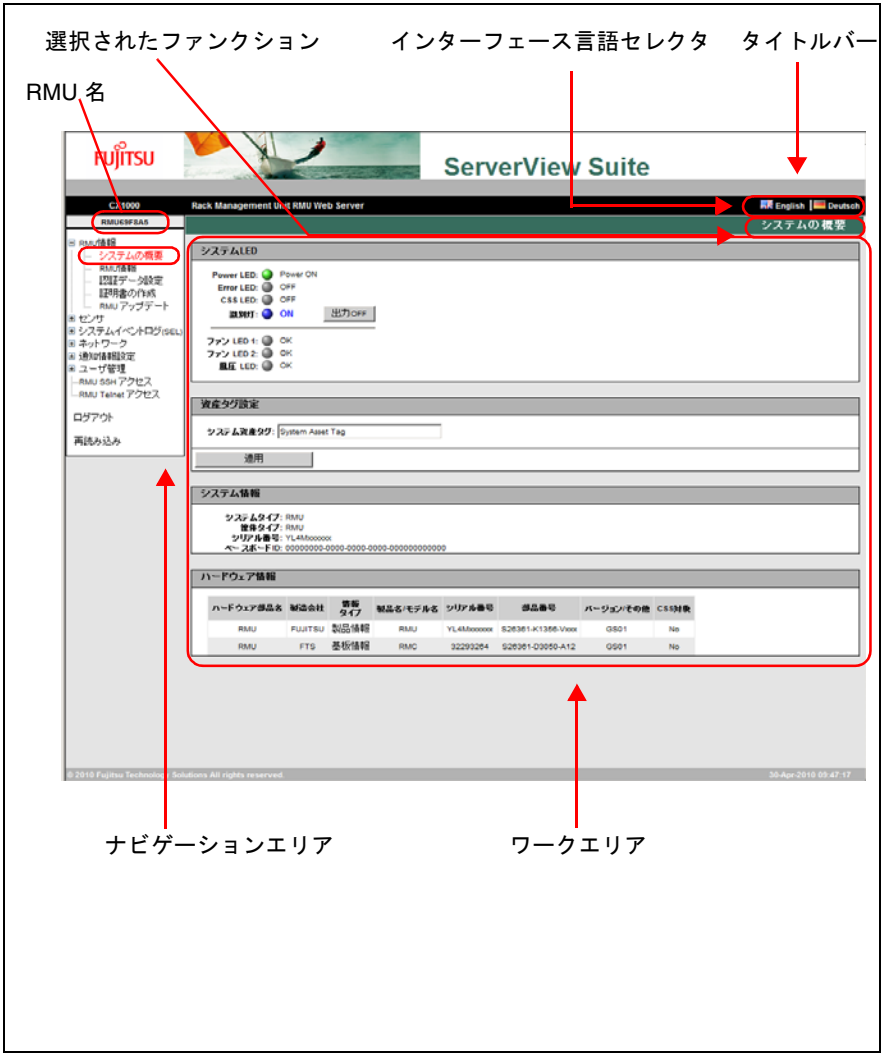


図 47: RMU Web インターフェース画面

RMU Web インターフェースの言語の選択

ワークエリアの上の黒いバーの右に、旗のアイコンがあります。このアイコンをクリックして、RMU Web インターフェースのナビゲーションエリア、メニューおよびダイアログボックスを表示する言語（ドイツ語、英語あるいは日本語）を選択してください。

ナビゲーションエリア

ナビゲーションエリアは、タスク別に配列された RMU の個々の機能 (ファンクション) へのリンクをノードで連結したメニューツリーの構造を含んでいます。これらのリンク (図 47: *System Overview* を参照) の中から 1 つをクリックすると、そのリンクが有効になり、その機能の出力、ダイアログボックス、オプション、リンクおよびボタンがワークエリアに表示されます。

個々の RMU 機能へのリンクの下に、リンク *Logout* (ログアウト) および *Refresh* (再読み込み) があります。

- *Logout* は、RMU セッションをダイアログボックスで確認した後にこれを終了させることができます。RMU のディレクトリサービスへの LDAP アクセスが設定されているかどうかで、セッションを閉じた後に現われるログイン画面が異なります (*LDAP enabled* オプション、214 ページ を参照)。
  - RMU のディレクトリサービスへの LDAP アクセスが設定されておらず (*LDAP enabled* オプションが有効になっていない)、しかも *Always use SSL Login* オプション (214 ページ を参照) が無効になっている場合は、次のようなログイン画面が現われます。

図 48: ログインページ (ログアウト後)

Login ボタンをクリックすると、RMU Web インターフェースのログイン画面が開きます (138 ページ の図 45 を参照)。お望みなら、ここから再度ログインできます。

– RMU のディレクトリサービスへの LDAP アクセスが設定されている (*LDAP enabled* オプションが有効になっている) か、*Always use SSL Login* オプション (214 ページ を参照) が有効になって (原稿 deactivated は誤植) いる場合は、対応するログイン画面が現われます (139 ページ の図 46 を参照)。

- *Refresh* をクリックすると、RMU Web インターフェースの内容が再読み込みされます。

  再読み込みの代わりに、内容が定期的に更新されるようにインターフェースを設定することもできます (188 ページ を参照)。

5.4 RMU I 情報 - RMU および管理対象ラックサーバに関する情報

RMU Information (RMU 情報) のエントリは、以下のページへのリンクを含みます。

– 147 ページ の「System Overview (システムの概要) - RMU および管理対象ラックサーバに関する一般情報」
– 152 ページ の「RMU 情報 - RMU に関する情報」
– 155 ページ の「認証データ設定 - DSA/RSA 証明書と DSA/RSA 秘密鍵のロード」
– 162 ページ の「自己署名入り証明書の生成 - 自己署名入り RSA 証明書の生成」
– 164 ページ の「RMU アップデート」

5.4.1 System Overview (システムの概要) - RMU および管理対象ラックサーバに関する一般情報

System Overview ページは以下の事項に関する情報を提供します。

– ラックサーバのシステム LED
– システム (RMU に関する一般情報)
– システムの FRU (保守部品) / IDPROM.

上記の情報表示に加え、*System Overview* ページでは、管理対象ラックシステムの顧客別資産タグを入力することができます。

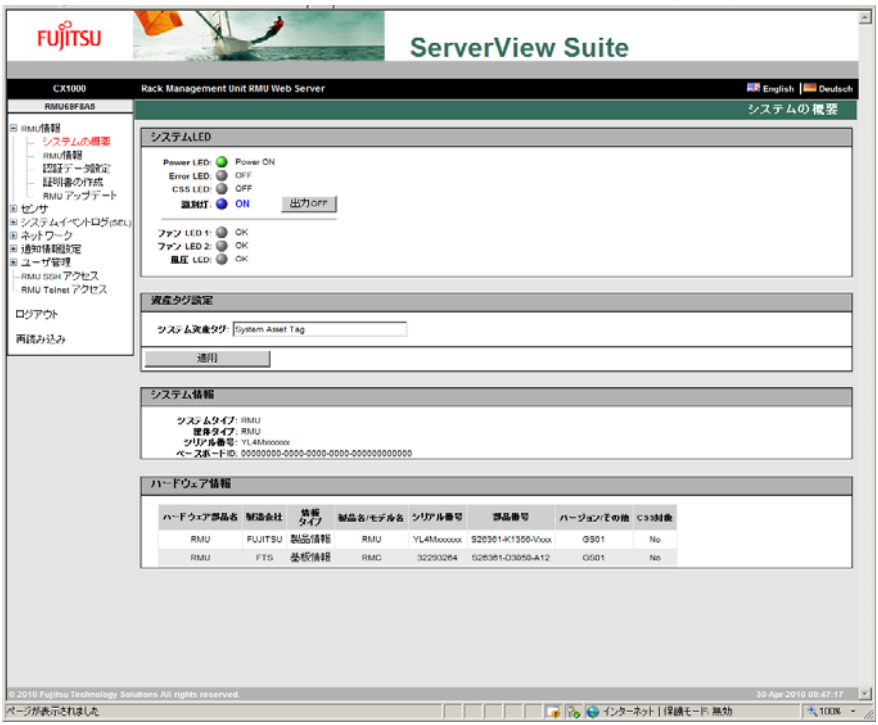


図 49: システムの概要 - ページ

システム LED

電源 LED、グローバルエラー LED、CSS LED および識別灯が *System Status* の下に示されます。PRIMERGY 識別灯をオン / オフすることもできます。

システム LED のほかに、*System Status* グループにはファン LED 2 個と圧力 LED が組み込まれていて、それぞれ、大型ラジアルファンと圧力センサに関する情報を提供します。

図 50: システムの概要ページ - システム LED

Power LED (電源 LED)

RMU の電源状態。
次の状態があり得ます。

- オン : “電源 ON” (緑) と “Power On” の表示
- オン : “スタンバイモード (緑) と “Suspend to RAM (Standby)” の表示 .
- Off: “電源 OFF” (オレンジ)

Error LED (エラー LED)

RMU のグローバルエラー LED の状態を知らせます。

状態情報 (RMU)	RMU 上のグローバルエラー LED	サーバの状態
オフ	点灯しない	致命的イベントなし
オン	オレンジに点灯	非 CSS コンポーネント故障予兆イベント
オレンジに点滅	オレンジに光る	致命的イベント (エラー)

CSS LED

RMU の CSS (Customer Self Service 顧客自己保守) LED の状態を知らせます。RMU は現在 CSS コンポーネントを一切含んでいないので、CSS LED はつねにオフになっています。

Identify LED (識別灯)

RMU / ラックサーバ識別灯。
次の状態があり得ます。

- オン (青)
- オフ (グレー)

Turn On/Turn Off

Turn On / Turn Off ボタンをクリックすると、識別灯はオン、オフを繰り返します。

Fan LED 1 / Fan LED 2 (ファン LED 1 / ファン LED 2)

RMU のファン FAN1 および FAN 2 の状態を知らせます。

状態情報 (RMU)	RMU 上の FAN 1 / Fan 2 LED	対応するファンの状態
オフ	点灯しない。	対応するファンでは : 致命的イベントなし。
オン	黄色に点灯。	対応するファンでは : 故障予兆イベントまたは致命的エラー。

圧力 LED

ラックサーバの圧力 LED の状態を知らせます。

状態情報	RMU 上の圧力 LED	対応する圧力センサの状態
オフ	点灯しない。	致命的イベントなし。
オン	オレンジに点灯	故障予兆または致命的圧力

資産管理情報

Asset Tag Configuration (資産管理情報) では、管理対象ラックシステムの顧客別資産タグを入力することができます。

顧客別資産タグで、管理対象ラックシステムに、在庫管理番号やその他の適当な識別番号を割り当てることができます。

Windows 対応システムの場合は、この顧客別資産タグは WMI (Windows Management Instrumentation) より自動的に提供されます。提供された資産タグはインハウスツールで評価したり、企業管理システム (CA Unicenter など) への統合に使用することができます。

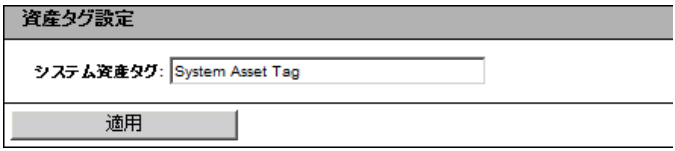


図 51: システムの概要 - システム状態ページ

System Asset Tag

ここに資産タグを入力できます。

► *その資産タグを承認するときは、Apply* をクリックします。

システム情報

System Information (システム情報) は RMU に関する情報をリストします。

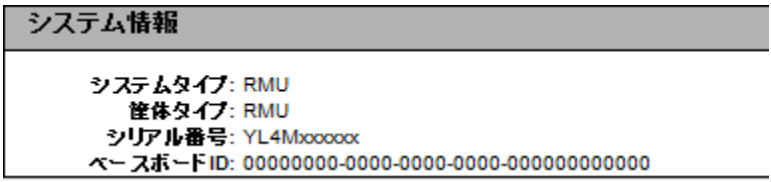


図 52: システムの概要ページ - システム情報

ハードウェア 情報

System FRU/IDPROM Information の下に、FRU (保守部品) に関する情報がリストされます。FRU はシステムから解放し取り外すことのできるコンポーネントです。CSS Component のコラムには、各コンポーネントについて、CSS (**顧客自己保守**) 機能がサポートされるか否かが表示されます。

ハードウェア情報

ハードウェア部品名	製造会社	情報タイプ	製品名/モデル名	シリアル番号	部品番号	バージョン/その他	CSS対象
RMU	FUJITSU	製品情報	RMU	YL4Mxxxxxx	S26361-K1356-Vxxx	GS01	No
RMU	FTS	基板情報	RMC	32293264	S26361-D3050-A12	GS01	No

図 53: システムの概要ページ - ハードウェア情報

5.4.2 RMU 情報 - RMU に関する情報

RMU Information (RMU 情報) ページは以下の情報を提供します。

– RMU のファームウェアと SDRR バージョンに関する情報の表示、ファームウェアセレクタの設定やファームウェアイメージのロードと、RMU の再起動。

– アクティブな RMU セッションに関する情報の表示 。

– ライセンスキーの RMU への登録 。

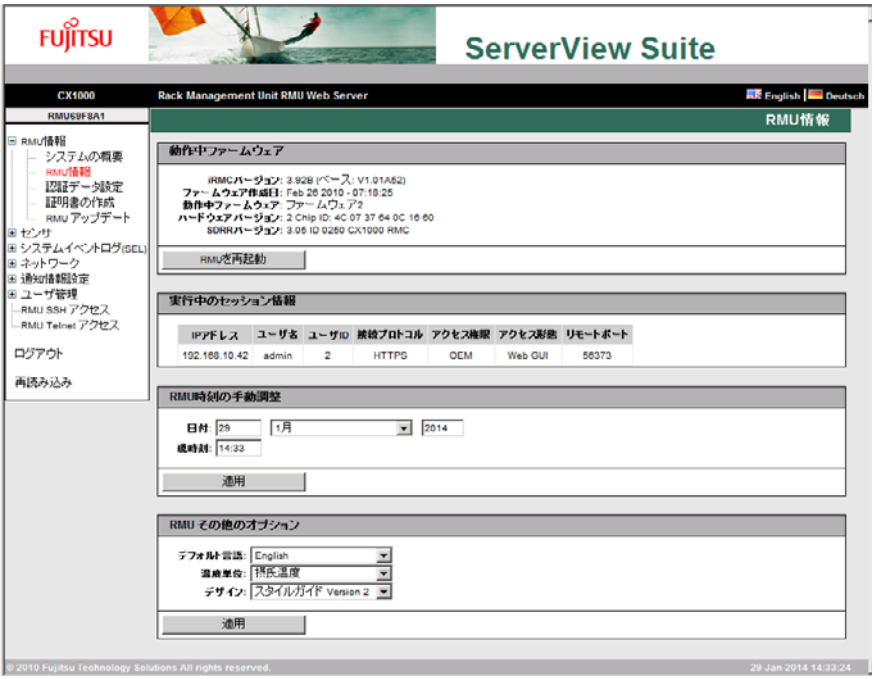


図 54: RMU 情報ページ

動作中ファームウェア

Running Firmware (動作中ファームウェア) では、RMU のファームウェアと SDRR バージョンに関する情報の表示と、RMU の再起動を行うことができます。

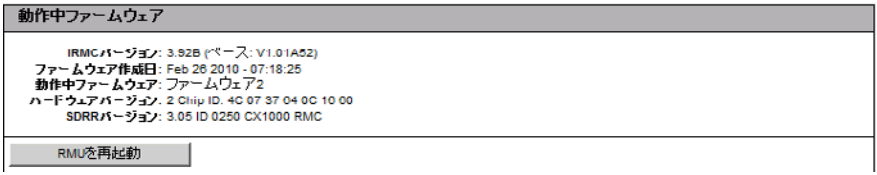


図 55: RMU 情報ページ - ファームウェア情報と RMU の再起動

Reboot RMU (RMU 再起動)
RMU を再起動します。

Reboot RMU ボタンは、管理対象サーバの BIOS POST フェーズの間無効となります。

実行中のセッション情報

Active Session Information (実行中のセッション情報) グループは、現在アクティブな RMU セッションをすべて示します。

図 56: RMU 情報ページ - 実行中のセッション情報

RMU の時計の手動調整

Manually adjust RMU time (RMU の時計の手動調整) グループは、RMU の時刻設定を入力することができます。

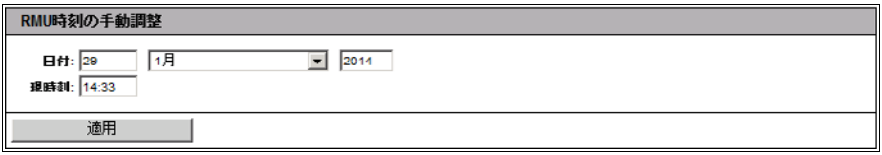


図 57: RMU 情報ページ - RMU の時計の手動調整

- *Apply* をクリックすると、設定した RMU の時刻が有効になります。

RMU その他の オプション

Miscellaneous RMU Options (RMU その他のオプション) グループでは、RMU Web インターフェースのレイアウトについて設定を行うことができます。

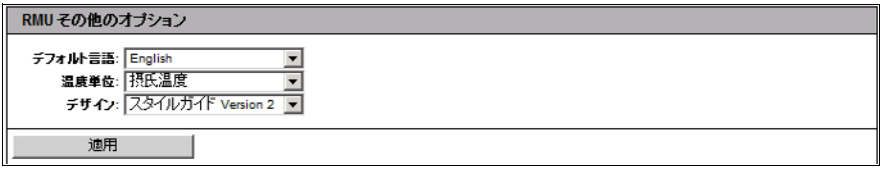


図 58: RMU 情報ページ - その他のオプション

Default Language (デフォルト言語)
使用言語 (ドイツ語 / 英語 / 日本語) の初期設定をします。次に RMU Web インターフェースを開くと、その言語がデフォルト設定で有効になります。しかし、インターフェース言語の変更はブラウザセッション内ではいつでも (作業の途中でも) 可能です。

Temperature Units (温度単位)
RMU Web インターフェースで温度を表示するときに使う単位 (摂氏 / 華氏) を指定します。指定した単位は現セッションに適用され、次回 RMU Web インターフェースを呼び出すときにプリセットされています。

Colour Schema (カラースキーム)
RMU Web インターフェースのディスプレイのカラースキームを指定します。この設定は現在アクティブなセッションすべてに適用され、次回 RMU Web インターフェースを呼び出すときにプリセットされています。

5.4.3 認証データ設定 - DSA/RSA 証明書と DSA/RSA 秘密鍵のロード

Certificate Upload (認証データ設定) ページでは、認証局（CA）からの署名入り X.509 DSA/RSA 証明書 (SSL) や DSA/RSA 秘密鍵 (SSH) を RMU にアップロードすることができます。

RMU にはあらかじめ定義されたサーバ証明書 (既定の証明書に戻す) が提供されています。セキュリティ保護された SSL/SSH 接続経由で RMU にアクセスしたい場合は、既定の証明書に戻すを認証局 (CA) の署名入り証明書にできるだけ早く置き換えることを推奨します。

X.509 DSA/RSA 証明書と DSA/RSA 秘密鍵の入力形式。

X.509 DSA/RSA 証明書も RSA/DSA も PEM エンコード形式 (ASCII/Base64) で入手できなければなりません。

図 59: 認証データ設定 - ページ

現在有効な (CA) DSA/RSA 証明書の表示

- *Certificate Information and Restore* (情報とリストア) のグループで、*View Certificate* (Web 証明書を表示) をクリックすると、現在有効な SSH/SSL 証明書が表示されます
- *Certificate Information and Restore* グループで、*View CA Certificate* (証明局の証明書を表示) をクリックすると、現在有効な CA 証明書が表示されます。

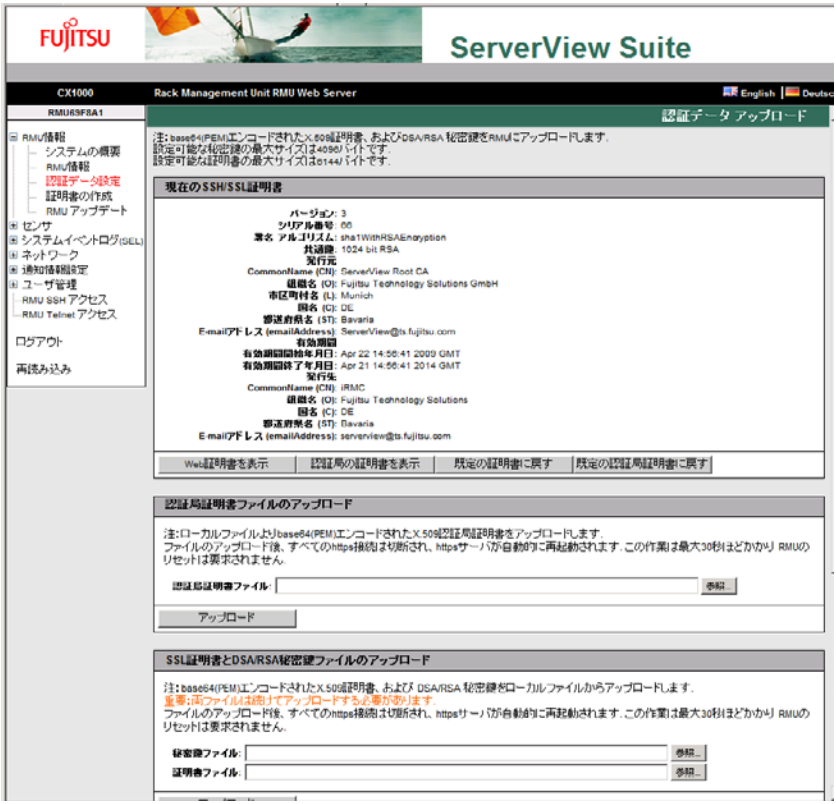


図 60: 認証データ設定ページ - 現在有効な SSL/SSH 証明書の表示

既定の証明書に戻す、既定の認証局証明書に戻すの復元

- *Certificate Information and Restore* グループで、*Default Certificate* (既定の証明書に戻す) をクリックし、本当にそうしたいと確認を与えると、ファームウェアで提供された既定の証明書に戻すが復元されます。
- *Certificate Information and Restore* グループで、*Default CA Certificate* (既定の認証局証明書に戻す) をクリックし、本当にそうしたいと確認を与えると、ファームウェアで提供された既定の認証局証明書に戻すが復元されます。

図 61: 認証データ設定ページ - 既定の認証局証明書に戻すの復元

ローカルファイルからの CA 証明書のロード

CA Certificate upload from file （証書局証明書ファイルのアップロード）グループを使用して、ローカルファイルから CA 証明書をロード します。

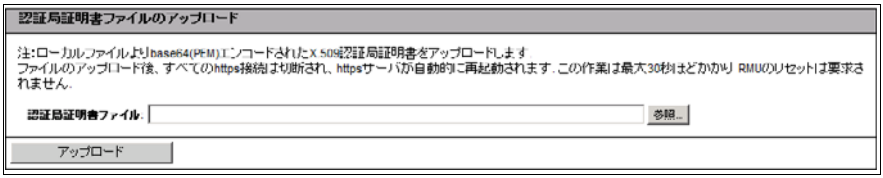


図 62: ローカルファイルからの CA 証明書の登録

次の手順で行ってください。

- CA 証明書を管理対象サーバ上のローカルファイルに保存します。
- *CA Certificate File* で、*右側の Browse...* (参照) ボタンをクリックして CA 証明書の入ったファイルに進み、このファイルを指定します。
- *Upload* ボタンをクリックすると、証明書あるいは秘密鍵が RMU に登録されます。

  証明書あるいは秘密鍵をアップロードすると、既存の HTTPS 接続はすべて閉じられ、HTTPS サーバは自動的に再起動します。このプロセスは最大 30 秒ほどかかることがあります。RMU の明示的リセットは必要ありません 。

- *View CA Certificate* (証明局の証明書を表示) ボタンをクリックして、証明書が正常に登録されたことを確認してください。

ローカルファイルからの DSA/RSA 証明書と DSA/RSA 秘密鍵のロード

次のグループを用いてこの操作を行います。
SSL Certificate and DSA/RSA private key upload from file（SSL 証明書と DSA/RSA 秘密鍵ファイルのアップロード）.

秘密鍵と証明書は必ず同時に RMU に登録してください、

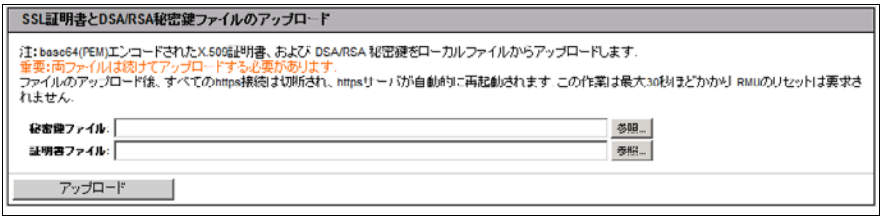


図 63: ローカルファイルからの DSA/RSA 証明書 / DSA/RSA 秘密鍵のロード

次の手順で行ってください。

- X.509 DSA/RSA (SSL) 証明書と DSA/RSA 秘密鍵を管理対象サーバ上の対応するローカルファイルに保存します。
- *Private Key File* および *Certificate File* で、対応する *Browse* (参照) ボタンをクリックして秘密鍵あるいは証明書が入っているファイルに進み、それぞれのファイルを指定します。
- *Upload* ボタンをクリックすると、証明書と秘密鍵が RMU に登録されます。

  証明書と秘密鍵をアップロードすると、既存の HTTPS 接続はすべて閉じられ、HTTPS サーバは自動的に再起動します。このプロセスには最大 30 秒ほどかかることがあります。**RMU の明示的リセットは必要ありません。**
- *View Certificate* (証明書を表示) ボタンをクリックして、証明書が正常に登録されたことを確認してください。

DSA/RSA 証明書 / DSARSA 秘密鍵の直接入力

この操作は次のグループを用いて行います。*SSL DSA/RSA certificate or DSA/RSA private upload via copy & paste* (コピー&ペーストによる SSL DSA/RSA 証明書または DSA/RSA 秘密鍵のアップロード)。

ルートアクセス権限証明書を RMU に登録するときは、この方法を使用しないこと。ルートアクセス権限証明書は必ずファイルを使用して登録してください (160 ページ を参照してください)。

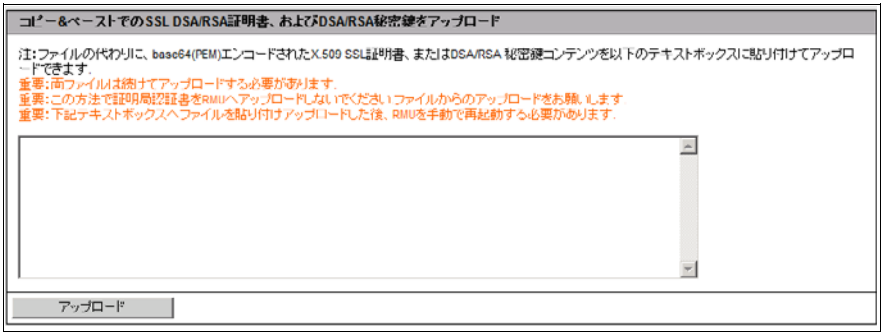


図 64: DSA/RSA 証明書 / DSA/RSA 秘密鍵の直接入力

次の手順で行ってください。

- X.509 DSA 証明書**または** DSA 秘密鍵を入力域にコピーします。

  同じアップロードで証明書と鍵を同時に入力することはできません。

- *Upload* ボタンをクリックすると、証明書または秘密鍵が RMU に登録されます。
- リモートマネージャを使用して RMU をリセットします (244 ページ を参照してください)。

  RMU に登録した証明書または秘密鍵を有効なものにするには、この操作が必要です。

- *View Certificate* (証明書を表示) ボタンをクリックして、証明書が正常に登録されたことを確認してください。

5.4.4 自己署名入り証明書の生成 - 自己署名入り RSA 証明書の生成

Generate Certificate(証明書の作成) ページで、自己署名入り証明書を作成することができます。

図 65: 自己署名入り証明書の生成 ページ

証明書情報および復元

Certificate Information and Restore (証明書情報および復元) グループで、現在有効な DSA/RSA 証明書を表示したり、既定のの RSA/DSA 証明書を復元することができます。

View Certificate (証明書を表示)
このボタンを使って、現在有効な DSA/RSA 証明書を見ることができます。

Default Certificate （既定の証明書に戻す）
このボタンを使って、本当にそうしたいと確認を与えた後、ファームウェアで提供された既定の証明書に戻すを復元することができます。

証明書の作成

次の手順で自己署名入り証明書を作成することができます。

- ► *Certificate Creation* (証明書の作成) の下に、必要な事項を入力します。
- ► *Create* (作成) をクリックすると、証明書が作成されます。

新しい証明書を生成すると、既存の HTTPS 接続がすべて切断され、HTTPS サーバが自動的に再起動します。キーの長さによって、最大 5 分ほどかかることがありります。RMU の明示的リセットは必要ありません。

5.4.5 RMU アップデート

RMU Firmware Update (RMU アップデート) ページでは、RMU ファームウェアをオンラインで更新することができます。そのためには、リモート管理端末上でローカルに、または TFTP サーバ上で、現在のファームウェアイメージを提供する必要があります。

このページでは、RMU ファームウェアに関する情報を見てファームウェアセレクタを設定することもできます。

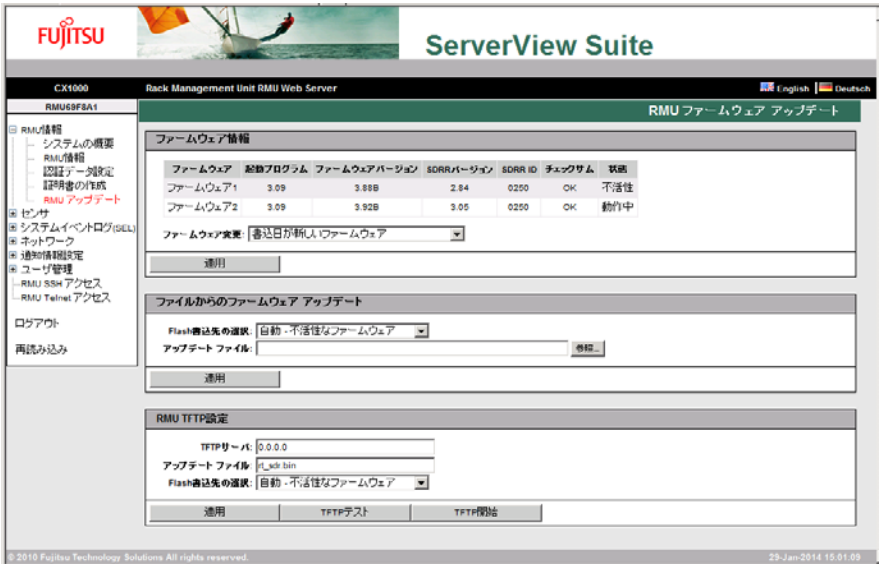


図 66: RMU アップデートページ

ファームウェアイメージ情報

Firmware Image Information (ファームウェアイメージ情報) の下で、RMU のファームウェアバージョンと SDRR バージョンに関する情報を見たり、ファームウェアセレクタを設定したりできます。

RMU ファームウェアおよびファームウェア更新に関する詳しい情報は、19 ページ の「ラック管理ユニット (RMU) - ファームウェア」の項を参照してください。

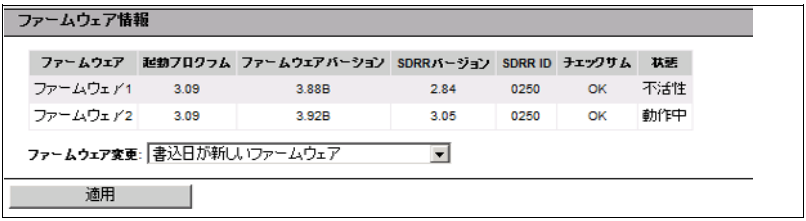


図 67: RMU アップデートページ - ファームウェアイメージ情報

Firmware Selector (ファームウェアセレクタ)

ファームウェアセレクタを使用して、次に RMU を再起動した時にどのファームウェアイメージをアクティブ化するかを指定します。

以下のオプションがあります。

- *Auto - FW Image with highest FW version*
  (自動 - 版数の最も高い FW イメージ)

  最新バージョンのファームウェアイメージが自動的に選択されます。

- *Low FW Image (low FW イメージ)*

  低いファームウェアイメージが選択されます。

- *High FW Image (high FW イメージ)*

  高いファームウェアイメージが選択されます。

- *Select FW Image with oldest FW version*
  (版数の最も古い FW イメージを選択)

  最も古いバージョンのファームウェアイメージが選択されます。

- *Select most recently programmed FW*
  (プログラム時期の最も新しい FW を選択)

  更新時期の最も新しいファームウェアイメージが選択されます。

– *Select least recently programmed FW*
(プログラム時期の最も古い FW を選択)

更新時期の最も古いファームウェアイメージが選択されます。

- *Apply* をクリックすると、ファームウェアセレクタが *Firmware Selector* で選択したオプションに設定されます。

ファイルからのファームウェアの更新

Firmware Update from File (ファイルからのファームウェアの更新) ページでは、RMU ファームウェアをオンラインで更新することができます。そのためには、ファイルに収めた現在のファームウェアイメージをリモート管理端末に搭載する必要があります。

RMU のための適切なファームウェアイメージを、次の URL からダウンロードすることができます。*http://support.ts.fujitsu.com/com/support/downloads.html*.

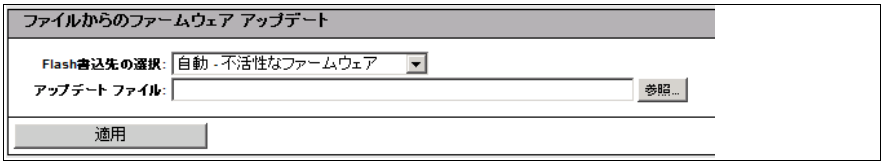


図 68: RMU アップデートページ - ファイルからのファームウェアの更新

Flash Selector (Flash 書込先の選択)
どんな RMU ファームウェアを更新するかを指定します。

以下のオプションがあります。

– *Auto - inactive firmware* (自動 - 不活性なファームウェア)

不活性なファームウェアが自動的に選択されます。

– *Low Firmware Image* (低ファームウェアイメージ)

低ファームウェアイメージ (ファームウェアイメージ 1) が選択されます。

– *High Firmware Image (高ファームウェアイメージ)*

高ファームウェアイメージ (ファームウェアイメージ 2) が選択されます。

Update file (アップデートファイル)
ファームウェアイメージが収められたファイル 。

下記のファイルの各々を使用して、更新実行のたびに、RMU ファームウェアのひとつのコンポーネント (ランタイムファームウェアと SDR レコード) を更新することができます。

RMU にはファイル *rt_sdr_<D-number>_4_08g_00.bin* も使用可能です。これを使うと、RMU ファームウェアの全コンポーネントが一回の操作で更新できます。

dcod<FW-Version>.bin
ランタイムファームウェアを更新します。

<SDR-Version>.SDR
SDR レコードを更新します。

Browse... (参照)
ファイルブラウザを開き、アップデートファイルに移動できるようにします。

- *Apply* ボタンをクリックすると、設定が有効になり、RMU アップデートがスタートします。

RMU TFTP 設定

Firmware Update from File (ファイルからのファームウェアの更新) ページで、RMU ファームウェアをオンラインで更新することができます。そのためには、ファイルに収めた現在のファームウェアイメージを TFTP サーバに搭載する必要があります。

RMU のための適切なファームウェアイメージを、次の URL からダウンロードすることができます。*http://support.ts.fujitsu.com/com/support/downloads.html*.

図 69: RMU アップデートページ - RMU TFTP 設定

TFTP Server (TFTP サーバ)
ファームウェアイメージのファイルを格納する TFTP サーバの IP address または DNS 名。

Update file (アップデートファイル)
ファームウェアイメージが収められたファイル

下記のファイルの各々を使用して、TFTP を起動するたびに、RMU ファームウェアのひとつのコンポーネント (ランタイムファームウェアと SDR レコード) を更新することができます。

RMU にはファイル *rt_sdr_<D-number>_4_08g_00.bin* も使用可能です。これを使うと、RMU ファームウェアの全コンポーネントが TFTP サーバを用いて一回の操作で更新できます。

dcod<FW-Version>.bin
ランタイムファームウェアを更新します。

<SDR-Version>.SDR
SDR レコードを更新します。

Flash Selector (Flash 書込先の選択)
どんな RMU ファームウェアを更新するかを指定します。

You have the following options:

– *Auto - inactive firmware (自動 - 不活性なファームウェア)*

不活性なファームウェアが自動的に選択されます。

– *Low Firmware Image* (低ファームウェアイメージ)

低ファームウェアイメージ (ファームウェアイメージ 1) が選択されます。

– *High Firmware Image* (高ファームウェアイメージ)

高ファームウェアイメージ (ファームウェアイメージ 2) が選択されます。

- *Apply* ボタンをクリックすると、設定が有効になります。
- *TFTP Test* ボタンをクリックすると、TFTP サーバとの接続状態がテストできます。
- *TFTP Start* ボタンをクリックすると、TFTP サーバからファームウェアイメージを収めたファイルがダウンロードされ、RMU ファームウェアの更新がスタートします。

5.5 センサ - センサの状態のチェック

“Sensors (センサ)” のエントリからは、管理対象ラックサーバのセンサのテストができるページに進むことができます。

– 170 ページ の「ファン - ファンのチェック」.
– 171 ページ の「温度 - 温度センサのチェック」.
– 172 ページ の「電圧 - 電圧センサのチェック」.
– 173 ページ の「圧力情報 - 圧力センサのチェック」.
– 174 ページ の「接点 / スイッチ情報 - コンタクトスイッチの設定」.
– 175 ページ の「電源装置 - 電源装置のチェック」.
– 176 ページ の「コンポーネントの状態 - RMU コンポーネントの状態のチェック」.

状態チェックが容易にできるように、センサの状態は現在値の形だけでなく、カラーコードと状態アイコンを用いても表示されます。

黒 	測定値は稼動時の正常な値の範囲内にあります。
オレンジ 	測定値は警告のしきい値を超えました。 システムの稼動はまだ損なわれてはいません。
赤 	測定値は致命的しきい値を超えました。 システムの稼動が損なわれる可能性があり、データの完全性が失われる危険があります。

表 8: センサの状態

5.5.1 ファン - ファンのチェック

Fans (ファン) ページは、システムファンとその状態に関する情報を提供します。

図 70: ファンページ

ファンテスト - ファンのテスト

Fan Test (ファンテスト) グループでは、ファンテストを自動的に開始する時刻を指定したり、ファンテストを明示的に開始させることができます。

Fan Check Time (ファンチェック時刻)
ファンテストが自動的に開始される時刻を入力します。

Disable Fan Test (ファンテストを無効化)
このオプションを選ぶと、ファンテストが実行されなくなります。

- *Apply* ボタンをクリックすると、設定が有効になります。

システムファン - システムファンが故障した場合のサーバの挙動を指定

System Fans (システムファン) グループは、システムファンの状態に関する情報を提供します。

5.5.2 温度 - 温度センサのチェック

Temperatur (温度) ページは、RMU の温度、周囲温度、および排気温度を測定する温度センサの状態に関する情報を提供します。

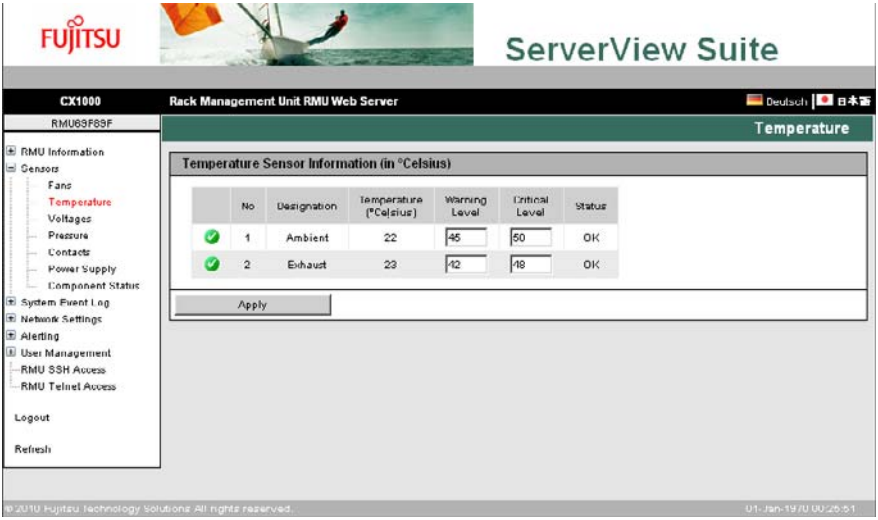


図 71: 温度ページ

Warning Level (警告レベル)
次の表示が始まる (対応するセンサの) 温度レベル

– 「警告」アイコン (オレンジ) がこの *Temperature* ページのエントリに表示されます。

– SEL エントリが生成されます (重大度レベル | *Major* 重大)。

Critical Level (致命的レベル)
次の表示が始まる対応するセンサの温度レベル

– 「致命的」アイコン (赤) がこの *Temperature* ページのエントリに肘されます。

– SEL エントリが生成されます (重大度レベル *Critical* 致命的)。

► *Apply* をクリックすると、設定が有効になります。

5.5.3 電圧 - 電圧センサのチェック

Voltages (電圧) ページは、RMU のコンポーネントに配置された電圧センサの状態に関する情報を提供します。

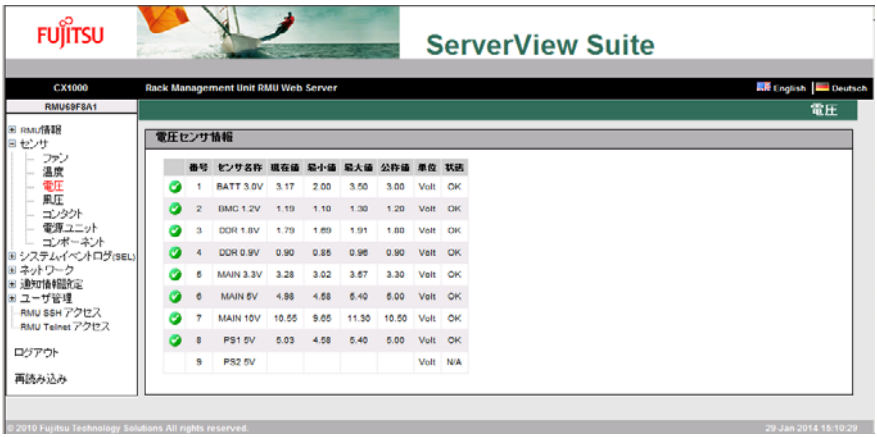


図 72: 電圧ページ

5.5.4 圧力情報 - 圧力センサのチェック

Pressure Information (圧力情報) ページは、RMU の低圧チャンバ内の陰圧を測定する圧力センサと、圧力設定値に関する情報を提供します。

さらに、圧力プロファイルを定義することにより圧力センサの設定を行うことができます。

図 73: 圧力情報ページ

Pressure Sensor Information (圧力センサ情報)
圧力センサの現在値と圧力設定値に関する情報を提供します。圧力設定値は、周囲温度と *Pressure Sensor Configuration* (圧力センサ設定) の下で設定する圧力プロファイルとから算定されます。

Pressure Sensor Configuration (圧力センサ設定)
ここで、あらかじめ定めた圧力プロファイル (高、中、低) を選択します。圧力プロファイルは低圧チャンバ内の陰圧の大きさを決めます (28 ページを参照してください)。

► *Apply* をクリックすると、設定が有効になります。

5.5.5 接点 / スイッチ情報 - コンタクトスイッチの設定

Contact/Switch Configuration (接点 / スイッチ設定) ページでは、RMU のリアパネルの 6 ピン端子経由で来る GPIO 入力の監視を設定することができます (see 18 ページ)。

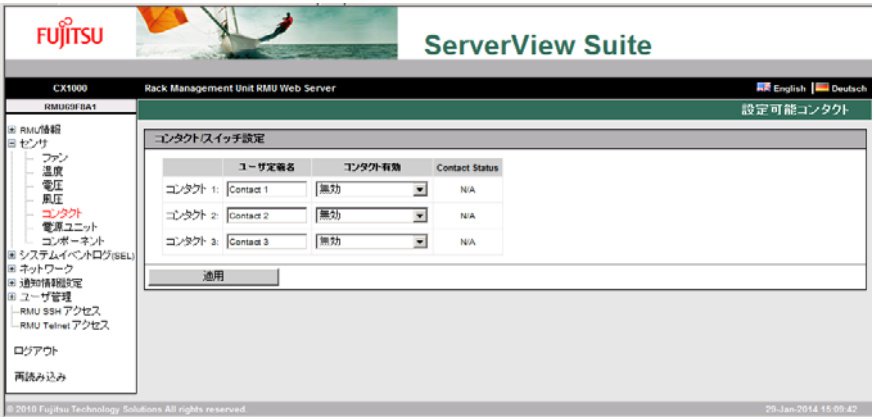


図 74: 接点 / スイッチ設定ページ

Contact 1 /contact 2 / Contact 3 (接点 1 / 接点 2 / 接点 3)
RMU のリアパネル上の汎用入力スイッチ、接点スイッチのユーザー定義名を指定します。

Contact active (コンタクトアクティブ)
対応するコンタクトスイッチが有効か無効かを指定します。

► *Apply* をクリックすると、設定が有効になります。

5.5.6 電源装置 - 電源装置のチェック

Power Supply (電源装置) ページは、電源装置から供給される電力に関する情報を提供します。

図 75: 電源装置ページ

5.5.7 コンポーネントの状態 - RMU コンポーネントの状態のチェック

Component Status (コンポーネントの状態) ページは、RMU コンポーネントの状態に関する情報を提供します。*CSS Component* (CSS コンポーネント) のコラムは、各々のコンポーネントについて、CSS (**C**ustomer **S**elf **S**ervice 顧客自己保守) 機能がサポートされるか否かを表示しています。

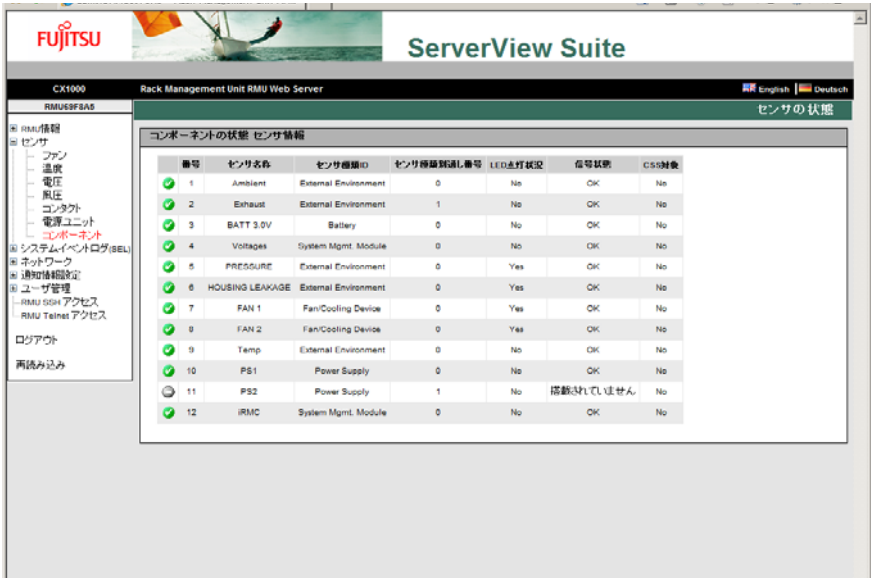


図 76: コンポーネントの状態ページ

5.6 システムイベントログ (SEL) - サーバのイベントログの表示および設定

System Event Log (システムイベントログ) エントリには、以下のリンクが載っています。これらは、サーバのイベントログ (システムイベントログ、SEL) の表示および設定に使用するページへのリンクです。

– 178 ページ の「システムイベントログ内容 - SEL および SEL エントリに関する情報の表示」.

– 181 ページ の「システムイベントログ設定 - SEL の設定」.

分かりやすくするため、イベント / エラーの各カテゴリに、カラーアイコンを割り当てています。

	致命的
	重大
	軽微
	情報
	顧客自己保守 (CSS) イベント

表 9: システムイベントログ - エラーカテゴリ

5.6.1 システムイベントログ内容 - SEL および SEL エントリに関する情報の表示

System Event Log Content (システムイベントログ内容) ページは SEL に関する情報を提供し、SEL エントリを表示します。*CSS Event* (CSS イベント) のコラムには、各々のイベントについて、そのイベントが CSS (**顧客自己保守**) コンポーネントによってトリガされたものか否かが表示されています。

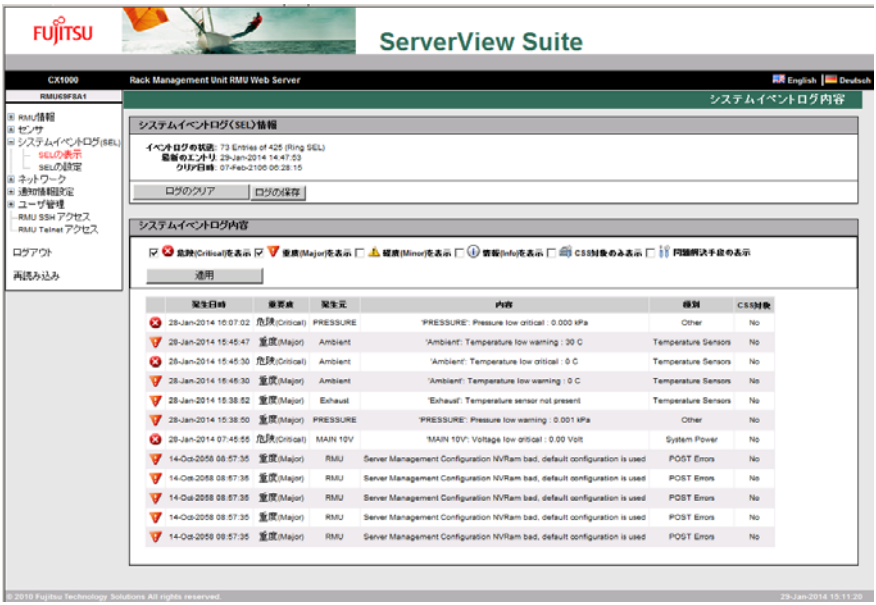


図 77: システムイベントログ内容ページ

システムイベントログ情報

System Event Log Information (システムイベントログ情報) グループは、SEL のエントリ数を報告します。最新のイベントがいつ追加または削除されたかも表示します。

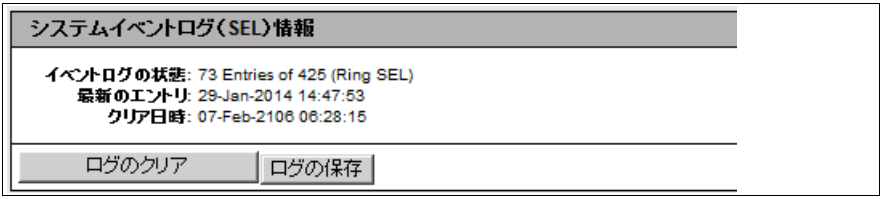


図 78: システムイベントログ内容ページ、システムイベントログ情報

Clear Event Log (イベントログを消去)

Clear Event Log ボタンをクリックすると、SEL のすべてのエントリが消去されます。

Save Event Log (イベントログを保存)

Save Event Log ボタンをクリックした後には、RMU から、SEL エントリを含むファイル *RMU_EventLog.sel* をダウンロードすることができます。

システムイベントログ内容

System Event Log Content (システムイベントログ内容) グループは、エラークラスでフィルタされた SEL エントリを表示します。

System Event Log Content グループで、現セッションが継続する間、フィルタ基準を変更することができます。ただし、ここで行う設定は次のログアウトまでしか有効でありません。その痕は、デフォルト設定がまた適用されます。

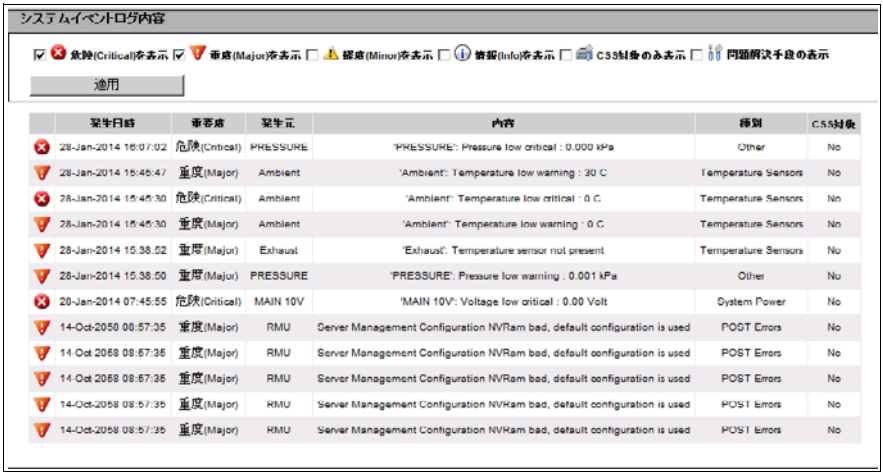


図 79: システムイベントログ内容ページ、システムイベントログ内容

Display Critical, *Display Major*, *Display Minor*, *Display Info*, *CSS only* *(致命的を表示、重大を表示、軽微を表示、情報を表示、CSS のみ表示)*
お望みなら、上記のデフォルト値以外の重大度レベルを選ぶこともできます。

Show Resolutions (解決法の提示)
このオプションを選ぶと、重大度レベルが致命的、重大、軽微の 各 SEL エントリについて、解決法の提案が示されます。

- *Apply* ボタンをクリックすると、上で行った設定が現セッションの間に限り有効化されます。

5.6.2 システムイベントログ設定 - SEL の設定

System Event Log Configuration (システムイベントログ設定) ページで、次の設定ができます。

– デフォルト時に *System Event Log Content* ページに表示される SEL エントリ (178 ページ を参照)。

– SEL をリングバッファにまとめるか、リニアバッファにまとめるか。

図 80: システムイベントログ設定ページ

Display Critical, *Display Major*, *Display Minor*, *Display Info*, *CSS only*
(致命的を表示、重大を表示、軽微を表示、情報を表示、CSS のみ表示)
ここで、デフォルト時にどの重大度レベルの SEL エントリが *System Event Log Content* ページに表示されるかを選択します。

Show Resolutions (解決法の提示)
このオプションを選ぶと、重大度レベルが致命的、重大、軽微の 各 SEL エントリについて、解決法の提案が示されます。

Ring SEL (リング SEL)
SEL はリングバッファにまとめられます。

IPMI SEL
SEL はリニアバッファにまとめられます。

リニア SEL が完全に満たされると、それ以上エントリを追加することはできません。

► *Apply* ボタンをクリックすると、設定が有効になります。

ヘルプデスク情報

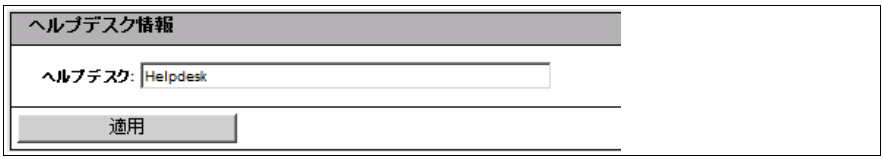


図 81: ヘルプデスク情報

Help desk (ヘルプデスク)
ヘルプデスクの表示に用いる文字列

► *Apply* ボタンをクリックすると、設定が有効になります。

5.7 ネットワーク設定 - LAN パラメータの設定

Network Settings (ネットワーク設定) エントリは、RMU の LAN パラメータを設定するときに使用するページへのリンクを一括しています。

– 184 ページ の「ネットワークインターフェース - RMU 上のイーサネット (Ethernet) 設定の 構成」.

– 187 ページ の「ポート番号とネットワークサービス設定 - ポート番号とネットワークサービス設定の設定」.

– 190 ページ の「DHCP 設定 -RMU のホスト名の設定」.

– 191 ページ の「DNS 設定 - RMU の DNS の有効化」.

5.7.1 ネットワークインターフェース - RMU 上のイーサネット (Ethernet) 設定の 構成

Network Interface (ネットワークインターフェース) ページでは、RMU のイーサネット設定の表示や変更を行うことができます。

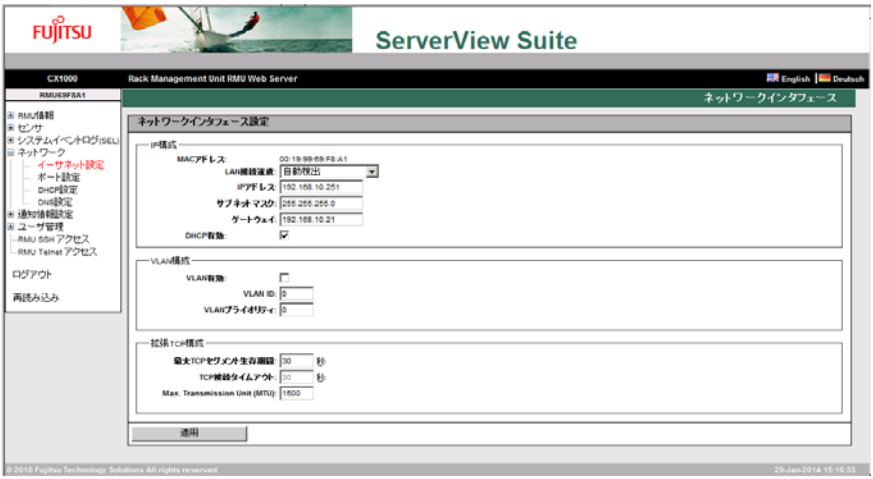


図 82: ネットワークインターフェースページ

注意！

イーサネット設定を変更するときは、事前にシステムに責任を持つネットワーク管理者に問い合わせてください。

RMU に不適切なイーサネット設定を行うと、専用の設定ソフトウェアを使うかまたはシリアルインターフェース経由でない限り RMU にアクセスできなくなります。

RMU 設定を行う *(Configure RMU Settings)* 許可を持つユーザーだけが、イーサネット設定を編集することを許されます (36 ページ の「ユーザー許可」の項 を参照してください)。

MAC Address (MAC アドレス)
RMU MAC アドレスがここに表示されます。

LAN Speed (LAN 速度)

LAN 速度。以下のオプションがあります。

- Auto Negotiation
- 100 MBit/s Full Duplex
- 100 MBit/s Half Duplex
- 10 MBit/s Full Duplex
- 10 MBit/s Half Duplex

Auto Negotiation (オートネゴシエーション) を選択すると、RMU に割り当てられたオンボード LAN コントローラが、接続されているネットワークポートに適正な転送速度と二重方式を自律的に決定します。

IP Address (IP アドレス)

LAN 内での RMU の IP アドレス。このアドレスは管理対象サーバの IP アドレスとは異なります。

静的アドレス (*DHCP enable* オプションが有効になっていない) で作業をする場合は、ここにアドレスを入力できます。そうでない (*DHCP enable* オプションが有効になっている) 場合は、RMU はこのフィールドをアドレスの表示にだけ使用します。

Subnet Mask (サブネットマスク)

LAN 内での RMU のサブネットマスク。

Gateway (ゲートウェイ)

LAN 内でのデフォルトゲートウェイの IP アドレス 。

DHCP Enabled (DHCP 有効)

このオプションを有効にすると、RMU はネットワーク上の DHCP サーバから LAN 設定を入手します。

ネットワーク上に 使える DHCP サーバがない場合は、DHCP オプションを有効にしないでください。
DHCP オプションを有効にしたのにネットワーク上に使える DHCP サーバがないと、RMU は探索ループに入ってしまいます (すなわち、DHCP サーバが見つかるまで探し続けることになります)。

(設定済みの RMU は、適切に設定された DHCP サーバにより DNS サーバに登録されることができます (sections 190 ページ の「DHCP 設定 -RMU のホスト名の設定」and 191 ページ の「DNS 設定 - RMU の DNS の有効化」を参照してください)。

VLAN Enabled (VLAN 有効)

このオプションを用いて、RMU に対する VLAN サポートを有効にすることができます。

VLAN Id

RMU が属するバーチャルネットワーク (VLAN) の VLAN ID 。許容値の範囲 : 1 ≤ *VLAN Id* ≤ 4094.

VLAN Priority (VLAN 優先度)

VLAN Id により指定された VLAN 内の RMU の VLAN 優先度 (ユーザー優先度)。
許容値の範囲 : 0 ≤ *VLAN Priority* ≤ 7 (デフォルト : 0).

► *Apply* ボタンをクリックすると、設定されたイーサネット設定が有効になります。

5.7.2 ポート番号とネットワークサービス設定 - ポート番号とネットワークサービス設定の設定

Ports and Network Services (ポート番号とネットワークサービス設定) ページでは、ポートとネットワークサービスの設定の表示や変更を行うことができます。

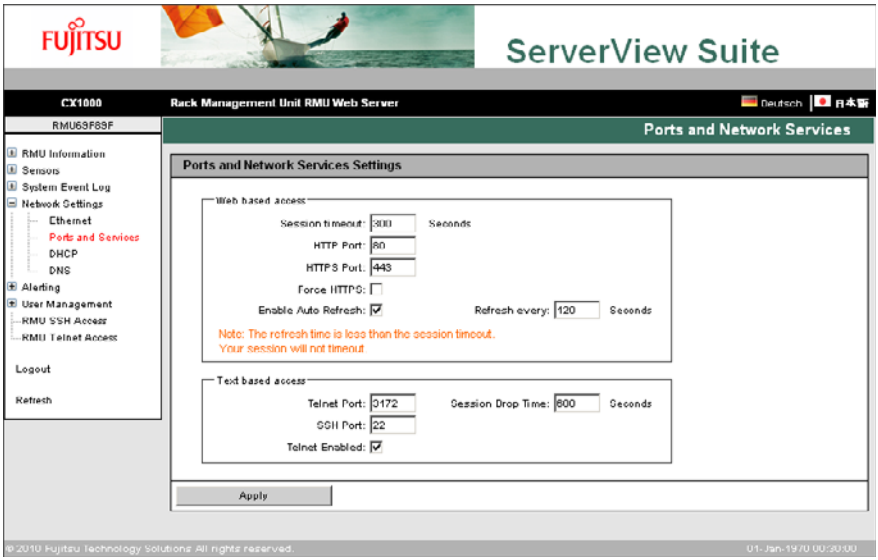


図 83: ポート番号とネットワークサービス設定ページ

RMU Web インターフェースでエントリフィールドが無効になっているポートについては、設定はサポートされません。

ウェブベースアクセス用ポート (Ports for web-based access)

Session Timeout (セッションタイムアウト)
通信がなされないときセッションが自動的に閉じるまでの時間 (秒数)。その後に RMU Web インターフェースのログインページが現われるので、必要に応じて再度ログインすることができます (138 ページ を参照してください)。

> *Refresh every ... seconds* (自動リフレッシュ間隔) フィールドに Session Timeout より短いリフレッシュ間隔の値を入力している場合は、通信がないまま Session Timeout で指定した時間が経過しても、セッションが自動的に閉じることはありません (189 ページ を参照)。

ネットワーク設定 - ポート番号とネットワークサービス設定

HTTP Port (HTTP ポート)
RMU の HTTP ポート
デフォルトポート番号 : 80
設定可能性 : はいデフォルト時に有効化
: はい通信方向
: 受信・送信

HTTPS Port (HTTPS ポート)
RMU の HTTPS (HTTP セキュア) ポート
デフォルトポート番号 : 443
設定可能性 : はい
デフォルト時に有効化 : はい
通信方向 : 受信・送信

Force HTTPS (強制 HTTPS)
Force HTTPS オプションを有効にすると、ユーザーはエントリフィールドで指定した HTTPS ポートで、RMU へのセキュリティ保護付きの接続のみを確立することができます。

Force HTTPS オプションを無効にすると、ユーザーはエントリフィールドで指定した HTTP ポートで、RMU へのセキュリティ保護のない接続を確立することができます。

> SSL 証明書の期限が切れていると、その旨のメッセージがブラウザに出されます。

Enable Auto Refresh (自動リフレッシュを有効化)
このオプションを有効にすると、RMU Web インターフェースの内容が自動的に定期的にリフレッシュ (再読み込み) されます。 *リフレッシュの間隔は Refresh every ... seconds* フィールドで指定してください。

Refresh every ... seconds (自動リフレッシュ間隔)
RMU Web インターフェースの内容を自動的にリフレッシュする間隔 (秒数) 。

リフレッシュ間隔として Session Timeout (188 ページ を参照) より短い値を入力している場合は、通信がないまま Session Timeout で指定した時間が経過してもセッションが自動的に閉じることはありません。

テキストベースアクセス用ポート (Ports for text-based access)

Telnet Port (Telnet ポート)
RUM の Telnet ポート
デフォルトポート番号 : 3172 設定可能性 : はい
デフォルト時に有効化 : いいえ
通信方向 受信・送信

Session Drop Time(セッションドロップ時間)
通信がなされないとき Telnt 接続が自動的に遮断されるまでの時間 (秒数)。

SSH Port (SSH ポート)
RMU の SSH (Secure Shell) ポート デフォルトポート番号 : 22 設定可能性 : はい
デフォルト時に有効化 t: はい
通信方向 : 受信・送信

Telnet enabled (Telnet 有効)
Telnet Enabled オプションを有効にしていると、エントリフィールドで指定した Telnet ポートで RUM への接続を確立することができます。

► *Apply* ボタンをクリックすると、上で行った設定が保存されます。

5.7.3 DHCP 設定 -RMU のホスト名の設定

DHCP Configuration (DHCP 設定) ページでは、RMU のホスト名を設定し、それにより “ダイナミック DNS” が使用できるようにします。ダイナミック DNS を使うと、DHCP サーバが自律的にネットワークコンポーネントの IP アドレスとシステム名を DNS サーバに渡しますので、識別が容易になります。

図 84: DHCP 設定ページ

Register DHCP Address in DNS (DHCP アドレスを DNS 登録)
RMU の DHCP サーバへの DHCP 名の転送を有効 / 無効にします。

Add Serial Number (シリアル番号を付加する)
RMU の MAC アドレスの最後の 3 バイトが RMU の DHCP 名に付加されます。

Add Extension (拡張を追加)
Extension 入力フィールドで指定された拡張が、RMU の DHCP 名に付加されます。

Extension (拡張)
RMU 名の拡張を入力します。

RMU Name (RMU 名)
RMU の DHCP にサーバ名の代わりに渡される RMU 名。

DNS Name (DNS 名)
RMU の設定済み DNS 名を示します。

- *Apply* ボタンをクリックすると、上で行った設定が保存されます。

5.7.4 DNS 設定 - RMU の DNS の有効化

DNS Settings (DNS 設定) ページでは、RMU のドメイン名サービス (DNS) を有効にすることができます。これにより、IP アドレスの代わりにシンボリック DNS 名を RMU の設定に使用できるようになります。

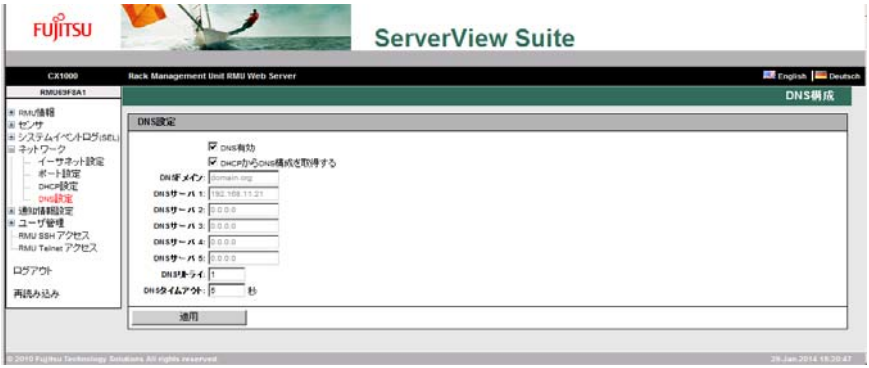


図 85: DNS 設定ページ

DNS enabled (DNS 有効)
RMU の DNS を有効 / 無効にします。

Obtain DNS configuration from DHCP (DHCP から DNS 設定を取得)
このオプションを有効にすると、DNS サーバの IP アドレスが自動的に DHCP サーバから取得されます。
この場合、5 台の DNS サーバがサポートされます。

この設定を有効にしない場合は、*DNS サーバのアドレスを DNS-Server 1 - DNS-Server 5* の 欄に最大 5 つまで入力することができます。

DNS Domain (DNS ドメイン)
オプション *Obtain DNS configuration from DHCP* が無効になっている場合、DNS サーバへの要求に用いるデフォルトのドメイン名を指定します。

DNS Server 1 .. 5

Obtain DNS configuration from DHCP のオプションが無効になっている場合は、ここに DNS サーバの名前を 5 つまで入力することができます。

► *Apply* ボタンをクリックすると、上で行った設定が保存されます。

5.8 警告 - 警告の設定

Alerting (警告) エントリは、RMU のための警告を設定するのに使用するページへのリンクを含みます。

– 194 ページ の「SNMP トラップ警告 - SNMP トラップ警告の設定」.

– 195 ページ の「Email 警告 - email 警告の設定」.

5.8.1 SNMP トラップ警告 - SNMP トラップ警告の設定

SNMP Trap Alerting (SNMP トラップ警告) ページでは、SNMP トラップ警告の設定を表示し、構成することができます。

SNMP トラップの最大 7 台の SNMP サーバへの転送がサポートされます。

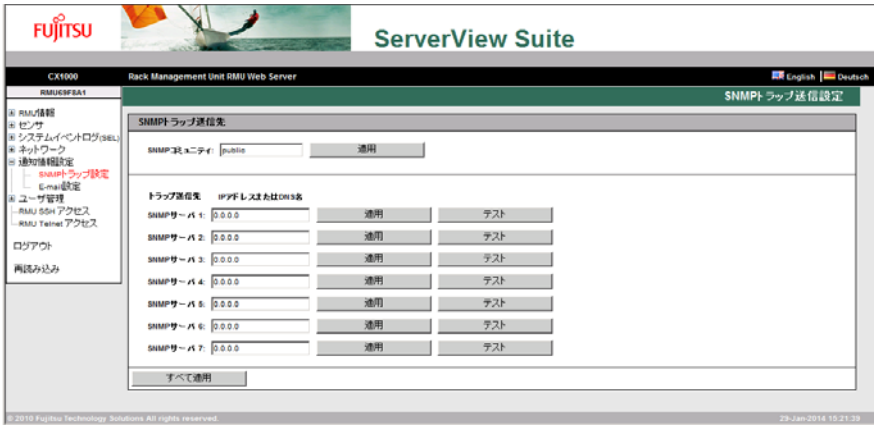


図 86: SNMP トラップページ

SNMP Community (SNMP コミュニティ)
SNMP コミュニティ名

- *Apply* ボタンをクリックすると、そのコミュニティ名が承認されます。

SNMP Server1 .. SNMP Server7 (トラップ宛先)
そのコミュニティに所属し、トラップ宛先として設定したいサーバの DNS 名または IP アドレス。

- *Apply* ボタンをクリックすると、その SNMP サーバがトラップ宛先として有効になります。
- *Test* ボタンをクリックすると、SNMP サーバへの接続がテストされます。

- *Apply All* をクリックすると、適切な場合、すべての設定が有効になります。

5.8.2 Email 警告 - email 警告の設定

Email Alerting (Email 警告) ページでは、
email 警告の設定を行うことができます。

2 台のメールサーバの設定がサポートされます。

Email 警告は各ユーザーに個別に指定することができます (204 ページ の「RMU ユーザー - RMU 上のローカルユーザー管理」の項 を参照してください)。

グローバル RMU ユーザー ID については Email 警告は現在サポートされません (201 ページ の「ユーザー管理 - ユーザーの管理」の項 を参照してください)。

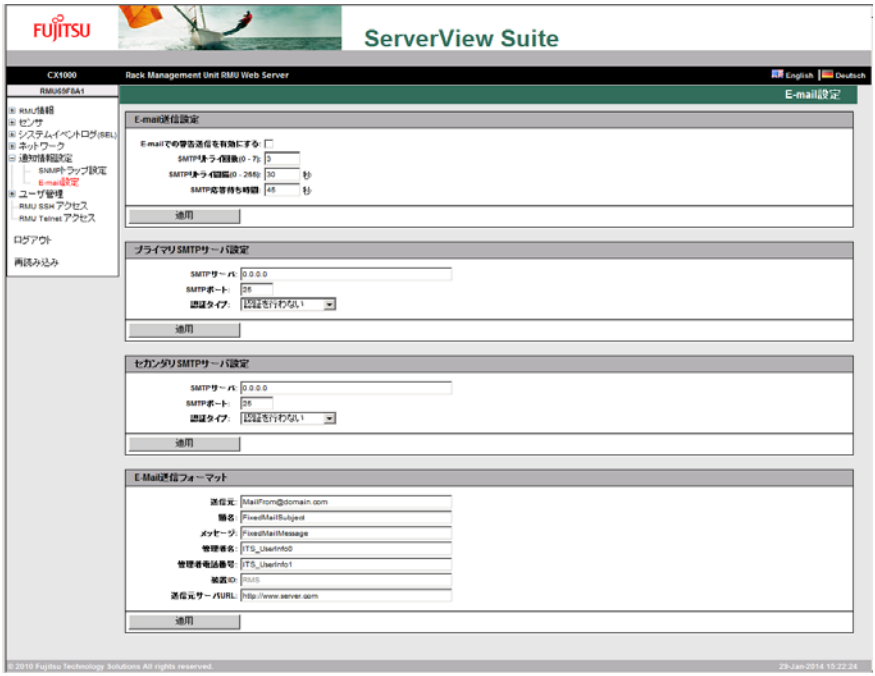


図 87: Email 警告ページ

グローバル Email ページング設定 - グローバル email 設定の 構成

Global Email Paging Configuration (グローバル Email ページング設定) グループでは、グローバル email 設定を構成することができます。

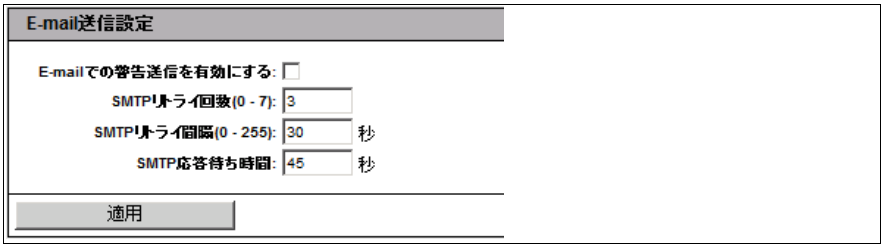


図 88: Email 警告ページ、グローバル Email 設定

Email Alerting Enabled (Email 警告有効)
このオプションを有効にします。

SMTP Retries (SMTP 再試行) (0 - 7)
SMTP 再試行の回数

SMTP Retry Delay (SMTP 再試行遅延時間) (0 - 255)
SMTP 再試行の間隔 (秒数) 。

SMTP Response Timeout (SMTP 応答タイムアウト)
SMTP 応答がタイムアウトとなる時間 (秒数) 。

- *Apply* ボタンをクリックすると、行った設定が有効になります。

プライマリ SMTP サーバ設定 - プライマリメールサーバの設定

Primary SMTP Server Configuration (プライマリ SMTP サーバ設定) グループでは、プライマリサーバ (SMTP サーバ) の設定を行うことができます。

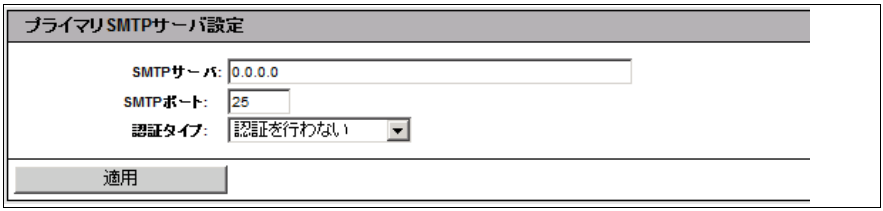


図 89: Email 警告ページ警告ページ、プライマリ SMTP サーバ設定

SMTP Server (SMTP サーバ)
プライマリメールサーバの IP アドレス

RMU のドメイン名サービス (DNS) を有効にすることができます (191 ページ の「DNS 設定 - RMU の DNS の有効化」を参照)。そうすれば、IP アドレスの代わりにシンボリック名を使用することができます。

SMTP Port (SMTP ポート)
メールサーバの SMTP ポート

Auth Type (認証タイプ)
RMU をメールサーバに接続するための認証タイプ。

– *None* (なし)
接続の認証なし。

– *SMTP AUTH (RFC 2554)* RFC 2554: 認証のための SMTP サービス拡張による認証。

この場合は、以下の情報が必要です。

Auth User Name (認証ユーザー名)
メールサーバの認証を求めるユーザー名

Auth Password (認証パスワード)
メールサーバの認証のためのパスワード

Confirm Password (パスワード確認)
入力したパスワードを確定します。

► *Apply* ボタンをクリックすると、行った設定が有効になります。

セカンダリ SMTP サーバ設定 - セカンダリメールサーバの設定

Secondary SMTP Server Configuration (セカンダリ SMTP サーバ設定) グループでは、セカンダリサーバ (SMTP サーバ) の設定を行うことができます。

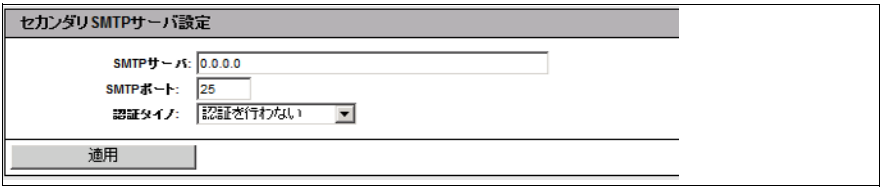


図 90: Email 警告ページ - セカンダリ SMTP サーバ設定

SMTP Server (SMTP サーバ)
セカンダリメールサーバの IP アドレス

RMU のドメイン名サービス (DNS) を有効にすることができます (191 ページ の「DNS 設定 - RMU の DNS の有効化」を参照)。そうすれば、IP アドレスの代わりにシンボリック名を使用することができます。

SMTP Port (SMTP ポート)
メールサーバの SMTP ポート

Auth Type (認証タイプ)
RMU をメールサーバに接続するための認証タイプ。

– *None* (なし)
接続の認証なし。

– *SMTP AUTH (RFC 2554)*
RFC 2554 : 認証のための SMTP サービス拡張 による認証。

この場合は、以下の情報が必要です。

Auth User Name (認証ユーザー名)
メールサーバの認証を求めるユーザー名

Auth Password (認証パスワード)
メールサーバの認証のためのパスワード

Confirm Password(パスワードの確認)
入力したパスワードを確定します。

► *Apply* ボタンをクリックすると、行った設定が有効になります。

メールフォーマット依存設定 - メールフォーマット依存設定の 構成

Mail Format dependent Configuration (メールフォーマット依存設定) グループでは、メールフォーマット依存設定を構成することができます。各ユーザーのメールフォーマットは、*New User Configuration - User <Name> Configuration - Email Format Configuration* (新規ユーザー設定 - ユーザー名設定 - Email フォーマット設定) ページ (204 ページ を参照) を用いて指定することができます。

以下の email フォーマットがサポートされます。

- 標準
- Fixed Subject
- ITS- フォーマット
- 富士通 REMCS フォーマット

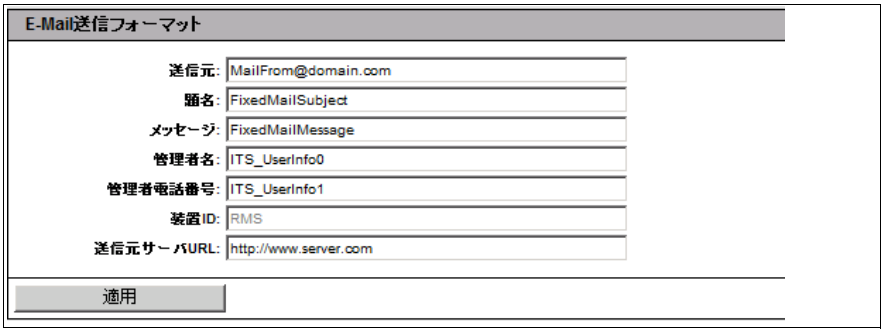


図 91: Email 警告ページ、メールフォーマット依存設定

メールフォーマットによっては、いくつかのエントリが無効となります。

From (送信元)
送信者の ID RMU>>。
すべてのメールフォーマットで有効。

> ここに入力された文字列が """@" を含んでいると、その文字列は有効な email アドレスと解釈されます。ここで指定しなくても、“admin@<ip-address>” は有効な email アドレスとして使用されます。

Subject (主題)
警告メールの決まった主題。
Fixed Subject メールフォーマットにのみ有効 (208 ページ を参照)。

Message (メッセージ)
メッセージ (email) のタイプ。
Fixed Subject メールフォーマットにのみ有効 (208 ページを参照)。

Admin Name (管理者名)
管理責任者の名前 (オプション)。
ITS メールフォーマットにのみ有効 (208 ページ を参照)。

Admin Phone (管理者電話)
管理責任者の電話番号 (オプション)。
ITS メールフォーマットにのみ有効 (208 ページ を参照)。

REMCS Id
この ID はシリアルナンバーに類似した追加サーバ ID です。
富士通 REMCS-Format にのみ有効です。

Server URL (サーバ URL)
ラックシステムの追加 URL (オプション)。この URL はマニュアルで入力しなければなりません。
標準メールフォーマットにのみ有効です。

► *Apply* ボタンをクリックすると、設定が保存されます。

5.9 ユーザー管理 - ユーザーの管理

User Management (ユーザー管理) エントリは、ローカルユーザー管理のページだけでなく、グローバルユーザー管理のためのディレクトリサービスの設定 (LDAP 設定) のページへのリンクも含みます。

– 202 ページ の「RMU ユーザー - RMU 上のローカルユーザー管理」.

– 213 ページ の「ディレクトリサービス設定 (LDAP) - RMU」.

5.9.1 RMU ユーザー - RMU 上のローカルユーザー管理

RMU User (RMU ユーザー) ページには、すべての設定済みユーザーを載せた表があります。各行にひとりの設定済みユーザーのデータが記載されています。ユーザー名はリンクの形式で実装されます。ユーザー名をクリックすると、*User “<name>” Configuration* (ユーザー “< 名 >” 設定) ウィンドウ (204 ページ) が開きます。このウィンドウで、そのユーザーの設定の表示や変更を行うことができます。

ユーザー ID 1 (“ヌルユーザー”) は IPMI 規格用に予約されているため、RMU 上でのユーザー管理には使用できません。

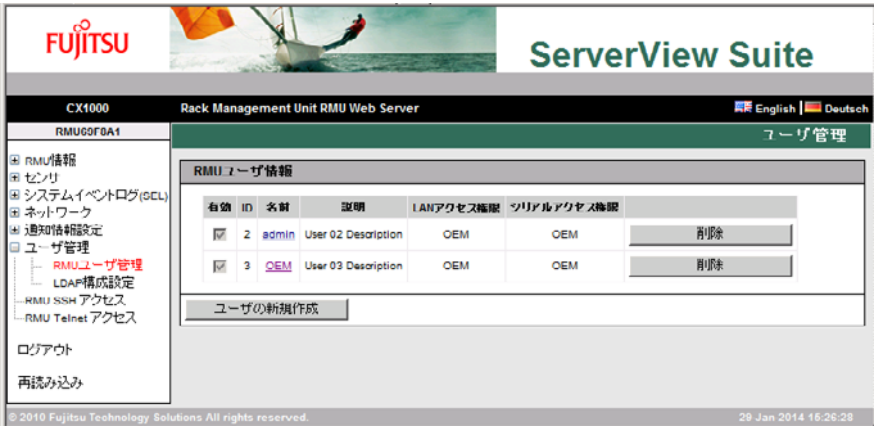


図 92: ユーザー管理ページ

Delete (削除)
: 設定済みユーザーの表には、各ユーザーエントリの後に *Delete* (削除) ボタンがあります。このボタンをクリックし、その選択を確定すると、対応するユーザーが削除されます。

New User (新規ユーザー)
: このボタンをクリックすると、*New User Configuration* (ユーザの新規作成) ページが開きます (203 ページ を参照)。ここで新規ユーザーの設定ができます。

新規ユーザー設定 - 新規ユーザーの設定

New User Configuration (ユーザの新規作成) ページでは、新規ユーザーの基本的設定を構成することができます。

各フィールドと選択リストの説明は、203 ページ 以下の ユーザの新規作成 - *ユーザー名の 設定ページにあります。*

l 図 93 で、ユーザー名 “User04” のユーザーの設定例を見ることができます。

図 93: ユーザー管理 - ユーザの新規作成ページ

User Information (ユーザー情報) グループで、ユーザーのアクセスデータを設定することができます。

ユーザー名の設定 - ユーザー設定 (詳細)

User "<name>" Configuration (ユーザー名の設定) ページでは、ユーザーの設定内容の表示、変更、拡張を行うことができます。

I 図 94 では、図 93 で作成したユーザーの設定を見ることができます。.

ユーザー ID はユーザー名の後に角括弧に入れて表示されます。

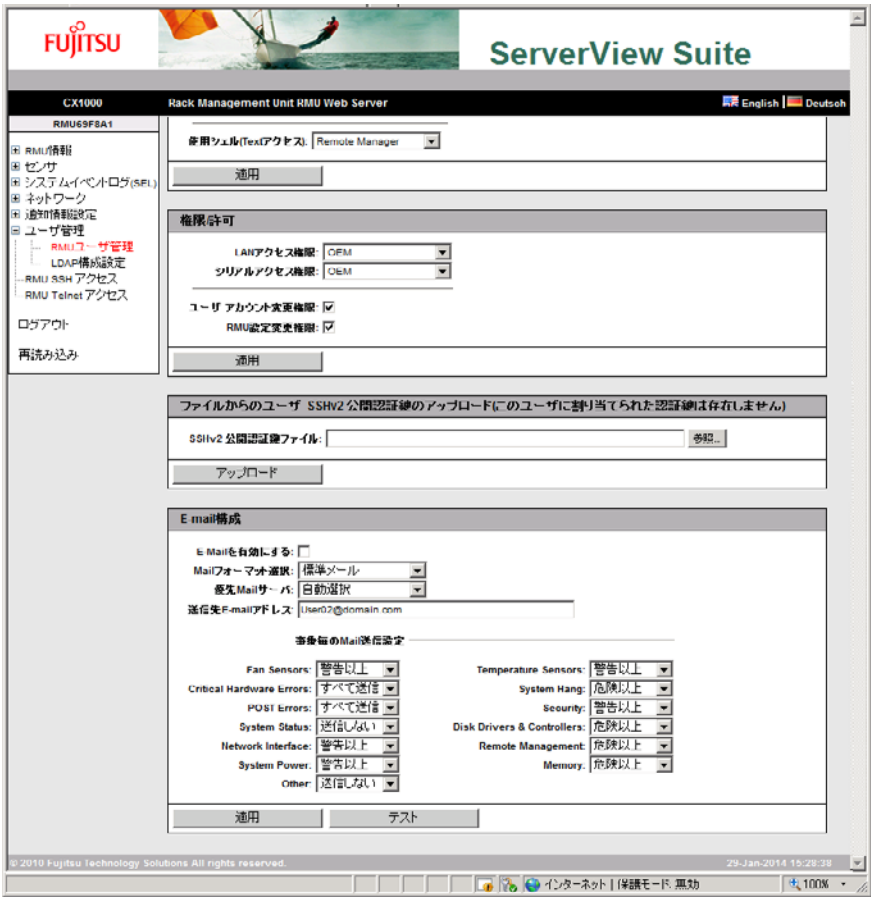


図 94: ユーザー管理 - ユーザー名の 設定ページ

RMU User Information (RMU ユーザー情報) グループでは、ユーザーのアクセスデータを設定することができます。

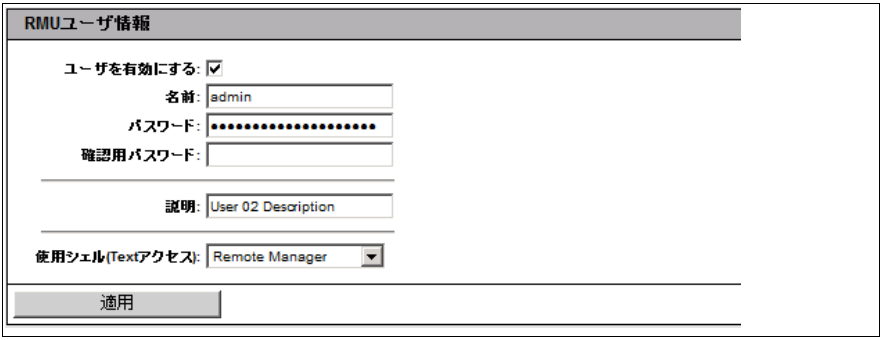


図 95: ユーザー管理 - ユーザー名の 設定ページ、ユーザー情報

User Enabled (ユーザー有効)
ユーザーをロックするときは、このオプションを無効にします。

Name (名前)
ユーザー名を入力します。

Password (パスワード)
ユーザーのパスワードを入力します。

Confirm Password (パスワードの確認)
ここにパスワードを再入力して確定します。

User Description (ユーザーの説明)
ここに設定済みユーザーの概説を入力します。

User Shell (ユーザーシェル)
ここで望むユーザーシェルを選択します。
以下のオプションがあります。

- *SMASH CLP*
  246 ページ の「コマンドラインシェル ... の起動 - SMASH シェルの起動」の項 を参照してください。
- *Remote Manager* (リモートマネージャ)
  231 ページ の「RMU シリアルポートインターフェース (リモートマネージャ)」の章 を参照してください。.
- *IPMI Terminal Mode* (IPMI ターミナルモード)
- *None* (なし)

► *Apply* ボタンをクリックすると、設定が有効になります。

Privileges / Permissions (特権 / 許可) グループでは、チャネル別ユーザー特権を設定することができます。

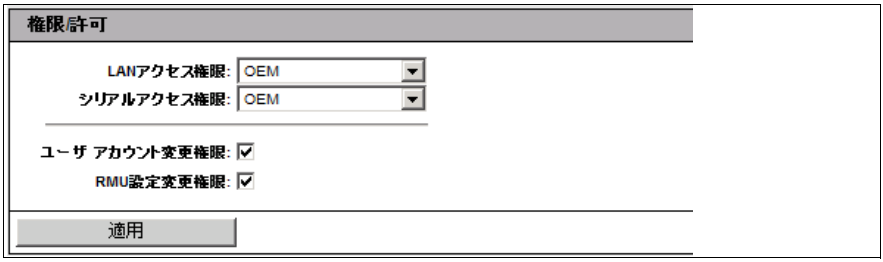


図 96: ユーザー管理 - ユーザー名の 設定ページ、特権 / 許可

LAN Channel Privilege (LAN チャネル特権)
ここで LAN チャネルの特権グループをユーザーに割り当てます。

- *User* (ユーザー)
- *Operator* (オペレータ)
- *Administrator* (管理者)
- *OEM*

特権グループに関連する許可に関する情報は 33 ページ の「RMU のユーザー管理」の章 を参照してください。

Serial Channel Privilege (シリアルチャネル特権)
ここでシリアルチャネルの特権グループをユーザーに割り当てます。
LAN Channel 特権と同じ特権グループが利用できます。

チャネル別許可に加えて、次のチャネル非依存許可を個別にユーザーに割り当てることもできます。

Configure User Accounts (ユーザーアカウントの設定)
ローカルユーザーアクセスデータを設定する許可。

Configure RMU Settings (RMU 設定の構成)
RMU 設定を構成する許可

► *Apply* ボタンをクリックすると、行った設定が有効になります。

User SSHv2 public Key uploag from file (ファイルからユーザー SSHv2 公開鍵のアップロード) グループでは、ローカルファイルからユーザー SSHv2 公開鍵を登録することができます。

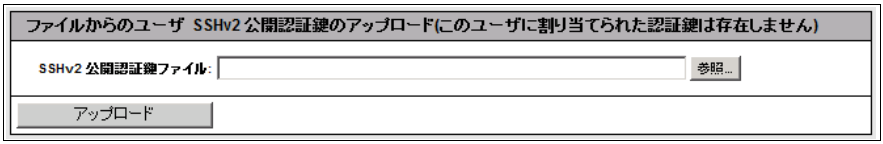


図 97: ユーザー管理 - ユーザー管理名の設定ページ、ファイルからユーザー SSHv2 公開鍵のアップロード

RMU ユーザーへの SSHv2 公開鍵認証について詳しくは、40 ページ の「ローカル RMU ユーザーの SSHv2 公開鍵認証」の項 を参照してください。

Email Configuration (Email 設定) グループでは、email フォーマットに関するユーザー別設定を構成することができます。

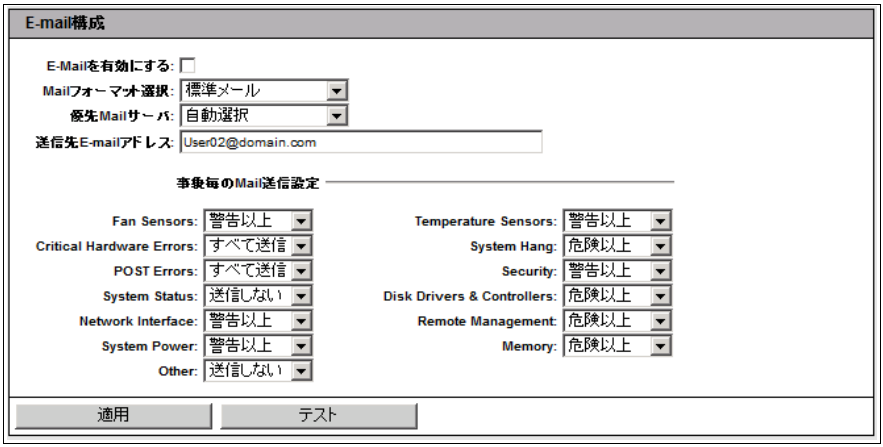


図 98: ユーザー管理 - ユーザー名の設定ページ、Email 設定

Email Enabled (Email 有効)

ユーザーにシステム状態について email で知らせるかどうかを指定します。

Mail Format (メールフォーマット)

選択した email フォーマットによりますが、*Email Alerting - Mail Format dependent Configuration (Emai 警告 - メールフォーマット依存設定) グループでいくつかの設定をすることができます* (199 ページ を参照)。

以下の email フォーマットが使用可能です。

- 標準
- *Fixed Subject*
- *ITS- フォーマット*
- *富士通 REMCS フォーマット*

Preferred Mail Server (優先メールサーバ)

優先メールサーバを選択します。
以下のオプションからひとつを選ぶことができます。

- *Automatic* (自動的)

  優先メールサーバが使えないなどの理由で、email をただちに首尾よく送信することができない場合は、その email は第 2 のメールサーバに送られます。

- *Primary* (プライマリ)

  プライマリ SMTP サーバとして設定されたメールサーバ (197 ページ を参照) だけが、優先メールサーバとして使用されます。

- *Secondary* (セカンダリ

  セカンダリ SMTP サーバとして設定されたメールサーバ (198 ページ を参照) だけが、優先メールサーバとして使用されます。

  emaill 送信のエラーはイベントログに記録されます。

Email Address (Email アドレス)

受取人の Email アドレス

Paging Severity Configuration (ページング重大度設定)
ここでは、RMU ユーザーに email で知らせるべきシステムイベントを設定することができます。

RMU のイベントログへのエントリはすべて、どれかのページンググループに割り当てられます。

以下の設定が各イベントグループに使用できます。

None (なし)
このページンググループには通知機能は無効にされます。

Critical (致命的)
システムイベントログへのエントリが CRITICAL と報告されると、RMU は email でユーザーに通知します。

Warning (警告)
システムイベントログへのエントリが Minor、Major または Critical と報告されると、RMU は email でユーザーに通知します。

All (すべて)
このグループでは、RMU はシステムイベントログに記載された一切のイベントをユーザーに通知します。

- *Test* ボタンをクリックすると、設定のテストが行われます。
- *Apply* ボタンをクリックすると、設定が有効になります。

Email Configuration (Email 設定) グループでは、email フォーマットに関するユーザー別設定を構成することができます。

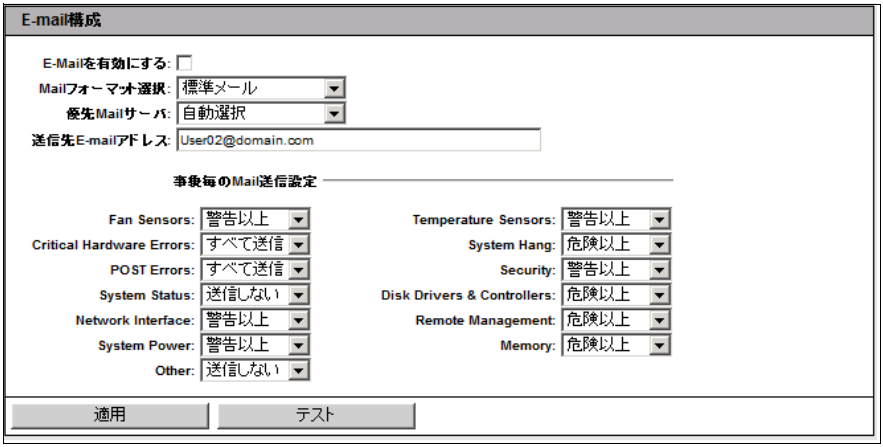


図 99: ユーザー管理 - ユーザー名の設定ページ、Email 設定

Email Enabled (Email 有効)

ユーザーにシステム状態について email で知らせるかどうかを指定します

Mail Format (メールフォーマット)

選択した email フォーマットによりますが、*Email Alerting - Mail Format dependent Configuration* (Emai 警告 - メールフォーマット依存設定) グループでいくつかの設定をすることができます (199 ページ を設定)。

以下の email フォーマットが使用可能です。

- *Standard* (標準)
- *Fixed Subject*
- *ITS-Format* (ITS- フォーマット)
- *Fujitsu REMCS Format* (富士通 REMCS フォーマット

Preferred Mail Server (優先メールサーバ)
優先メールサーバを選択します。
以下のオプションからひとつを選ぶことができます。

– *Automatic* (自動的)

  優先メールサーバが使えないなどの理由で、email をただちに首尾よく送信することができない場合は、その email は第 2 のメールサーバに送られます。

– *Primary* (プライマリ)

  プライマリ SMTP サーバとして設定されたメールサーバ (197 ページ を参照) だけが優先メールサーバとして使用されます。

– *Secondary* (セカンダリ)

  セカンダリ SMTP サーバとして設定されたメールサーバ (198 ページ を参照) だけが優先メールサーバとして使用されます。

email 送信エラーはイベントログに記録されます。

Email Address (Email アドレス)
受取人の Email アドレス。

Paging Severity Configuration (ページング重大度設定)

ここでは、RMU ユーザーに email で知らせるべきシステムイベントを設定することができます。

RMU のイベントログへのエントリはすべて、どれかのページンググループに割り当てられます。

以下の設定が各イベントグループに使用できます。

None (なし)

このページンググループでは通知機能は無効になっています。

Critical (致命的)

システムイベントログへのエントリが CRITICAL と報告されると、RMU は email でユーザーに通知します。

Warning (警告)

システムイベントログへのエントリが Minor、Major または Critical と報告されると、RMU は email でユーザーに通知します。

All (すべて)

このグループでは、RMU はシステムイベントログに記載された一切のイベントをユーザーに通知します。

► *Apply* ボタンをクリックすると、設定が有効になります。

5.9.2 ディレクトリサービス設定 (LDAP) - RMU

のディレクトリサービスの設定

ディレクトリサービス経由でグローバルユーザー管理を行うためには、*Directory Service Configuration* (ディレクトリサービス設定) ページで RMU を適切に設定する必要があります。

現在のところ、RMU LDAP アクセスへのポートがあるのは次のディレクトリサービスです。Microsoft Active Directory、Novell eDirectory、および Open LDAP。

次の文字は、LDAP で文字列を検索するためのメタキャラクタとして指定されています。*, \ , &, |, !, =, <, >, ~, :

したがって、ユーザーはこれらの文字を相対識別名（RDN）の要素として使用することはできません。

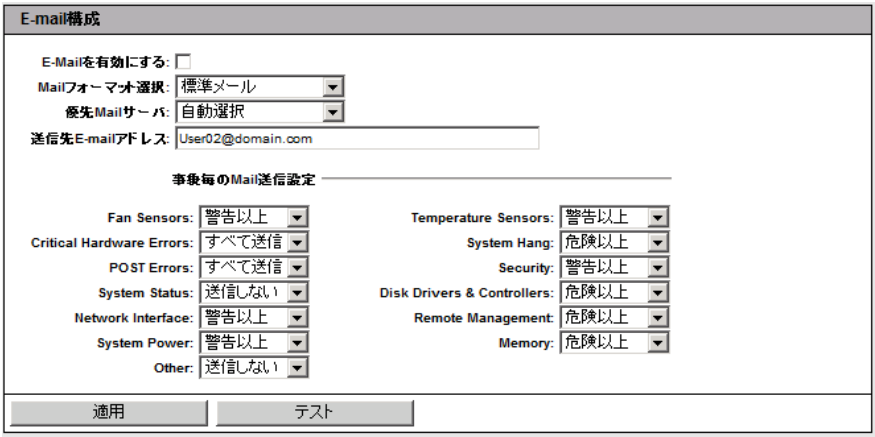


図 100: ディレクトリサービス設定ページ (LDAP 設定)

LDAP Enable (LDAP 有効)

このオプションは、RMU が LDAP 経由でディレクトリサービスにアクセスできるかできないかを指定します。LDAP 経由のディレクトリサービスが可能なのは、*LDAP Enable* が有効になっている場合だけです 。

LDAP Enable にチェックを入れると、かならずログイン情報 (214 ページ を参照) が SSL 暗号とともに、ウェブブラウザと RMU の間で転送されます。

LDAP SSL Enable (LDAP SSL 有効)

このオプションにチェックを入れると、RMU とディレクトリサーバの間のデータ転送が SSL 暗号化されます。

LDAP SSL Enable は、RMU Web インターフェースのページがオープン時に SSL で保護されるか保護されないかに影響を与えません。

LDAP SSL Enable を有効化するのは、ドメインコントローラ証明書がインストールされている場合に 限るべきです。

Disable Local Login (ローカルログインを無効化)

このオプションを有効にすると、すべてのローカル RMU ユーザー ID がロックされ、ディレクトリサービスが管理するユーザー ID だけが有効となります。

注意！

オプション *Disable Local Login* を有効にしながら、ディレクトリサービスへの接続が失敗すると、RMU へのログインは不可能となります。

Always use SSL Login (つねに SSL ログインを使用)

このオプションは LDAP を無効にした場合にのみ意味があります。

このオプションを有効にすると、LDAP が無効にされていても、つねに HTTP SSL セキュリティ保護されたログインページが使用されます。*Always use SSL Login* を有効にせず、しかも LDAP が無効にされている場合に限り、Digest Authentication Login (ダイジェスト認証ログイン) によりセキュリティ保護されたマスクが用いられます。

Directory Server Type (ディレクトリサービスのタイプ)
使用するディレクトリサーバのタイプ

以下のディレクトリサービスがサポートされます。

- *Active Directory*: Microsoft Active Directory
- *Novell*: Novell eDirectory
- *OpenLDAP*: OpenLDAP

► *Apply* ボタンをクリックすると、行った設定が有効になります。

選択するディレクトリサービスによって、表示される入力フィールドが異なります。

- *Active Directory* の場合は、216 ページ の「RMU を Microsoft Active Directory 用に設定」を参照してください。
- *eDirectory* and *Open LDAP* の場合は、220 ページ の「RMU を Novell eDirectory / OpenLDAP 用に設定」を参照してください。

5.9.2.1 RMU を Microsoft Active Directory 用に設定

Active Directory を選んだ後に *Apply* をクリックして選択を確定すると、*Directory Service Configuration* ページの次のような変異形が示されます。

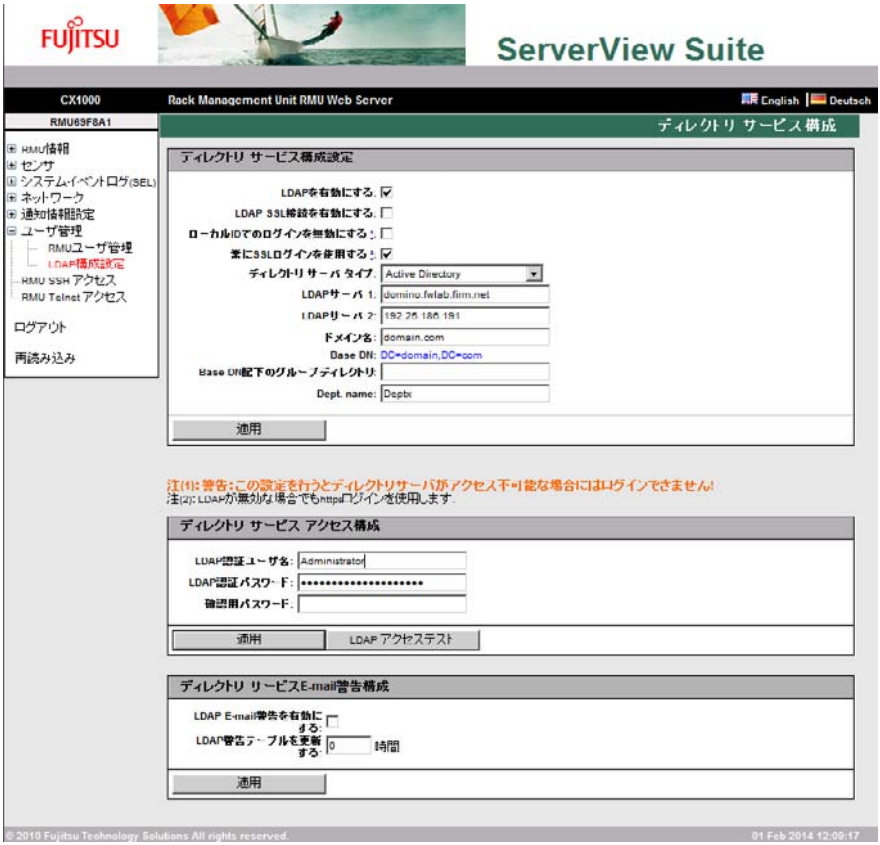


図 101: ディレクトリサービス設定 : Microsoft Active Directory の詳細項目

例として図 101 に示したエントリ内容は、78 ページ の「Microsoft Active Directory による RMU ユーザー管理」の項 に示した例および図を参照しています。

次の手順で行ってください。

- *Global Directory Service Configuration*
  (グローバルディレクトリサービス設定) グループ の詳細項目を記入します。

図 102: グローバルディレクトリサービス設定 : Microsoft Active Directory の詳細項目

LDAP Server 1 (LDAP サーバ 1)
使用する LDAP ディレクトリサーバの IP アドレスまたは DNS 名。

LDAP Server 2 (LDAP サーバ 2)
バックアップサーバとして保守され、LDAP Server 1 が不調の場合にディレクトリサーバとして使用される LDAP サーバの IP アドレスまたは DNS 名。

Domain Name (ドメイン名)
ディレクトリサーバの完全な DNS パス名。

Base DN (ベース DN)
Base DN は Domain Name から自動的に導き出されます。

Department Name (部署名)
部署名は、ディレクトリサービスではユーザー許可と警告ロールを確認するために使用されます、部署 X のサーバと部署 Y のサーバでは、ユーザーに認められた許可が異なることがあります。

- *Apply* をクリックすると、設定が有効になります。

- *Directory Service Access Configuration* (ディレクトリサービスアクセス設定) グループで LDAP アクセスデータを設定します。

ここで行う設定は、グローバルユーザー ID に関連する警告のために必要なものです。警告が有効になっていない場合は、*この Directory Service Access Configuration* グループでの設定は無意味です。

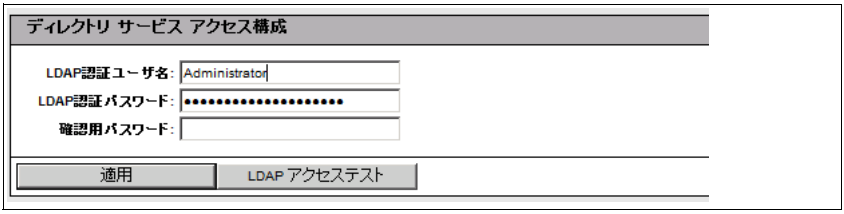


図 103: Microsoft Active Directory: ディレクトリサービスアクセス設定

LDAP Auth User Name (LDAP 認証ユーザー名)
RMU が LDAP サーバにログオンするときに使用するユーザー名。

LDAP Auth Password (LDAP 認証パスワード)
User Name の項で指定されたユーザーが、LDAP サーバ上での自分自身の認証のために指定するパスワード。

Confirm Password (パスワードを確定)
LDAP Auth Password の項で入力したパスワードを再度入力してください。

Test LDAP Access (LDAP アクセスをテスト)
LDAP ディレクトリサーバへのアクセスデータをチェックし、LDAP の状態をその結果として示します (図 104 を参照)。

このテストは基本的なアクセスデータ (“Is the LDAP server present? LDAP サーバは存在しますか ?”, “Is the user configured? ユーザーは設定されていまか ?”) をチェックするだけで、ユーザーを完全に認証するものではありません。

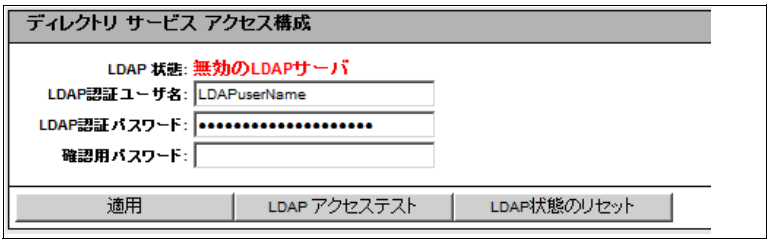


図 104: Microsoft Active Directory: LDAP サーバへの接続状態

- *Reset LDAP Status* をクリックすると、状態表示がリセットされます。

- *Apply* をクリックすると、行った設定が有効になります。

- *Directory Service Email Alert Configuration* (ディレクトリサービス Email 警告設定) グループで、グローバル email 警告の設定を行います。

図 105: ディレクトリサービス Email 警告設定

LDAP Email Alert Enable (LDAP Email 警告有効)
グローバル email 警告を有効 にします。

LDAP Alert Table Refresh [Hours] (警告テーブル更新 [時間数])
email テーブルが規則的に更新される間隔を指定します。値 “0” は、テーブルを規則的に更新しないという意味です。

- *Apply* をクリックすると、設定が有効になります。

5.9.2.2 RMU を Novell eDirectory / OpenLDAP 用に設定

Novell または *OpenLDAP* を選んだ後に *Apply* をクリックしてその選択を確定すると、*Directory Service Configuration* (ディレクトリサービス設定) ページの次のような変異形が表示されます。

Novell eDirectory と OpenLDAP では、*Directory Service Configuration* (ディレクトリサービス設定) ページの構成が同じです。

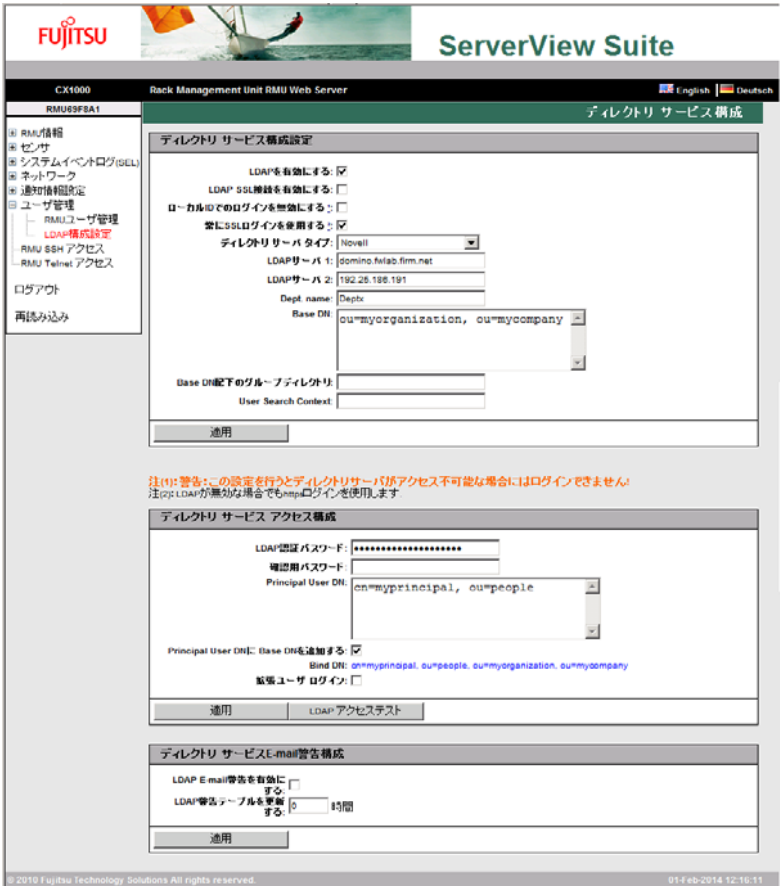


図 106: グローバルディレクトリサービス設定 .: Novell eDirectory / Open LDAP の詳細項目

例として図 106 に示した入力内容は、91 ページ の「Novell eDirectory による RMU ユーザー管理」の項 で示した例および図を参照しています。

次の手順で行ってください。

- *Global Directory Service Configuration* group (グローバルディレクトリサービス設定) グループ の詳細項目を記入します。

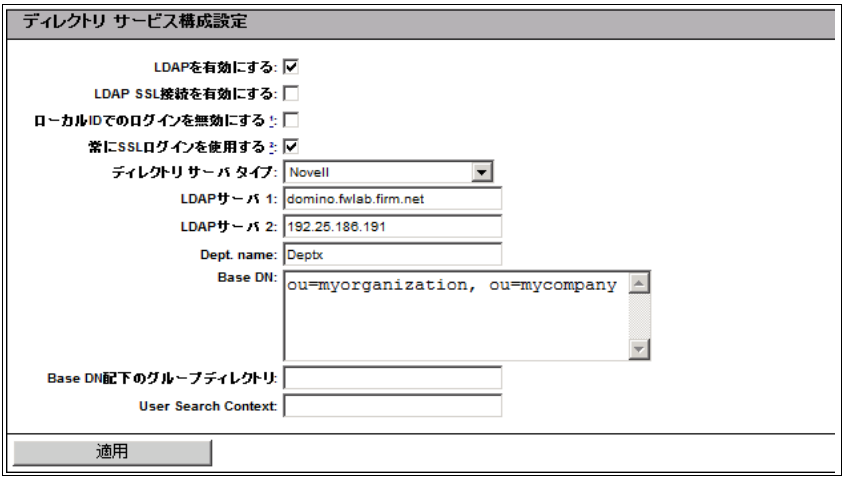


図 107: グローバルディレクトリサービス設定： Microsoft Active Directory の詳細項目

LDAP Server 1 (LDAP サーバ 1)
使用する LDAP ディレクトリサーバの IP アドレスまたは DNS 名。

LDAP Server 2 (LDAP サーバ 2)
バックアップサーバとして保守され、LDAP Server 1 が不調の場合にディレクトリサーバとして使用される LDAP サーバの IP アドレスまたは DNS 名。

Department Name (部署名)
部署名。ディレクトリサービスはユーザー許可を確認するときに部署名を必要とします。部署 X のサーバと部署 Y のサーバでは、ユーザーに認められた許可が異なることがあります。

Base DN (ベース DN)
Base DN は eDirectory または Open LDAP サーバの完全識別名で、OU (組織単位) *iRMCgroups* を含むツリーまたはサブツリーで表現されます。

Groups directory as sub-tree from base DN
(ディレクトリをベース DN からのサブツリーとしてグループ化)
組織単位 *iRMCgroups* の、Base DN のサブツリーとしてのパス名 (グループ DN コンテキスト)。

User Search Context (ユーザー検索コンテキスト)
組織単位 Users の、Base DN のサブツリーとしてのパス名 (ユーザー検索コンテキスト)。

► *Apply* をクリックすると、行った設定が有効になります。

► *Directory Service Access Configuration* (ディレクトリサービスアクセス設定) グループで LDAP アクセスデータを設定します。

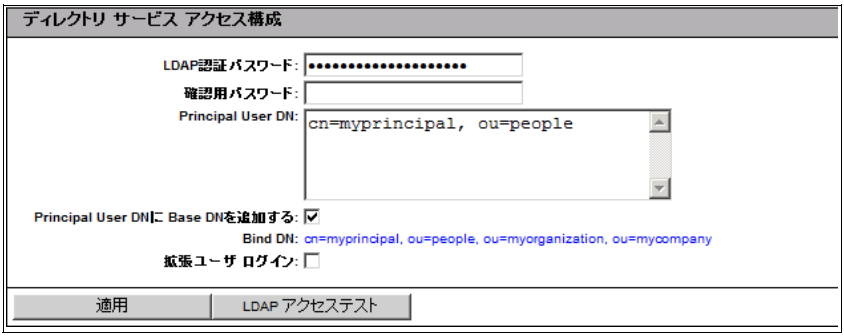


図 108: Microsoft Active Directory: ディレクトリサービスアクセス設定

LDAP Auth Password (LDAP 認証パスワード)
プリンシパルユーザーが LDAP サーバ上での自分自身の認証のために使用するパスワード 。

Confirm Password (パスワードを確定)
LDAP Auth Password の項で入力したパスワードを再度入力してください。

Principal User DN (プリンシパルユーザー ID)
汎用 RMU ユーザー ID (プリンシパルユーザー) の完全識別名、すなわち、オブジェクトパスと属性の詳細な記述。RMU は、この DN で、RMU ユーザーの権限を LDAP サーバにクエリします。

Append Base DN to Principal User DN (プリンシパルユーザー ID にベース ID を付加)
このオプションを有効にすると、Principal User DN の項で Base DN を指定する必要がありません。この場合には、*Base DN* の項で指定したベース DN が、*Global Directory Service Configuration* グループで使用されます。

Bind DN (バインド DN)

Bind DN には、LDAP 認証に用いられるプリンシパルユーザー DN が示されます。

Enhanced User Login (拡張ユーザーログイン)

ユーザーがログインする際の柔軟性を拡張します。

Enhanced User Login を選択し、Apply ボタンで有効にすると、User Login Search Filter (ユーザーログイン検索フィルタ) という、標準ログイン検索フィルタを含む追加フィールドが現われます。

注意！

LDAP 構文に精通している方でない限り、このオプションを有効にしないこと。うっかり違法な検索フィルタを指定したり有効化したりすると、User Login Search Filter オプションを無効にした後、グローバルログインでしか RMU にログインできなくなります。

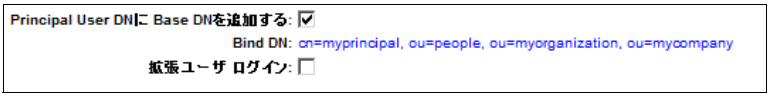


図 109: “Enhanced User Login”の LDAP 検索フィルタ

ログイン時、プレースホルダ “%s” は対応するグローバルログインに置き換えられます。“cn=” の代わりに別の属性を指定することで、標準フィルタを修正することができます。これで、この検索フィルタの基準を満たすグローバルログインはすべて、RMU にログインすることを許されます。

注意！

LDAP 構文に精通している方でない限り、このオプションを有効にしないこと。うっかり違法な検索フィルタを指定したり有効化したりすると、User Login Search Filter オプションを無効にした後、グローバルログインでしか RMU にログインできなくなります。

Test LDAP Access (LDAP アクセスをテスト)

LDAP ディレクトリサーバへのアクセスデータをチェックし、LDAP の状態をその結果として示します (図 104 を参照)。

このテストは基本的なアクセスデータ (“Is the LDAP server present? LDAP サーバは存在しますか ?”, “Is the user configured? ユーザーは設定されていまか ?”) をチェックするだけで、ユーザーを完全に認証するものではありません。

図 110: eDirectory / OpenLDAP: LDAP サーバへの接続の状態

- ► *Reset LDAP Status* をクリックすると、状態表示がリセットされます。

► *Apply* をクリックすると、行った設定が有効になります。

► *Directory Service Email Alert Configuration* (ディレクトリサービス Email 警告設定) グループで、グローバル email 警告の設定を行います。

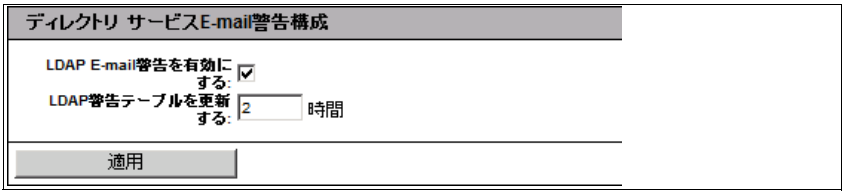


図 111: ディレクトリサービス Email 警告設定

LDAP Email Alert Enable (グローバル Email 警告有効)
グローバル Email 警告を有効にします。

LDAP Alert Table Refresh [Hours] (LDAP 警告テーブル更新 [時間数])
email テーブルが規則的に更新される間隔を指定します。値 “0” はテーブルを規則的に更新しないという意味です。

► *Apply* をクリックすると、行った設定が有効になります。

5.10 Telnet/SSH (リモートマネージャ) 経由の RMU 操作

RMU には Telnet/SSH ベースのインターフェースが使用できます。このインターフェースはリモートマネージャと呼ばれています。リモートマネージャの英数字ユーザーインターフェースからは、システムおよびセンサ情報、電源管理機能、エラーイベントログにアクセスすることができます。SMASH CLP シェルを起動させることもできます。

リモートマネージャは、RMU Web インターフェースから次のようにして呼び出すことができます。

– *RMU SSH Access* リンクを用いて、SSH (**S**ecure **Sh**ell) で暗号化した Telnet の RMU への接続を開始させます。

– RMU Telnet Access リンクを用いて、暗号化しない Telnet の RMU への接続を開始します。

RMU Web インターフェースからリモートマネージャを呼び出すと、自動的に Java Applet が起動し、Telnet/SSH クライアントを実装します。Java Applet を用いた Telnet/SSH の Remote Manager へのアクセスは便利のために提供するものです (たとえば、SSH クライアントは Windows オペレーティングシステムと一緒に提供されません)。しかし、リモートマネージャへのアクセスには、任意の Telnet または SSH クライアントを使用することができます。

Java Applet を使用して SSH 接続を確立した場合は、公開鍵認証はサポートされません。

リモートマネージャを用いた RMU の操作は 232 ページ の「リモートマネージャの操作」の項 に説明があります。

最大パラレルセッション数

– Telnet: 4 まで
– SSH: 4 まで
– Telnet と SSH を合わせて : 4 まで

管理対象サーバに関する要求 条件

Telnet 経由のアクセスが RMU に対して有効になっていなければなりません (section 187 ページ の「ポート番号とネットワークサービス設定 - ポート番号とネットワークサービス設定の設定」を参照してください)。

デフォルト時には Telnet プロトコルによるアクセスはセキュリティ上の理由により無効になっています。パスワードが平文で送信されるからです。

SSH/Telnet 接続の確立とリモートマネージャへのログイン

SSH および Telnet 接続のスクリーンディスプレイは、接続固有情報の表示が違っているだけですが、SSH 接続のディスプレイを下に示します。

- ナビゲーションバーで、リンク *RMU SSH Access* (SSH) または *RMU Telnet Access* (Telnet) をクリックします。

  SSH または Telnet 接続用の Java Applet が起動し、次のウィンドウが表示されます (この場合は SSH 接続の例を使用)。

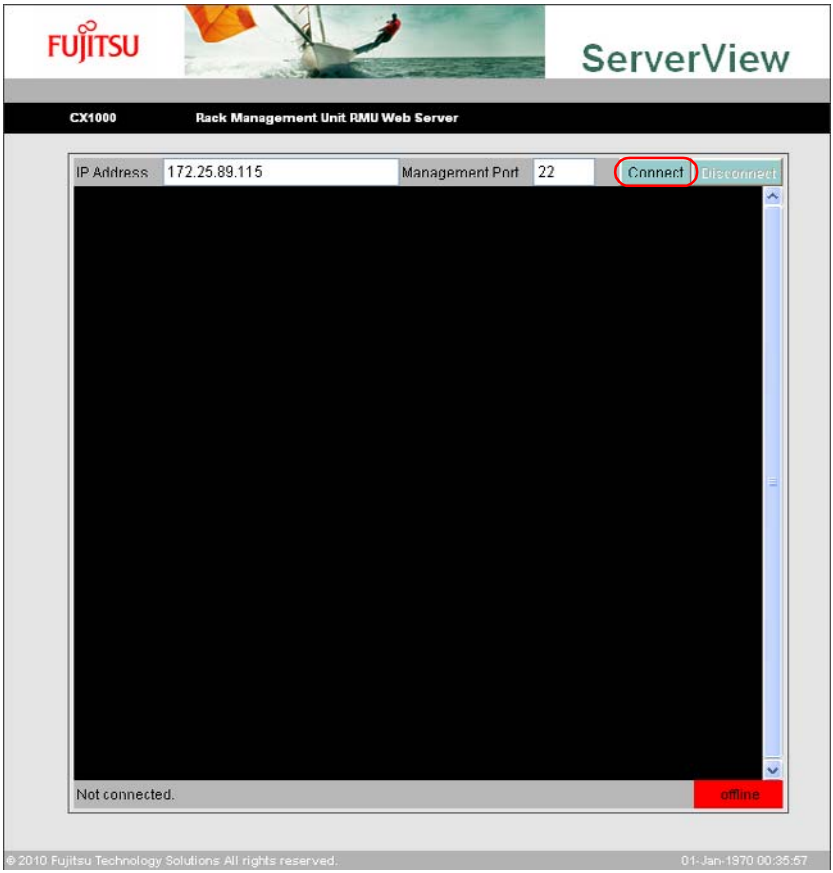


図 112: SSH の RMU への接続の確立

► 接続バーで、*Connect* (接続) をクリックします。

RMU への接続が確立されるとすぐ、ユーザー名とパスワードを入力するように求められます。

– *SSH 接続からのリモートマネージャへのログインログイン*

管理対象サーバのホストキーがまだリモート管理端末に登録されていない場合は、SSH クライアントはセキュリティ警告を発するとともに、手順の進め方についてサジェスチョンを示します。

次のようなログインウィンドウが表示されます。

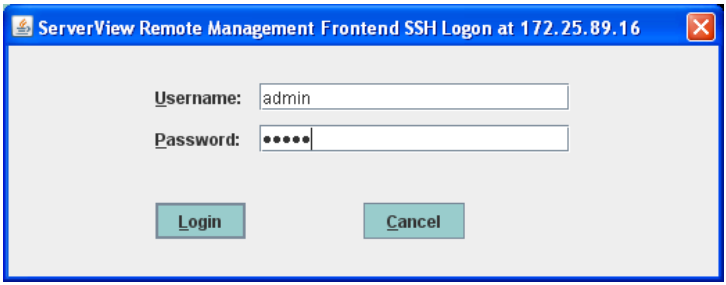


図 113: SSH 接続 : リモートマネージャへのログイン

► ユーザー名とパスワードを入力し、*Login* をクリックして入力を確定してください。.

そうすると、リモートマネージャのメインメニューが表示されます (229 ページ の図 115 を参照)。

– *Telnet 接続からのリモートマネージャへのログイン*

リモートマネージャへのログインウィンドウが表示されます。

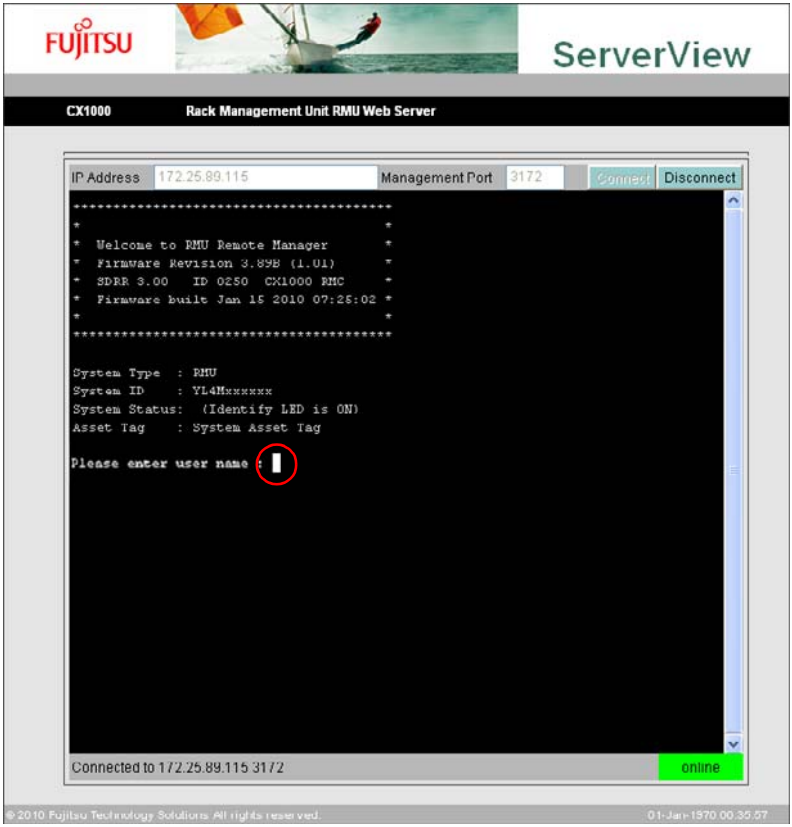


図 114: Telnet 接続 : リモートマネージャへのログイン

ServerView エージェントがある時点ですでにシステム上で起動しているかいないかで、ログインウィンドウの表示は、システム情報付きとシステム情報なしになります (235 ページ を参照)。

► ユーザー名とパスワードを入力し、Enter を押して入力を確定してください。

すると、リモートマネージャのメインメニューが表示されます (229 ページ の図 115 を参照)。

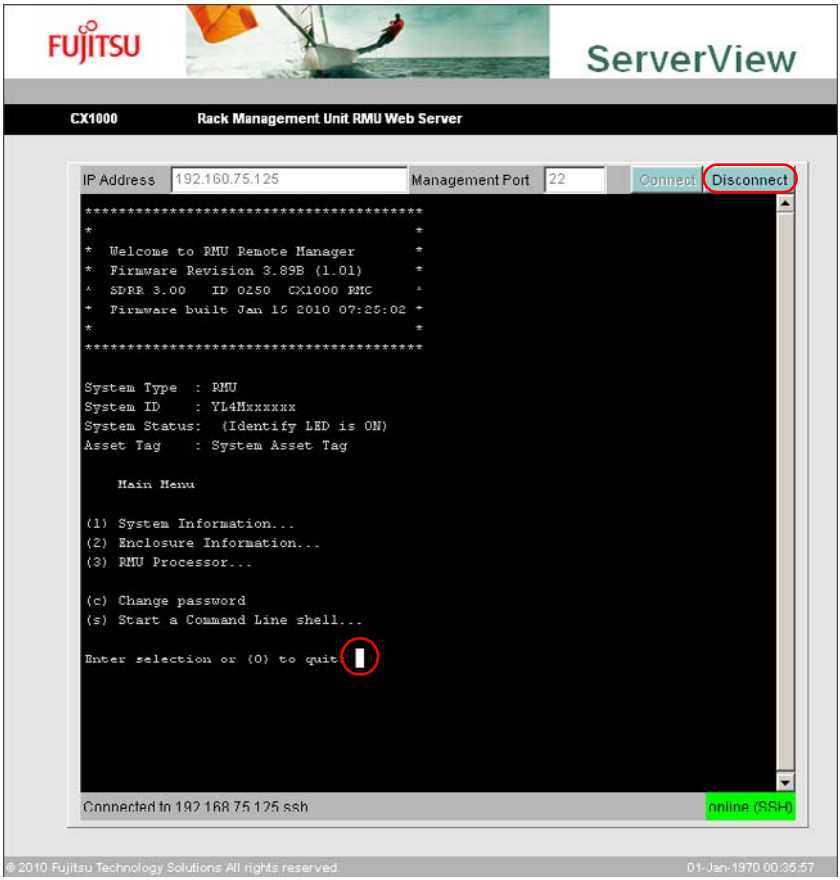


図 115: リモートマネージャのメインメニュー

Telnet/SSH 接続の終了

- リモートマネージャへの接続を閉じるときは、リモートマネージャウィンドウの接続バー内の *Disconnect* ボタンをクリックするか、またはリモートマネージャのメインメニューの 0 キーを押すかします (図 115 を参照)。

6 RMU シリアルポートインターフェース (リモートマネージャ)

RMU には Telnet ベースのインターフェースが使用可能です。このインターフェースはリモートマネージャと呼ばれています。次のインターフェーでリモートマネージャを呼び出すことができます。

– RMU Web インターフェース (137 ページ を参照してください)。
– 任意の Telnet/SSH クライアント

RMU は SSH (**S**ecure **Sh**ell) 経由のセキュリティが確保された接続をサポートします。リモートマネージャインターフェースは Telnet 接続と SSH 接続で同じです。VT100 シーケンスが解釈できる Telnet/SSH client であればどれでも、RMU へのアクセスに使用できます。とはいっても、RMU Web インターフェースを使用することを推奨します。

最大パラレルセッション数

– Telnet: 4 まで
– SSH: 4 まで
– Telnet と SSH を合わせて : 4 まで

管理対象サーバに関する要求条件

Telnet 経由のアクセスが RMU に対して有効になっていなければなりません (187 ページ の「ポート番号とネットワークサービス設定 - ポート番号とネットワークサービス設定の設定」の項 を参照してください)。

デフォルト時には Telnet プロトコルによるアクセスはセキュリティ上の理由により無効になっています。パスワードが平文で送信されるからです。

6.1 リモートマネージャの操作

リモートマネージャの操作を図 116 の例に基づいて説明します。この図の示すのは、リモートマネージャのメインメニューからの抜粋です。

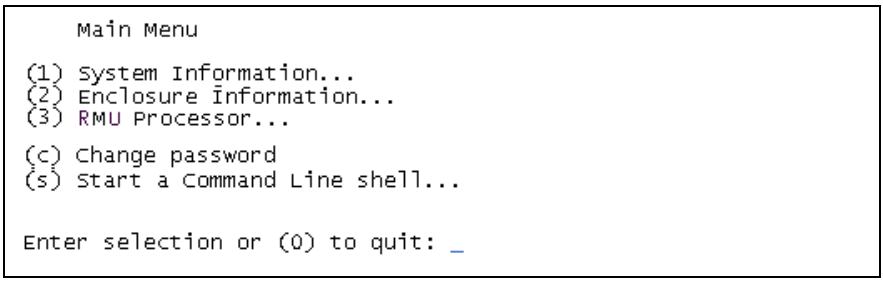


図 116: リモートマネージャの操作

- 必要なメニュー項目を、その項目の前にある数字または文字を入力して選択します。たとえば、“Change password”なら “c” を入力します。

  ユーザーが使用を許されていないファンクションはダッシュ (-) で、また提供されていないファンクションはアステリスク (*) で指示してあります。

- リモートマネージャを閉じるときは、0 または連結キー Ctrl D を押します。該当するイベントはイベントログに書き込まれます。

6.2 メニューの概要

RMU のリモートマネージャメニューは、以下の構造になっています。

- **システム情報**
  - シャシ情報
  - メインボード情報
- **外装情報**
  - システムイベントログ
    - システムイベントログの表示 (テキスト、新しいものから)
    - システムイベントログの表示 (テキスト、古いものから)
    - システムイベントログのダンプ （raw データ、新しいものから）
    - システムイベントログのダンプ （raw データ、古いものから）
    - システムイベントログ情報の表示
    - システムイベントログの消去
  - 温度
  - 電圧
  - ファン
  - 圧力
  - 接点 / スイッチ
  - コンポーネントの状態
  - すべてのセンサのリスト

- **RMU プロセッサ**
  - IP パラメータの設定
  - IP パラメータのリスト
  - 識別灯のトグル
  - RMU のリセット (ウォームリセット)
  - RMU のリセット (コールドリセット)
- **パスワードの変更**
- **コマンドラインシェルの起動**

6.3 ログイン

RMU への接続が確立されるとすぐに、リモートマネージャのログインウィンドウ (Telnet/SSH ウィンドウ) がリモート管理端末のターミナルクライアントに表示されます。

SSH 接続でログインするとき : 管理対象サーバのホストキーがまだリモート管理端末に登録されていない場合は、SSH クライアントはセキュリティ警告を発するとともに、手順の進め方についてサジェスチョンを示します。

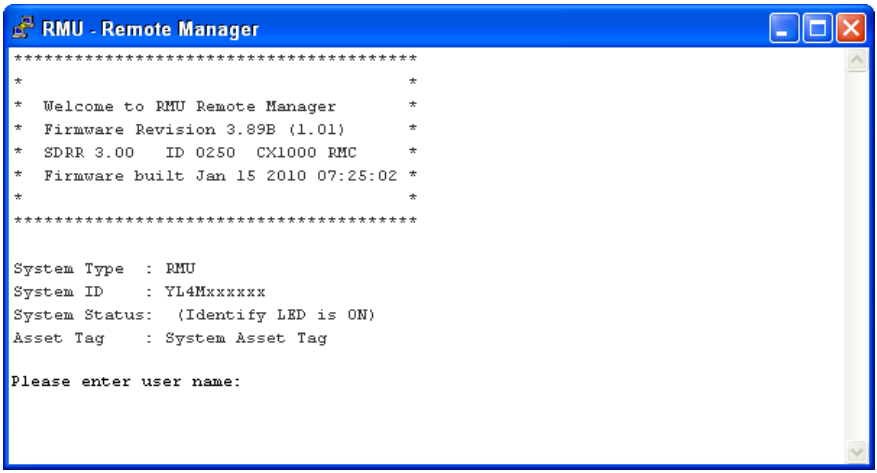


図 117: リモートマネージャ : ログインウィンドウ (システム情報付き)

リモートマネージャウィンドウには、影響を受ける RMU に関する情報が載っています。その情報はサーバを識別し、その稼動状態 (電源状態) を表示します。サーバについてはいくつかの詳細情報 (システム名など) だけが、しかもそのサーバが適切に設定されている場合に限り示されます。

- リモートマネージャが使用できるためには、ユーザー名とパスワードでログインしなければなりません。

  次に、該当するイベントがイベントログに書き込まれ、リモートマネージャの関連のあるメインメニューが表示されます (236 ページ の「リモートマネージャのメインメニュー」の項 を参照してください)。

  ログインプロセスは Ctrl D を使っていつでも終了できます。

6.4 リモートマネージャのメインメニュー

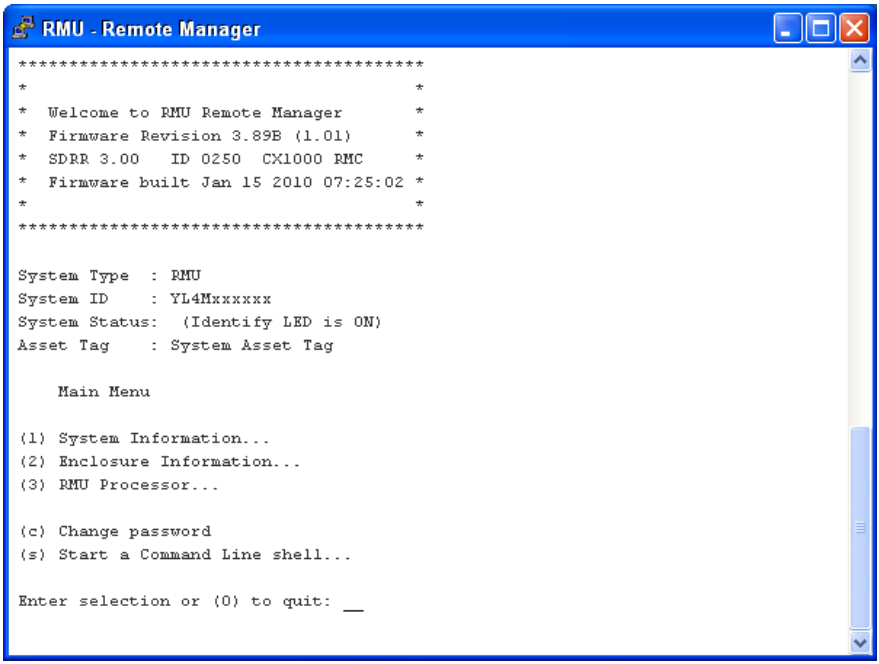


図 118: リモートマネージャ : メインメニューウィンドウ

リモートマネージャのメインメニューには、次のファンクションが載っています。

System Information... (システム情報)	RMU に関する情報を表示します (239 ページ の「システム情報 - RMU に関する情報」の項 を参照)。
Enclosure Information... (外装情報)	現在のシステム状態に関する情報を要求。たとえば、エラーログとイベントログからのエラーやイベントのメッセージ (温度、ファンなど) をチェックします。 (240 ページ の「外装情報 - システムイベントログとセンサ状態」の項 を参照)。
RMU Processor... (RMU プロセッサ)	RMU を設定します (たとえば、ファームウェアの更新や IP アドレスの変更など) (244 ページ の「RMU プロセッサ - IP パラメータ、識別灯 および RMU リセット」の項 を参照)。
Change password (パスワードの変更)	パスワードを変更します (239 ページ の「パスワードの変更」の項 を参照)。
Start a Command Line shell... (コマンドラインシェルの起動)	コマンドラインシェルを起動します (246 ページ の「コマンドラインシェル ... の起動 - SMASH シェルの起動」の項 を参照)。

表 10: リモートマネージャのメインメニュー

6.5 必要なユーザー許可

次表に、リモートマネージャの個別のファンクションを使用するために要求されるユーザー許可の概要を示します。

リモートマネージャのメニュー項目	IPMI 特権レベルで許可				必要な許可	
	OEM	管理者	オペレータ	ユーザー	ユーザーアカウントの設定	RMU 設定の構成
System Information... (システム情報)	X	X	X	X		
Enclosure Information (外装情報)	X	X	X	X		
System Eventlog - View/Dump System Eventlog (システムイベントログ - システムイベントログの表示 / ダンプ)	X	X	X	X		
System Eventlog - Clear System Eventlog (システムイベントログ - システムイベントログの消去)	X	X	X			
Sensor overviews (システム概要 (*温度、ファン* ...))	X	X	X	X		
RMU Processor... (RMU プロセッサ)	X	X	X	X		
RMU Processor... - List IP Parameters (RMU プロセッサ... - IP パラメータのリスト)						X
RMU Processor... - Configure IP Parameters (RMU プロセッサ... - IP パラメータの設定)						X
RMU Processor... - Toggle Identify LED (RMU プロセッサ... - 識別灯のトグル)	X	X	X	X		
RMU Processor... - Reset RMU (warm/cold reset) (RMU プロセッサ ... - RMU のリセット (ウォーム / コールドリセット))	X	X				X
Change Password (パスワードの変更)					X	
Start a command Line shell... (コマンドラインシェルの起動)	X	X	X	X		

表 11: リモートマネージャのメニューを使う許可

6.6 パスワードの変更

Change password (パスワードの変更) メニュー項目から、ユーザーアカウント設定の特権を持つユーザー (36 ページ を参照) は、自分のパスワードパスワードや他のユーザーのパスワードを変更することができます。

6.7 システム情報 - RMU に関する情報

メインメニューから System Information... (システム情報) を選ぶと、次のメニューが現われます。

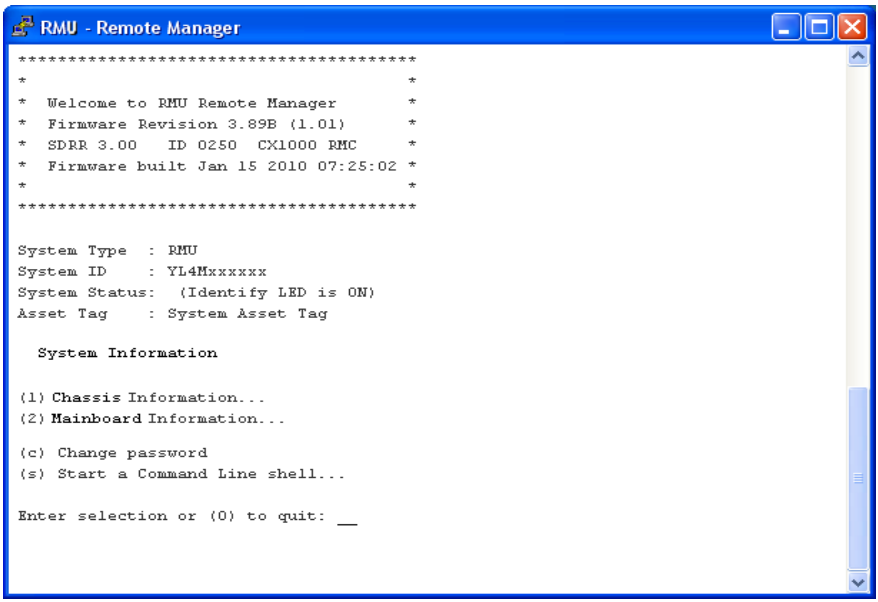


図 119: リモートマネージャ : システム情報ウィンドウ

サブメニューには次のファンクションがあります。

シャシ情報	RMU のシャシとその製品データに関する情報。
メインボード情報	RMU のメインボードとその製品データに関する情報。

表 12: システム情報メニュー

6.8 外装情報 - システムイベントログとセンサ状態

メインメニューから *Enclosure Information...* (外装情報) を選ぶと、次のメニューが現われます。

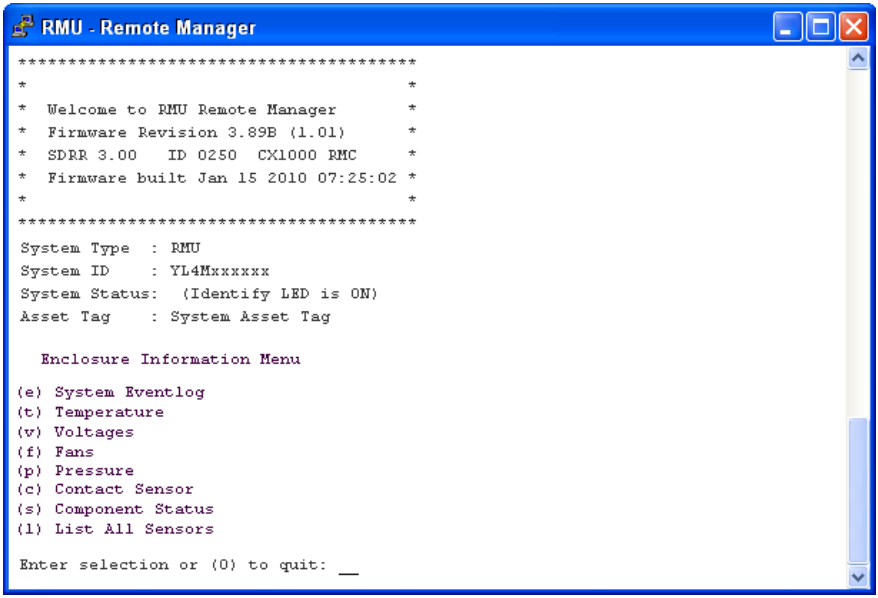


図 120: リモートマネージャ : 外装情報ウィンドウ

サブメニューには次のファンクションがあります。

システムイベントログ	*System Eventlog* メニューを呼び出します (section 242 ページ の「システムイベントログ」を参照).
温度	温度センサとその状態に関する情報を表示します。
電圧	電圧センサとその状態に関する情報を表示します。
ファン	ファンとセンサとその状態に関する情報を表示します。
圧力	RMU の低圧チャンバ内の陰圧を測定する圧力センサの状態に関する情報と、圧力設定値を表示します。

表 13: 外装情報メニュー

接触センサ r	RMU のリアパネルの 6 ピン端子に関する情報を表示します。
コンポーネントの状態	PRIMERGY 診断 LED をそなえたすべてのセンサに関する詳細な情報を表示します。
全センサのリスト	すべてのセンサの詳細な情報を表示します。

表 13: 外装情報メニュー

システムイベントログ

Enclosure Information... (外装情報) サブメニューから *System Eventlog* (システムイベントログ) を選ぶと、次のメニューが現われます。

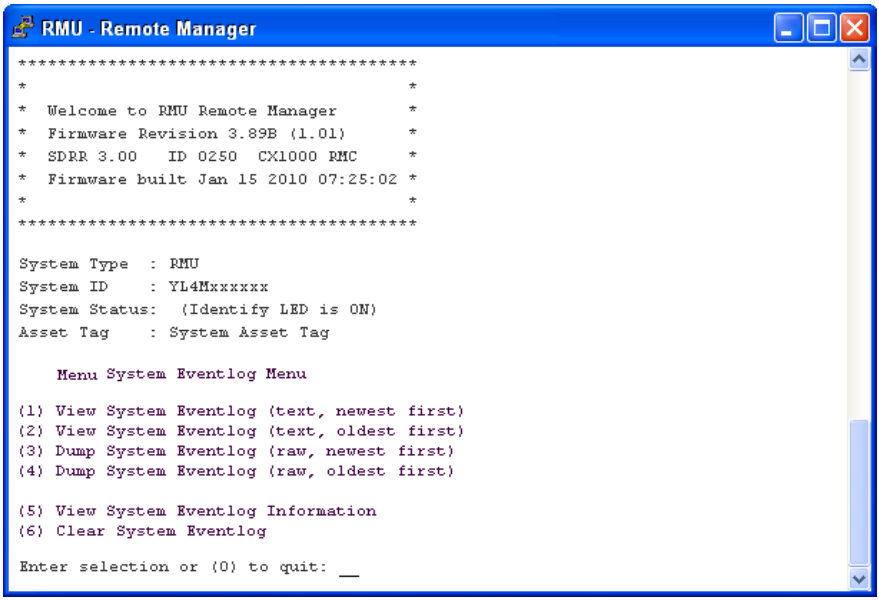


図 121: リモートマネージャ : システムイベントログ

サブメニューには以下のファンクションがあります。

View System Eventlog (text, newest first) (システムイベントログの表示 (テキスト、新しいものから))	イベントログの内容が可読の形式で、入力時期の新しいものから順に画面に出力されます。
View System Eventlog (text, oldest first) (システムイベントログの表示 (テキスト、古いものから))	イベントログの内容が可読の形式で、入力時期の古いものから順に画面に出力されます。
Dump System Eventlog (raw, newest first) (イベントログのダンプ (raw データ、新しいものから))	イベントログの内容が入力時期の新しいものから順にダンプされます。
Dump System Eventlog (raw, oldest first) (イベントログのダンプ (raw データ、古いものから))	イベントログの内容が入力時期の古いものから順にダンプされます。
View System Eventlog Information (システムイベントログ情報の表示)	イベントログに関する情報を表示します。
Clear System Eventlog (システムイベントログの消去)	イベントログの内容を消去します。

表 14: システムイベントログのメニュー

6.9 RMU プロセッサ - IP パラメータ、識別灯 および RMU リセット

メインメニューから *Service Processor...* (サービスプロセッサ) を選ぶと、次のメニューが現われます。

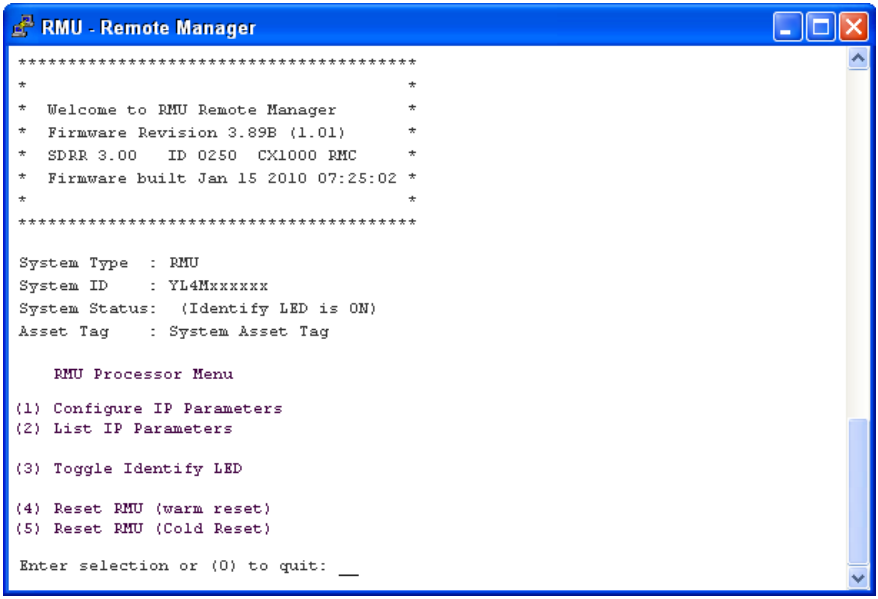


図 122: リモートマネージャ : サービスプロセッサウィンドウ

サブメニューには以下のファンクションがあります。

Configure IP Parameters (IP パラメータの設定)	IP アドレス、サブネットマスク、およびデフォルトのゲートウェイを設定します。DHCP を有効にするかどうかも指定できます。
List IP Parameters (IP パラメータのリスト)	IP パラメータを表示します。
Toggle Identify LED (識別灯のトグル)	識別灯のオン / オフを切り替えます。
Reset RMU (warm reset) (RMU のリセット (ウォームリセット))	RMU をリセットします。接続は閉じられます。インターフェースだけが再初期化されます。
Reset RMU (cold reset) (RMU のリセット (コールドリセット))	RMU をリセットします。接続は閉じられます。RMU 全体が再初期化されます。

表 15: サービスプロセッサのメニュー

Reset RMU (Cold Reset) または *Reset RMU (Warm Reset)* の後には、サーバを再起動することを推奨します。

6.10 コマンドラインシェル ... の起動 - SMASH シェルの起動

メインメニューの Start a Command Line shell... (コマンドラインシェル ... の起動) からは、SMASH CLP シェルを起動することができます。SMASH CLP は “**S**ystems **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol” (サーバハードウェア用システム管理アーキテクチャ、コマンドラインプロトコル) の略です。このプロトコルにより、管理端末と管理対象サーバとの Telnet または SSH ベース接続が可能になります。SMASH CLP に関して詳しくは、247 ページ の「コマンドラインプロトコル (CLP)」の項 を参照してください。

メインメニューから *(s) Start a Command Line shell...* を選択すると、次のウィンドウが現われます。

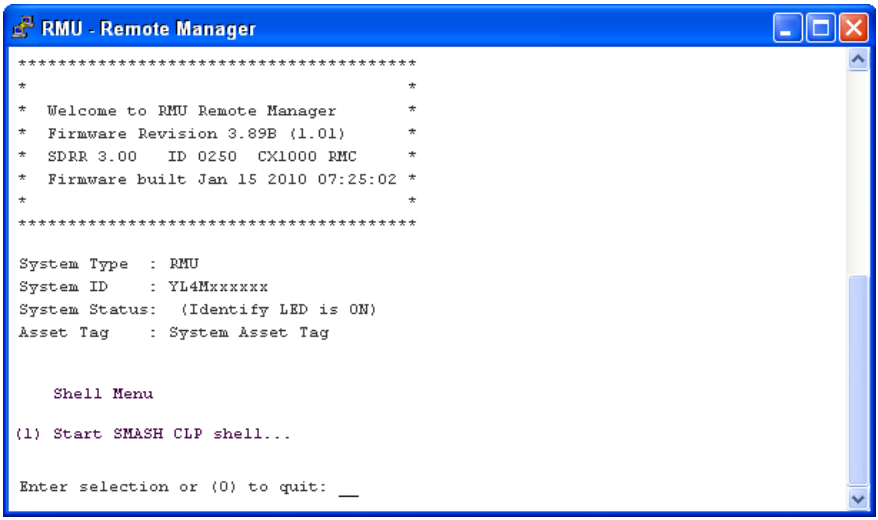


図 123: リモートマネージャ : SMASH CLP シェル ... 起動ウィンドウ

- *(1) Start a SMASH CLP shell...* を選ぶと、SMASH CLP シェルが起動します。

6.11 コマンドラインプロトコル (CLP)

RMU はユーザーシェルとして知られる多様なテキストベースのユーザーインターフェースをサポートします。このようなインターフェースは、個々のユーザーで異なる設定をすることができます。

Systems **M**anagement **A**rchitecture for **S**erver **H**ardware (SMASH) イニシアティブは、下記の目標のもとにいくつかの仕様を定義しています。

– 異質 (ヘテロジニアス) なコンピュータ環境を管理するための標準化されたインターフェースの提供。

– 統一的なインターフェース、ハードウェアおよびソフトウェア発見、リソースアドレッシング、データモデルをそなえたアーキテクチャフレームワークの提供。

SMASH に関する詳しい情報は下記のリンクで見ることができます。

http://www.dmtf.org/standards/smash

SMASH CLP シンタックス

SMASH CLP は、インターネット上で、また企業およびサービスプロバイダー環境で、コンピュータを管理するための共通コマンドラインシンタックスとメッセージプロトコルセマンティックスを指定します。SMASH CLP に関する詳しい情報は、DMTF ドキュメント “Server Management Command Line Protocol Specification (SM CLP) DSP0214” で知ることができます。

CLP の一般的シンタックス (構文) は次の通りです。

<verb> [<options>] [<target>] [<properties>]

<verb>

Verb (動詞) は、実行すべきコマンドやアクションを指定します。動詞のリストは、たとえば、次のような活動を記述します。

– データの設定 (*set*) および検索 (*show*)、

– ターゲットの状態の変更 (*reset*, *start*, *stop*)、

– 現セッションの管理 (*cd*, *version*, *exit*) 、

– コマンドに関する情報の返送 (*help*)。

RMU システムでは、*oemfujitsu* という動詞が、OEM 専用コマンドの使用も可能にします。

<options>

コマンドオプションは、動詞のアクションまたは挙動を修正します。オプションはコマンドラインコマンドライン上で動詞の直後に続くことができ、つねにダッシュ ("-") により導入されなければなりません。

オプションを使って、たとえば、次のことができます。

- 出力フォーマットの定義
- コマンドの反復実行の許可
- コマンドのバージョンの表示
- ヘルプの要求

<target>

target> (ターゲット) は、コマンドにより操作されるオブジェクトのアドレスやパス、すなわちコマンドのターゲットを指定します。ターゲットは単一の管理対象要素、たとえば、ハードディスク、ネットワークアダプタ (Network Interface Card, NIC)、あるいは、マネジメントプログラム (Management Assistance Program, MAP) それ自体であることができます。しかしターゲットは、トランスポートサービスのようなサービスであることも可能です。

マネジメントプログラムにより管理できる複数の管理対象要素を、単一の <target の下に包摂することができます。たとえば、システム全体というターゲットです。

各コマンドにはひとつのターゲットしか指定できません。

<properties>

<properties> (プロパティ) は、コマンドを実行するよう要求されているコマンドのターゲットのプロパティを記述します。こうして、<properties> は、コマンドにより検索あるいは修正されるべきターゲットのクラスのプロパティを特定します。

CLP 内のユーザーデータ (概要)

CLP 内のデータは階層構造をなしています。コマンド *cd* を使うと、この構造内を移動することができます。

CLP 内のユーザーデータの概要を 図 124 に示します。長方形でかこった名前は、コマンドターゲットを示します。階層のいずれのレベルでも、コマンド / 動詞 *show* が、利用可能なターゲット、プロパティ、および動詞を表示します。

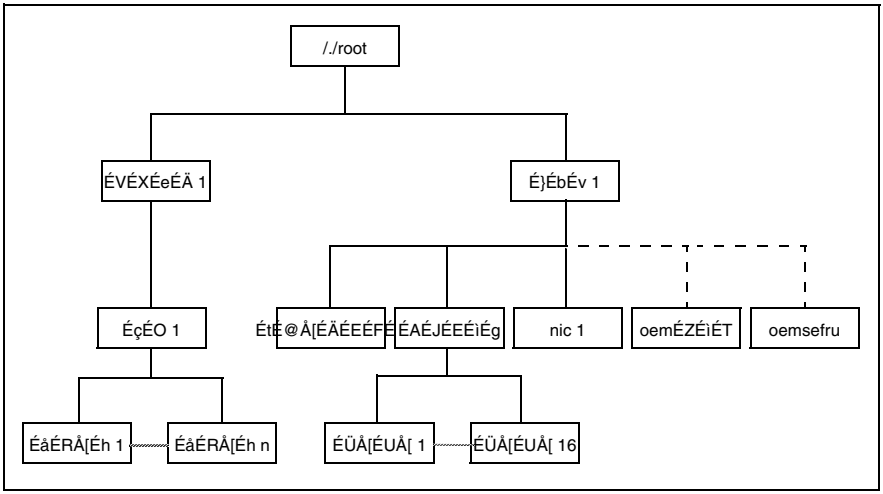


図 124: SMASH CLP 内のユーザーデータの構造

CLP コマンドの階層

CLP コマンド階層の概要を 250 ページ の表 16 に示します。

Target \ Verb	Properties	Comment	cd	show	help	exit	version	set	reset	start	stop	load	oemfsc
/		Root	X	X	X	X	X						
system1 **map1**													
system1	name enabledstate	Host System	X	X	X	X	X		System	PON	POFF		
...log1		Event Log (SEL)	X	X	X	X	X		RMU				X
....record<n>	number date time sensordescription eventdescription eventdirection	Single SEL entry	X	X	X	X	X		RMU				X
map1	name	RMU	X	X	X	X	X		RMU				X
...firmware	version	RMU FW	X	X	X	X	X		RMU			X	X
...accounts		Accounts	X	X	X	X	X	X	RMU				X
.....user<n>	username password group	User	X	X	X	X	X	X	RMU				X
...nic1	networkaddress oemfsc_nonvol_networkaddress oemfsc_mask oemfsc_nonvol_mask oemfsc_gateway oemfsc_nonvol_gateway oemfsc_dhcp_enable oemfsc_nonvol_dhcp_enable oemfsc_vsi_path oemfsc_vsi_server oemfsc_vsi_permission oemfsc_vsi_sustain	LAN	X	X	X	X	X	X	RMU				X
...oemfsc_sensors		OEM Sensors	X	X	X	X	X		RMU				X
.....oemfsc_sensor_num<n>lun<m>	oemfsc_reading oemfsc_status oemfsc_sensortype oemfsc_readingtype	Single Sensor	X	X	X	X	X		RMU				X
...oemfsc_frus		FRU	X	X	X	X	X		RMU				X
.....oemfsc_fru_devid<n>lun<m>	oemfsc_description	Single FRU	X	X	X	X	X		RMU				X

表 16: CLP コマンドの階層

索引