インストールガイド - 日本語

FUJITSU

FUJITSU Software ServerView Suite

Remote Management

iRMC S2/S3 - integrated Remote Management Controller

2012年07月版

DIN EN ISO 9001:2008 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 9001:2008
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 iRMC S2/S3 の概要

最新のサーバシステムはますます複雑になり、システム管理面の必要条件も増加しています。

こうした状況に対応するため、システムを集中制御する BMC（Baseboard Management Controller：ベースボード管理コントローラ）とプラットフォーム管理ハードウェアの間にメッセージベースの標準インターフェースを実現しようと、多くのベンダーが提携して IPMI（Intelligent Platform Management Interface）イニシアティブが設立されました。IPMI の詳細については、21 ページ の「IPMI のテクニカルな背景」の項を参照してください。

iRMC S2（integrated Remote Management Controller：リモートマネジメントコントローラ）は、統合 LAN 接続および従来は RSB（RemoteView Service Board：リモートサービスボード）のようなプラグインボードを追加した場合にのみ利用可能だった拡張機能を実現する BMC です。これにより、システムの状態に関係なく PRIMERGY サーバの総合制御が可能です。特に「Out-bound」状態の PRIMERGY サーバに対して有効です。

図 1: PRIMERGY サーバのシステムボード上の iRMC S2

iRMC S2/S3 は最新 PRIMERGY サーバのシステムボード上にある自立したシステムであり、専用のオペレーティングシステムおよび専用 Web サーバ、独立ユーザー管理、独立警告システムがあります。サーバがスタンバイモードの場合でも、iRMC S2/S3 の電源は ON のままです。本書では、iRMC S2/S3 の設定方法および利用可能なさまざまなユーザーインターフェースを説明してい ます。

1.1 本書の目的と対象

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。
IPMI の背後の基本的なテクノロジーに関して説明を行った後、次の事項に関する詳細を説明します。

- iRMC S2/S3 へのログオン
- iRMC S2/S3 の設定
- iRMC S2/S3 のユーザー管理
- iRMC S2/S3 によるビデオリダイレクション
- iRMC S2/S3 によるリモートストレージ
- iRMC S2/S3 Web インターフェース
- iRMC S2/S3 の Telnet/SSH ベースインターフェース（リモートマネージャ）
- サーバ設定による iRMC S2/S3 の設定
- ファームウェアのアップデート
- iRMC S2/S3 によるオペレーティングシステムのリモートインストール
- IPMI OEM コマンド

サービス

PRIMERGY サーバのリモートマネジメントに関する質問は、サービス＆サポートパートナーにお問い合わせください。

参照情報

http://www.ts.fujitsu.com

1.2 iRMC S2/S3 のファンクション

iRMC S2/S3 は広範囲にわたるファンクションを標準サポートしますが、AVR（Advanced Video Redirection：ビデオリダイレクション）およびリモートストレージと組み合わせれば、さらに 2 つの PRIMERGY サーバリモートマネジメント拡張ファンクションが利用可能です。AVR およびリモートストレージの使用には、別売のライセンスキーが必要です。

標準 iRMC S2/S3 ファンクション

- ブラウザアクセス

  iRMC S2/S3 には専用の Web サーバが搭載されているため、管理端末から標準 Web ブラウザでアクセスできます

- セキュリティ（SSL、SSH）

  HTTPS ／ SSL によるセキュアな Web サーバアクセスおよびセキュアなグラフィカルコンソールリダイレクション（マウスおよびキーボード付き）をサポートします。iRMC S2/S3 へのアクセスは、リモートマネージャから SSH による暗号化設定を行って接続を保護できます。リモートマネージャの iRMC S2/S3 インターフェースは、英数字専用です。

- ServerView 統合

  ServerView エージェントが iRMC S2/S3 を検出し、自動的に関連サーバに適用します。したがって ServerView リモートマネジメントフロントエンドを使って、ServerView Operations Manager から iRMC S2/S3 Web インターフェースおよびテキストコンソールリダイレクトを直接開始できます。

- 電源制御

  システムの状態に関係なく、次の 3 つの方法でリモート管理端末から管理対象サーバの電源の投入および切断が可能です。

  – iRMC S2/S3 Web インターフェース
  – リモートマネージャおよび CLP（Command Line Interface：コマンドラインインターフェース）
  – スクリプト

- 消費電力制御

  iRMC S2/S3 は、管理対象サーバの消費電力制御を総合的に行います。最小消費電力から最大パフォーマンスまで、電力制御モードを指定できます。モードは、必要に応じて切り替えられます。

- CSS（Customer Self Service：カスタマセルフサービス）

  変化したサーバコンポーネントが CSS コンポーネントの場合、iRMC S2/S3 Web インターフェース上のサーバコンポーネントおよびセンサ、電源ユニットなどのためのサマリー表の各列に情報が表示されます。さらに、SEL（System Event Log：システムイベントログ）のエラーリストには、CSS コンポーネントが始動したあらゆるイベントが表示されます。

- テキストコンソールのリダイレクション

  ServerView リモートマネジメントフロントエンドから、iRMC S2/S3 への Telnet/SSH セッションを開始できます。テキストコンソールのリダイレクションが開始され、リモートマネージャが起動します。iRMC S2/S3 インターフェースは、英数字専用です。

- BMC の基本機能

  iRMC S2/S3 は、電圧監視およびイベントログ、リカバリ制御などの BMC 基本機能をサポートしています。

- 「ヘッドレス」システム操作

  管理対象サーバに、マウスもしくはモニタ、キーボードが接続されていなくてもリダイレクションが可能です。これにより、コストの 低減、筐体のケーブリングのより一層の簡略化およびセキュリティの強化を実現しています。

- 識別灯

  筐体ロッカー内に多数設置されている場合などにシステムが容易に識別できるように、iRMC S2/S3 Web インターフェースから識別灯を起動できます。

- Error LED

  Error LED は、管理対象システムの状態と CSS の状態を常時示しています。

- 電源 LED

  電源 LED は、サーバの電源の ON ／ OFF の状態を示しています。

- LAN

  サーバ内蔵のシステム NIC（Network Interface Card）の LAN インターフェースには、管理 LAN 専用になっているシステムと設定を選べるシステムがあります。

  – 管理 LAN 専用に設定
  – 管理 LAN とシステムで共用するように設定
  – システム用に完全に開放

  レンチ記号がついたポートは、iRMC S2/S3 用です。40 ページ の図 7 を参照してください。

- CLP（Command Line Interface：コマンドラインインターフェース）

  リモートマネージャに加えて、iRMC S2/S3 は DMTF（Distributed Management Task Force：分散管理タスクフォース）標準の SMASH CLP（System Management Architecture for Server Hardware Command Line Protocol）をサポートしています。

- インタラクティブもしくはスクリプトベースでの容易な設定

  iRMC S2/S3 は、次の方法で設定できます。

  – iRMC Web インターフェース
  – SVOM のサーバの設定
  – サーバマネージメントツール IPMIVIEW
  – BIOS 設定

  サーバの設定もしくは IPMIVIEW からスクリプトでの設定もできるため、ServerView Installation Manager によるサーバの初期設定時に、iRMC S2/S3 を設定できます。多数のサーバをスクリプトベースで設定することも可能です。

- CSS パネル（ローカルサービスパネル）のサポート

  PRIMERGY サーバに CSS パネル（ローカルサービスパネル）が付いている場合には、障害が発生したモジュールを特定して自分で交換することができます。

- ローカルユーザー管理

  iRMC S2/S3 には独自のユーザー管理機能があり、最大 16 ユーザーまでをパスワード付きで作成し、所属するユーザーグループに応じたさまざまな権限を適用できます。

- ディレクトリサービスによるグローバルユーザー管理

  iRMC S2/S3 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集中保存されます。サーバ上で集中管理されるユーザー ID は、ネットワーク上の全 iRMC S2/S3 から共有されます。

  次のディレクトリサービスをサポートしています。

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – OpenDS

- CAS ベースのシングルサインオン（SSO）認証

  iRMCS2 は CAS（Centralized Authentication Service）設定をサポートしており、CAS ベースのシングルサインオン（SSO）認証用の iRMC S2/S3 Web インターフェースを設定できます。

  CAS サービスの SSO ドメイン内のアプリケーションに初めてログインすると（iRMC S2/S3 Web インターフェースなど）、CAS 固有のログイン画面でログイン認証情報の入力が要求されます。CAS サービスによる認証に成功すると、ユーザはログイン認証情報を再び入力せずに、iRMC Web インターフェースと SSO ドメイン内の他のサービスへのアクセスが許可されます。

- DNS ／ DHCP

  iRMC S2/S3 では自動ネットワーク設定が可能です。初期値として設定されている名前と DHCP を使って、iRMC S2/S3 は DHCP サーバから IP アドレスを受け取ります。iRMC S2/S3 名は DNS（Domain Name Service：ドメインネームサービス）によって登録され、最大 5 つの DNS サーバがサポートされます。DNS/DHCP が利用できない場合は、静的 IP アドレスも使用できます。

- 電源ユニット

  iRMC S2/S3 は、システムの予備電源ユニットから電力が供給されます。

- 警告管理

  iRMC S2/S3 の警告通知（アラーティング）には、次の 3 種類があります。

  – SNMP による PET（Platform Event Traps：プラットフォームイベントトラップ）送信

  – E-mail による警告の直接送信

  – モデム／シリアルインターフェース接続しての警告送信

  また iRMC S2/S3 は、あらゆる関連情報を ServerView エージェントへ提供します。

- SEL（System Event Log：システムイベントログ）の表示、フィルタリングおよび退避

  次の方法で、SEL の内容を表示および退避し、削除できます。

  – iRMC S2/S3 Web インターフェースを利用

  – iRMC S2/S3 の Telnet/SSH ベースのインターフェース（リモートマネージャ）を利用

- iEL（iRMC Event Log：内部イベントログ）の表示、フィルタリングおよび退避次の方法で、iEL の内容を表示および退避し、削除できます。

  – iRMC S2/S3 Web インターフェースを利用

  – iRMC S2/S3 の Telnet/SSH ベースのインターフェース（リモートマネージャ）を利用

iRMC S2/S3 の拡張機能

iRMC S2/S3 は、標準機能に加えて AVR およびリモートストレージ機能をサポートしています。

- AVR（Advanced Video Redirection：ビデオリダイレクション）

  iRMC S2/S3 はビデオリダイレクション（AVR）をサポートし、次の利点があります。

  – 標準 Web ブラウザによる操作。管理端末に Java 実行環境以外の追加ソフトウェアをインストールする必要がありません。

  – システムから独立したグラフィカルおよびテキストコンソールのリダイレクション（マウスおよびキーボード含む）です。

  – リモートアクセスによる起動監視および BIOS 管理、オペレーティングシステム操作が可能です。

– 異なる 2 箇所から 1 台のサーバに同時「仮想接続」しての作業が可能です。ハードウェア圧縮およびビデオ圧縮により、ネットワーク負荷も軽減されます。

– サーバ側のモニタの停止サポート。AVR セッション中のサーバ側の画面上で実行中のユーザー入力および作業が権限のない人間に見られることがないように、AVR セッション中に管理対象の PRIMERGY サーバ側の画面出力を停止することができます。

– 低帯域幅

  データ転送速度が低下した場合、現在の AVR セッションの色深度に対する帯域幅（bpp、ビット / ピクセル）を低く設定できます。

- リモートストレージ

  リモートストレージにより、「仮想」ドライブが利用可能です。物理的にはリモート管理端末上に 存在している「仮想」ドライブを、リモートストレージサーバによりネットワーク使用します。

  「仮想」ドライブとリモートストレージの組み合わせは、次のようにローカルドライブとほとんど 同じように使用できます。

  – データの読み出しおよび書き込み
  – リモートストレージからの起動
  – ドライバおよび小規模アプリケーションのインストール
  – リモート管理端末からの BIOS アップデート
    （USB による BIOS アップデート）

  リモートストレージは、リモート管理端末上の「仮想ドライブ」として、次のデバイスタイプをサ ポートしています。

  – CD ROM
  – DVD ROM
  – USB メモリスティック
  – フロッピーイメージ
  – CD ISO イメージ
  – DVD ISO イメージ

  また、リモートストレージサーバは、「仮想ドライブ」としてネットワーク上に ISO イメージを実現します。

  リモートストレージでは、リモート管理端末に最大 2 つの「仮想」ドライブ同時接続を行うか、リモートストレージサーバにより ISO イメージのプロヴィジョンを行うかが選択可能です。

1.3 iRMC S2/S3 の操作インターフェース

iRMC S2/S3 には、次の操作インターフェースがあります

- iRMC S2/S3 Web インターフェース（Web インターフェース）

  iRMC S2/S3 Web サーバへは、Microsoft Internet Explorer もしくは Mozilla Firefox などの標準 Web ブラウザで接続します。

  iRMC S2/S3 の Web インターフェースにより、あらゆるシステム情報およびファン速度や電圧などセンサデータの表示を行います。また、テキストベースコンソールリダイレクションの設定、開始、グラフィカルコンソールリダイレクション（AVR、Advanced Video Redirection）の開始を行います。さらに、管理者権限では、iRMC S2/S3 Web インターフェースでの接続設定が可能です。iRMC S2/S3 Web サーバへのアクセスは、HTTP ／ SSL によるセキュアなアクセスです。

  Web インターフェースによる iRMC S2/S3 操作の詳細については、139 ページ の「iRMC S2/S3 Web インターフェース」の章を参照してください。

- リモートマネージャ：LAN によるテキストベース Telnet/SSH インターフェース

  リモートマネージャは、次の場所から起動できます。

  – ServerView Operations Manager
  – iRMC S2/S3 Web インターフェース
  – Telnet/SSH クライアント

  リモートマネージャは、英数字インターフェースで、システム、センサ情報、電源管理機能および エラーイベントログへのアクセスを行います。さらに、テキストコンソールのリダイレクションもしくは SMASH CLP シェルを起動します。SSH（Secure Shell：セキュアシェル）を通してリモートマネージャを起動すると、リモートマネージャおよび管理対象サーバ間の接続は暗号化されます。

  リモートマネージャを利用した iRMC S2/S3 操作の詳細については、325 ページ の「Telnet/SSH 経由の iRMC S2/S3 (リモートマネージャ)」の章を参照してください。

- リモートマネージャ（シリアル）:「シリアル 1」によるテキストベースシリアルインターフェース

  リモートマネージャ（シリアル）は、リモートマネージャインターフェースと同じです。

1.4 iRMC S2/S3 で使用される通信プロトコル

iRMC S2/S3 通信プロトコルとポートを、表 1 に示します。

接続のリモート側	通信方向	接続の iRMC S2/S3 側 （ポート番号 / プロトコル）
RMCP	→	623/UDP
	←	623/UDP
HTTP ポート	→	80/TCP
	←	80/TCP
HTTPs ポート	→	443/TCP
	←	443/TCP
Telnet	→	3172/TCP
	←	3172/TCP
SSH	→	22/TCP
	←	22/TCP
トラップ	→	162/UDP
Email	→	25/TCP
	←	25/TCP
リモートストレージ	→	5901/TCP
	←	5901/TCP
VNC ポート		
標準ポート	→	80/TCP
	←	80/TCP
セキュアポート	→	443/TCP
	←	443/TCP

表 1: iRMC S2/S3 で使用される通信プロトコルとポート

iRMC S2/S3 ファームウェアバージョン 5.00 以降では、リモートストレージポートはリモートストレージサーバおよびクライアント内部の通信にのみ使用されます。AVR のリモートストレージの場合は 、（Java アプレット経由で）http ポートを使用します。

1.5 IPMI のテクニカルな背景

iRMC S2/S3 により、IPMI インターフェースから BMC 機能が利用可能です。

IPMI（Intelligent Platform Management Initiative）とは

IPMI は、複雑さを増すサーバシステム管理に対応するために生まれました。サーバシステム監視のための新しいソリューションをもとめて、多くのベンダーがこのイニシアティブに参加しています。

IPMI という名前が、ソリューションのアプローチの方向性を示しています。システムの監視機能およびリカバリ機能が、プラットフォーム管理ハードウェアおよびファームウェア上に直接実装されます。

IPMI の目的

IPMI は、システムを集中制御する BMC（Baseboard Management Controller：ベースボード管理コントローラ）とインテリジェントなプラットフォーム管理ハードウェアの間に、抽象化されたメッセージベースの標準インターフェースを実現することをめざしました。

IPMI は、さまざまなプラットフォーム管理モジュールの主要特性を、標準仕様としてまとめたもの なのです。

IPMI 規格

IPMI 規格仕様は、次のとおりです。

「IPMI は、特定の管理ソフトウェアに依存しないハードウェアレベルインターフェースの規格であり、監視および制御機能を DMI、WMI、CIM、SNMP などの標準管理ソフトウェアインタ ーフェースを通して提供する。ハードウェアレベルのインターフェースであるため、標準的な管 理ソフトウェアスタックの最下位に位置する。」22 ページ の「IPMI とその他の管理規格との関係」を参照してください。

IPMI の利点

IPMI 仕様は、プロセッサもしくは BIOS、オペレーティングシステムごとのインベントリおよびログ、リカバリ、監視といった機能の独立性を保証します。

したがって、シャットダウンや電源遮断も、プラットフォームの管理のもとに行われます。

IPMI とその他の管理規格との関係

IPMI は、各オペレーティングシステム上のシステム管理ソフトウェアと連動して使用するのに最適です。IPMI の機能を管理アプリケーションおよびオペレーティングシステムの管理機能と組み合わせることによって、強力なプラットフォーム管理環境が実現します。

図 .2 に、IPMI および管理ソフトウェアスタックの関係の概要を示します。

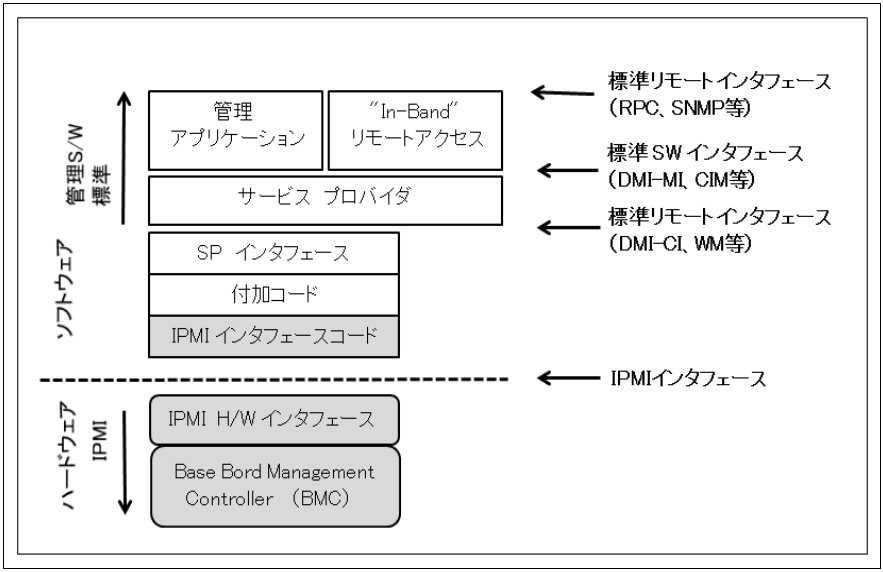


図 2: 管理ソフトウェアスタック上の IPMI の位置づけ

IPMI および IPMB、ICMB

IPMI イニシアティブの規格は、次の 3 つの仕様で構成されています。

– *IPMI（Intelligent Platform Management Interface）*
IPMI ベースのシステムが実現するべき高レベルのアーキテクチャ、電流指令、イベントフォーマット、データパケット、およびさまざまな特性を規定しています。

– *IPMB（Intelligent Platform Management Bus）*
プラットフォーム管理ハードウェアの内部モジュール間の標準接続のための I2C ベース（write only）バス仕様です。リモートマネジメントモジュールへの標準インターフェースとしても機能します。

– *ICMB（Intelligent Chassis Management Bus）*
プラットフォーム管理情報のやりとり、および複数システムにまたがる制御を行う外部バスインタ ーフェースです。IPMB 接続するデバイス上で機能するようにデザインされています。ServerView リモートマネジメント環境では、まだ実装されていません。

IPMI の実装

IPMI 実装の中核となるのは、BMC（Baseboard Management Controller）です。BMC には、次の役割があります。

– システム管理ソフトウェアおよびプラットフォーム管理ハードウェア間のインターフェースのとりまとめ

– 監視およびイベントログ、リカバリ制御の自立機能の実現

– システム管理ソフトウェアおよび IPMB 間のゲートウェイとしての役割

IPMI を利用した管理コントローラを設置すれば、プラットフォーム管理の範囲が広がります。IPMB は I2C ベースのシリアルバス仕様であり、管理コントローラ内部および管理コントローラ間の通信に使用されます。

IPMI により、複数の管理コントローラと組み合わせた拡張性のあるアーキテクチャを実装できます。複数のコントローラにより、電源装置およびホットスワップ RAID ドライブモジュールなどの異なるサブシステムを監視する複雑なサーバシステムが構築できます。

IPMI には、IPMI コマンドを処理できない「インテリジェントでない」I2C モジュール上の IPMB に接続された管理コントローラをとおしてアクセスを行うための「低レベル」I2C コマンドもあります。

IPMI の基本構成要素の概要を 24 ページ の図 3 に示します。

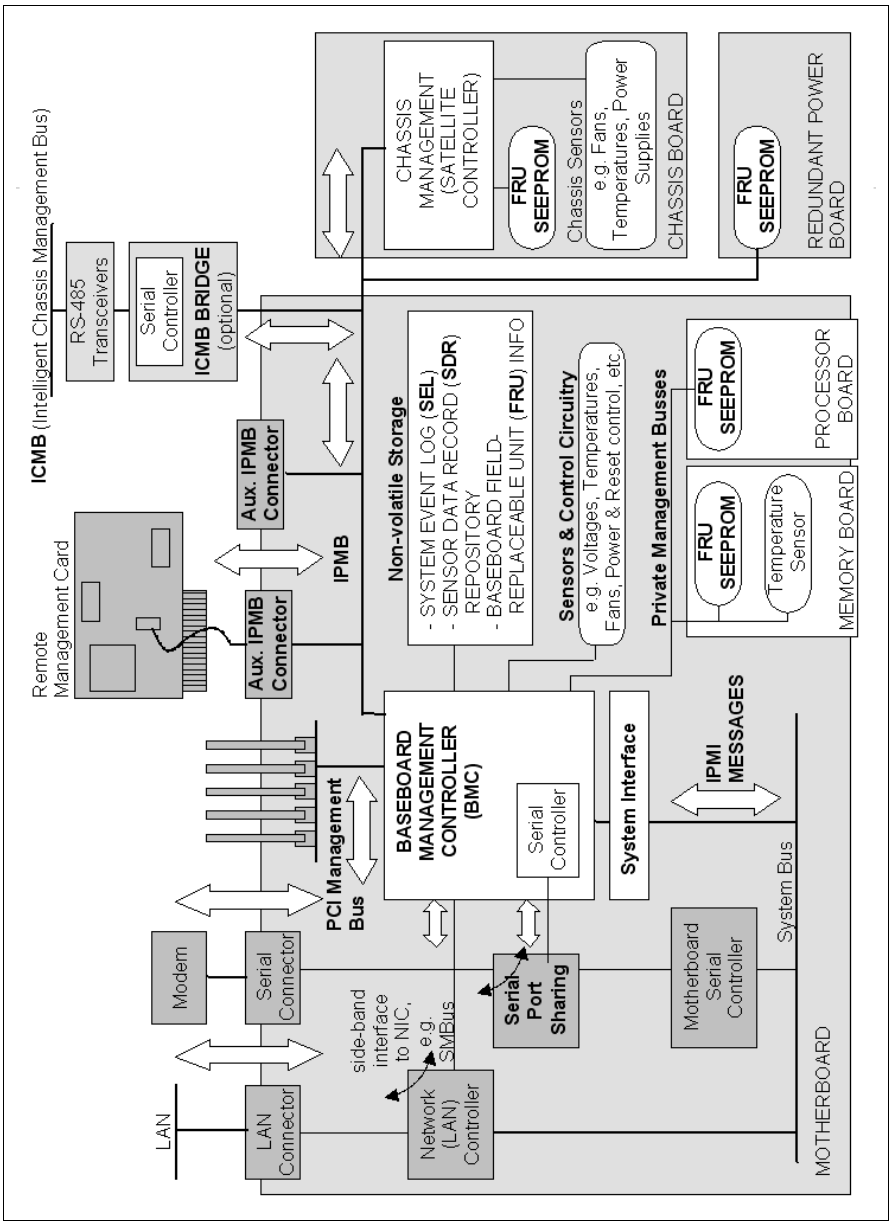


図 3: IPMI ブロックダイアグラム

IPMI と「In-bound」および「Out-bound」管理

システム管理の分野では、「In-bound」および「Out-bound」管理は次のように区別されます。

– 「In-bound」管理は、管理対象サーバ上でオペレーティングシステムが動作している場合の管理です。

– 「Out-bound」管理は、障害が発生している等、管理対象サーバ上でオペレーティングシステムが動作していない場合の管理です。

IPMI 規格にしたがったシステム環境では異なるインターフェースが利用できるため、「In-bound」管理もしくは「Out-bound」管理のどちらにも対応します。

IPMI-over-LAN

IPMI-over-LAN は、IPMI 規格の LAN インターフェース仕様の新しい名称です。管理対象システムの BMC との間で IPMI メッセージを送受信する方法を規定する仕様で、RMCP（Remote Management Control Protocol：リモートマネジメント制御プロトコル）データパケットにカプセル化されます。RMCP データパケットは、イーサネット LAN 接続を通し IPv4 UDP 転送されます。

もともと RMCP プロトコルは、オペレーティングシステムが動作していないシステム機器の管理のための規格であり、シンプルな問い合わせ／応答のプロトコルです。

BMC に適用されたオンボード LAN コントローラ上には、以上のような接続インターフェースがあります。

このインターフェースはオンボード LAN コントローラ上でのみ機能し、LAN カード上では機能しません。

UDP 下で RCMP が使用する 2 ポートのうち、BMC は LAN コントローラとの通信にポート 623 （プライマリ RMCP ポート）使用します。

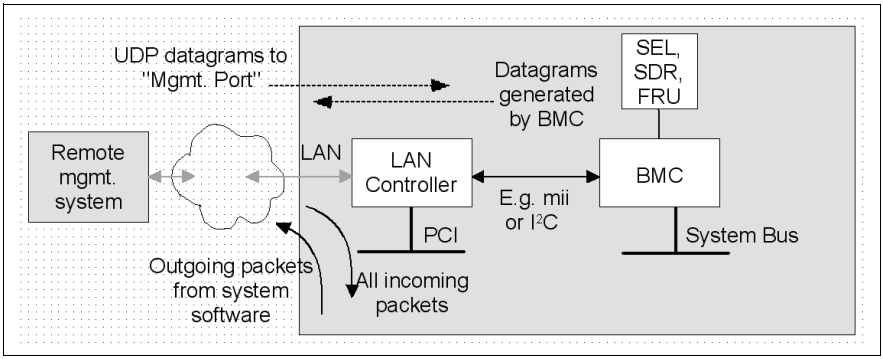


図 4: BMC および LAN コントローラ

SOL (Serial Over LAN）インターフェース

SOL は IPMI V2.0 規格の一部であり、LAN 接続でのシリアルデータ転送のインターフェースです。特に、管理対象コンピュータのシリアルコントローラおよびリモート管理端末の間の LAN によるシリアルデータストリーム転送のパケットフォーマットおよびプロトコルを規定します。SOL は IPMI-over-LAN 仕様にもとづいています。

SOL 接続の確立には、まずリモートマネジメントアプリケーションが BMC との間に IPMI-over-LAN セッションを開始します。これが完了した段階で、リモート管理端末が SOL サービスを起動します。シリアルコントローラおよびリモート管理端末の間のデータトラフィックは、IPMI コマンドと同じ IPMI セッションで処理されます。

SOL 接続確立後すぐに、次のようにして、シリアルコントローラおよびリモート管理端末の間のデータ転送が行われます。

– シリアルコントローラからリモート管理端末への転送 シリアルコントローラからのデータストリームは BMC による分割後、圧縮されて LAN をとおしてリモート管理端末に送られます。

– リモート管理端末からシリアルコントローラへの転送リモート管理端末から送られてきた圧縮文字列は BMC によって解凍され、文字ストリームとしてシリアルコントローラに転送されます。

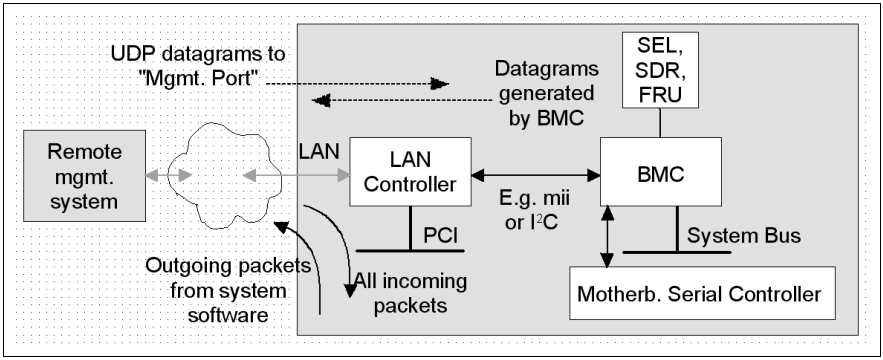


図 5: BMC および SOL

管理対象システムおよびリモート管理端末の BMC 間の SOL メッセージとして、SOL 文字データが交換されます。SOL メッセージは RMCP+ データパケットにカプセル化され、IPv4 によりイーサネット LAN 接続をとおして UDP で転送されます。RMCP+ プロトコルは RMCP プロトコルにもとづいていますが暗号化、認証などの拡張機能があります。

Serial over LAN では、管理対象サーバの BIOS もしくはオペレーティングシステムによるコンソールリダイレクションによる「ヘッドレス」管理が可能です。したがって、高価な集信装置は不要です。

IPMI のチャネルコンセプト

「チャネル」はさまざまな接続キャリアにより IPMI メッセージを BMC にルートするメカニズムであり、9 チャネルまでサポートされます。システムインターフェースおよびプライマリ IPMB は固定ですが残りの 7 チャネルは自由に実装できます。

チャネルには、「セッションベース」チャネルおよび「セッションレス」チャネルがあります。「セッション」のコンセプトには 、ユーザー認証のコンセプト（28 ページ の「ユーザーの識別」）および単一チャンネルで複数の IPMI メッセージストリームをルーティングするためのコンセプトの 2 種類があります。

「セッションベース」チャネルの例には LAN チャネルもしくはシリアル／モデムチャネルがあり、「セッションレス」チャネルの例には、システムインターフェースおよび IPMB があります。

ユーザーの識別

「セッションベース」チャネル（27 ページ の「IPMI のチャネルコンセプト」）では、ユーザーログ インが必要です。「セッションレス」チャネルでは、ユーザー認証の必要はありません。

IPMI では、ユーザー設定はチャネル単位です。つまり、LAN チャネルもしくはシリアルチャネルのどちらで BMC にアクセスしているかによって、ユーザーは異なる特権を持つことができます。

引用

IPMI 標準に関する情報は、次の Web サイトで見ることができます。（英語サイト）

http://developer.intel.com/design/servers/ipmi/index.htm

1.6 DCMI（データセンター管理インターフェース）

iRMC S2/S3 は DCMI（データセンター管理インターフェース）プロトコルをサポートしており、これは IPMI V2.0 規格に準拠しています。DCMI は、大規模データセンターに展開されたサーバシステムの管理と効率を向上させるために開発されてました。

データセンター内のサーバのハードウェア管理要件を満たすため、DCMI は特に次の主要機能をサポートします。

- インベントリ機能（サーバ識別）
- 電源管理と消費電力監視
- 電力消費の監視と管理
- イベントログ
- 温度監視

DCMI の詳細情報は、DCMI ホームページに掲載されています。

http://www.intel.com/technology/product/DCMI

1.7 以前のバージョンのマニュアルからの変更点

iRMC S2/S3 - integrated Remote Management Controller
（2012 年 7 月版）

本マニュアルでは、iRMC S2/S3 **ファームウェアバージョン 6.5x** について説明し、オンラインマニュアル『iRMC S2/S3 - integrated Remote Management Controller』（2012 年 5 月版）を置き換えるものです。

このマニュアルには、以下の更新が含まれています。

- 第 7 章「iRMC S2/S3 Web インターフェース」で、「ゼロワット技術」機能について説明されています。
- 以前の第 12 章「IPMI OEM コマンド」が拡大され、以下のセクションを含む付録（「12 付録」）になりました。
  - 12.1「iRMC S2/S3 でサポートされる IPMI OEM コマンド」（以前の第 12 章「IPMI OEM コマンド）
  - 12.2「SCCI およびスクリプト設定を使用した iRMC S2/S3 の設定」（新しい節）

iRMC S2/S3 - integrated Remote Management Controller
（2012 年 5 月版）

このマニュアルは、iRMC S2/S3 **ファームウェアバージョン 6.5x** について記載されており、オンラインマニュアル『iRMC S2 - integrated Remote Management Controller』（2011 年 11 月版）の改訂版です。

iRMC S2/S3 の新機能（7 章「iRMC S2/S3 Web インターフェース」に記載）:

- エージェントレス HDD 監視（iRMC S3 のみ）

  管理するサーバが「エージェントレス HDD 監視」機能（「アウトオブバンド HDD 監視」とも呼ばれます）をサポートする場合、個々の HDD の HDD<n> ステータスは、専用のライトパスステータスセンサーで直接読み取られて iRMC S3 に報告されるので、ServerView エージェントが実行されていなくても表示することができます。

- BIOS 設定のバックアップ / リストア、BIOS のフラッシュ：

  管理するサーバの BIOS が該当する機能要件を満たす場合は、iRMC S2/S3 で以下を行うことができます。

  - 複数の BIOS パラメータを ServerView® WinSCU XML 形式でバックアップし、それらを ServerView® WinSCU XML 形式でファイルからリストアできます。
  - 「ファイルからアップロード」するか TFTP 経由で BIOS をアップデートできます。
- サーバタイプによっては、「*電源制御オプション*」で「*静音操作*」を選択できます。

iRMC S2/S3 - integrated Remote Management Controller（2011 年 5 月版）

本マニュアルでは、iRMC S2/S3 **ファームウェアバージョン 5.5x** について説明し、オンラインマニュアル『iRMC S2 - integrated Remote Management Controller』（2011 年 4 月版）を置き換えるものです。

本マニュアルは iRMC S2 と iRMC S3 の両方に適用されます。iRMC S2 と iRMC S3 との機能面での差異を、マニュアル内で個別に取り上げています。

iRMC S2 - integrated Remote Management Controller（2011 年 4 月版）

2011 年 4 月版の iRMC S2 マニュアルでは iRMC S2 **ファームウェアバージョン 5.5x** について説明し、オンラインマニュアル『iRMC S2 - integrated Remote Management Controller』（2010 年 7 月版）を置き換えるものです。

- iRMC S2 の新機能 :
  - システムイベントログ（IPMI SEL）の他に、iRMC S2 に内部イベントログ機能が追加されました。
  - iRMC S2 で IPv4 と IPv6 アドレスの両方がサポートされるようになりました。
  - iRMC S2 が Open DS ディレクトリサービスをサポートするようになりました。
  - iRMC S2 設定（iRMC S2 ファームウェア設定）を iRMC S2 Web インターフェースからリストアできます。
  - Email での警告通知がグローバル iRMCS2 ユーザ ID についてもサポートされます。
- 第 5 章「ビデオリダイレクション（AVR）」:

  いくつかのマイナーチェンジに加えて、AVR ウィンドウのメニューに「*Power Control*」エントリが追加され、AVR ウィンドウからサーバの電源切断やリブートを直接実行できるようになりました。

- 第 7 章「iRMC S2 Web インターフェース」:
  - *電源ユニット*ページ : 一部のタイプのサーバで、*電源冗長構成*機能が実装されました。
  - *システムイベントログ内容*ページ :

    GUI 言語「German」:
    イベントの説明と解決方法はドイツ語で記述されます。

    GUI 言語「日本語」:
    解決方法は日本語で記述されます。
  - 「*DNS 構成*」ページに以前の「*DHCP 構成*」ページの機能が組み込まれ、「DHCP 構成」ページはなくなりました。
  - 新しい iRMC S2 に対応する新規および変更されたページに、上記の機能が組み込まれます。
- 第 8 章「リモートマネージャ」:

  新しい iRMC S2 に対応する新規または変更されたメニューには、内部イベントログおよび IPv6 アドレッシングが組み込まれています。
- 第 9 章「Server Configuration Manager」:

  新しい iRMC S2 に対応する新規または変更されたメニューページには、IPv6 アドレッシングと Open DS サポートが組み込まれています。

1.8 ServerView Suite リンク集

リンク集により、富士通は ServerView Suite および PRIMERGY サーバに関するさまざまなダウンロードや詳細情報を提供します。

ServerView Suite には、以下のトピックに関するリンクがあります。

- サポートデスク
- マニュアル
- 製品情報
- セキュリティ情報
- ソフトウェアのダウンロード

ダウンロードには以下が含まれます。

- ServerView Suite の現在のソフトウェアバージョンおよびその他の Readme ファイル。
- ServerView Update Manager により PRIMERGY サーバをアップデートする場合、および ServerView Update Manager Express により個々のサーバをローカルでアップデートする場合の、システムソフトウェアコンポーネントの情報ファイルおよびアップデートセット。
- ServerView Suite のすべてのドキュメントの最新バージョン。

ダウンロードは富士通 Web サーバから無償で入手できます。

PRIMERGY サーバには、以下のトピックに関するリンクがあります。

- サポートデスク
- マニュアル
- 製品情報
- スペアカタログ

リンク集へのアクセス

ServerView Suite のリンク集へアクセスする方法はいくつかあります。

1. ServerView Operations Manager から。

   ► 開始ページまたはメニューバーで *ヘルプ – リンク*を選択します。

   ServerView リンク集の開始ページが開きます。

2. ServerView Suite DVD 2 から、または 富士通マニュアルサーバで ServerView Suite のオンラインドキュメントの開始ページを使用する。

   次のリンクを使用して、オンラインドキュメントの開始ページにアクセスします。

   http://manuals.ts.fujitsu.com

   ► 左側の選択リストで *Industry standard servers* を選択します。

   ► メニュー項目 *PRIMERGY ServerView Links* をクリックします。

   ServerView リンク集の開始ページが開きます。

3. ServerView Suite DVD 1 から。

   ► ServerView Suite DVD 1 の開始ウィンドウで、*Select ServerView Software Products* を選択します。

   ► *Start* をクリックします。ServerView Suite のソフトウェア製品が表示されるページが開きます。

   ► メニューバーで *Links* を選択します。

   ServerView リンク集の開始ページが開きます。

1.9 ServerView Suite のマニュアル

ServerView Suite のマニュアルは、各サーバシステムに付属の ServerView Suite DVD 2 に収録されています。

マニュアルはインターネットからも無料でダウンロードできます。インターネットのオンラインドキュメントは、*http://manuals.ts.fujitsu.com* の *Industry standard servers* リンクをクリックすると入手できます。

1.10 本文中の記号

本ユーザーガイドで使用している記号には、次の意味があります。

 **注意**	健康障害の兆候もしくはデータ消失やハードウェア障害にいたる可能性のある危険に対する注意を喚起
	重要な情報およびヒント
►	実行するべきアクション
イタリックテキスト	コマンドおよびメニュー項目、ボタン名、オプション名、ファイル名、パス名
< テキスト >	最新値で置き換えるべき変数
固定スペースフォント	システム出力
固定スペースフォント 太字固定スペースフォント	キーボード入力するコマンドは太字の等幅フォント
[大括弧]	オプション項目
{ 中括弧 }	「|」で区切られた選択項目
[キーボード] [記号]	キーはキーボード記号で表示。大文字入力が必要な場合は、たとえば 大文字の A に対して ［シフト］-［A］と表示 複数キーを同時に押す場合は、キーボード記号間をハイフンで結ぶ。

表 2: 表記規約

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 iRMC S2/S3 初期設定接続

iRMC S2/S3 への接続は、初期設定のまま一切の設定なしで行えます。

2.1 接続要件

リモート管理端末：

– Windows: Internet Explorer バージョン 7.x 以降
Linux: Mozilla Firefox 3.x 以降

– コンソールリダイレクション：
Sun Java Virtual Machine バージョン 1.5.0_06 以降

ネットワーク：

– ネットワーク上に DHCP サーバが必要です。

– IP アドレスではなく英字名で、iRMC S2/S3 Web インターフェースにログインする場合、ネットワーク上の DHCP サーバはダイナミック DNS 設定されている必要があります。

– DNS の設定が必要です。設定していないと、IP アドレスを要求されます。

2.2 iRMC S2/S3 の初期設定値

管理者 ID および iRMC S2/S3 の DHCP 名の初期設定値は、iRMC S2/S3 ファームウェアにあります。

管理者 ID の初期設定値 :

「*管理者 ID*」: *admin*

「*パスワード*」: *admin*

管理者 ID およびパスワードは、両方とも大文字と小文字を区別します。

セキュリティ上、最初のログイン後に新しい管理者アカウントを作成し、管理者アカウントの初期設定値は削除するようにしてください。最低でも、パスワードの変更は必ず行ってください。265 ページ の「ユーザ管理 - ユーザの管理」の項を参照してください。

DHCP 取得 IP の DNS 登録名 初期設定値（iRMC S2/S3）

DHCP 取得 IP の DNS 初期名（iRMC S2/S3）は、次のフォーマットになっています。
「*IRMC < シリアル番号 >*」

シリアル番号は、iRMC S2/S3 の MAC アドレスの最後の 3 バイトです。iRMC S2/S3 の MAC アドレスは、使用している PRIMERGY サーバのラベルに記載されています。

ログイン後、iRMC S2/S3 の MAC アドレスは、241 ページ の「ネットワークインターフェース設定 - iRMC S2/S3 のイーサネット設定」の項のページの欄上に read-only で表示されます。

2.3 iRMC S2/S3 Web インターフェースでのログイン

► リモート管理端末上の Web ブラウザを開き、iRMC S2/S3 の DNS 名もしくは IP アドレスを入力してください。

iRMC の DNS 名は使用している PRIMERGY サーバのラベルに記載されています。

次のログインプロンプトが表示されます。

図 6: iRMC S2/S3 Web インターフェースログインプロンプト

ログインプロンプトが表示されない場合は、LAN の接続状態を確認してください。46 ページ の「LAN インターフェースのテスト」の項を参照してください。

► アカウントの初期値を入力してください。

「*ユーザー名*」: admin

「*パスワード*」: admin

► [*OK*] を押して確認してください。

iRMC S2/S3 Web インターフェースについては、150 ページ の「システム情報 - サーバに関する情報」の項を参照してください。

3 iRMC S2/S3 の設定

iRMC S2/S3 の設定は、次のツールで行います。

– BIOS ／ TrustedCore ／ UEFI セットアップユーティリティ（42 ページ）

– iRMC S2/S3 Web インターフェース（139 ページ）

– Server Configuration Manager （351 ページ）

本章では、次の事項について説明しています。

– BIOS ／ TrustedCore セットアップユーティリティによる LAN インターフェースの設定（42 ページ）

– BIOS ／ TrustedCore ／ UEFI セットアップユーティリティによる LAN を経由したテキストコンソールのリダイレクションの設定（47 ページ）

– iRMC S2/S3 シリアルインターフェースの設定および使用（56 ページ）

– iRMC S2/S3 の Web インターフェースの設定（63 ページ）

3.1 iRMC S2/S3 LAN インターフェースの設定

次の事項について説明しています。

– LAN インターフェースの必要条件

– BIOS ／ TrustedCore® ／ UEFI セットアップユーティリティの LAN インターフェースの設定

– LAN インターフェースのテスト

iRMC S2 接続の「スパニングツリー」のツリーは、停止しておいてください。（例：「Port Fast=enabled; Fast Forwarding=enabled」）

3.1.1 必要条件

IP アドレスの設定に関しては、次の点に注意する必要があります。

– LAN ケーブルが正しいポートに接続されている必要があります。40 ページ の「正しい LAN ポートへの接続」の項を参照してください。

– iRMC S2 およびシステムの IP アドレス間の相互動作。41 ページ の「iRMC S2/S3 とシステムの IP アドレス間相互動作」の項を参照してください。

3.1.1.1 正しい LAN ポートへの接続

LAN 接続インターフェースは、iRMC S2 に適用されたオンボード LAN コントローラ上にあります。26 ページ の図 4 を参照してください

PRIMERGY サーバには、システムボードの LAN インターフェースが 2 つのものと 3 つのものとがあります。レンチ記号がついているポートが、iRMC S2 用ポートです。40 ページ の図 7 のポート 1 および左上のポートです。

LAN ケーブルが正しいポートに接続されていることを確認してください。

レンチ記号がついているポートは、PRIMERGY サーバによって異なります。

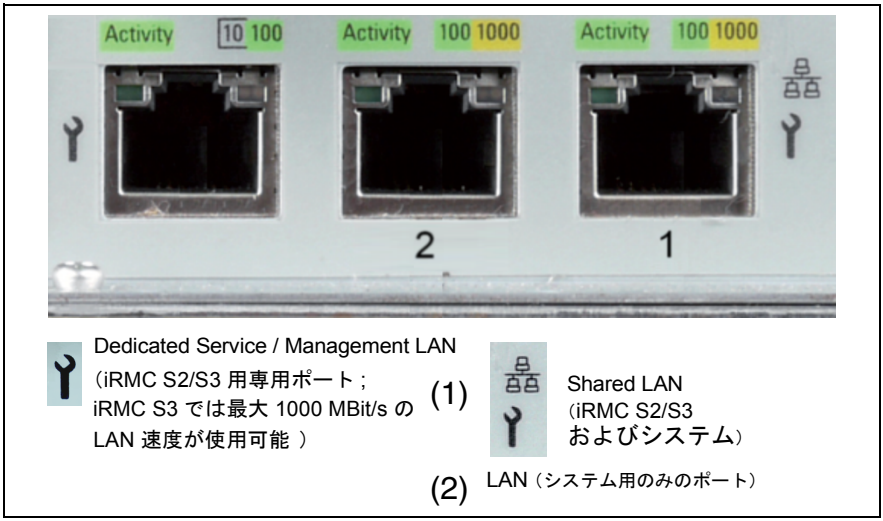


図 7: iRMC S2/S3 用ポート（レンチ記号で示した箇所）

3.1.1.2 iRMC S2/S3 とシステムの IP アドレス間相互動作

オペレーティングシステムではなく iRMC S2/S3 に確実にデータパケットを転送するために、PRIMERGY サーバの LAN コントローラには、iRMC S2/S3 専用の IP アドレスが必要です。

iRMC S2/S3 の IP アドレスは、システム（オペレーティングシステム）とは別でなければなりません。

3.1.1.3 他のサブネットからのアクセス

リモート管理端末が、DHCP を使用しないで管理対象サーバの iRMC S2/S3 に別サブネットからアクセスする場合、ゲートウェイを設定する必要があります。

3.1.2 LAN インターフェースの設定：Configuration tools

iRMC S2/S3 の LAN インターフェースの設定には、いくつかの方法があります。

PRIMERGY サーバの機種によって、設定方法が異なります。

- BIOS セットアップユーティリティもしくは TrustedCore（42 ページ）
- iRMC S2/S3 Web インターフェースの使用（240 ページ の「ネットワーク設定 - LAN パラメータの設定」の項を参照してください）。
- サーバの設定を使用（351 ページ の「Server Configuration Manager を使用した iRMC S2/S3 の設定」の章を参照してください）。

3.1.3 BIOS/TrustedCore/UEFI セットアップユーティリティを使用した LAN インターフェースの設定

iRMC S2/S3 の LAN インターフェースを、BIOS/TrustedCore/UEFI セットアップユーティリティを使用して設定できます。

– BIOS/TrustedCore セットアップユーティリティを使用して、iRMC S2 の LAN インターフェースを設定します。

– UEFI（**U**nified **E**xtensible **F**irmware **I**nterface）セットアップユーティリティを使用して、iRMC S3 の LAN インターフェースを設定します。

3.1.3.1 BIOS ／ TrustedCore セットアップユーティリティによる LAN インター フェースの設定

IPv6 アドレスは BIOS/TrustedCore セットアップユーティリティではサポートされていません。

▶ 管理サーバの BIOS / TrustedCore セットアップユーティリティを起動します。サーバの起動時に ［F2］ を押してください。

▶ LAN パラメータ設定メニューを起動します。

– BIOS :「*Advanced*」–「*IPMI*」– 「*LAN Setting*」

– TrustedCore :「*Server*」–「*IPMI*」–「*LAN Setting*」

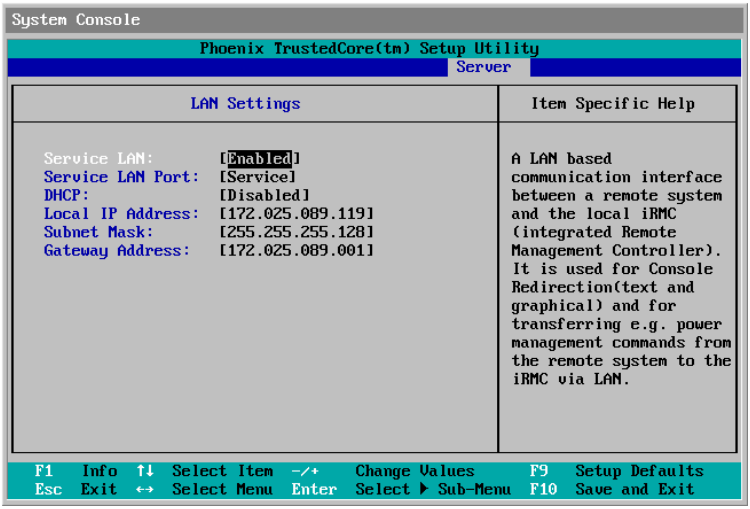


図 8: LAN 設定メニュー（TrustedCore セットアップユーティリティの場合）

► 次の設定を行ってください。

「*Service LAN*」
「*Enabled*」に設定してください。

「*Service LAN Port*」
「*Service*」に設定することを推奨します。

TX150 S6 PRIMERGY の場合は、必ず「Service」に設定してください。

「*DHCP*」
DHCP を有効にした場合、iRMC S2 の LAN 設定はネットワーク上の DHCP サーバから自動的に行われます。「*Local IP Address*」、「*Subnet Mask*」などの値も自動的に設定されます。

利用できる DHCP サーバがない場合には、DHCP オプションを有効にしないでください。iRMC S2 は常時 DHCP サーバをサーチしており、利用できる DHCP サーバがない場合に DHCP オプションを有効にするとサーチがループします。

iRMC S2 Web インターフェースから DHCP および DNS サービスの利用を指定できます。これについては、251 ページ の「DNS 構成 - iRMC S2/S3 の DNS の設定」の項を参照してください。
何も指定しない場合、iRMC S2 の DHCP 初期設定時には DHCP *前がわたされます：「iRMC ＜MAC アドレスの最後の 3 バイト＞」*。

「*Local IP Address*」
管理するシステムの iRMC S2 の IP アドレスを入力します

「*Subnet Mask*」
ネットワークのサブネットマスクを入力します。

「*Gateway Address*」
ゲートウェイの IP アドレスを入力します。

- ► 設定を保存します。
- ► iRMC S2 のコンソールリダイレクションを使用する場合は、47 ページ の「BIOS ／ TrustedCore ／ UEFI セットアップユーティリティによる LAN を経由したテキストコンソールのリダイレクションの設定」の項 の記述にしたがって設定を続けてください。

  iRMC S2 のテキストコンソールのリダイレクションを使用しない場合は、BIOS/TrustedCore 設定を終了し、46 ページ の「LAN インターフェースのテスト」の項の記述にしたがって設定を続けてください。

3.1.3.2 UEFI セットアップユーティリティを使用した iRMC S3 の LAN インターフェースの設定

► 管理対象サーバの UEFI セットアップユーティリティを呼び出します。
サーバの起動中に F2 を押します。

► 「*iRMC LAN parameter configuration*」メニューを呼び出します。

「Server Mgmt」- 「iRMC LAN Parameters Configuration」

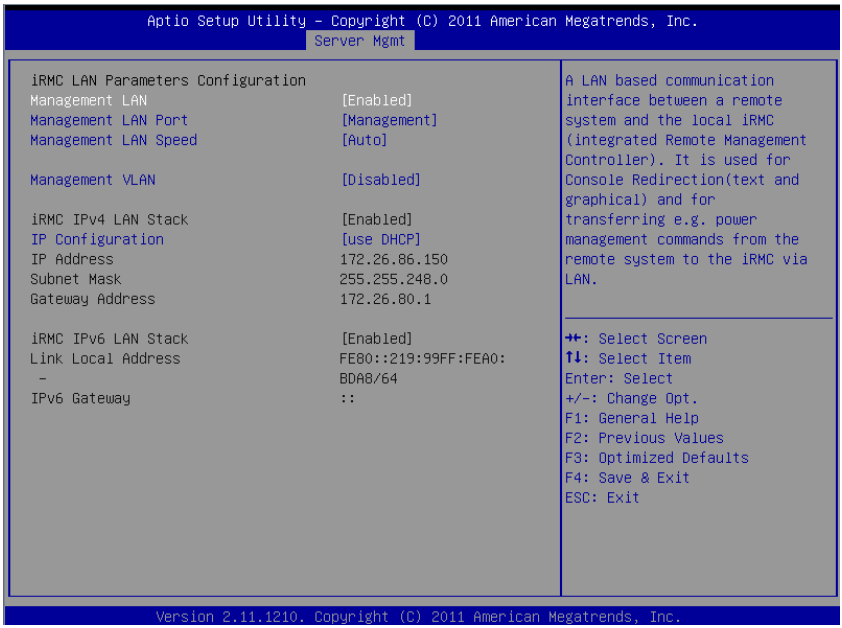


図 9: 「iRMC LAN Parameters Configuration」メニュー

► 以下の設定を行います。

Management LAN
値を「*Enabled*」に設定します。

Management LAN Port
「*Management*」設定を推奨します。

残りの設定の指定方法については、240 ページ の「ネットワーク設定 - LAN パラメータの設定」の項を参照するか、またはお使いのサーバの『BIOS (Aptio) Setup Utility』マニュアルを参照してください。

► 設定を保存します。

► iRMC S3 でコンソールリダイレクションを使用する場合は、52 ページ の「iRMC S3 のテキストコンソールリダイレクションの設定」の項の記述にしたがって設定を続けてください。

iRMC S3 でテキストコンソールリダイレクションを使用しない場合は、UEFI セットアップを終了して、次の「LAN インターフェースのテスト」の項に進みます。

3.1.4 LAN インターフェースのテスト

次の手順で、LAN インターフェースをテストします。

► Web ブラウザから、iRMC S2/S3 Web インターフェースにログインしてください。ログインプロンプトが表示されない場合には、LAN インターフェースが動作していない可能性があります。

► Ping コマンドで、iRMC S2/S3 接続をテストしてください。

3.2 BIOS ／ TrustedCore ／ UEFI セットアップユーティリティによる LAN を経由したテキストコンソールのリダイレクションの設定

テキストコンソールのリダイレクション設定およびサーバのオペレーティングシステムにより、テキストコンソールのリダイレクションには 2 種類の利用方法があります。

– BIOS POST フェーズ終了時にテキストコンソールのリダイレクションを停止する。

– BIOS POST フェーズ終了後も、オペレーティングシステムが稼働している間はテキストコンソールのリダイレクションが利用可能である。

本節では、次の事項を説明します。

– BIOS ／ TrustedCore セットアップユーティリティによる LAN をとおしたテキストコンソールのリダイレクションの設定

– UEFI セットアップユーティリティを使用した LAN 経由のテキストコンソールリダイレクションの設定（iRMC S3 向け）

– オペレーティングシステムの稼働中にコンソールリダイレクションを行う場合に考慮するべきオペ レーティングシステムの特別な必要条件

iRMC S2/S3 Web インターフェースからも LAN を通したテキストコンソールのリダイレクションを設定できます。294 ページ の「BIOS テキストコンソール - テキストコンソールのリダイレクションの 設定と開始」の項を参照してください。

3.2.1 iRMC S2 のテキストコンソールリダイレクションの設定

► 管理対象サーバの BIOS ／ TrustedCore セットアップユーティリティを起動します。サーバの起動中に ［F2］ を押してください。

Peripheral Configuration Menu 設定

► Peripheral Configuration Menu を起動します。

「*Advanced*」– 「*Peripheral Configuration*」

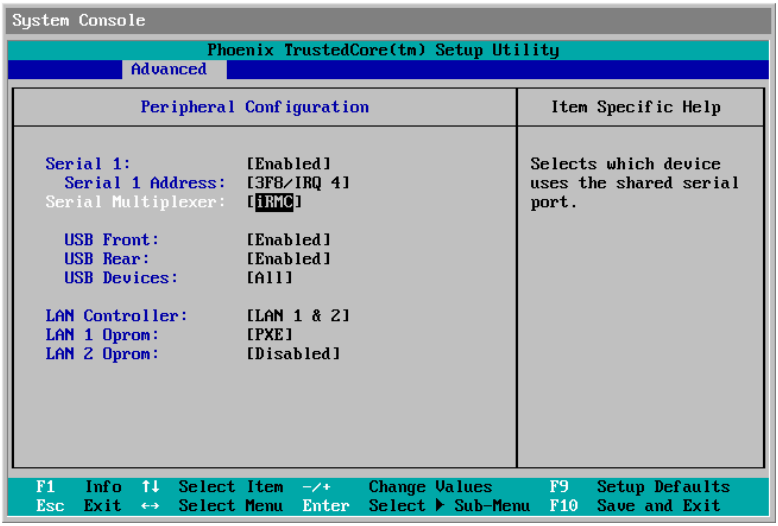


図 10: 周辺機器設定メニュー（TrustedCore セットアップユーティリティ表示）

► 次の設定を行ってください。

「*Serial 1*」

「*Enabled*」に設定してください。

「*Serial 1 Address*」

最初に表示されたペア値を使用してください。

「*Serial Multiplexer*」

「*iRMC*」に設定してください。

Console Redirection Menu 設定

► *Console Redirection* Menu を起動してください。

「*Server*」–「*Console Redirection*」

表示される Console Redirection Menu のイメージは、ご使用のセットアップユーティリティ（BIOS もしくは TrustedCore）によって異なります。

► **BIOS** セットアップユーティリティで次の設定を行ってください

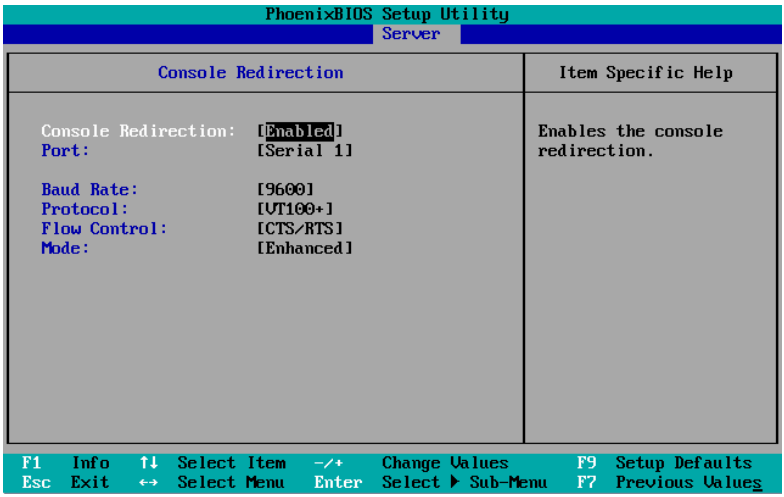


図 11: コンソールリダイレクションメニュー（BIOS セットアップユーティリティ表示）

「*Console Redirection*」
「*Enabled*」に設定してください。

「*Port*」
「*Serial 1*」に設定してください。

「*Baud Rate*」
ボーレートを指定してください。

「*Protocol*」
設定を変更しないでください（使用しているターミナルによって異なります）。

「*Flow Control*」
設定を変更しないでください（使用しているターミナルによって異なります

「*Mode*」

POST フェーズ終了後、オペレーティングシステム稼働中のコンソールリダイレクションの動作を指定します。54 ページ の「OS 動作中のコンソールリダイレクションの使用」の項を参照してください。

「*Standard*」

BIOS POST フェーズ終了時にコンソールリダイレクションを停止します。

「*Enhanced*」

BIOS POST フェーズ終了後もコンソールリダイレクションを利用できます。

- **TrustedCore** セットアップユーティリティで次の設定を行ってください。

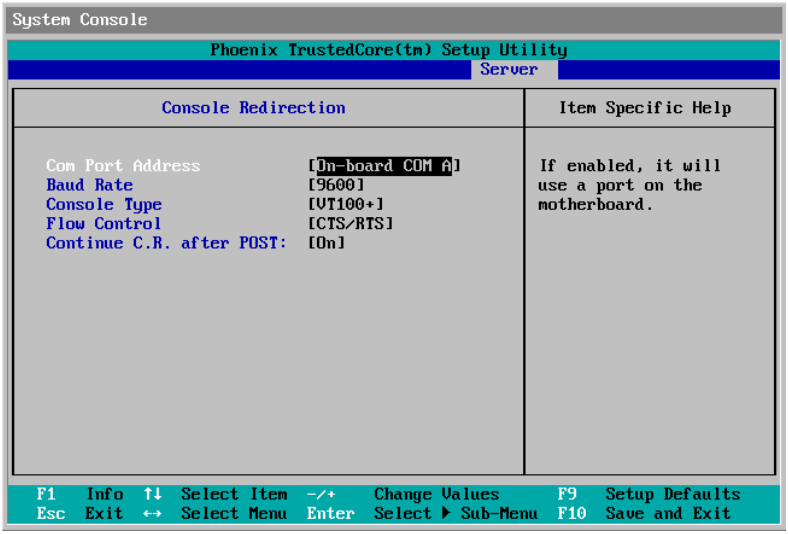


図 12: コンソールリダイレクションメニュー（TrustedCore セットアップユーティリティ表示）

「*Com Port Address*」

「*On-board COM A*」に設定してください。

「*Baud Rate*」

ボーレートを指定してください。

「*Console Type*」
設定を変更しないでください（ご使用のターミナルによって異なります）

「*Flow Control*」
設定を変更しないでください（ご使用のターミナルによって異なります）。

「*Continue C.R. after POST*」
POST フェーズ終了後、オペレーティングシステム稼働中のコンソールリダイレクションの動作を指定します。54 ページ の「OS 動作中のコンソールリダイレクションの使用」の項を参照してください。

「*Off*」
BIOS POST フェーズ終了時にコンソールリダイレクションを停止し。

「*On*」
BIOS POST フェーズ終了後もコンソールリダイレクションを利用できます。

BIOS / TrustedCore セットアップの終了

- 設定を保存して、BIOS/TrustedCore セットアップユーティリティを終了してください
- 46 ページ の「LAN インターフェースのテスト」の項の記述に従って設定を続行してください。

3.2.2 iRMC S3 のテキストコンソールリダイレクションの設定

- ► 管理対象サーバの UEFI セットアップユーティリティを呼び出します。サーバの起動中に F2 を押します。
- ► 「*Server Mgmt*」メニューを呼び出します。

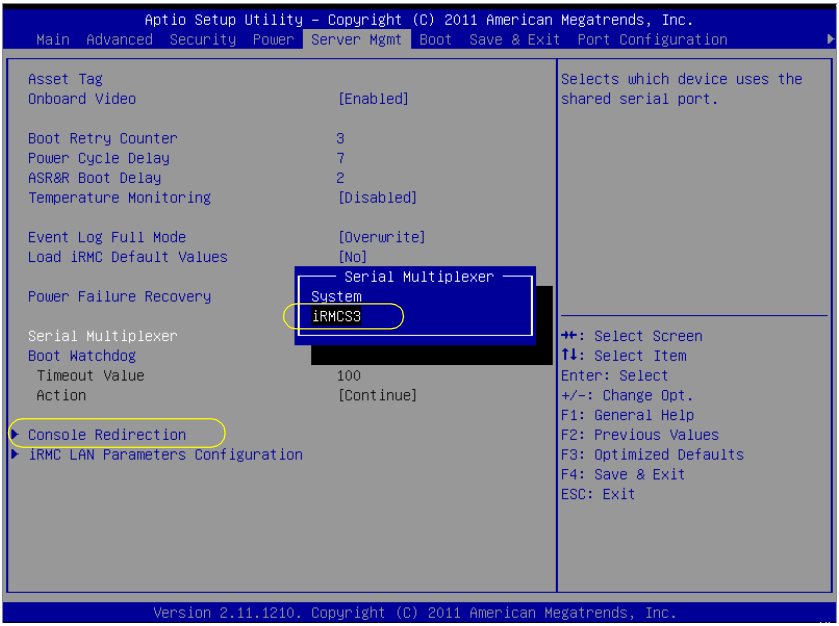


図 13: 「Server Mgmt」メニュー

- ► 以下の設定を行います。

Serial Multiplexer

値を「*iRMCS3*」に設定します。

► 「*Console Redirection*」メニューを呼び出します。

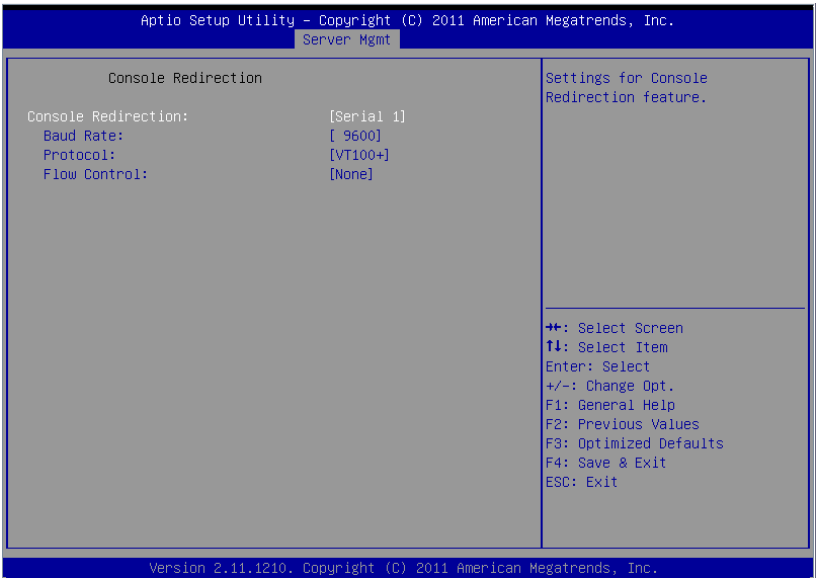


図 14: 「Console Redirection」メニュー

► 「*Console Redirection*」メニューで次の設定を行います。

Console Redirection

値を「*Serial 1*」に設定します。この場合、ターミナルは最初のシリアルインターフェースを使用します。

Baud Rate

ボーレートを指定します。

Protocol

この設定は変更しません （設定は使用するターミナルのタイプに依存します）。

Flow Control

設定は使用するターミナルのタイプに依存します。設定は、ターミナルと管理対象サーバで同一にする必要があります。

UEFI セットアップユーティリティの終了

► 設定を保存して、UEFI セットアップユーティリティを終了します。

► 46 ページ の「LAN インターフェースのテスト」の項に進みます。

3.2.3 OS 動作中のコンソールリダイレクションの使用

管理対象サーバのオペレーティングシステムによっては、BIOS POST フェーズの終了後もコンソールリダイレクションを使用することができます。

DOS

コンソールリダイレクションモードの BIOS 設定は、次のように行ってください。49 ページ の「Console Redirection Menu 設定」を参照してください。

– BIOS セットアップユーティリティ：「*Mode: Enhanced*」

– TrustedCore セットアップユーティリティ：「*Continue C.R. after POST: On*」

Windows Server 2003/2008

Windows インストール中に有効にした場合は、コンソールリダイレクションは自動的に設定されます。

コンソールリダイレクションが Windows インストールの完了後に有効にされた場合は、コンソールリダイレクションを手動で設定する必要があります。

Windows Server 2003 / 2008 では、POST フェーズの終了後、コンソールリダイレクションは自動的に処理されます。設定は一切不要です。オペレーティングシステム起動中は、Windows Server 2003 SAC コンソールが転送されます。

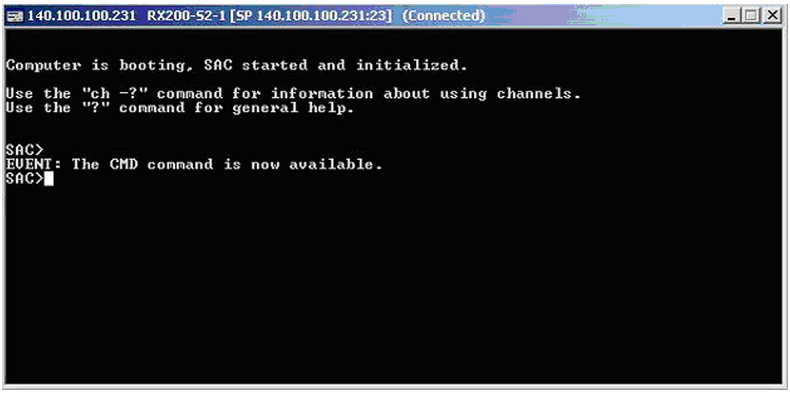


図 15: Windows Server 2003 SAC コンソール

Linux

POST フェーズの終了後もコンソールリダイレクションを処理するように、Linux オペレーティングシステムを設定する必要があります。設定すれば、リモート管理端末から無制限にアクセスできます。

設定項目

プログラムのバージョンによって設定が異なります。

SuSE および RedHat（SuSE は未サポート）
次の行を、*/etc/inittab* ファイルの最後に追加してください。

「xx:12345:respawn:/sbin/agetty < ボーレート > ttyS0」

RedHat
次のカーネル起動パラメータを /etc/grub.conf ファイルに追加してください。

「console=ttyS0,< ボーレート > console=tty0」

SuSE（未サポート）
次のカーネル起動パラメータを /boot/grub/menu.lst ファイルに追加してください。

「console=ttyS0,<baud-rate> console=tty0」

3.3 iRMC S2/S3 シリアルインターフェースの設定および使用

iRMC S2/S3 のシリアルインターフェースでは、次のことが可能です。

– ヌルモデムケーブル（RS-232C のクロスケーブル）により端末アプリケーションリモートマネージャ（シリアル）を使用できます。62 ページ の「シリアル接続管理インターフェースの利用方法」の項を参照してください。

– **iRMC S2 のみ：**モデムにより警告を転送できます。iRMC S2 の Web インターフェースから設定します。257 ページ の「シリアル / モデム通知設定 - モデム経由通知設定」の項を参照してくだ。

3.3.1 iRMC S2 を使用したシリアルインターフェースの設定

BIOS の設定

- 管理対象サーバの BIOS ／ TrustedCore セットアップユーティリティを起動します。サーバの起動中に［F2］を押してください。
- Peripheral Configuration Menu（周辺機器設定メニュー）を起動してシリアルポートを設定してください。

  「*Advanced*」– 「*Peripheral Configuration*」

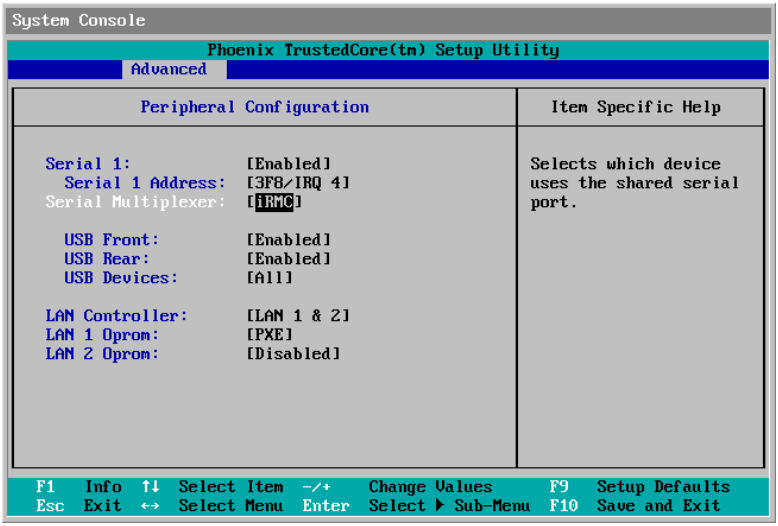


図 16: 周辺機器設定メニュー（TrustedCore セットアップユーティリティ表示）

- 次の設定を行ってください。

  「*Serial 1*」
  「*Enabled*」に設定してください。

  「*Serial 1 Address*」
  最初に表示されたペア値を使用してください。

  「*Serial Multiplexer*」
  iRMC に設定してください。

次の値はメニューには表示されませんが、事前に設定されています。
62 ページ の「端末プログラム（VT100+）：」を参照してください。

「*Bits per second*」
9600 に設定してください。

「*Data bits*」
8 に設定してください。

「*Parity*」
「*None*」に設定してください。

「*Stop bits*」
1 に設定してください。

「*Flow Control*」
「*None*」に設定してください。

BIOS ／ TrustedCore セットアップの終了

- 設定を保存して、BIOS ／ TrustedCore セットアップユーティリティを終了してください。
- 46 ページ の「LAN インターフェースのテスト」の項の記述に従って設定を続行してください。

3.3.2 iRMC S3 を使用したシリアルインターフェースの設定

► 管理対象サーバの UEFI セットアップユーティリティを呼び出します。サーバの起動中に F2 を押します。

► 「*Server Mgmt*」メニューを呼び出します。

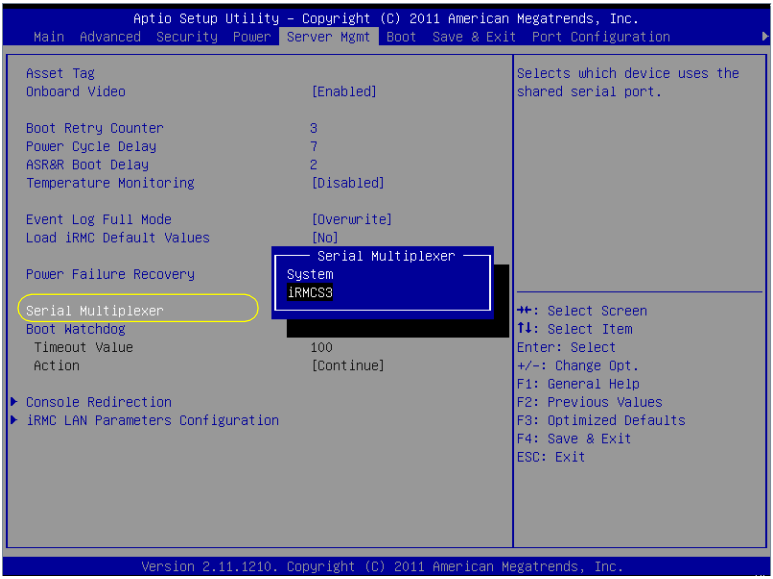


図 17: 「Server Mgmt」メニュー

► 以下の設定を行います。

Serial Multiplexer

値を「*iRMCS3*」に設定します。

► 「*Serial Port 1 Configuration*」メニューを呼び出して、シリアルポートを設定します。

「Advanced」– 「*Super IO Configuration*」– 「*Serial Port 1 Configuration*」:

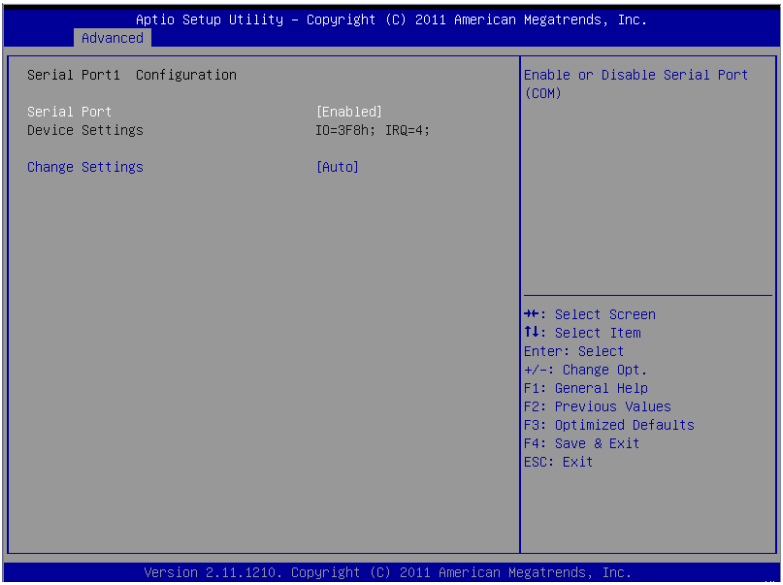


図 18: Serial Port 1 設定メニュー

► 次の設定を行ってください。

「*Serial Port*」
「*Enabled*」に設定してください。

「*Device Settings*」
ベース I/O アドレスと、対応するシリアルポートへのアクセスに使用される割り込みを表示します（IO=3F8h; IRQ=4 など）。

指定された値のペアを受理します。

以下の値はメニューには表示されず、事前に設定されています（62 ページの「端末プログラム（VT100+）」を参照）。

「*Bits per second*」
9600 に設定してください。

「*Data bits*」
8 に設定してください。

「*Parity*」
「*None*」に設定してください。

「*Stop bits*」
1 に設定してください。

「*Flow Control*」
「*None*」に設定してください。

UEFI セットアップユーティリティの終了

► 設定を保存して、UEFI セットアップユーティリティを終了します。

► 46 ページ の「LAN インターフェースのテスト」の項に進みます。

3.3.3 シリアル接続管理インターフェースの利用方法

ヌルモデムケーブルでコンピュータを接続して端末プログラム（VT100+）を開始すると、シリアル接続端末プログラムにアクセスできます。シリアル接続管理インターフェースは、リモートマネージャインターフェースとまったく同じです。325 ページ の「Telnet/SSH 経由の iRMC S2/S3 (リモートマネージャ)」の章を参照してください。

前提条件

管理対象サーバ :

iRMC 上の「Serial Multiplexer BIOS」を設定する必要があります。57 ページ の「iRMC S2 を使用したシリアルインターフェースの設定」の項を参照してください。

端末プログラム（VT100+）:

次のように、端末プログラムのポートセッティングを行ってください。

「*Bits per second*」

9600 に設定してください。

「*Data bits*」

8 に設定してください。

「*Parity*」

「*None*」に設定してください。

「*Stop bits*」

1 に設定してください。

「*Flow Control*」

「*None*」に設定してください。

3.4 iRMC S2/S3 の Web インターフェースの設定

- iRMC S2 Web インターフェースを起動してください。140 ページ の「iRMC S2/S3 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。

3.4.1 LAN パラメータ設定

- ナビゲーション領域の ［*ネットワーク設定*］をクリックしてください。240 ページ の「ネットワーク設定 - LAN パラメータの設定」の項を参照してください。

LAN の設定

- 「*ネットワークインターフェース*」のページで LAN 設定を行ってください。設定の詳細については、240 ページ の「ネットワーク設定 - LAN パラメータの設定」の項を参照してください。

ポートとネットワークサービスの設定

- 「*ポートとネットワークサービス*」のページでポートおよびネットワークサービスを設定してください。設定の詳細については、255 ページ の「警告通知 - 警告通知の設定」の項を参照してください。

DHCP 設定

- 「*DHCP 設定*」のページで DHCP の設定を行ってください。設定の詳細については、265 ページ の「ユーザ管理 - ユーザの管理」の項を参照してください。

DNS 設定

- 「*DNS 設定*」のページで DNS の設定を行ってください。設定の詳細については、294 ページ の「コンソールリダイレクション - コンソールのリダイレクト」の項を参照してください。

3.4.2 通知の設定

通知設定のページは、ナビゲーション領域の 「*通知情報設定*」にまとめられています。255 ページ の「警告通知 - 警告通知の設定」の項を参照してください。

SNMP による通知送信の設定

- ナビゲーション領域の「*SNMP トラップ*」をクリックしてください。「*SNMP トラップ*」のページが表示されます。
- SNMP トラップ送信を設定してください。設定の詳細については、256 ページ の「SNMP トラップ送信設定 - SNMP トラップ通知の設定」の項を参照してください

モデムによる携帯電話への送信の設定 (iRMC S2 のみ)

- ナビゲーション領域の［*シリアル／モデム*」をクリックしてください。「シリアル／モデム通知」のページが表示されます。
- モデムによる送信を設定してください。設定の詳細については、257 ページ の「シリアル / モデム通知設定 - モデム経由通知設定」の項を参照してください。

E-mail 通知の設定（E-mail による通知）

- ナビゲーション領域の「*Email*」をクリックしてください。「*E-mail 通知*」のページが表示されます。
- E-mail 通知を設定してください。設定の詳細については、259 ページ の「Email 設定 - Email 送信設定」の項を参照してください。

3.4.3 テキストコンソールのリダイレクションの設定

- 「*BIOS テキストコンソール*」ウィンドウで、テキストコンソールのリダイレクションを設定してください。設定の詳細については、294 ページ の「BIOS テキストコンソール - テキストコンソールのリダイレクションの 設定と開始」の項を参照してください。

4 iRMC S2/S3 のユーザー管理

iRMC S2/S3 によるユーザー管理には 2 種類の異なるユーザー ID を使用します。

– ローカルユーザー ID は iRMC S2/S3 内部の不揮発性記憶装置に保存され、iRMC S2/S3 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 iRMC S2/S3 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
  – OpenDS

本章では以下について説明します。

– iRMC S2/S3 によるユーザー管理の概念
– ユーザー権限
– iRMC S2/S3 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 iRMC S2/S3 によるユーザー管理の概念

iRMC S2/S3 によるユーザー管理は、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 iRMC S2/S3 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、iRMC S2/S3 は以下のように処理します（合わせて 67 ページ の図 19 も参照してください）。

1. iRMC S2/S3 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、iRMC S2/S3 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、iRMC S2/S3 はステップ 2 の検証手順を継続します。
2. iRMC S2/S3 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 iRMC S2/S3 を操作する権限があるかどうかを確認します。

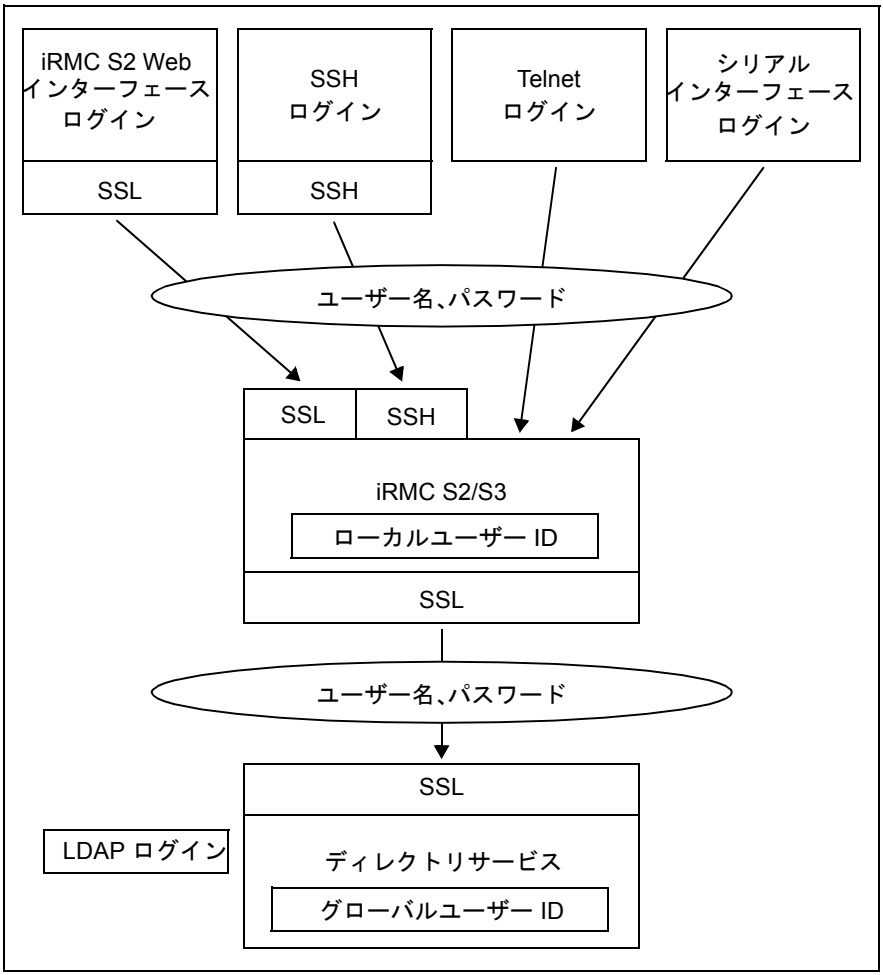


図 19: iRMC S2/S3 経由のログイン認証

iRMC S2/S3 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 iRMC S2/S3 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。

iRMC S2/S3 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、276 ページを参照）。

4.2 ユーザー権限

iRMC S2/S3 は以下の 2 つの相互補完的なユーザー権限を区別します。

– チャネル別の権限（チャネル別許可グループ割り当て）

– iRMC S2/S3 独自の機能によるアクセス許可

iRMC S2/S3 機能を使用するために必要な特権と許可は次の通りです。

– iRMC S2/S3 Web インターフェースについては、142 ページを参照

– リモートマネージャについては、333 ページを参照

チャネル別権限（チャンネル別許可グループ）

iRMC S2/S3 は各々のユーザー ID を次の 4 つの チャンネル別許可グループのうちのいずれかに割り当てます。

– User
– Operator
– Administrator
– OEM

iRMC S2/S3 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、iRMC S2/S3 に LAN 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 権限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権限レベルに関連づけられます。

iRMC S2/S3 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
- **iRMC S2/S3 設定の設定**
  iRMC S2/S3 設定を設定する許可
- **Video Redirection 許可**
  アドバンストビデオリダイレクション（AVR）を「ビューモード」、「フルコントロールモード」で使用する許可
- **リモートストレージ許可**
  リモートストレージ機能を使用する許可

初期設定のユーザー ID

iRMC S2/S3 のファームウェアには、iRMC S2/S3 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（265 ページ の「ユーザ管理 - ユーザの管理」の項を参照）。

4.3 iRMC S2/S3 のローカルユーザー管理

iRMC S2/S3 には 固有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、iRMC S2/S3 内部の不揮発性記憶装置に保存されます。ユーザー管理は手作業で、またはスクリプトを使用して操作できます。

iRMC S2/S3 上のユーザー管理には次のオプションが使用可能です。

– Web インターフェースによるユーザー管理
– Server Configuration Manager によるユーザー管理
– Server Management Tool （IPMIVIEW）によるユーザー管理

4.3.1 iRMC S2/S3 Web インターフェースによるローカルユーザー管理

iRMC S2/S3 上のユーザー管理には「*ユーザ アカウント変更権限*」が必要です。

設定されたユーザーのリストは Web インターフェースで表示できます。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。

► iRMC S2/S3 Web インターフェースを起動します（140 ページ の「iRMC S2/S3 Web インターフェースへのログイン」の項を参照）。

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」*-*「iRMC S2 ユーザ管理」*をクリックします。

*「ユーザ管理」*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（266 ページを参照）。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。
このページに関しては、265 ページ の「ユーザ管理 - ユーザの管理」の項に説明があります。

新しいユーザーの設定

► *「ユーザ管理」*ページで、*［ユーザの新規作成］*ボタンをクリックします。

*「新規ユーザの構成」*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。このページに関しては、267 ページ の「新規ユーザの構成 - 新規ユーザの構成」の項に説明があります。

ユーザーの設定変更

► *「ユーザ管理」*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 〈name〉の設定」*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。このページに関しては、268 ページ の「ユーザ “<name>” 構成 - ユーザ設定（詳細）」の項に説明があります。

ユーザーの削除

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

4.3.2 Server Configuration Manager でのローカルユーザー管理

前提条件：

管理対象サーバには最新の ServerView エージェントをインストールしておく必要 があります。

iRMC S2/S3 上のユーザー管理には*「ユーザ アカウント変更権限」*許可が必要です。

設定されたユーザーのリストは Server Configuration Manager で表示できます。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。

Server Configuration Manager を起動します 351 ページ の「Server Configuration Manager を使用した iRMC S2/S3 の設定」の章を参照)。

個々の Configuration Manager ダイアログの詳細は、Server Configuration Manager のオンラインヘルプを参照してください。

4.3.3 iRMC S2/S3 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、iRMC S2/S3 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、iRMC S2/S3 ユーザーの SSHv2 鍵を iRMC S2/S3 にアップロードし、iRMC S2/S3 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。

iRMC S2/S3 は以下の種類の公開鍵をサポートしています。

– SSH DSS（最低条件）
– SSH RSA（推奨）

iRMC S2/S3 へ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（86 ページを参照）。

公開鍵認証

iRMC S2/S3 の公開鍵認証は、おおむね以下のように処理されます。

iRMC S2/S3 にログインする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 iRMC S2/S3 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 iRMC S2/S3 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（74 ページを参照）。
2. ファイルから SSHv2 鍵を iRMC S2/S3 にアップロードします（78 ページを参照）。
3. *「PuTTY」* または *「ssh」* プログラムを iRMC S2/S3 への SSHv2 アクセス用に設定します（80 ページを参照）。

4.3.3.1 SSHv2 の公開鍵と秘密鍵の作成

SSHv2 の公開鍵と秘密鍵は以下の方法で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

次の手順に従います。

► ユーザーの Windows コンピュータで *PuTTYgen* を起動します。

PuTTYgen が起動すると次の画面が表示されます。

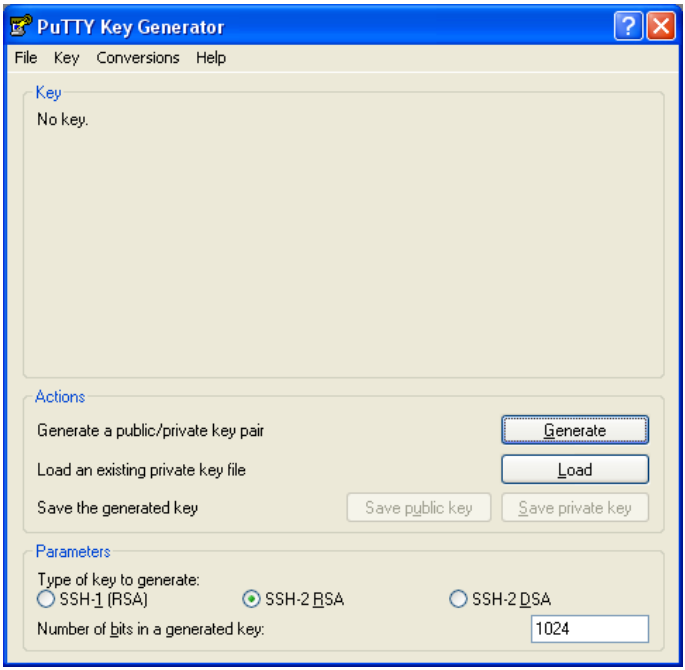


図 20: PuTTYgen：SSHv2 の新しい公開鍵と秘密鍵の作成

► *「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（75 ページ の図 21 を参照）。

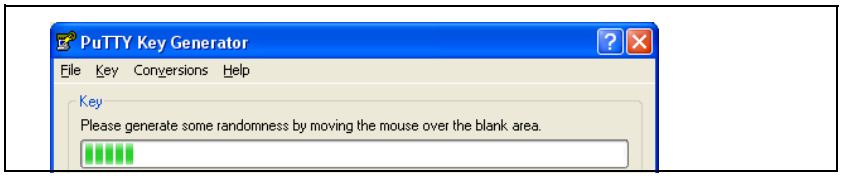


図 21: PuTTYgen：新しい鍵のペアの作成（プログレスバー）

► 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。

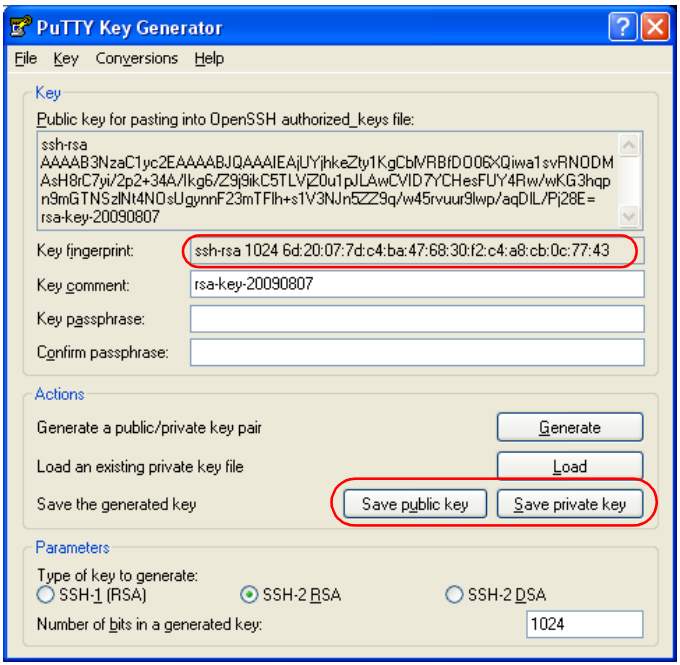


図 22: PuTTYgen：新しい秘密 SSHv2 鍵の作成（プログレスバー）

► *[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 iRMC S2 に公開鍵をアップロードすることができます（78 ページを参照）。

► *[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（80 ページを参照）。

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* で OpenSSH ユーザーガイドを参照してください。

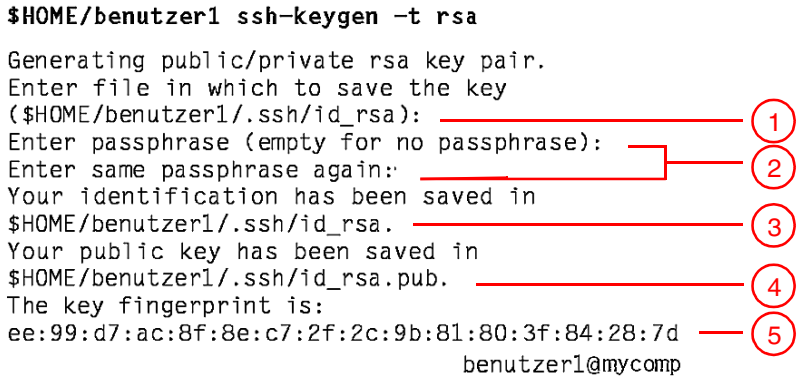
次の手順に従います。

- *「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



解説

1. 「*ssh-keygen*」は 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。

4.3.3.2 SSHv2 鍵のファイルから iRMC S2/S3 へのアップロード

次の手順に従います。

► iRMC S2 Web インターフェースで、「*iRMC S2/S3 ユーザ管理*」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。

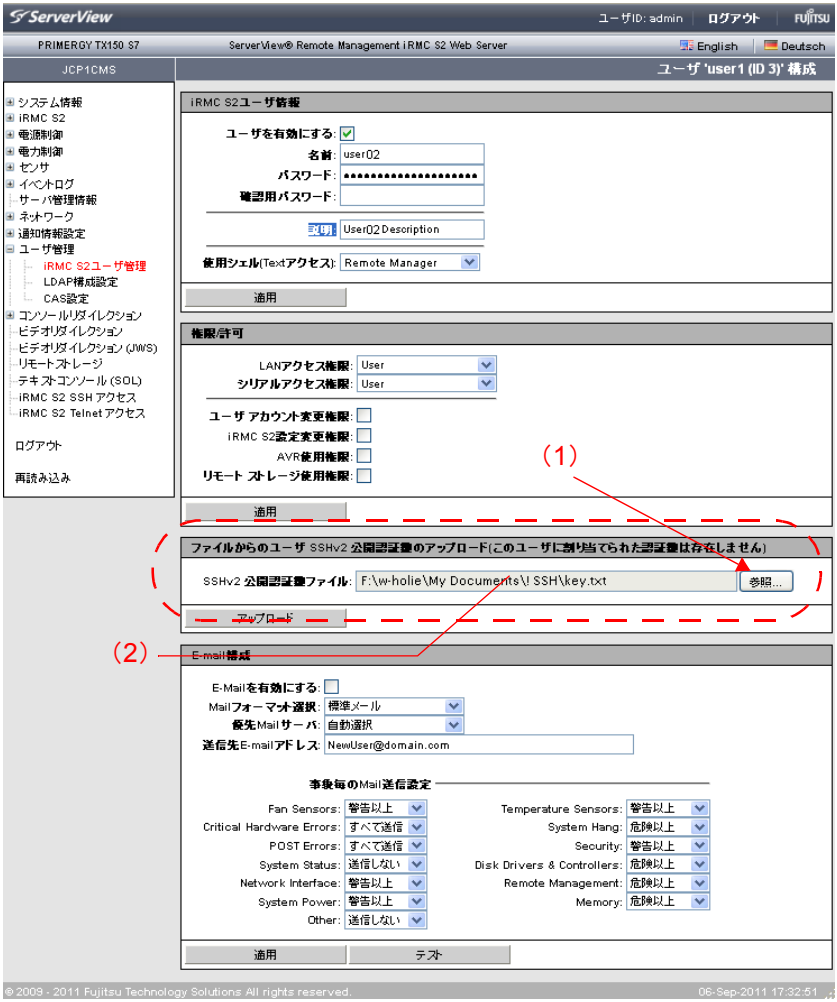


図 23: iRMC S2/S3 Web インターフェース：公開 SSHv2 鍵の iRMC S2/S3 へのアップロード

- *「ファイルからのユーザ SSHv2 公開認証鍵のアップロード」*グループの中の *［参照］*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］*ボタンをクリックして公開鍵を iRMC S2/S3 にアップロードします。

  鍵が正常にアップロードされると、iRMC S2/S3 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。

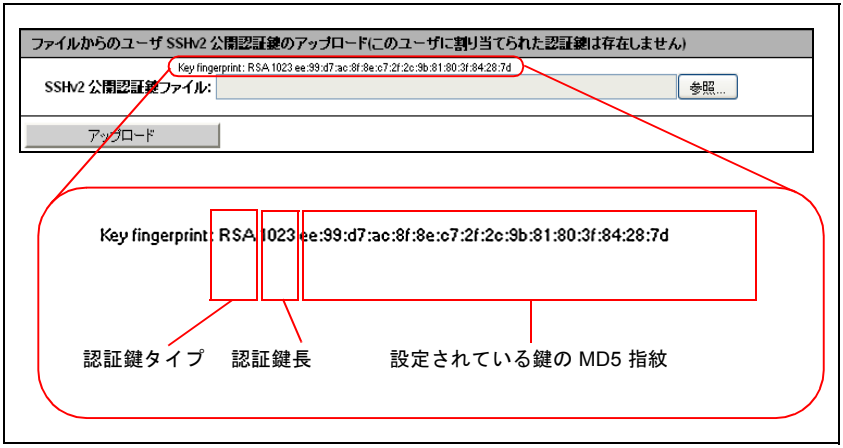


図 24: 鍵指紋の表示

セキュリティのため、ここに表示された鍵指紋が *PuTTYgen*（75 ページ の図 22 を参照）の *「鍵指紋」*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。

4.3.3.3 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、iRMC S2/S3 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。

次の手順に従います。

- ユーザーの Windows コンピュータで *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。

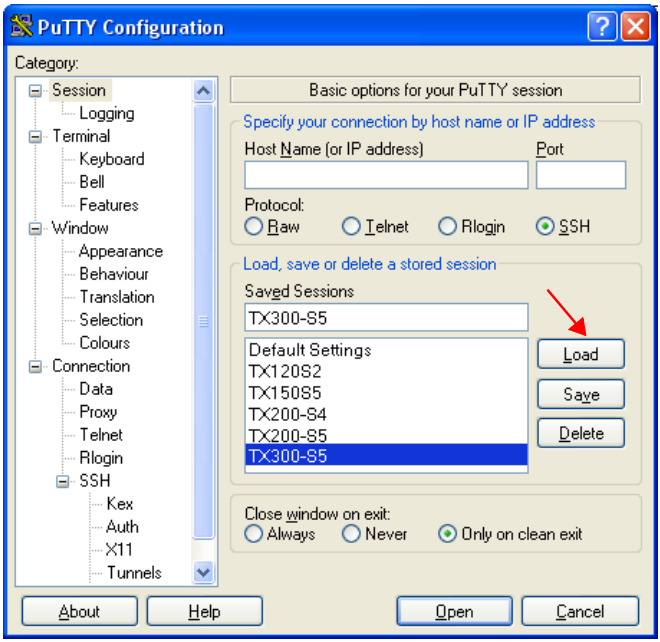


図 25: PuTTY：SSH セッションの選択とロード

- SSHv2 鍵を使用したい iRMC S2/S3 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きます。

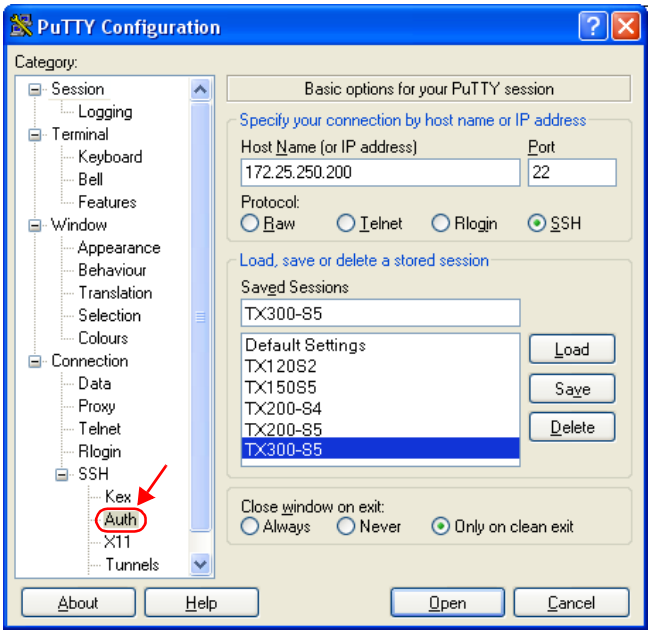


図 26: PuTTY : SSH セッションのロード

► *「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（82 ページ の図 27 を参照）。

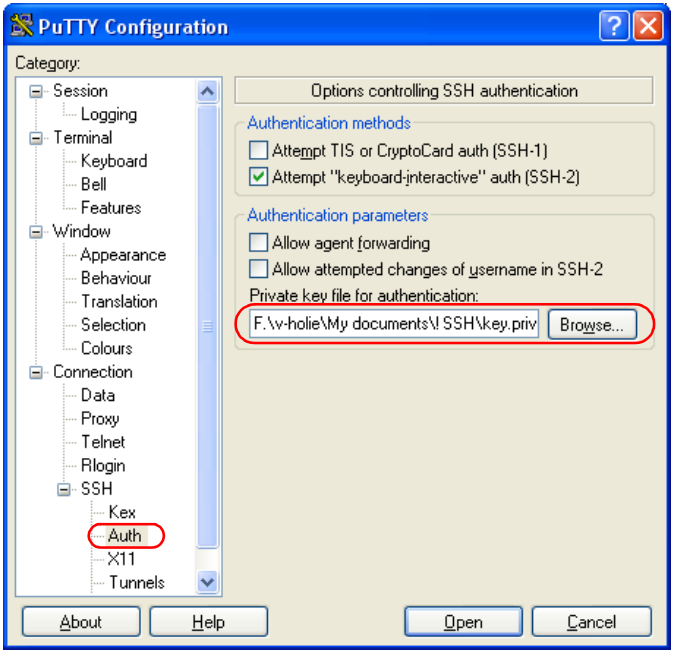


図 27: SSH 認証のオプションの設定

► iRMC S2/S3 で使用する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（75 ページを参照）であり、iRMC S2/S3 にロードされた公開鍵では**ありません**。

「*Connection - Data*」で、iRMC S2/S3 に自動ログインするユーザー名を追加指定できます。

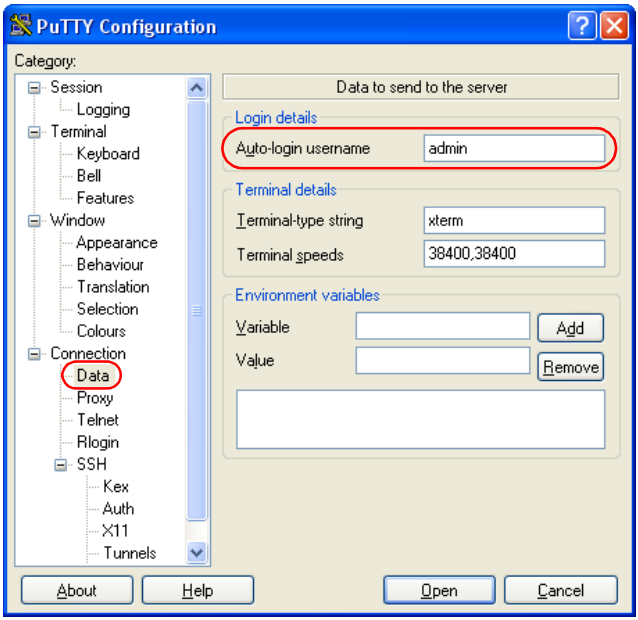


図 28: PuTTY：iRMC S2/S3 に自動ログインするユーザー名の指定

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 iRMC S2/S3 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、iRMC S2/S3 上のローカルログインとして設定され、関連する SSHv2 鍵は iRMC S2/S3 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しか付与しないでください。ほかのどのユーザーに対しても、アクセスを拒否してください。
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

次の手順に従います。

- 「*ssh*」を起動して、SSHv2 認証により iRMC S2/S3 にログインします。

  ssh -l [<user>] <iRMC_S2/S3>

  または

  ssh [<user>@]<iRMC_S2/S3>

  <user>
  : iRMC S2/S3 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、iRMC S2/S3 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。

  <iRMC_S2/S3>
  : ユーザーがログインしようとする iRMC S2/S3 名または、iRMC S2/S3 の IP アドレス。

例 : iRMC S2/S3 上の SSHv2 認証ログイン

次の *ssh* 呼び出しでは、76 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、iRMC S2 ユーザー *「user4」* のために iRMC S2 にロードされていると見なされます（78 ページを参照）。

ユーザーは自身のローカルコンピュータから、*「$HOME/User1」* でログインユーザー *「user4」* を使用して、以下のように iRMC S2 "RX100_S52-iRMC" にログインすることができます。

```
ssh user4@RX100_S52-iRMC
```

4.3.3.4 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
```

5 ビデオリダイレクション（AVR）

ビデオリダイレクション機能を使用するには有効なライセンスキーが必要です。

ビデオリダイレクション（AVR）を使用すると、管理対象管理対象サーバのマウスとキーボードをリモートの管理端末から操作することができ、管理対象サーバの現在のグラフィック画面とテキスト出力を表示させることができます。

AVR Java アプレットを使用するとリモートストレージ機能も使用できます。（113 ページ の「リモートストレージ」の章を参照してください。

本章では次の点について説明します :

– AVR 設定の確認
– AVR の使用
– AVR ウィンドウのメニュー

5.1 要求事項：AVR 設定の確認

AVR を使用する前に以下の重要な設定を確認してください。

管理対象サーバ上のグラフィックモード設定

AVR は下記のグラフィックモードをサポートします :

解像度	リフレッシュレート ［Hz］	最大色深度［ビット］
640 x 480 (VGA)	60; 75; 85	32
800 x 600 (SVGA)	56; 60; 72; 75; 85	32
1024 x 768 (XGA)	60; 70; 75; 85	32
1152 x 864	60; 70; 75	32
1280 x 1024 (UXGA)	60; 70; 75; 85	16
1280 x 1024 (UXGA)	60	24
1600 x 1200 (UXGA)	60; 65	16
1680 x 1050[1)]	60	16
1920 x 1080[1)]	60	16
1920 x 1200[1)]	60	16

表 3: サポート可能なディスプレイ設定

1. iRMC S3 のみ

サーバに高解像度のグラフィックモードが設定されている場合（表中で背景色がグレイになっているもの）は、iRMC S2/S3 Web インターフェース上で表示されます。

サポートされるのは VESA 準拠のグラフィックモードのみです。

サポートされるテキストモード

iRMC S2/S3 は下記の共通テキストモードをサポートします。

– 40 x 25
– 80 x 25
– 80 x 43
– 80 x 50

ディスプレイ設定の情報はお使いの OS のヘルプ画面から参照してください。

キーボード設定

以下のキーボード設定は同一でなければなりません。

– リモート管理端末上
– 管理対象サーバ
– iRMC S2/S3 上

5.2 AVR の使用方法

- AVR を起動させるには、iRMC S2/S3 Web インターフェース上の「*ビデオリダイレクション (AVR)* 」ページの［ ビデオ リダイレクションの開始］または［ビデオリダイレクション (JWS) ］ボタンをクリックしてください。（304 ページを参照してください。）

  「*ビデオリダイレクション*」ウィンドウ（AVR ウィンドウ）が開き、管理対象サーバ上のディスプレイが表示されます。

  AVR ウィンドウには以下の機能も含まれています。

  - メニューバー :「*設定*」および「*拡張機能*」メニューにより、AVR 設定しコントロールすることができます。（104 ページを参照してください。）「*リモートストレージ*」はリモートストレー ジ機能の呼び出しに使用します。（108 ページを参照してください。.
    「*言語*」メニュー（110 ページ参照）を使用すると、AVR ウィンドウのメニューとダイアログボックスに表示される言語（日本語／英語）を設定できます。
  - 統合された特殊キー（94 ページを参照してください）。
  - 「*サーバ側モニタ <status>*」インディケータは管理対象サーバのサーバ側モニタの電源ががオンになっているかどうかを表示します。（93 ページ の「サーバ側のモニタ ON/OFF 機能」の項を参照してください。）

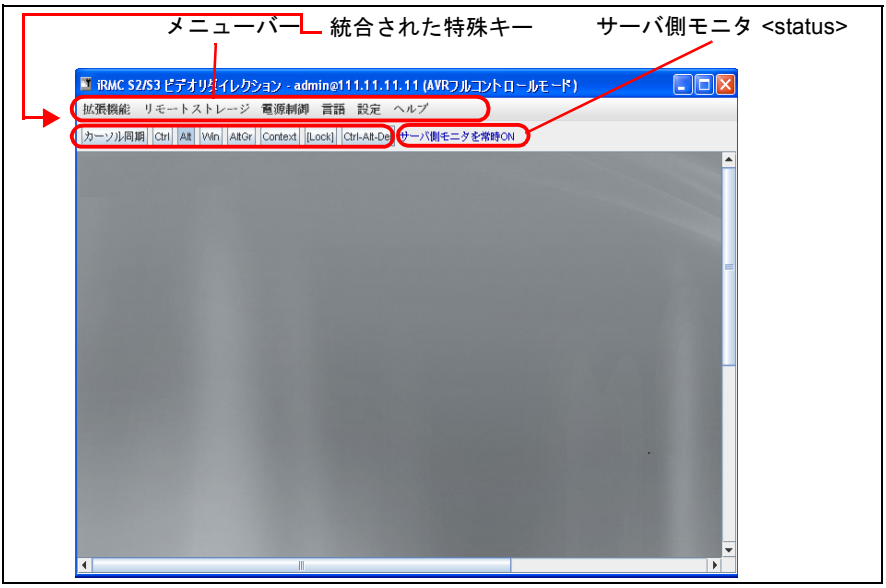


図 29: アドバンストビデオリダイレクション（AVR）ウィンドウ

5.2.1 低帯域幅の使用

データ転送速度が低下した場合、現在の AVR セッションの色深度に対する帯域幅（bpp、ビット / ピクセル）を低く設定できます（112 ページを参照）。

現在存在しているフルコントロールセッションによって、フルコントロールの取得が拒否される場合、セッションは参照モードのままになります。

5.2.2 AVR の複数接続

AVR は 2 つのユーザーセッションを同時に行うことができます。一方のユーザーはサーバをフルコントロールでき（フルコントロールモード）、他方のユーザーはサーバのキーボードとマウス操作を監視すること（ビューモード）ができます。

AVR を初めて起動すると最初にビューモードとなります。その後、フルコントロールモードに切り替えるかどうかが必ず尋ねられます。フルコントロールモードへ切り替えることを決定したときに、他にフルコントロールモードが使用されている場合には、そのセッションはビューモードに切り替えられます。

5.2.3 サーバ側のモニタ ON/OFF 機能

iRMC S2/S3 の「*サーバ側モニタ Off*」機能により、AVR セッションを行う間管理対象サーバのサーバ側モニタの電源をオフにすることができます。この方法により、AVR を使用してサーバ側モニタ上で行ったインプットや実行した処理を見られることはありません。識別用 LED が点滅してサーバが「サーバ側モニタ ON ／ OFF」モードであることを示します。

「サーバ側モニタ ON ／ OFF」機能は、iRMC S2/S3 Web インターフェースの「*ビデオ リダイレクション (AVR)*」ページから設定することができます（304 ページを参照してください。）システムを適切に設定したら、リモートの管理端末からサーバのサーバ側モニタを以下のようにオンオフできます。

– 「*拡張機能*」メニューのフルコントロールモードから

– Administrator　または OEM の権限がある場合、直接「*ビデオ リダイレクション (AVR)*」から

新たに AVR セッションが開始されたときには、必ずサーバ側モニタを自動的にスイッチオフにする設定をすることもできます。

サーバ側モニタの現在の状態は、AVR ウィンドウで、統合された特殊キーの右上に青地で表示されます :

サーバ側モニタが常時オン
: サーバ側モニタは、「*サーバ側モニタの出力を切替可能にする*」オプション（309 ページ参照）が無効にされるので、サーバ側モニタは、常時スイッチオン状態でオフにすることはできません。

サーバ側モニタオン
: サーバ側モニタはオンになっていますがスイッチオフできます。

サーバ側モニタオフ
: サーバ側モニタはオフになっていますがスイッチオンできます。

サーバ側モニタが常時オフ
: サーバ側モニタは常時スイッチオフで、スイッチオンにはできません。管理対象サーバ上で高解像度のグラフィックモードが設定されているためです。（表 3 を参照してください。）

5.2.4 キーボードのリダイレクション

キーボードのリダイレクションは AVR ウィンドウにフォーカスされている場合のみ可能です。

- キーボードのリダイレクションが機能していない場合にはまず AVR ウィンドウをクリックしてください。
- キーボードの反応がない場合は、AVR ウィンドウがビューモードになっていないかどうかを確認してください。フルコントロールモードに切り替える方法は、106 ページに説明があります。

特殊キーの組合せ

AVR は通常のキーの組合せはすべてサーバに伝えられます。ウィンドウズキーなどの特殊キーは伝送されません。[ALT] + [F4] などの一部の特殊キーの組合せは伝送できません。クライアントのオペレーティングシステムにより中断されるからです。このような場合は、特殊キーの同時使用またはグラフィカルキーボードを使用してください。

統合された特殊キー

AVR ウィンドウのメニューバーの下に、特殊キーのバーがあります。これらのキーは「スティックキー」として機能します。すなわちクリックすると押したままの状態が続き、もう一度クリックするとまた元の位置に戻ります。

統合された特殊キーを使用すると、たとえば、キーボード上で押しても AVR に伝送されないウィンドウズキーや特殊キーの組合せを使用することができます。

図 30: AVR ウィンドウ - 統合された特殊キー

［カーソル同期］
　このキーを押してマウスポインタを同期させます。（合わせて96 ページ の「マウスポインタの同期」の項を参照してください。）

［Ctrl］
　左の CTRL キー（キーボードの［Ctrl］キーに相当します）。

［Alt］
　Alt（ernate）キー（キーボードの［Alt］キーに相当します）。

［Win］
左右のウィンドウズキー（キーボードの左右の［Ctrl］キーと［Alt ］キーの間にあるキーに相当します）。

［Alt Gr］
Alt（ernate）Gr（aphic）キー（キーボードの［Alt Gr］キーに相当します）。

［Context］
選択したメニューのコンテキストメニューです（キーボードの［Shift］+［F10］キーの組合せに相当します）。

［Lock］
Caps lock キー（キーボードの［Caps Lock］キーに相当します）。

［Ctrl-Alt-Del］
キーボードの［Ctrl］+ ［Alt］+ ［Del］の組合せに相当します。

グラフィカルキーボード

グラフィカルキーボード（図 31 参照）はキーボードを代替する機能があります。グラフィカルキーボードを使用するとすべてのキーの組合せを使用できます。すなわち、グラフィカルキーボードでは実際のキーボードを完全に代替する機能が使用可能です。

グラフィカルキーボードは「*拡張機能*」メニュー（105 ページ参照）から起動できます。

図 31: グラフィカルキーボード（日本語レイアウト（JP））

セキュアキーボード

iRMC S2/S3 Web インターフェースを HTTPS 接続している場合は、キーボードの入力は、セキュア SSL 接続により伝送されます。

5.2.5 マウスのリダイレクト

管理対象サーバのマウスポインタは、リモート管理端末のマウスに同期して動かすことができます。マウスのリダイレクション設定は、AVR ウィンドウで「*パフォーマンス設定*」メニュー（111 ページ参照）の「*マウス動作モード*」タブから設定します。

5.2.5.1 マウスポインタの同期

AVR ウィンドウを最初に開いたときには、リモート管理端末のマウスポインタ（サーバ側マウスポインタ）はまだ管理対象サーバのマウスポインタに同期していないこともあります。

両方のマウスポインタを以下のいずれかの方法で同期させてください。（図 32 を参照してください。）：

- AVR ウィンドウ、メニューバーの［カーソル同期］をクリックしてください。
- サーバ側マウスポインタを AVR ウィンドウの左上隅まで動かと、管理対象サーバのマウスポインタは自動的にこの動きに追随します。
  両方のマウスが完全に重なればにポインタは同期します。

カーソル同期ボタンを押下する。

又は

（1）操作側のマウスカーソルを画面左上に移動する。

（2）サーバのマウスカーソルも自動的に同じ場所へ移動する。

（3）操作側とサーバのマウスカーソルが重なり、
シンクロ動作が開始される。

図 32: サーバ側マウスポインタと管理対象サーバのマウスポインタの同期化

マウスポインタを正常に同期させるには、管理対象サーバ側で特定の設定を行う必要があります。管理対象サーバが「ServerView Installation Manager」を使ってインストールされていれば、この設定は Matrox VGA インストレーションによって自動的に初期設定されています。

事前に指定された設定を変更したなどの理由でマウスポインタの同期が正常に機能しない場合、以下の説明する設定を行ってマウスポインタの正しい同期を復元できます。管理対象サーバで設定する必要があります。

マウスポインタの同期が正常に機能しない場合、たとえば初期設定が変更されている 場合には、以下に説明する設定を行えば正常なマウスポインタの同期に戻すことができます。この設定は管理対象サーバ側で行う必要があります。

5.2.5.2 管理対象 Windows サーバ：マウスポインタ同期設定の調整

Windows サーバの場合は、マウスポインタ同期の設定はバッチファイルを使用する方法か、Windows スタートメニューとコンテキストメニューを使用する方法のいずれかで行うことができます。

次の設定を調整してください。

– マウスポインタの速度
– ハードウェアアクセラレーション

バッチプログラムを使用して設定の調整を行う場合は、調整するマウスポインタの速度やハードウェアアクセラレーション用のドライバのみでなく Matrox のグラフィックドライバをインストールします。

管理対象サーバの設定は、直接管理対象サーバでもできますが、AVR を使用してリモートの管理端末から行うこともできます。

バッチプログラムを使用する管理対象サーバ設定の調整

以下の通り進めます :

► コマンドプロンプトウィンドウを開きます。

► 関連する Matrox VGA ドライバインストール（32 ビットまたは 64 ビット）用のバッチプログラム install_kronos2_vga.bat があるフォルダに切り替えます。

デフォルト設定では install_kronos2_vga.bat プログラム *C:\Program Files\Fujitsu\ServerView Suite\Installation Manager\ Content\V10.09.12.00\DRV\VIDEO\MATROX\iRMC\W2K*

の下にあります。また、「ServerView Suite」の DVD 1 にも入っています。

► 「*setup.bat*」とタイプしてバッチプログラムを起動してください。

► バッチプログラムが実行されたら、管理対象サーバをリブートします。

Windows スタートメニューとコンテキストメニュー使用する管理対象サーバ

設定の調整
以下の手順でマウスポインタを調整します :

► 次の通り選択します。

「*スタート*」→ 「*設定*」→「*コントロールパネル*」→「*マウス*」
さらに「*ポインタ オプション*」タブを選択します。

その結果以下のウィンドウが開かれます。

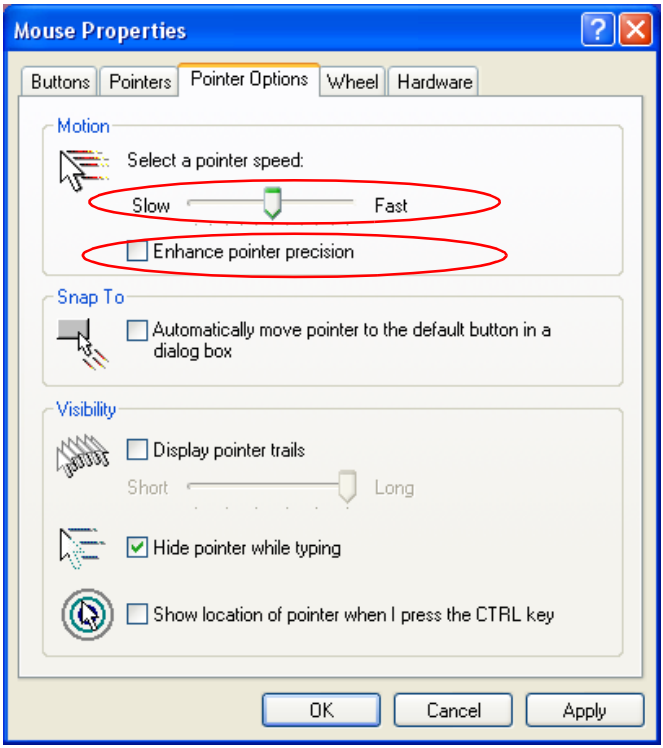


図 33: マウスプロパティウィザード、ポインターオプションタブ

► 「*ポインタの速度を選択する*」は中位の値に設定します。

► 「*ポインタの制度を高める*」オプションは無効にします。

► [*OK*] ボタンをクリックして設定をセーブします。

以下の手順でハードウェアアクセラレータを調整します。

- ► デスクトップの背景を右クリックします。
- ► 現れたコンテキストメニューから、次のように選択します。

  「*ポインタの精度を高める*」タブ、[*詳細設定*] ボタン、「*トラブルシューティング*」タブその結果以下のウィンドウが開かれます。

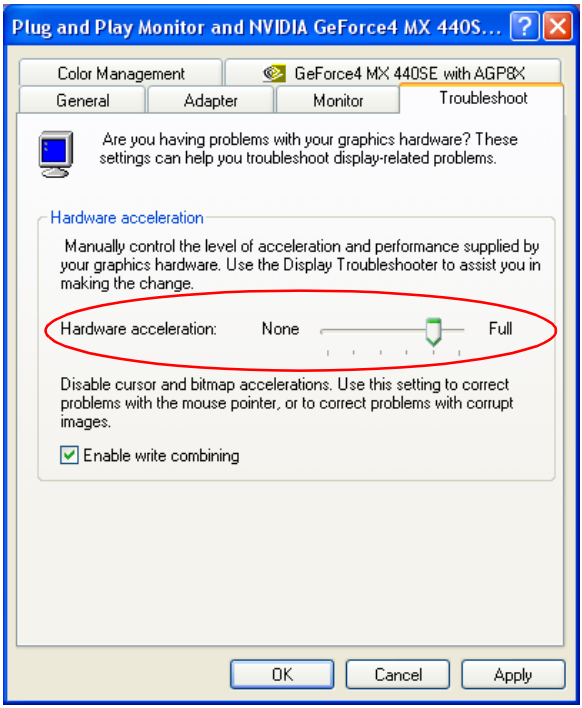


図 34: プロパティ トラブルシューティング : – ハードウェアアクセラレータ

- ► 「*ハードウェアアクセラレータ*」を図 34 で示された値に設定してください。
- ► [*OK*] ボタンをクリックして設定をセーブします。

5.2.5.3 管理対象 Linux サーバ : マウスポインタ同期設定の調整

前提条件 ：管理対象サーバは以下の Linux オペレーティングシステムのいずれかが稼働していることが前提となります。

– Red Hat 4.x
– Red Hat 5.x
– Suse 9.x
– Suse 10.x
– Suse 11.x

SuseLinux および Redhat Linux では異なるグラフィカルユーザーインターフェース (GUI) を使用することができます。最も重要な GUI を以下に示します。

– Gnome
– KDE

管理対象サーバのマウスポインタの同期設定は、コマンドを使用するかメニューのガイドに従うかして調整することができます。

次の設定を調整してください。

– *Mouse motion acceleration = 1*
– *Mouse motion threshold =1*

管理対象サーバの設定は、直接管理対象サーバでもできますが、AVR を使用してリモートの管理端末から行うこともできます。

管理対象サーバ仮設定のコマンドによる調整

「xset」コマンドを使用して「*Pointer acceleration*」と「*Pointer threshold*」の今回のセッションの間使用する設定をします。（推奨値はどちらも 1 です。）

コマンドのシンタックス

xset m(ouse)][*acceleration*][*threshold*]

以下の通り進めます。

► コマンドラインツールを呼び出します。

► 「*xset*」コマンドを以下の引数で実行します。

xset m 1 1

設定ファイル (KDE) による管理対象サーバの永久設定の調整

以下の通り **KDE** の永久設定を行います。

- テキストファイル */root/.kde/share/config/kcminputrc* の設定を以下のように変更します。

  [Mouse]
  Acceleration=1
  Threshold =1

サーバをリブートした後に数値を設定し直す必要はありません。

メニューガイドによる管理対象サーバの永久設定の調整

サーバを再起動した後に数値を設定し直す必要はありません。

以下の通り **KDE** の永久設定を行います。

以下に説明する **KDE** の手順は **SuSE Linux** のみに適用されます。
SuSE Linux は未サポートです。

- 以下の順序で選択します。

  「*N*」→「*Control Center*」→「*Peripheral* 」→「*Mouse - Advanced*」タブ

  「*Mouse - Control Center*」ウィンドウが開きます。

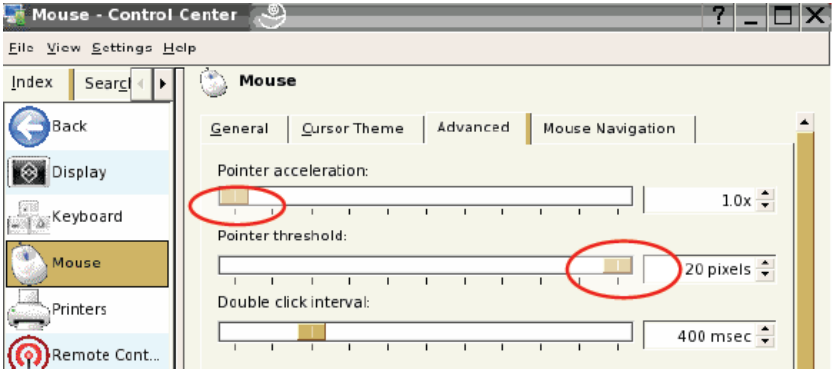


図 35: マウスコントロールセンターウィンドウ

► *Mouse Control Center* ウィンドウで下記の数値を設定します。

– 「*Pointer acceleration: 1.0x* 」（最小値）
– 「*Pointer threshold: 20* ピクセル」（最大値）

► 設定をセーブします。

► 管理対象サーバをリブートします。

サーバを再起動した後に数値を設定し直す必要はありません。

以下の通り **Gnome** の永久設定を行います。

► シェルの中から「*gconf-editor*」エディタを呼び出します。

► 「*desktop*」→「*gnome*」→「*peripherals*」→「*mouse*」

► 次の属性変数を変更します。

motion_acceleration 1
motion_threshold 1

5.3 AVR ウィンドウのメニュー

AVR ウィンドウのメニューバーには以下のメニューがあります。

– 「*拡張機能*」メニューを使用して AVR セッションのコントロールができます。グラフィカルキーボードを使用可能にすることもできます。

– 「*リモートストレージ*」メニューを使用してリモートストレージ接続の設定と解除ができます。

– 「*電源制御*」メニューを使用して、サーバの電源投入 / 切断やリブートを行うことができます。

– 「*言語*」メニューでは「AVR」メニューとダイアログ表示に使用する言語（ドイツ語、英語または日本語）の設定ができます。

– 「*設定*」メニューはマウス、キーボード、および、ログイン設定の設定ができます。

5.3.1 拡張機能メニュー

「拡張機能」メニューから以下の機能を選択できます。

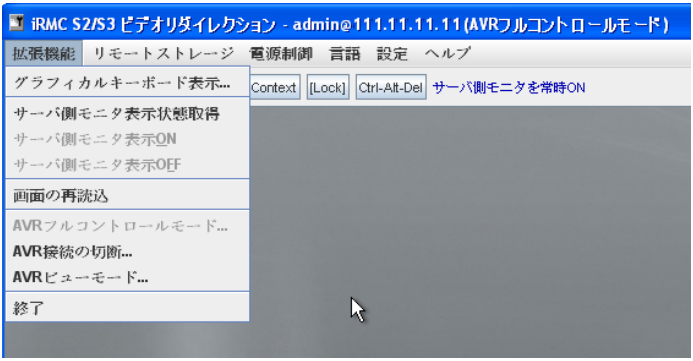


図 36: AVR ウィンドウ - 「拡張機能」メニュー

「*グラフィカルキーボード表示 ...*」
グラフィカルキーボードが開きます。（図 31 を参照してください。）

「*サーバ側モニタ表示状態取得*」
サーバ側モニタ状態の表示をリフレッシュします。

「*サーバ側モニタ表示 ON*」
管理対象サーバのサーバ側モニタ出力を有効にします。

サーバ側モニタの出力が OFF されていても、以下のケースではこの機能は使用できなくなります。

- ビューモードにあるとき、
- 管理対象サーバに高解像度のグラフィックモードが設定されている場合 （88 ページ の表 3 を参照してください）。
  サーバ側モニタ＜状態＞表示 *：*
  サーバ側モニタを常時 OFF

「サーバ側モニタを常時 OFF」
管理対象サーバのサーバ側モニタ出力を無効にします。

サーバ側モニタの出力が ON されていても、以下のケースではこの機能は使用できなくなります。

- ビューモードにあるとき、
- AVR を起動したときに、「サーバ側モニタ出力 OFF」オプションがサーバ側モニタで有効になっていない場合。
(308 ページを参照してください。)
サーバ側モニタ＜状態＞表示：
サーバ側モニタを常時 ON

「*画面の再読込*」
AVR ウィンドウをリフレッシュします。

「*AVR フルコントロールモード...*」
フルコントロールモードに切り替えます （すでにフルコントロールモードになっている場合は、この機能は無効です)。

他の AVR によってフルコントロールセッションがすでに存在している場合は、その旨が他の操作中 AVR に通知されます。他の操作中 AVR 側でフルコントロールセッションを拒否され場合、セッションはビューモードのままになります。

「*AVR 接続の切断 ....*」
別の AVR セッションを終了させます。

「*AVR 接続の切断 ...*」で終了させることができるの別の AVR セッションのみです。

現在のセッションを終了させるには「*OK*」を選択します。

現在の AVR セッションのリストが表示されます。

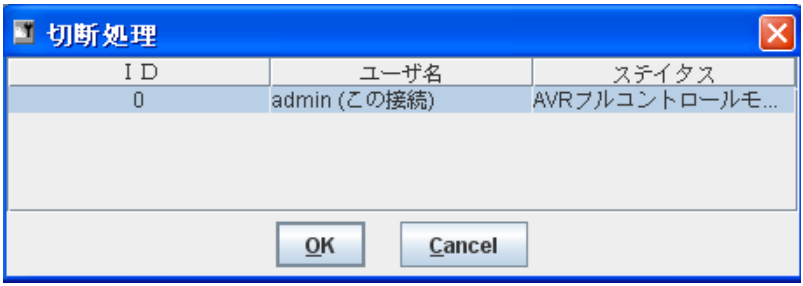


図 37: 「拡張機能」メニュー - セッションの切断

- ► 終了させたい「AVR」セッションを選択します。
- ► [*OK*] をクリックして選択した AVR セッションの終了を確定します。
- ► 選択した「AVR」セッションを終了させたくない場合は [*Cancel*] をクリックしてください。

「*AVR ビューモード ...*」
ビューモードに切り替えます。（すでにビューモードになっている場合はこの機能は使用できません。）

「*終了*」
現在の「AVR」セッションを終了させます。

5.3.2 リモートストレージメニュー

「リモートストレージ」の下の「*リモートストレージ...*」機能を呼び出します。

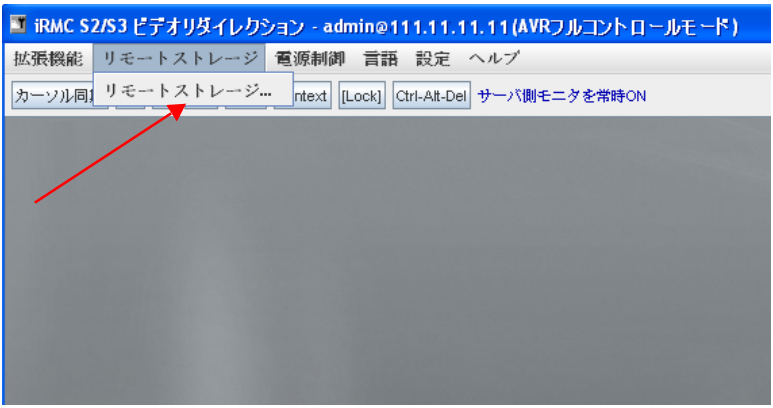


図 38: AVR ウィンドウ -「リモートストレージ」メニュー

リモートストレージ

「*リモートストレージ...*」をクリックすると「*ストレージデバイス*」ウィンドウが開きます。（117 ページを参照してください。） このウィンドウを使用してリモートストレージとしてリモート管理端末にメディアを取り付けまたは取り外すことができます。（113 ページ の「リモートストレージ」の章を参照してください。）

5.3.3 「電源制御」メニュー

「*電源制御*」メニューを使用して、サーバの電源投入 / 切断やリブートを行うことができます。

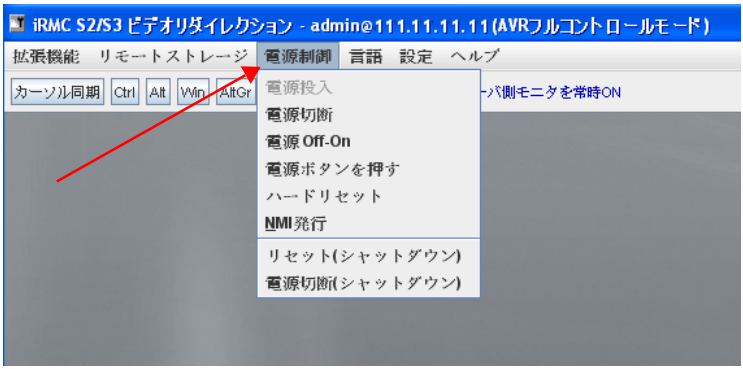


図 39: AVR ウィンドウ - 「電源制御」メニュー

電源投入
: サーバの電源を投入します。

電源切断
: オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。

電源 Off-On
: サーバの電源が完全に切断され、設定した時間の経過後、再び投入されます。この時間は、「*ASR&R オプション*」グループの「*パワーサイクル間隔*」フィールドで設定できます（237 ページを参照）。

電源ボタンを押す
: インストールされているオペレーティングシステムと設定されている動作に依存して、電源オフボタンを短く押してさまざまな動作をトリガできます。これらの動作では、コンピュータのシャットダウンや、スタンバイモードまたはスリープモードへの切り替えができます。

ハードリセット
: オペレーティングシステムの状態にかかわらず、サーバを完全に再起動します（コールドスタート）。

NMI 発行
マスク不可能な割り込み（NMI：Non-Maskable Interrupt）を初期化します。NMI は、システムの標準の割り込みマスクテクノロジで無視できるプロセッサ割り込みです。

リセット (シャットダウン)
正常にシャットダウンして、再起動します。
このオプションは、ServerView エージェントがインストールされていて、かつ、iRMC S2/S3 にサインオンして「接続中」の場合のみ使用できます。

電源切断 (シャットダウン)
グレースフルシャットダウンし、電源を切断します。
このオプションは、ServerView エージェントがインストールされていて、かつ、iRMC S2/S3 にサインオンして「接続中」の場合のみ使用できます。

5.3.4 言語メニュー

「*言語*」メニューから AVR ウィンドウのメニューとダイアログの表示に使用する言語を選択します。

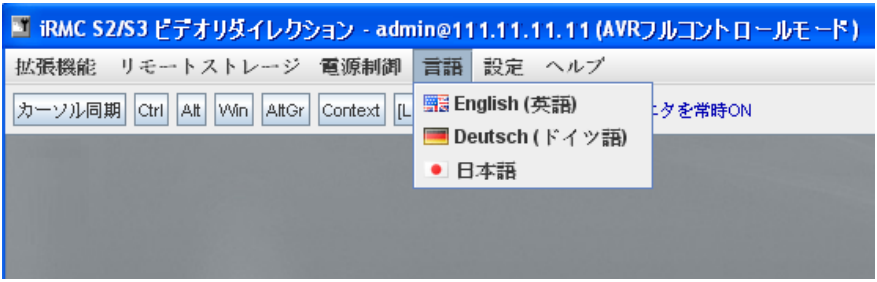


図 40: AVR ウィンドウ -「言語」メニュー

5.3.5 設定メニュー

「*パフォーマンス設定*」メニューを使用して、マウスモード、キーボードレイアウト、グローバルロギング、低帯域幅、内部 TCP ポートを設定できます。

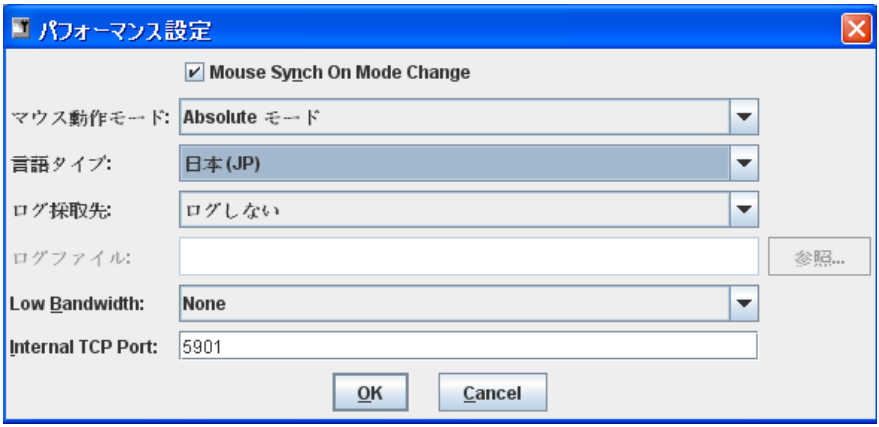


図 41: AVR ウィンドウ - 「プリファレンス」メニュー

サーバ側でビデオリダイレクションが「*Num Lock On*」モードで実行された場合、クライアント側も「*Num Lock ON*」に切り替わります。

Mouse Synch On Mode Change

デフォルト : 有効
マウスポインタの同期を、マウスモードの変更後（以下を参照）に維持するかどうかを指定します。

マウス動作モード

マウスモード（「*操作側を非表示 (Relative)*」、「*Absolute モード*」、または「*Relative モード*」）を指定します。

サーバの OS に応じて、以下の設定を指定する必要があります。

- Windows: 「*Absolute モード*」、「操作側を非表示 (Relative)」、または「Relative モード」
- Linux: 「操作側を非表示 (Relative)」または「Relative モード」

デフォルト設定 : 「*Absolute モード*」

Keyboard Layout

仮想コンソールのキーボードレイアウトを指定します。

管理対象サーバのキーボードレイアウトもそれに応じて設定する必要があり、AVR クライアントと AVR サーバのキーボードレイアウト設定は同一である必要があります。

ログ採取先

デフォルト : ログしない
ログの採取を実行するかどうかを指定します。

ログ採取をやめるには「*ログしない*」を設定して、無効にする必要があります。

ログファイル

グローバルロギングのログファイルを指定します。

「*ログ採取先*」での選択内容に応じて、このオプションは無効になります。

Low Bandwidth

データ転送速度が低下した場合、同じ iRMC S2/S3 でのすべての AVR セッションの色深度に対する帯域幅（bpp、ビット / ピクセル）を低く設定できます。

None

デフォルト。
これより低い帯域幅はありません。

3 bpp

3 bpp 色深度（8 色）。

8 bpp

8 bpp 色深度（256 色）。

Internal TCP Port

デフォルト : 5901
AVR クライアントで使用される統合されたリモートストレージクライアントの内部 TCP ポートを指定します。

6 リモートストレージ

リモートストレージ機能を使用するには有効なライセンスキーが必要です。

リモートストレージはネットワーク上にどこにでも置ける「バーチャル」ドライブを使用可能とします。2 個のメディアまでリダイレクトすることができます。

バーチャルドライブのソースは次のように選ぶことができます。

– AVR Java アプレットを使用するリモート管理端末の物理ドライブまたはイメージファイルをとして。（115 ページを参照してください。）

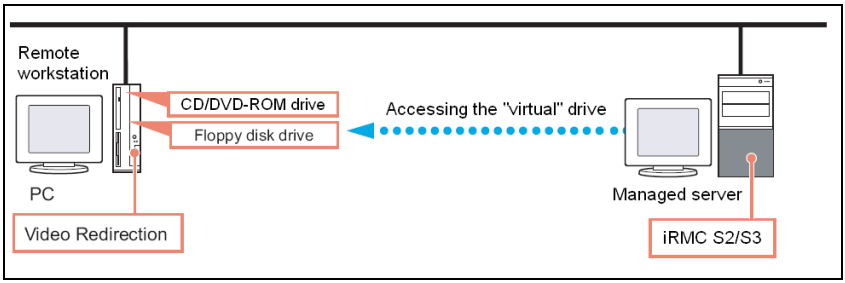


図 42: リモート接続によるリモートストレージ

– リモートストレージサーバ経由ネットワークセントラルの CD/DVD ISO イメージとして。（130 ページを参照してください。）

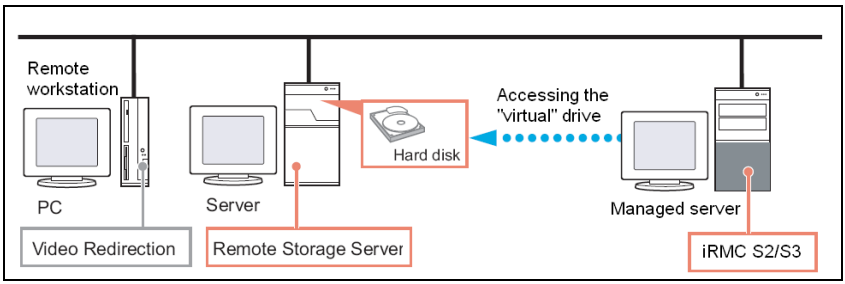


図 43: リモートストレージサーバによるリモートストレージ

パラレルリモートストレージ接続

以下のどちらかのみ実行が可能です。

– **最大 2 台**のリモート管理端末のバーチャルドライブへのリモートストレージ接続（接続が AVR Java アプレット上で確立されている場合）

または

– **1** 台のリモートストレージサーバへのリモートストレージ接続。

AVR Java アプレット経由とリモートストレージサーバ経由のリモートス トレージ接続を同時に確立させることはできません。

iRMC S2 Web インターフェースの「*リモートストレージ*」ページを使用して、現在のリモートストレージ接続のステータス情報の表示、リモートストレージサーバへの接続確立を行う事ができます。（315 ページを参照してください。）

6.1 リモート管理端末上のリモートストレージの規定

リモート管理端末上のバーチャルドライブのソースを規定すれば、リモートストレージ機能は以下のデバイスタイプをサポートします。

- Floppy
- CD ISO イメージ
- DVD ISO イメージ
- CD、DVD

フロッピーディスク、および光学ストレージメディア（CD、DVD）は自動的に表示されます（選択対象になります）。その他のリモートストレージメディアをリモートストレージとして利用できるようにするには、該当するデバイスタイプを手動で選択する必要があります。

リモートストレージとして接続されたデバイスは、iRMC S2/S3 によって、USB 接続されたデバイスとして認識されます。USB 接続がない場合（USB ドライバがない場合）は、これらは使用できません。

バーチャルドライブはリモート管理端末から PRIMERGY サーバにオペレーティングシステムをインストールする場合にも使用可能です。（375 ページ の「iRMC S2/S3 によるオペレーティングシステムのリモートインストール」の章を参照してください。）

本節では次の点について説明します。

- リモートストレージの起動
- リモートストレージのストレージメディアの規定
- ストレージメディアのリモートストレージへの接続
- リモートストレージ接続の解除
- リモートストレージに使用可能としたメディアの取り出し

6.1.1 リモートストレージの開始

リモートストレージ機能は、AVR Java アプレットを使用して開始します。（304 ページ の「ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の 開始」の項を参照してください。）

- iRMC S2/S3 Web インターフェースを起動します（140 ページ の「iRMC S2/S3 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。）
- 「*ビデオ リダイレクション (AVR)*」ページを開いて [*ビデオ リダイレクションの開始*] ボタンをクリックし、ビデオリダイレクションを起動させます。（304 ページ の「ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の 開始」の項を参照してください。）

  その結果 AVR ウィンドウが開かれます。
- AVR ウィンドウのメニューバーから、以下を選びます。
  リモートストレージ - リモートストレージ...

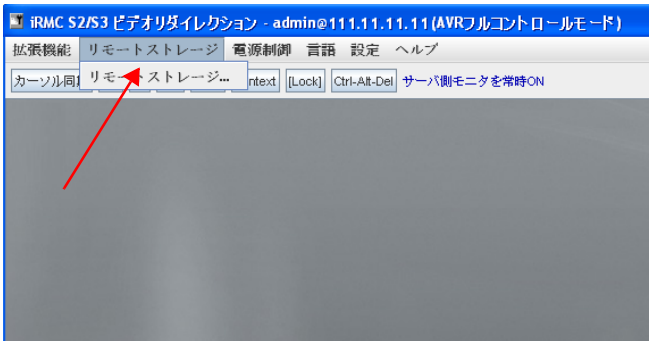


図 44: AVR ウィンドウ - 「リモートストレージ」- 「リモー トストレージ ...」

「*ストレージデバイス*」ダイアログボックスが開き、現在リモートストレージとして使用可能なストレージメディアがリストされます。

Windows システムの「ストレージデバイス」ダイアログボックス

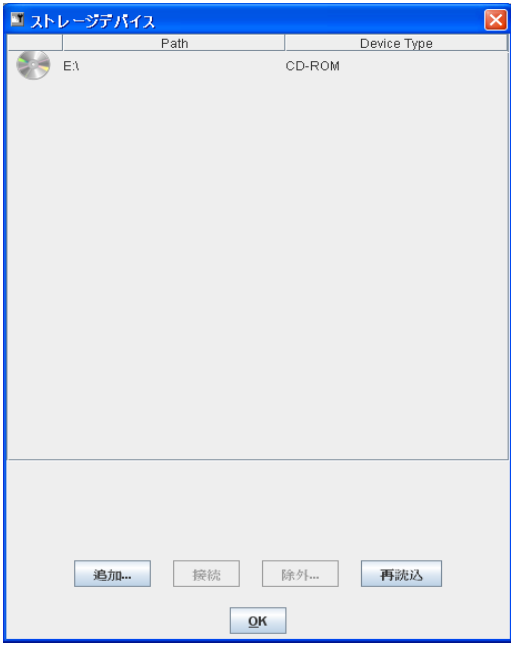


図 45: 「ストレージデバイス」ダイアログボックス

フロッピーディスクドライブ、および光学ドライブ（CD ROM、DVD ROM）にストレージメディアが挿入されていれば、コンテンツは自動的に表示されます。

フロッピーディスクドライブと CD ROM/DVD ROM ドライブは、メディアが挿入されていなければ、リストに表示されません。

ストレージメディアが挿入されていてもコンテンツが自動的に表示されない場合には、ストレージメディアはローカルのエクスプローラに占有されています。

Linux システムの「ストレージデバイス」ダイアログボックス

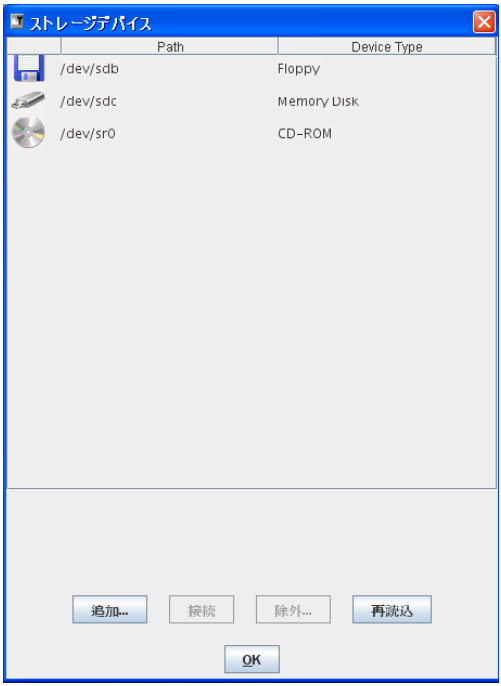


図 46: 「ストレージデバイス」ダイアログボックス

ストレージメディアが Linux システムにマウントされ、リモートストレージデバイスとして認識できる必要があります。マウントされたストレージメディアは「*ストレージデバイス*」ダイアログボックスに自動的に表示されます。

6.1.2 リモートストレージのストレージメディアの追加

► 「*ストレージデバイス*」ダイアログボックスで［*追加*］をクリックします。
「*ストレージデバイスの追加*」ダイアログボックスが開きます。

Windows システムの「ストレージデバイスの追加」ダイアログボックス

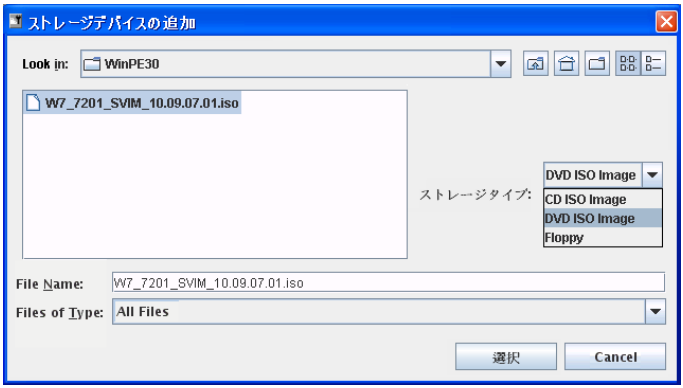


図 47: 「ストレージデバイスの追加」ダイアログボックス (Windows)

Linux システムの「ストレージデバイスの追加」ダイアログボックス

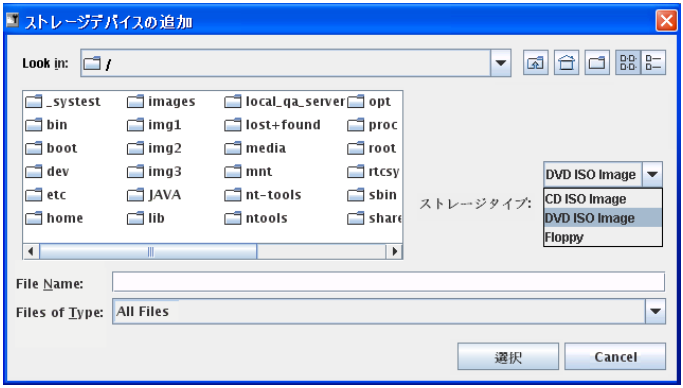


図 48: 「ストレージデバイスの追加」ダイアログボックス (Linux)

- 「*ストレージデバイスの追加*」ダイアログボックスで、現在のリモート管理端末からリモートストレージとして使用可能にしたいリモートストレージメディアのディレクトリに移行します。
- 「*ストレージタイプ*」の下から必要なデバイスのタイプを選択します。

  以下のタイプのストレージを選択できます。

  – Floppy
  – CD ISO イメージ
  – DVD ISO イメージ

  ストレージデバイスを Linux システムにマウントする必要があります。
- リモートストレージとして接続したいストレージメディアを「*ファイル名*」の下に指定します :

  – ISO image (ISO/NRG image) である場合には、ファイル名を入力してください。または、エクスプローラでファイル名をクリックしてください。
  – ドライブである場合には、ドライブ名を入力してください。たとえば、
    – ドライブ D の「D」(Windows)
    – */dev/...* (Linux)

「ストレージデバイスの追加」ダイアログボックス : ストレージメディアの選択 (Windows)

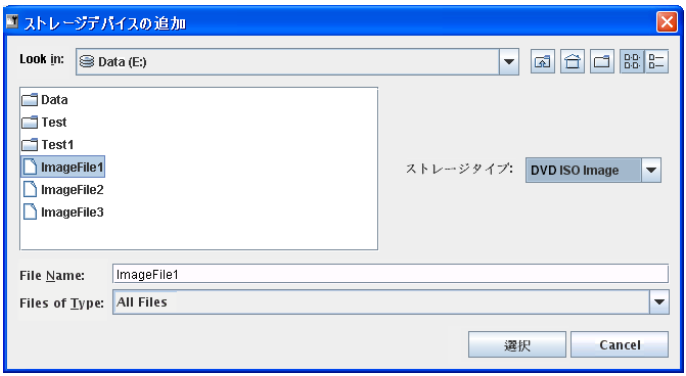


図 49: 「ストレージデバイスの追加」ダイアログボックス : ストレージメディアの選択

［ストレージデバイスの追加］ダイアログ：ストレージメディアの選択 (Linux)

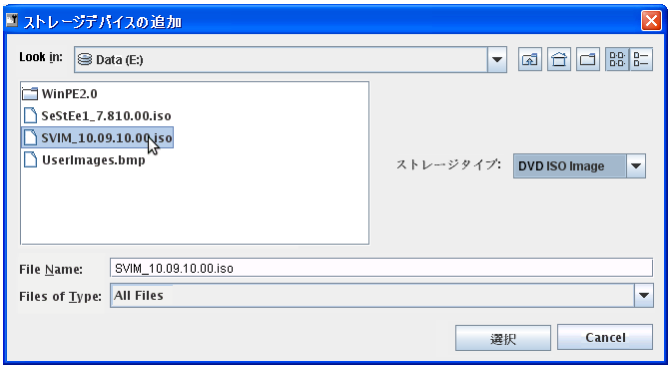


図 50: 「ストレージデバイスの追加」ダイアログボックス：ストレージメディアの選択

► ［*選択*］クリックして選択を確定します。

選択されたストレージメディアがリモートストレージとして使用可能になり、「*ストレージデバイス*」ダイアログボックスに表示されます。

「ストレージデバイス」ダイアログボックスの表示 (Windows)

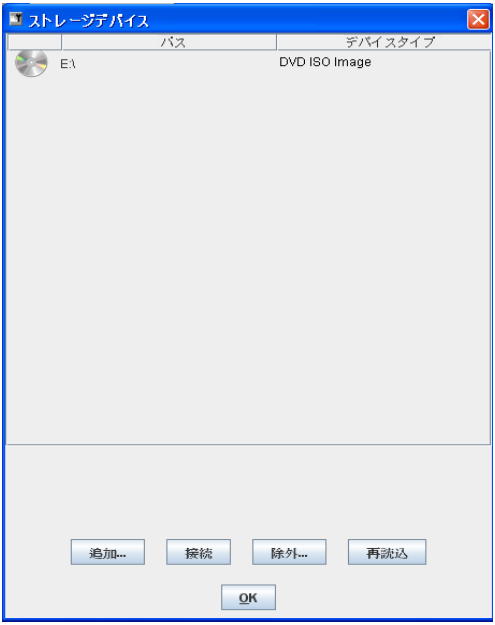


図 51: ストレージデバイスダイアログボックス：追加されたストレージメディアが表示される

「ストレージデバイス」ダイアログボックスの表示 (Linux)

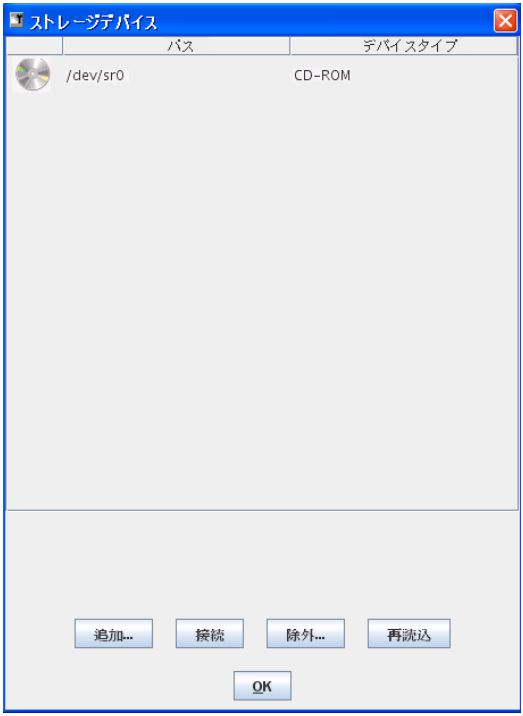


図 52: 「ストレージデバイス」ダイアログボックス：追加されたストレージメディアが表示される

6.1.3 ストレージメディアのリモートストレージの接続

- 「*ストレージデバイス*」ダイアログボックス（図 50 および 122 ページ の図 51 参照）で、リモートストレージとして接続したいストレージメディアをクリックします。
- 「*接続*」をクリックして、選択したストレージメディアをリモートストレージとして接続してください。

  「*ストレージデバイス*」ダイアログボックスが開き、安全な取り外しに関するメッセージが表示されます。ストレージメディアがリモートストレージとして接続されます。

  2 台のストレージデバイスをリモートストレージとして同時に接続したい場合は、接続が確立される前に確認ダイアログボックスが表示されます。（126 ページ の「同時に 2 つのストレージデバイスをリモートストレージとして接続する」を参照してください）。

ストレージデバイスダイアログボックス：リモートストレージ接続の表示 (Windows)

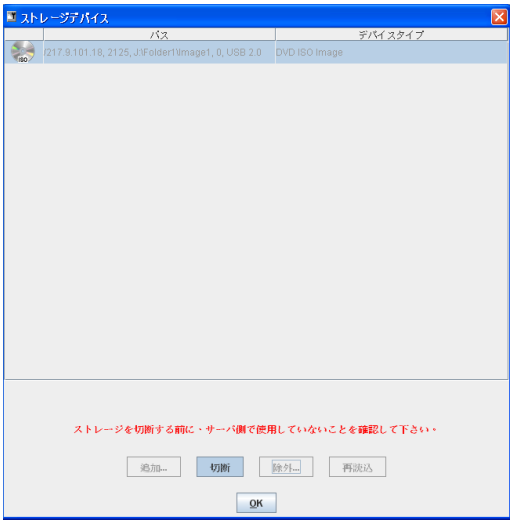


図 53: 「ストレージデバイス」ダイアログボックス：ストレージメディアがリモートストレージ として接続される。

ストレージデバイスダイアログボックス：リモートストレージ接続の表示 (Linux)

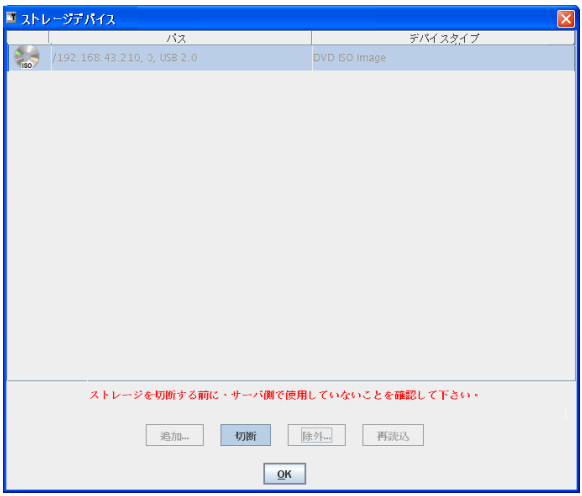


図 54: 「ストレージデバイス」ダイアログボックス：ストレージメディアがリモートストレージとして接続される。

同時に 2 つのストレージデバイスをリモートストレージとして接続する

以下の項の例では、2 つのストレージメディアを Windows システム上のリモートストレージとして同時に接続する方法を示しています。Linux システムにも同じ手順が適用されます。

図 55 では、2 つのストレージデバイスがリモートストレージとして指定されています。

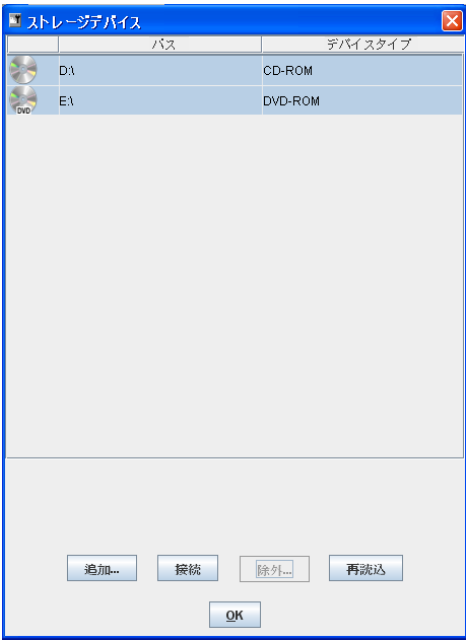


図 55: 「ストレージデバイス」ダイアログ : 2 つのストレージデバイスをリモートストレージとして接続する

- 2 つのストレージデバイスを選択して「*接続*」をクリックして、ストレージデバイスをリモートストレージとして接続します。

  ストレージデバイスの USB 1.1 および USB 2.0 への割り当てがシステムから推奨されます（126 ページ の図 55 を参照）。

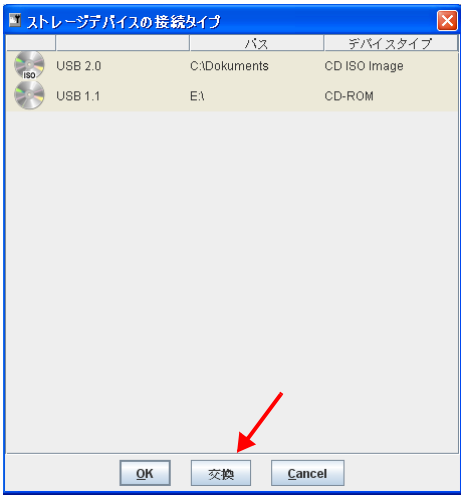


図 56:「ストレージデバイスの接続タイプ」ダイアログボックス：USB 1.1 および USB 2.0 の割り当て

► ストレージデバイスの USB 1.1 と USB 2.0 への割り当てを入れ替えたい場合には［交換］をクリックしてください。

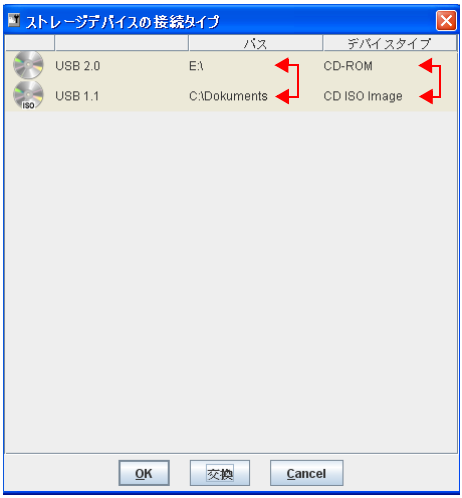


図 57:「 ストレージデバイスの接続タイプ」ダイアログボックス：入れ替えられた USB 1.1 と USB 2.0 の割り当て

► 「*OK*」をクリックして、ストレージデバイスをリモートストレージとして接続してください。

6.1.4 リモートストレージ接続の切断

リモートストレージ接続は、AVR セッションが切断されたときに自動的に解放されます。

► 「*ストレージデバイス*」ダイアログボックスを開いてください。（116 ページ の「リモートストレージの開始」の項を参照してください。）

リモートストレージとして接続されたストレージメディアのリストが表示されます（Windows の例です）。

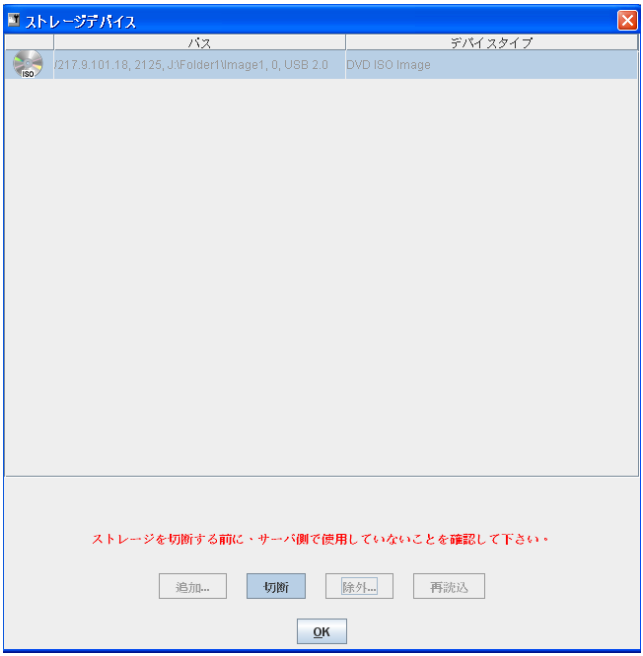


図 58: 「ストレージデバイス」ダイアログボックス：リモートストレージの切断

► 安全な取り外し、すなわちストレージメディアにアクセスしているアプリケーションやプログラムがないことを確認してください。

► ［*切断*］をクリックして、すべてのリモートストレージ接続を解除してください。

6.1.5 ストレージメディアの除外

以下の通りストレージメディアをリモートストレージに使用可能なメディアのリストから除外してください。

► 「*ストレージデバイス*」ダイアログボックスを開いてください。（116 ページ の「リモートストレージの開始」の項を参照してください。

リモートストレージとして使用可能なストレージメディアのリストが表示されます（Windows の例です）。

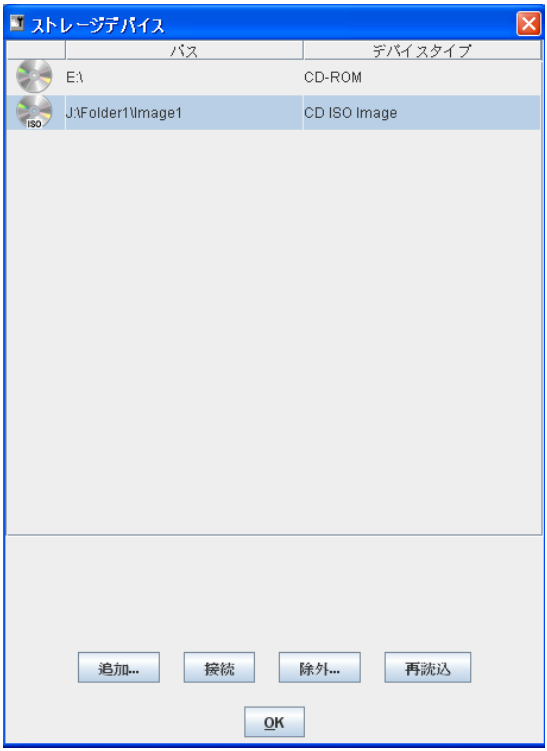


図 59: 「ストレージデバイス」ダイアログボックス：リモートストレージメディアの除外

► 取り出したいストレージメディアを選択してください。

► ［*除外* ....］をクリックしてストレージメディアを除外してください。

6.2 リモートストレージサーバを経由するリモートストレージの追加

リモートストレージサーバを利用して、iRMC S2/S3 によって管理され、PRIMERGY サーバが何台でもリモートストレージとして使用できるイメージファイル（ISO/NRG イメージ）を追加することができます。このイメージファイルを使用してリモート管理端末から 1 台または複数の PRIMERGY サー バをブートすることができます。（375 ページ の「iRMC S2/S3 によるオペレーティングシステムのリモートインストール」の章を参照してください。）

リモートストレージサーバは Windows システムに使用することができます

リモートストレージサーバは Windows 32 でビット版でも 64 ビット版でも使用できます。64 ビットシステムに、同時に 32 ビット版と 64 ビット版のリモートストレージサーバを同時にインストールすることはできません。

リモートストレージサーバの個々のバリアントは ServerView Suite の DVD 1 の中で、

「SVSoftware\Software\RemoteView\iRMC」の下にあります。

PRIMERGY サーバがリモートストレージ経由で使用可能な ISO イメージの作成

お使いの PRIMERGY サーバで、リモートストレージサーバにより使用可能にされたイメージファイルを使用する場合は、以下の要件を満たさなければなりません。

- リモートストレージサーバがインストールされていること（131 ページとを参照してください。）
- リモートストレージサーバが起動されていること（135 ページと を参照してください。）
- 管理対象サーバの iRMC S2/S3 がリモートストレージサーバに接続されていること（315 ページを参照してください。）

WinPE 2.x- ベースの ISO イメージからのブート

iRMC S2/S3 が稼働し 3.60A 以前のファームウェアの場合、PRIMERGY サーバは WinPE 2.x- ベースの ISO イメージからのブートする必要があります。（例えば、Windows Server 2008 、ServerView Installation Manager 等。）

6.2.1 リモートストレージサーバのインストール

リモートストレージサーバのインストール用の
「*RemoteStorageServer_Installer32.exe*」と
「*RemoteStorageServer_Installer64.exe*」インストールプログラムはそれぞれ ServerView Suite の DVD 1 の中の
「*SVSoftware\Software\RemoteView\iRMC\Widows_32*」と
「*SVSoftware\Software\RemoteView\iRMC\Widows_x64*」の下にあります

インストールが正常に完了すると、インストールディレクトリに、*RemoteStorageServer.exe* を含めていくつかのファイルが生成されます。

6.2.2 リモートストレージサーバの実行モード

リモートストレージサーバは必要に応じて以下のモードで実行することができます。

– バックグラウンドのサービスとして

– スタンドアローンプログラムとして

リモートストレージサーバの実行モードはグラフィカルユーザーインターフェースを使って設定します。（132 ページを参照してください。）

リモートストレージサーバのサービスとしての実行

以下の点に注意が必要です。

– イメージファイルは、ネットワーク上のコンピュータにも、リモートストレージサーバが稼働しているのと同じホストにも、どちらにも置くことができます。

  イメージファイルをリモートストレージサーバが稼働しているのコンピュータ以外に置く場合には、イメージファイルのパスを UNC 表記で指定しなければなりません。また、イメージファイルのアクセス権限があるユーザーアカウントも必要です。

– リモートストレージサーバが置かれたホストを起動すると、リモートストレージサーバも自動的に起動します。リモートストレージサーバはその後、「手動」で終了するかホストがシャットダウンされるまで実行されます。

– リモートストレージサーバが置かれたホストをブートすると、イメージファイルは自動的に使用可能になります。

リモートストレージサーバをスタンドアロンプログラムとして実行する

以下の点に注意してください。

– イメージファイル（ISO/NRG イメージ）が、リモートストレージサーバまたは割り当てられたネットワークドライブ上にローカルに存在することがあります。

– リモートストレージサーバが存在するホストが起動されるとき、イメージファイルを「手動」で開始する必要があります。

6.2.3 リモートストレージサーバの設定、起動、および、終了

リモートストレージサーバはグラフィカルユーザーインターフェース (GUI) を使用して設定、起動および終了します。

リモートストレージサーバのグラフィカルユーザーインターフェース呼び出し

リモートストレージサーバのグラフィカルユーザーインターフェースを以下の通り呼び出してください。

► 次のように選択します :「スタート」→「プログラム」→「Fujitsu RemoteStorageServer」→「Remote Storage Server」

リモートストレージサーバのグラフィカルユーザーインターフェースが表示されます。

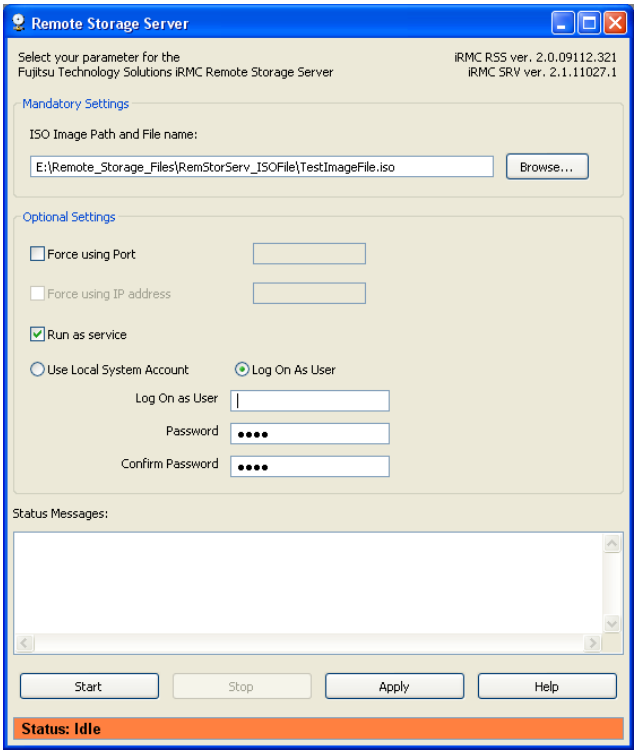


図 60: リモートストレージサーバのグラフィカルユーザーインターフェース（この例では「アイドル」状態）

リモートストレージサーバの設定

設定は、リモートストレージサーバが「アイドル」状態にあるとき、すなわち実行されていないときのみ可能です。

グラフィカルユーザーインターフェースで、リモートストレージとして実行可能にするイメージファイルを他のパラメータと合わせて指定してください。

ISO イメージのパスとファイル名 :

- イメージファイルのパスと名前をフィールドに直接入力してください。

  または

- ［*Browse...* ］ボタンをクリックし、次に、「*Choose a file*」ダイアログに移動して必要なイメージファイルを選択し、確定します。

  リモートストレージサーバをサービスとして稼働させる場合（135 ページ「*Run as Service*」オプション参照）および、イメージファイルをネットワーク上のコンピュータに置く場合は、イメージファイルのパスを UNC 表記で指定する必要があります。また、「*Log On As User*」（135 ページ 参照）の下に入力したアカウントが有効であ り、イメージファイルが置かれた領域を共有するアクセス権限があることを確認しな ければなりません。

ポート番号による指定

iRMC S2/S3 のリモートストレージポートに初期値のポート番号 (5901) 以外のポート番号を設定した場合（250 ページ）、このオプションを有効化し、設定したポート番号を関連するフィールドに入力する必要があります。

IP アドレスによる指定

リモートストレージサーバが実行されるホストが複数の LAN 接続されている場合は、リ モートストレージサーバがサービスとして実行される場合には、それに使用される LAN 接続に IP アドレスを指定することができます。
初期設定では、リモートストレージサーバは最初に検出された LAN 接続を使用します。

サービスとしての稼働
リモートストレージサーバがバックグラウンドでサービスとして実行される場合にはこのオプションを有効にして下さい。（131 ページを参照してください。）

► 次の 2 つのオプションからどちらかを選択します。

ローカルのシステムアカウント使用
リモートストレージサーバはローカルのシステムアカウントに下でサービスとして実行されます。

この場合には、イメージファイル（ISO/NRG イメージ）をローカルのドライブに置くことはできません。

ユーザーとしてログオン
また、イメージファイルのアクセス権限があるユーザーアカウントも必要です。

ユーザー名を以下の書式で指定してください。

– ローカルユーザーには、*.\Logon-Name*

– ドメインユーザーには、

DOMAIN\LogOnName
または
LogOnName@DOMAIN<mailto:LogOnName@DOMAIN>

イメージファイルは、「*Log On As User* 」オプションが有効になっていれば、ネットワークドライブに置くことができます。この場合は、指定されたアカウントにはイメージファイルが置かれたネットワークドライブのアクセス 権限が必要です。また、イメージファイルは UNC 表記で指定しなければなりません。（134 ページの入力フィールド「*ISO Image Path or Filename*」を参照してください。）

［*Apply* ］ボタンをクリックして設定を有効にしてください。

リモートストレージサーバの開始

► ［*Start*］ボタンをクリックしてリモートストレージサーバをサービスとして、または、スタンドアローンとして開始させます。

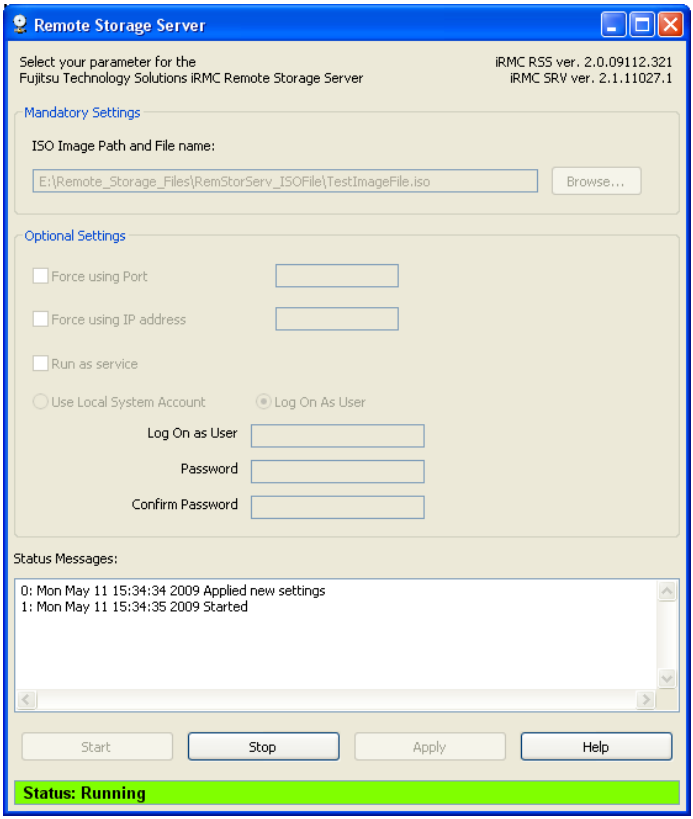


図 61: リモートストレージサーバが実行された（稼働している）状態

ステータスメッセージ
作成されたリモートストレージサーバの実行ステートのログがここに表示されます。

実行モードが「*Run as service*」に設定されている場合は（135 ページ参照）、、リモートストレージサーバはリモートストレージサーバがインストールされたコンピュータが 起動されたときに自動的に起動されます。

リモートストレージサーバの実行は、グラフィカルユーザーインターフェースを終了させても自動的に中断されることはありません。

リモートストレージサーバの終了

- ［*Stop* ］ボタンをクリックしてリモートストレージサーバの実行を終了させます。

6.2.4 Windows によるリモートストレージサーバ

リモートストレージサーバは 32 ビット版でも 64 ビット版でも使用できます。64 ビットシステムに、同時に 32 ビット版と 64 ビット版のリモートストレージサーバを同時にインストールすることはできません。

7 iRMC S2/S3 Web インターフェース

iRMC S2/S3 は固有のオペレーティングシステムを持つだけでなく、Web サーバとしても稼動し、固有のインターフェースを提供します。iRMC S2/S3 Web インターフェースのメニューとダイアログ ボックスの表示言語は、ドイツ語、英語、日本語のいずれかを選択できます。

iRMC S2/S3 Web インターフェースで値を入力するときに、ツールチップ形式のヒントが表示されることがあります。

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。

7.1 iRMC S2/S3 Web インターフェースへのログイン

► リモートワークステーションから Web ブラウザを開いて、iRMC S2/S3 の DNS 名（構成されている場合）（251 ページを参照）または IP アドレスを入力します。

iRMC S2/S3 にディレクトリサービスへの LDAP アクセスが構成されているかどうかによって、表示されるログイン画面が異なります（「*LDAP 有効*」オプションについて、276 ページを参照）。

ログイン画面が表示されない場合は、LAN 接続（46 ページ の「LAN インターフェースのテスト」の項を参照）を確認してください。

– iRMC S2/S3 にディレクトリサービスへの LDAP アクセスが構成されておらず（「*LDAP 有効*」オプションが無効）、かつ「*常に SSL ログインを使用する*」オプション（276 ページを参照）が無効な場合、次のログイン画面が表示されます。

図 62: iRMC S2/S3 Web インターフェースのログイン画面（LDAP アクセスが構成されておらず、かつ、「常に SSL ログインを使用する」オプションが無効な場合）

► 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。

ユーザ名：admin

パスワード: admin

*ユーザ名*と*パスワード*は、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（268 ページ の「ユーザ “<name>” 構成 - ユーザ設定（詳細）」を参照）。

► 「*OK*」をクリックして、入力を確定してください。

– iRMC S2/S3 にディレクトリサービスへの LDAP アクセスが構成されている
（「*LDAP 有効*」オプションが有効）か、または「*常に SSL ログインを使用する*」オプションが有効な場合、次のログイン画面が表示されます。

図 63: iRMC S2/S3 Web インターフェースのログイン画面（LDAP アクセスが構成されている場合）

ユーザ名とパスワードは、送信時に必ず SSL により保護されます。「*安全（SSL）*」オプションが有効な場合、Web ブラウザと、iRMC S2/S3 間のすべての通信は、HTTPS によって行われます。

► 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（268 ページ の「ユーザ “<name>” 構成 - ユーザ設定（詳細）」を参照）。

► 「*ログイン*」をクリックして、ログインを確定します。

iRMC S2/S3 Web インターフェースが開き、*「システム情報」ページ*（150 ページを参照）が表示されます。

7.2 必要なユーザ権限

表 4 に、iRMC S2/S3 Web インターフェースの各々のファンクションを使用するために必要な権限の概要を示します。

iRMC S2/S3 Web インターフェースのファンクション	IPMI 権限レベルによる許可				必要な許可			
	OEM	Administrator	Operator	User	ユーザアカウント変更権限	iRMC S2/S3 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*システムの概要*」ページの表示	X	X	X	X				
識別灯のオン / オフ	X	X	X	X				
「*資産タグ設定*」の設定						X		
「*オペレーティングシステムの情報*」の編集 1)						X		
「*システム構成情報*」ページの表示	X	X	X	X				
「エラーカウンタのリセット」						X		
「SPD データを表示」	X	X	X	X				
「*BIOS パラメータ設定のバックアップ / リストア*」ページの表示 1)	X	X	X	X				
「 *BIOS パラメータ設定のバックアップ / リストア*」の編集 1)	X	X						
「*BIOS アップデート設定*」ページの表示 1)	X	X	X	X				
「BIOS アップデート」の実行 1)	X	X						
「*iRMC S2/S3 情報*」ページの表示	X	X	X	X				
*「iRMC S2/S3 を再起動」*の実行	X	X						
iRMC S2/S3 へのライセンスキーのアップロード						X		
「*その他のオプション*」の設定						X		
「*iRMC S2/S3 ファームウェア設定の保存*」ページの表示					X	X		

表 4: 固有の iRMC S2/S3 Web インターフェースを使用するための権限

iRMC S2/S3 Web インターフェースのファンクション	IPMI 権限レベルによる許可				必要な許可			
	OEM	Administrator	Operator	User	ユーザアカウント変更権限	iRMC S2/S3 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*ユーザ設定*」の選択					X			
その他すべての設定オプションの選択						X		
iRMC S2/S3 設定の WinSCU XML 形式でのファイルからのインポート					X	X		
「*認証データアップロード*」ページの表示 / 編集						X		
「*自己署名 RSA 証明書の作成* 」ページの表示と編集						X		
「*iRMC S2/S3 ファームウェアアップデート*」ページの表示	X	X	X	X				
ファームウェアセレクタの設定	X	X						
「*ファイルからのファームウェアアップデート*」の実行						X		
TFTP 経由でのファームウェアアップデート（「*iRMC S2/S3 TFTP 設定*」）。						X		
「*Power On/Off*」ページの表示	X	X	X	X				
「*起動オプション*」の変更						X		
「*電源制御*」の使用	X	X	X					
「*電源制御オプション*」ページの表示と編集						X		
「*電源装置情報*」ページの表示	X	X	X	X				
「*消費電力制御*」ページの表示と編集						X		
「*現在の全体消費電力*」ページの表示 [2)]						X		
「*消費電力モニタリング履歴*」ページの表示と編集 [2)]						X		
「*ファン*」ページの表示	X	X	X	X				
ファンテストの開始（「*ファンテスト*」グループ）	X	X	X	X				

表 4: 固有の iRMC S2/S3 Web インターフェースを使用するための権限

iRMC S2/S3 Web インターフェースのファンクション	IPMI 権限レベルによる許可				必要な許可			
	OEM	Administrator	Operator	User	ユーザアカウント変更権限	iRMC S2/S3 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*ファンテスト時刻*」の設定（「*ファンテスト*」グループ）						X		
個々のファンの選択（「*システムファン*」グループ）						X		
「*異常時動作 / シャットダウン待ち時間*」の設定						X		
「*温度*」ページの表示	X	X	X	X				
温度センサの異常時動作の指定						X		
「*電圧*」ページの表示	X	X	X	X				
「*電源ユニット*」ページの表示	X	X	X	X				
冗長電源の設定						X		
「*センサの状態*」ページの表示	X	X	X	X				
「*システムイベントログ内容*」ページの表示	X	X	X	X				
システムイベントログ（SEL）のクリア	X	X	X					
「ログの保存」（SEL）	X	X	X	X				
SEL エントリ表示の重要度の定義	X	X	X	X				
「*iRMC S2 イベントログ内容*」ページの表示	X	X						
内部イベントログ（iEL）のクリア	X	X						
「ログの保存」（iEL）	X	X						
SEL エントリ表示の重要度の定義	X	X						
「*システムイベントログ設定*」ページの表示	X	X	X	X				
「*システムイベントログ設定*」設定の編集						X		
「*iRMC S2 イベントログ内容画面で表示させるログの規定値*」設定の編集						X		
「*サーバ管理情報*」ページの表示と編集						X		

表 4: 固有の iRMC S2/S3 Web インターフェースを使用するための権限

iRMC S2/S3 Web インターフェースのファンクション	IPMI 権限レベルによる許可				必要な許可			
	OEM	Administrator	Operator	User	ユーザアカウント変更権限	iRMC S2/S3 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*ネットワークインターフェース*」ページの表示						X		
「*ポート番号とネットワークサービス*」ページの表示と編集						X		
「*DNS 構成*」ページの表示と編集						X		
「*SNMP トラップ送信設定*」ページの表示と編集						X		
「*シリアル / モデム通知設定*」ページの表示と編集						X		
「*E-mail 設定*」ページの表示と編集						X		
「*iRMC S2/S3 ユーザ情報*」ページの表示と編集					X			
「*ディレクトリ サービス構成*」ページの表示と編集						X		
「*CAS 設定*」ページの表示					X	X		
「*CAS 一般設定*」の編集						X		
「*CAS ユーザ権限と許可*」の編集					X			
「*BIOS テキストコンソール*」ページの表示	X	X	X	X				
「*BIOS コンソールリダイレクションオプション*」の変更						X		
「コンソールリダイレクションの開始」	X	X	X	X				
電源管理とテキストコンソールリダイレクションのウィンドウでのログオン	X	X						
テキストコンソールの起動（「*Enter Console*」）	X	X						
「*ビデオリダイレクション（AVR）*」ページの表示と編集							X	
「*リモートストレージ*」ページの表示と編集								X
「*iRMC S2/S3 SSH アクセス*」の開始	X	X	X	X				
SSH ログイン	X	X	X	X				

表 4: 固有の iRMC S2/S3 Web インターフェースを使用するための権限

iRMC S2/S3 Web インターフェースのファンクション	IPMI 権限レベルによる許可				必要な許可			
	OEM	Administrator	Operator	User	ユーザアカウント変更権限	iRMC S2/S3 設定変更権限	AVR 使用権限	リモートストレージ使用権限
「*iRMC S2/S3 Telnet アクセス*」の開始	X	X	X	X				
Telnet ログイン	X	X	X	X				

[1] 実行中のエージェントがない場合のみの動作

[2] システムによっては使用できない機能

表 4: 固有の iRMC S2/S3 Web インターフェースを使用するための権限

7.3 ユーザインターフェースの構造

iRMC S2/S3 Web インターフェースの構造を以下に示します。

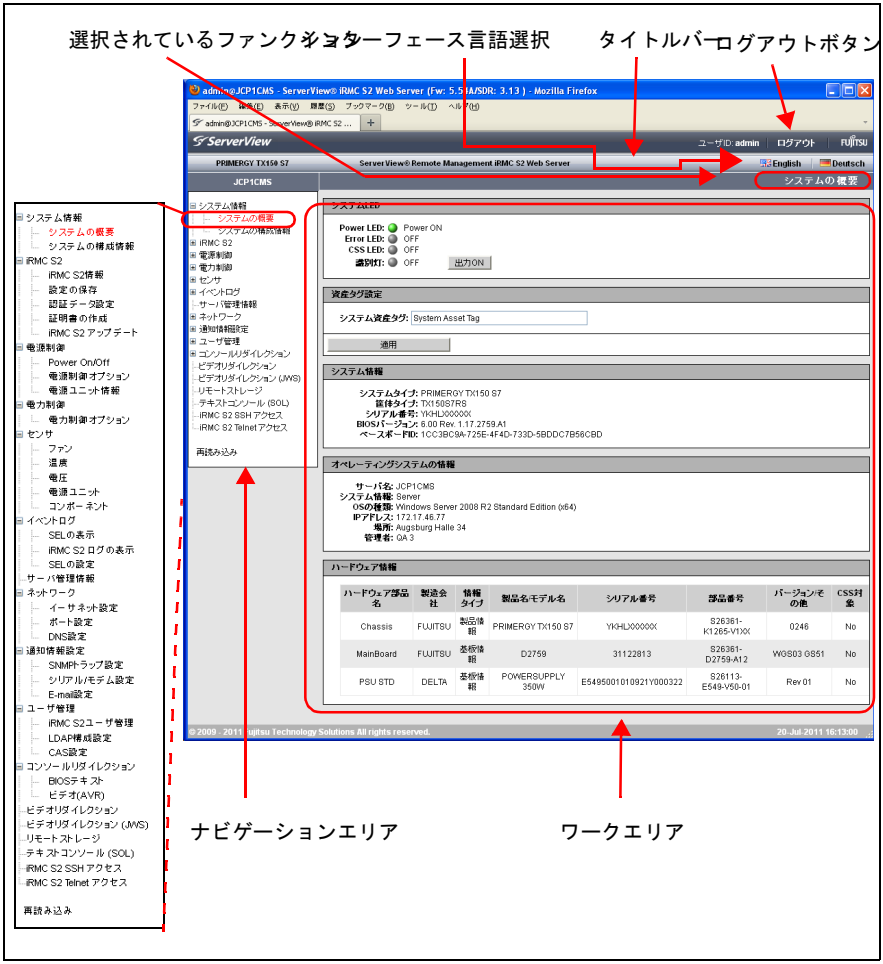


図 64: iRMC S2/S3 Web インターフェースの構造

iRMC S2/S3 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、iRMC S2/S3 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、日本語のいずれか）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には、iRMC S2/S3 の個々のファンクションをタスクベースに並べたメニューツリー構造があります。これらのリンクのいずれかをクリックすると（図 64 :「*システムの概要*」）、そのリンクが有効になり、そのファンクションのワークエリアが表示され、任意の出力、ダイアログボックス、オプション、リンクおよびボタンが表示されます。

個々の iRMC S2/S3 ファンクションの下に、「*ログアウト*」と「*再読み込み*」のリンクがあります。

- 「*ログアウト*」は、ダイアログボックスでの確認の後、iRMC S2/S3 のセッションを終了させることができます。iRMC S2/S3 にディレクトリサービスへの LDAP アクセスが構成されているかどうかによって、セッション終了後に表示されるログイン画面が異なります（「*LDAP 有効*」オプションについて、276 ページを参照）。
  - iRMC S2/S3 にディレクトリサービスへの LDAP アクセスが構成されておらず（「*LDAP 有効*」オプションが無効）、かつ「*常に SSL ログインを使用する*」オプション（276 ページを参照）が無効な場合、次のログイン画面が表示されます。

図 65: ログインページ（ログアウト後）

「*ログイン*」ボタンをクリックして iRMC S2/S3 Web インターフェースのログイン画面を表示します（140 ページ の図 62 を参照）。必要な場合、再びログインできます。

– iRMC S2/S3 にディレクトリサービスへの LDAP アクセスが構成されているか
（「*LDAP 有効*」オプションが有効）、「*常に SSL ログインを使用する*」オプション（276 ページを参照）が無効な場合、適切なログイン画面が表示されます（141 ページ の図 63 を参照）。

- 「*再読み込み*」ボタンをクリックすると、iRMC S2/S3 Web インターフェースの内容を再読み込みすることができます。

  再読み込みの代わりに、内容が定期的に自動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（248 ページ の「自動リフレッシュ有効」を参照）。

7.4 システム情報 - サーバに関する情報

「*システム情報*」エントリには、以下のページへのリンクがあります。

– 151 ページ の「システム概要 - サーバに関する一般情報」

– 156 ページ の「システム構成情報 - サーバコンポーネントに関する情報」

7.4.1 システム概要 - サーバに関する一般情報

「*システムの概要*」ページには、以下の情報が表示されます。

- システムの状態
- システム（一般情報）
- 管理対象サーバのオペレーティングシステム
- システムの FRU（フィールド交換可能ユニット）/IDPROM
- 管理対象サーバの現在の全体消費電力

また、「*システムの概要*」ページでは、管理対象サーバにユーザ固有の資産タグを入力できます。

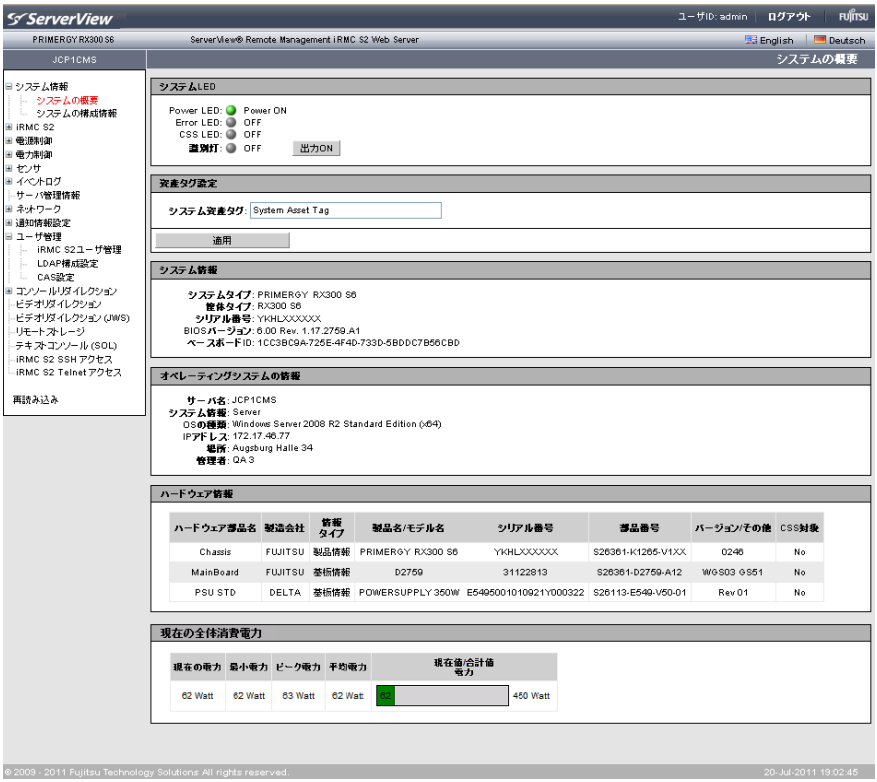


図 66: 「システムの概要」ページ

システム LED

保守ランプ、CSS LED、識別灯のステータスが、「*システム LED*」に表示されます。PRIMERGY の識別灯のオン / オフを切り替えることもできます。

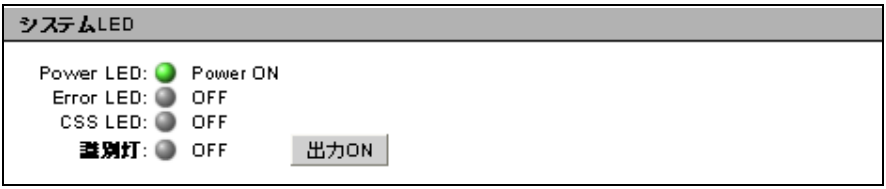


図 67: 「システムの概要」ページ - システム LED

Power LED

サーバの電源状態を示します。
以下の状態があります。

- 点灯：「Power ON」（緑色）
- 点灯：スタンバイモード（緑色）、「RAM へのサスペンド（スタンバイ）」
- 消灯：「Power OFF」（オレンジ色）

Error LED

サーバの保守ランプに関する情報：

ステータス情報 (iRMC S2/S3)	サーバの保守ランプ	サーバの状態
消灯	点灯しない	クリティカルイベントなし
点灯	赤く点灯	非 CSS コンポーネントに故障予兆イベントあり
点滅	赤く点滅	クリティカルイベントあり

CSS LED

サーバの CSS（Customer Self Service）に関する情報：

ステータス情報 (iRMC S2/S3)	サーバの CSS LED	サーバの状態
消灯	点灯しない	サーバ稼働中

ステータス情報（iRMC S2/S3）	サーバの CSS LED	サーバの状態
点灯	オレンジに点灯	CSS コンポーネントに故障予兆イベントあり
点滅	オレンジに点滅	CSS コンポーネント故障

識別灯

サーバ の識別灯です。
以下の状態があります。

– 点灯（青色）
– 消灯（灰色）

出力 ON/ 出力 OFF

「*出力 ON/ 出力 OFF*」ボタンで、PRIMERGY の識別灯の点灯 / 消灯を切り替えます。

資産タグ設定

「*資産タグ設定*」で、管理対象サーバにユーザ固有の資産タグを入力できます。

ユーザ固有の資産タグを使用して、インベントリ番号または選択したその他の ID をサーバに割り当てることができます。

Windows 対応システムの場合は、このユーザ固有の資産タグは WMI（Windows Management Instrumentation）より自動的に提供されます。資産タグは、社内ツールで評価したり、企業管理システム（CA Unicenter など）の統合に使用できます。

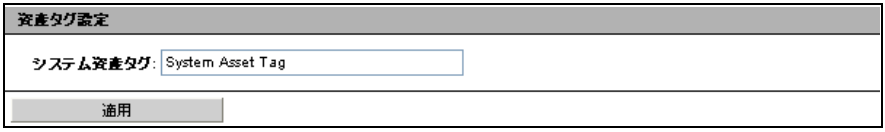


図 68: 「システムの概要」ページ - 資産タグ設定

システム資産タグ

ここに資産タグを入力できます。

► 「*適用*」をクリックして資産タグを適用します。

システム情報

*「システム情報」*には、管理対象サーバの情報が表示されます。

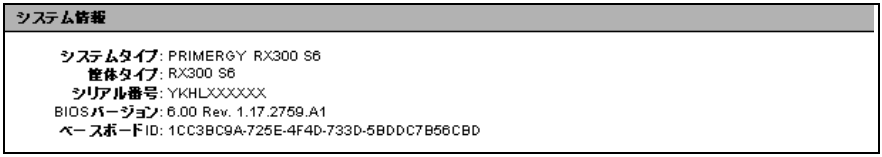


図 69: 「システムの概要」ページ - システム情報

オペレーティングシステムの情報

*「オペレーティングシステムの情報」*には、管理対象サーバのオペレーティングシステムに関する情報が表示されます。

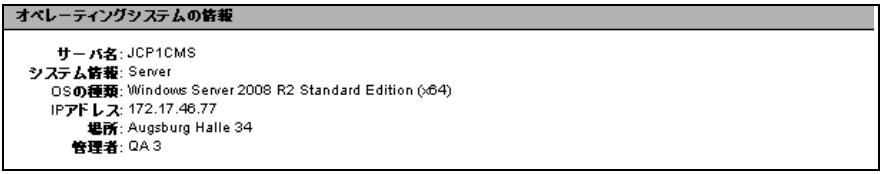


図 70: 「システムの概要」ページ - オペレーティングシステムの情報

ServerView エージェントが実行中でない場合は「*場所*」と「*管理者*」フィールドを編集できますが、実行中は編集できません。

ServerView エージェントの起動後に、ユーザの初期値はエージェントが自動検出した値に上書きされます。

ハードウェア情報

FRU（**F**ield **R**eplaceable **U**nit）に関する情報が「*ハードウェア情報*」に表示されます。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 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

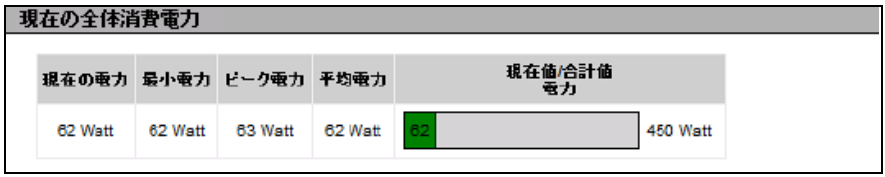
ハードウェア情報

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
Chassis	FUJITSU	製品情報	PRIMERGY RX300 S6	YKHLXXXXXX	S26361-K1265-V1XX	0246	No
MainBoard	FUJITSU	基板情報	D2759	31122813	S26361-D2759-A12	WGS03 GS51	No
PSU STD	DELTA	基板情報	POWERSUPPLY 350W	E5495001010921Y000322	S26113-E549-V50-01	Rev 01	No

図 71: 「システムの概要」ページ - ハードウェア情報

現在の全体消費電力

このオプションは、一部の PRIMERGY サーバではサポートされていません。



現在の全体消費電力

現在の電力	最小電力	ピーク電力	平均電力	現在値/合計値 電力
62 Watt	62 Watt	63 Watt	62 Watt	62 / 450 Watt

図 72: 「システムの概要」ページ - 現在の全体消費電力

「*現在の全体消費電力*」には、設定された間隔で測定されたサーバの消費電力量の現在値、最小値、最大値、平均値が表示されます。

グラフィカルな表示でも、サーバの可能な最大消費電力量と現在の消費電力量を比較して表示しています。

7.4.2 システム構成情報 - サーバコンポーネントに関する情報

「*システム構成情報*」ページには、CPU およびメインメモリモジュールに関する情報が表示されます。「*CSS 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

以下のステータスアイコンは、システムコンポーネントの状態を示します。

	OK：コンポーネントの状態は良好です。
	コンポーネントのスロットが空いています。
	警告：コンポーネントの状態が低下しています。
	欠陥：コンポーネントに欠陥があります。

表 5: システムコンポーネントの状態

図 73: 「システム構成情報」ページ

TPM（Trusted Platform Module）をサポートする PRIMERGY サーバの場合、このページは TPM が有効か無効かを示します。

CPU 情報

このグループでは、管理対象の PRIMERGY サーバの CPU の状態、ID、CSS の機能、および性能に関する情報を提供します。

システムメモリ情報

このグループでは、管理対象の PRIMERGY サーバのメインメモリモジュールの状態、ID、CSS の機能、および性能に関する情報を提供します。

選択
個々のメモリモジュールを選択し、適用する動作を「*一覧からメモリアクションを選択してください*」から選択できます。

すべて選択
すべてのメモリモジュールを選択します。

すべて選択解除
選択を解除します。

一覧からメモリアクションを選択してください
このリストから、選択したメモリに適用する動作を選択します。

BX92x S3 サーバブレードではエラーカウンタのリセットは不可能です。新しいモジュールは自動的に検出されるために iRMC S3 と BX92x S3 サーバブレードではエラーカウンタを明示的にリセットする必要がありません。

選択モジュールへの適用
選択した動作を選択したモジュールに適用します。

SPD データを表示 / すべて選択解除
「*SPD データを表示 / すべて選択解除*」ボタンをクリックすると、個々のメモリコンポーネントのベンダー固有の詳細（SPD（**S**erial **P**resence **D**etect）データ）を表示 / 非表示できます。

メモリの SPD データは、コンポーネントおよびサーバに統合された EEPROM に保存されるので、BIOS によって自動的にメモリコンポーネント（RAM、DIMM）が検出されます。

7.5 BIOS - BIOS 設定のバックアップ / リストア、BIOS のフラッシュ

「*System Information*」エントリには、以下のページへのリンクが含まれます。

– 159 ページ の「バックアップ / リストア - BIOS の単一パラメータのバックアップ要求と、バックアップのファイルへの保存」

– 163 ページ の「BIOS - 「ファイルからアップロード」するか TFTP 経由での BIOS のアップデート」

これらのページは、管理するサーバの BIOS が該当する機能要件を満たす場合のみ表示されます。

7.5.1 バックアップ / リストア - BIOS の単一パラメータのバックアップ要求と、バックアップのファイルへの保存

「*BIOS パラメータ設定のバックアップ/ リストア*」には以下のオプションがあります。

– 単一の BIOS パラメータを ServerView® WinSCU XML 形式でバックアップし、バックアップをファイルに保存します。

– 単一の BIOS パラメータ設定をファイルから ServerView® WinSCU XML 形式でリストアします。

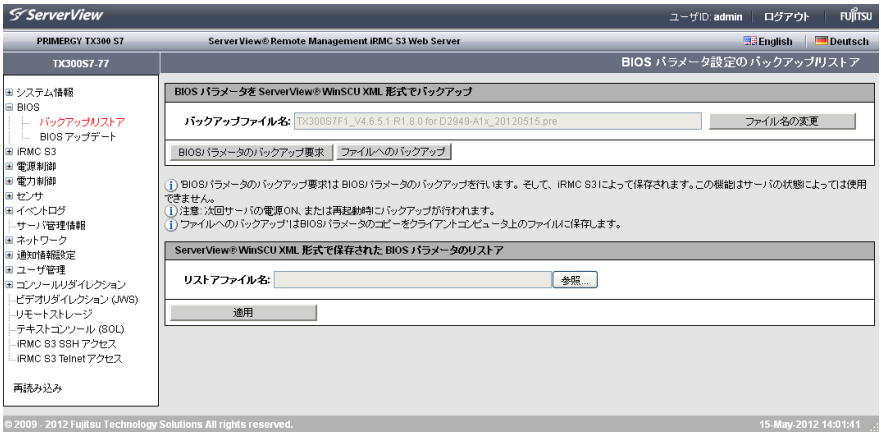


図 74: 「BIOS パラメータ設定のバックアップ / リストア」ページ

7.5.1.1 単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップ

「*BIOS パラメータを ServerView® WinSCU XML 形式でバックアップ*」グループでは、単一の BIOS パラメータの設定を ServerView® WinSCU XML 形式でバックアップして、バックアップをファイルに保存できます。

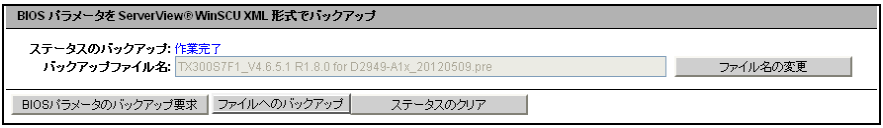


図 75: 単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップ

ステータスのバックアップ
現在のバックアッププロセスのステータスを表示します。正常終了すると「作業完了」と表示されます。「*ステータスのバックアップ*」は、バックアップが現在進行中であるか、完了直後のみ表示されます。

このステータスは、「*ステータスのクリア*」ボタンをクリックするとクリアすることができます。このボタンは、ステータスが現在表示されている場合のみ有効です。

ステータスのクリア
「*ステータスのバックアップ*」に表示されるステータス情報をクリアします。このボタンは、「*ステータスのバックアップ*」に現在ステータスが表示されている場合のみ有効です。

バックアップファイル名
デフォルトでは、この入力フィールドは無効です（グレー表示されています）。最初、iRMC S2/S3 が動的に生成したファイル名が表示されます。

ファイル名の変更
「*バックアップファイル名*」が有効になり、任意のファイル名（*.pre*）を入力できます。

ファイル名の変更
変更したファイル名を保存し、今後、このファイル名がデフォルト
で「バックアップファイル名」に表示されます 。

BIOS パラメータのバックアップ要求

単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップを開始します。バックアップ（「*バックアップファイル名*」フィールドで指定した名前が使用されます）が iRMC S2/S3 にローカルで保存されます。

バックアッププロセスが開始されると、現在のプロセスのステータスが「*ステータスのバックアップ*」に表示されます。

バックアッププロセスについての注意事項

- バックアッププロセス中は、すべてのボタンと入力フィールドが無効です。
- 管理するサーバの電源が切れている場合は、自動的に投入されます。
- 管理するサーバの電源が入っている場合は、リブートが必要です。リブートしないと、バックアッププロセスが「起動待ち」状態のままになります。
- 管理するサーバの電源は、バックアップが完了すると切れます。

ファイルへのバックアップ

BIOS バックアップデータの iRMC S2/S3 ローカルコピーをファイル（*< 任意のファイル名 >.pre*）に保存できるブラウザダイアログが開きます。

このボタンは、単一の BIOS パラメータの ServerView® WinSCU XML 形式でのバックアップが iRMC S2/S3 のローカルストアで使用できる場合のみ表示されます。

7.5.1.2 単一の BIOS パラメータの ServerView® WinSCU XML 形式でのリストア

「*ServerView® WinSCU XML 形式で保存された BIOS パラメータのリストア*」グループでは、単一の BIOS パラメータの設定を ServerView® WinSCU XML 形式のリストアファイルからリストアできます。

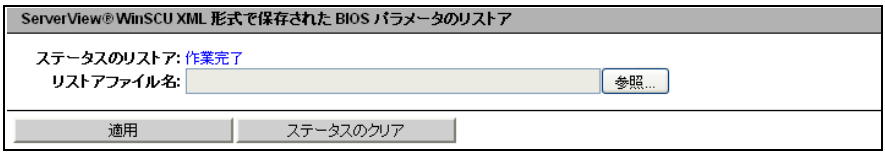


図 76: ServerView® WinSCU XML 形式で保存された BIOS パラメータのリストア

ステータスのリストア
現在のリストアプロセスのステータスを表示します。正常終了すると「作業完了」と表示されます。「*ステータスのリストア*」は、リストアが現在進行中であるか、完了直後のみ表示されます。

このステータスは、「*ステータスのクリア*」ボタンをクリックするとクリアすることができます。このボタンは、ステータスが現在表示されている場合のみ有効です。

ステータスのクリア
「*ステータスのバックアップ*」に表示されるステータス情報をクリアします。このボタンは、「*ステータスのバックアップ*」に現在ステータスが表示されている場合のみ表示されます。

リストアファイル名
入力フィールドをクリックするか、「*参照*」ボタンをクリックすると、ServerView® WinSCU XML 形式の単一の BIOS パラメータのバックアップが含まれるファイル（*.pre*）へ移動できるブラウザダイアログが開きます。

適用
「*リストアファイル名*」フィールドに指定したファイル名に基づいて、単一の BIOS パラメータ設定のリストを開始します。

リストアプロセスが開始されると、現在のプロセスのステータスが「*ステータスのリストア*」に表示されます。

リストアプロセスについての注意事項

- リストアプロセス中は、すべてのボタンと入力フィールドが無効です。
- 管理するサーバの電源が切れている場合は、自動的に投入されます。
- 管理するサーバの電源が入っている場合は、サーバをリブートします。リブートしないと、リストアプロセスが「起動待ち」状態のままになります。
- 管理するサーバの電源は、リストアが完了すると切れます。

7.5.2 BIOS - 「ファイルからアップロード」するか TFTP 経由での BIOS のアップデート

「*BIOS アップデート設定*」ページには、管理するサーバの現在の BIOS 版数が表示され、このページで「ファイルからアップロード」するか TFTP 経由で BIOS をアップデートできます。

PRIMERGY サーバの適切な BIOS イメージは ServerView Suite DVD 1 に保存されています。また、*http://support.ts.fujitsu.com/com/support/downloads.html* からダウンロードすることもできます。

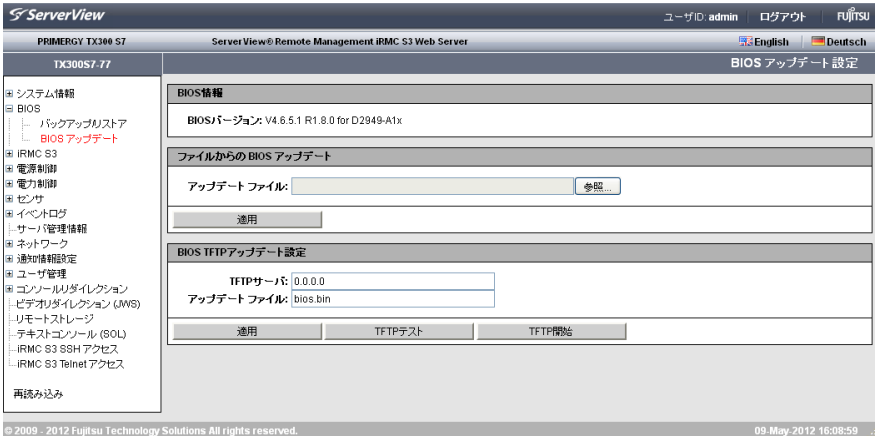


図 77: 「BIOS TFTP アップデート設定」ページ

BIOS のアップデート（フラッシュ）- イベントと注意事項の指針

以下の概要は、「ファイルからアップロード」する BIOS のアップデートと TFTP 経由での BIOS のアップデートの両方に該当します。

この概要に記載される手順を開始する方法の詳細は、この項で後で説明します。

すべてのアップデートプロセスの間、現在のアップデートプロセスが「*BIOS TFTP アップデート設定*」ページに表示されます。

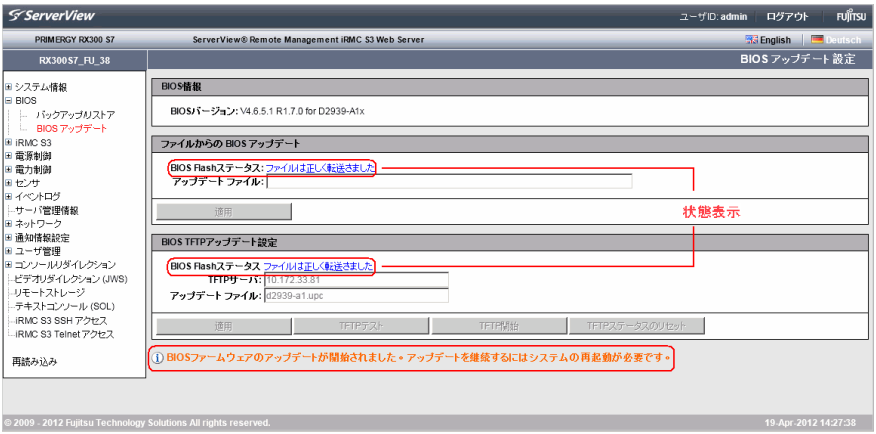


図 78: BIOS アップデート - （TFTP）ダウンロードが正常終了

BIOS のアップデートには、以下の手順が含まれます。

1. 最初の手順で、アップデートファイルをダウンロードします。

   アップデートファイルは *UPC* ファイルである必要があります。

   アップデートファイルをダウンロードすると、以下のようになります。

   – サーバの電源が切れている場合は、自動的に電源が投入され、フラッシュプロセスが開始されます。

   – サーバの電源がすでに投入されている場合は、サーバを再起動して、フラッシュプロセスを開始する必要があります。

   注意！

   BIOS アップデートが現在進行中の場合、サーバの電源を切ったり再起動したり**しないでください**。

2. その後、フラッシュデータがメモリへ転送されます。転送が正常終了すると、ステータス画面が表示されます。
3. 実際のフラッシュプロセスが開始される前に、フラッシュ / アップデートイメージがチェックされます。

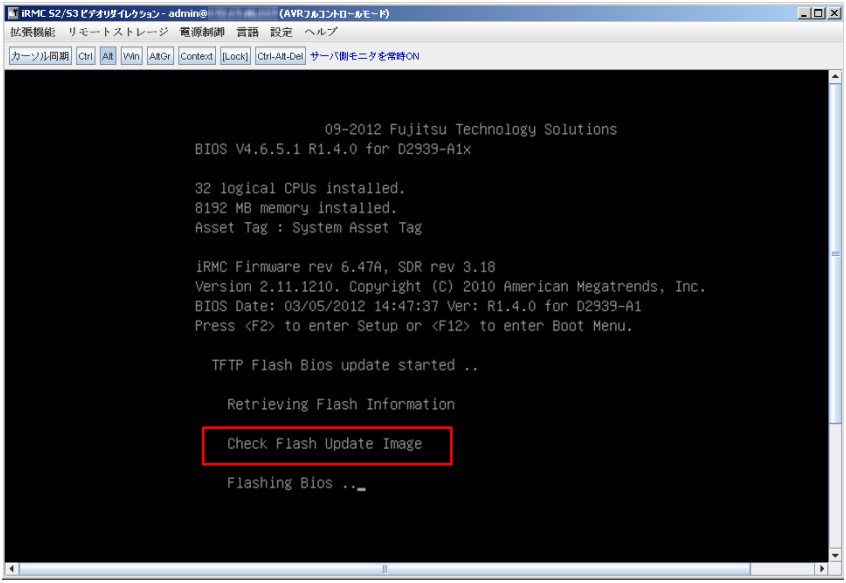


図 79: BIOS アップデート - フラッシュ / アップデートイメージのチェック

4. フラッシュ / アップデートイメージのチェックが正常終了すると、実際のフラッシュプロセスが開始されます。ステータスインジケータに、フラッシュプロセスが何パーセント完了したか表示されます。
5. BIOS アップデートが正常終了すると、サーバの電源が切れます。以下のエントリがシステムイベントログ（SEL）に書き込まれます：

   `BIOS TFTP or HTTP/HTTPS flash OK`

BIOS 情報

このグループには、管理するサーバの現在の BIOS 版数に関する情報が表示されます。

ファイルからの BIOS アップデート

「*ファイルからの BIOS アップデート*」グループでは、管理するサーバの BIOS をオンラインアップデートできます。この場合、現在の BIOS イメージをファイルに提供する必要があります。

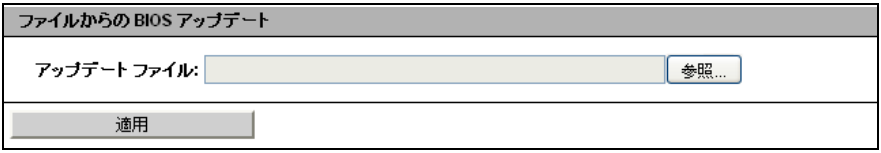


図 80: 「BIOS アップデート設定」ページ - ファイルからの BIOS アップデート

アップデートファイル
BIOS イメージが格納されるファイル

「*ファイルからの BIOS アップデート*」機能を実行するには、*UPC* 形式のファイルが必要です。

参照
アップデートファイルに移動できるファイルブラウザが開きます。

► 「*適用*」をクリックすると、設定が有効になり、BIOS のフラッシュが開始されます。

注意！

BIOS アップデートが現在進行中の場合、サーバの電源を切ったり再起動したり**しないでください**。

BIOS TFTP アップデート設定

「*BIOS TFTP アップデート設定*」グループでは、管理するサーバの BIOS をオンラインアップデートできます。この場合、現在の BIOS イメージを TFTP サーバ上のファイルに提供する必要があります。TFTP を起動すると、BIOS がフラッシュされます。

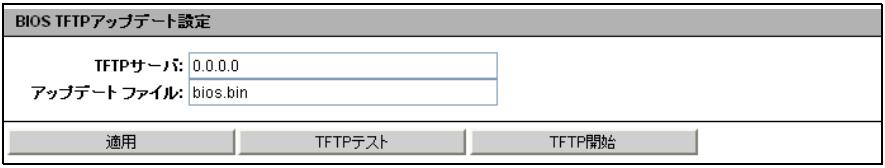


図 81: 「BIOS アップデート設定」ページ - BIOS TFTP アップデート設定

TFTP サーバ
BIOS イメージを含むファイルが格納される TFTP サーバの IP アドレスまたは DNS 名

アップデートファイル
BIOS イメージが格納されるファイル

「*BIOS TFTP アップデート設定*」機能を実行するには、*UPC* 形式のファイルが必要です。

- 「*適用*」をクリックすると設定が有効になります。
- 「*TFTP テスト*」をクリックすると、TFTP サーバへの接続をテストします。
- 「*TFTP 開始*」をクリックすると、BIOS イメージを含むファイルを TFTP からダウンロードして、BIOS のフラッシュを開始します。

注意！

BIOS アップデートが現在進行中の場合、サーバの電源を切ったり再起動したり**しないでください**。

7.6 iRMC S2/S3 - 情報、ファームウェアおよび認証

「*iRMC S2/S3*」エントリには、以下のページへのリンクがあります。

– 169 ページ の「iRMC S2/S3 情報 - iRMC S2/S3 に関する情報」
– 173 ページ の「iRMC S2/S3 ファームウェア設定の保存 - ファームウェア設定の保存」
– 175 ページ の「認証情報のアップロード - DSA/RSA 証明書および DSA/RSA 秘密鍵のアップロード」
– 182 ページ の「自己署名証明書の作成 - 自己署名 RSA 証明書の作成」
– 184 ページ の「iRMC S2/S3 ファームウェアアップデート」

7.6.1 iRMC S2/S3 情報 - iRMC S2/S3 に関する情報

「*iRMC S2/S3 情報*」ページでは、以下のオプションを提供します。

– iRMC S2/S3 のファームウェアおよび SDRR バージョンに関する情報の表示、ファームウェアの選択、ファームウェアイメージのロード、および、iRMC S2/S3 の再起動

– 実行中の iRMC S2/S3 セッションに関する情報の表示

– iRMC S2/S3 へのライセンスキーのアップロード

– iRMC S2/S3 Web インターフェースのレイアウトの設定

図 82: 「iRMC S2/S3 情報」ページ

動作中ファームウェア

「*動作中ファームウェア*」では、iRMC S2/S3 のファームウェアおよび SDRR バージョンに関する情報の表示と、iRMC S2/S3 の再起動ができます。

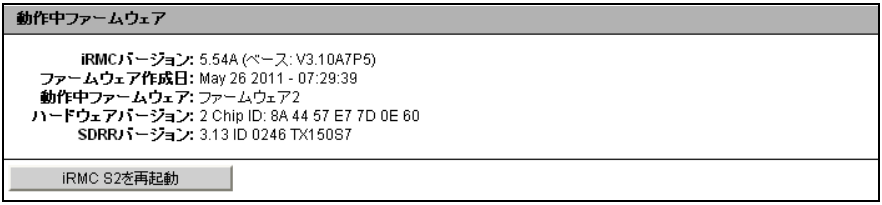


図 83: 「iRMC S2/S3 情報」ページ - ファームウェア情報の表示と iRMC S2/S3 の再起動

iRMC S2/S3 を再起動

iRMC S2/S3 を再起動します。

「*iRMC S2/S3 を再起動* 」ボタンは、管理対象サーバが BIOS POST フェーズの間は使用できません。

実行中のセッション情報

「*実行中のセッション情報*」グループには、実行中の iRMC S2/S3 セッションがすべて表示されます。

実行中のセッション情報

IPアドレス	ユーザ名	ユーザID	接続プロトコル	アクセス権限	アクセス形態	リモートポート
217.9.101.18	admin	2	HTTP	OEM	Web GUI	0
217.9.101.18	cg_test	7	HTTP	Administrator	Web GUI	4282

図 84: 「iRMC S2/S3 情報」ページ - 実行中のセッション情報

ライセンスキー

「*ライセンスキー*」グループで、iRMC S2/S3 にライセンスキーをアップロードすることができます。

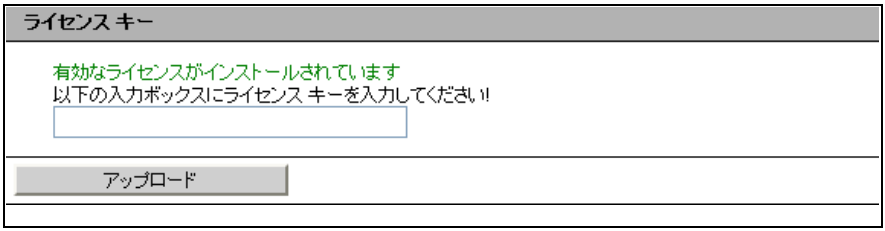


図 85: 「iRMC S2/S3 情報」ページ - ライセンスキー

iRMC S2/S3 の「*ビデオリダイレクション（AVR）*」ファンクション（304 ページを参照）と「*リモートストレージ*」ファンクション（315 ページを参照）を使用するには、有効なライセンスキーが必要です。

ライセンスキーは購入できます。

アップロード
このボタンをクリックすると、入力フィールドのライセンスキーが iRMC S2/S3 にアップロードされます。

iRMC S2/S3 その他のオプション

「*iRMC S2/S3 その他のオプション*」グループでは、iRMC S2/S3 Web インターフェースのレイアウトを設定できます。

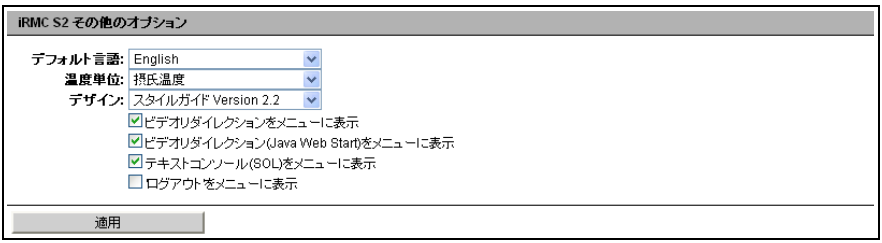


図 86: 「iRMC S2/S3 情報」ページ - その他のオプション

デフォルト言語
言語の初期設定を行います（ドイツ語 / 英語 / 日本語のいずれか）。次回 iRMC S2/S3 Web インターフェースを呼び出す際に有効になります。

温度単位

iRMC S2/S3 Web インターフェースで表示する温度の単位（摂氏 / 華氏）を設定します。この設定は現在のセッションに適用され、次回 iRMC S2/S3 Web インターフェースを呼び出す際に有効になります。

デザイン

iRMC S2/S3 Web インターフェースを表示するためのカラースキーマを設定します。この設定は現在のセッションに適用され、次回 iRMC S2/S3 Web インターフェースを呼び出す際に有効になります。

ビデオリダイレクションをメニューに表示

「*ビデオリダイレクション*」リンクをナビゲーションエリアに追加します。このリンクを使用して直接ビデオリダイレクションを開始できます（311 ページ の「ビデオリダイレクション - AVR の開始」を参照）。

ビデオリダイレクション（Java Web Start）をメニューに表示

「*ビデオリダイレクション（JWS）*」リンクをナビゲーションエリアに追加します。このリンクを使用して直接ビデオリダイレクション（Java Web Start）を開始できます（311 ページ の「ビデオリダイレクション - AVR の開始」を参照）。

テキストコンソール（SOL）メニューに表示

「*テキストコンソール（SOL）*」リンクをナビゲーションエリアに追加します。このリンクを使用して直接テキストコンソールリダイレクションを開始できます（297 ページ の「テキストコンソールのリダイレクション（LAN 上のシリアル通信）- テキストコ ンソールのリダイレクションの開始」の項を参照）。

' ログアウト ' をメニューに表示

このオプションは、「iRMC S2/S3 情報」ページが「*スタイルガイド Version 2.2*」のデザインで表示されている場合のみ使用できます。

「*ログアウト*」リンクをナビゲーションエリアに追加します。このリンクを使用してナビゲーションエリアでログアウトできます。

7.6.2 iRMC S2/S3 ファームウェア設定の保存 - ファームウェア設定の保存

「*iRMC S2/S3 ファームウェア設定の保存*」ページでは、現在のファームウェア設定および iRMC S2/S3 の他の多くの設定をファイルに保存できます。また、ファームウェア設定を iRMC S2/S3 に再びアップロードすることもできます。

– 「*iRMC S2/S3 ファームウェア設定を ServerView® WinSCU の XML 形式で保存*」で選択されたファームウェア設定は、それぞれ、*iRMC_S2_settings.pre* または *iRMC_ S3_settings.pre* というファイル名で保存されます。WinSCU では、「*インポート*」ボタンでファームウェア設定を iRMC S2/S3 に再びアップロードできます。

– 「*iRMC S2/S3 ファームウェア設定をバイナリ（BMCCLONE.exe）で保存*」で選択されたファームウェア設定は、それぞれ、*iRMC_S2_settings.bin* または *iRMC_ S3_settings.bin* というファイル名で保存されます。「*ServerView の XML 形式で保存された iRMC S2/S3 ファームウェア設定の読み込み*」グループを使用してファームウェア設定を iRMC S2/S3 に再びアップロードできます。

注意！

設定は、必ず「*iRMC S2/S3 ファームウェア設定を ServerView® WinSCU の XML 形式で保存*」を使用して保存してください。

「*iRMC S2/S3 ファームウェア設定をバイナリ（BMCCLONE.exe）で保存*」は、管理対象サーバのシステムモジュールを置き換えている場合のみ使用してください。

ユーザ設定を保存する場合（「*ユーザ設定*」）、「*ユーザアカウント変更権限*」権限が必要です。その他の場合はすべて、「*iRMC S2/S3 設定の構成*」権限で十分です。

図 87: 「iRMC S2/S3 ファームウェア設定の保存」ページ

iRMC S2/S3 ファームウェア設定の保存

保存

選択した設定を保存するには、「*保存*」をクリックします。

すべて保存

すべての設定を保存するには、「*すべて保存*」をクリックします。

ServerView の XML 形式で保存された iRMC S2/S3 ファームウェア設定の読み込み

設定ファイル

ServerView® WinSCU の XML 形式の設定ファイル（デフォルト：*iRMC_S2_settings.bin*/*iRMC_S3_settings.bin*）。このファイルからファームウェア設定を iRMC S2/S3 にアップロードします。

参照

設定ファイルに移動できるファイルブラウザが開きます。

7.6.3 認証情報のアップロード - DSA/RSA 証明書および DSA/RSA 秘密鍵のアップロード

「*認証情報のアップロード*」ページでは、認証機関（CA）からの署名付 X.509 DSA/RSA 証明書（SSL）、または DSA/RSA 秘密鍵（SSH）を iRMC S2/S3 にアップロードすることができます。

iRMC S2/S3 は、あらかじめ定義されたサーバ認証証明書（規定の証明書）を提供します。セキュアな SSL/SSH で、iRMC S2/S3 に接続したい場合、認証機関（CA）からの署名付認証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 認証および DSA/RSA 秘密鍵の入力フォーマット：

X.509 DSA/RSA 証明書も RSA/DSA も PEM エンコード形式（ASCII/Base64）に対応してる必要があります。

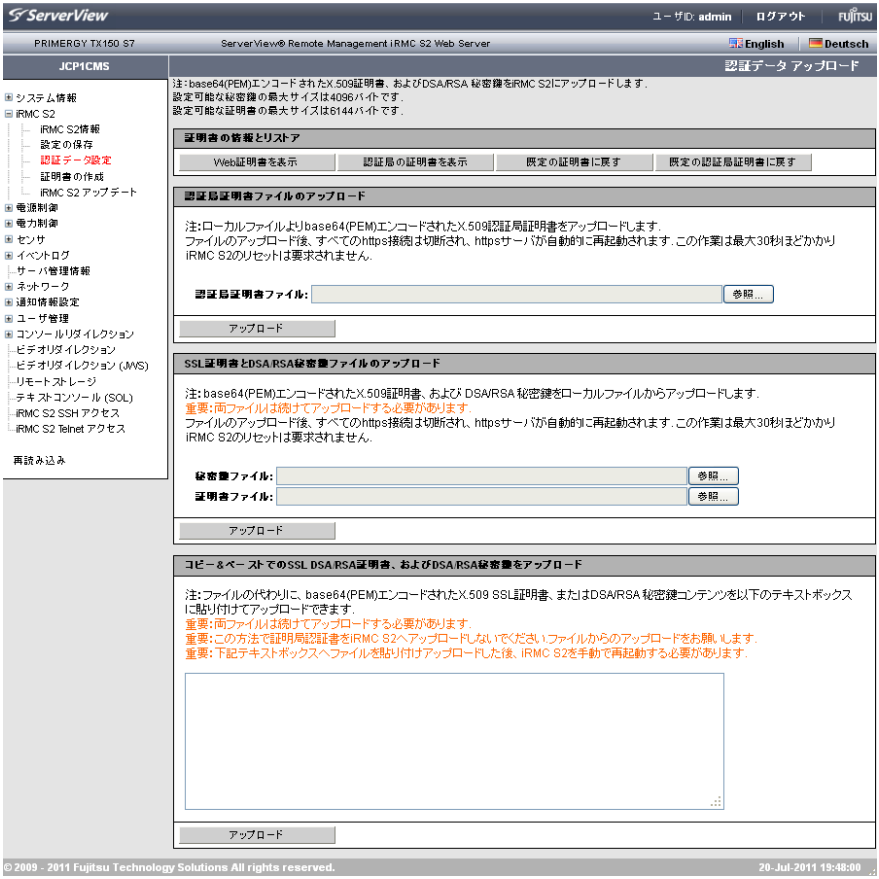


図 88: 「認証データアップロード」ページ

現在有効な （CA）DSA/RSA 証明書の表示

- ► 「*証明書の情報とリストア*」グループで「*Web 証明書を表示*」をクリックすると、有効な SSH/SSL 証明書が表示されます。
- ► 「*証明書の情報とリストア*」グループで「*認証局の証明書を表示*」をクリックすると、現在の有効な認証局証明書が表示されます。

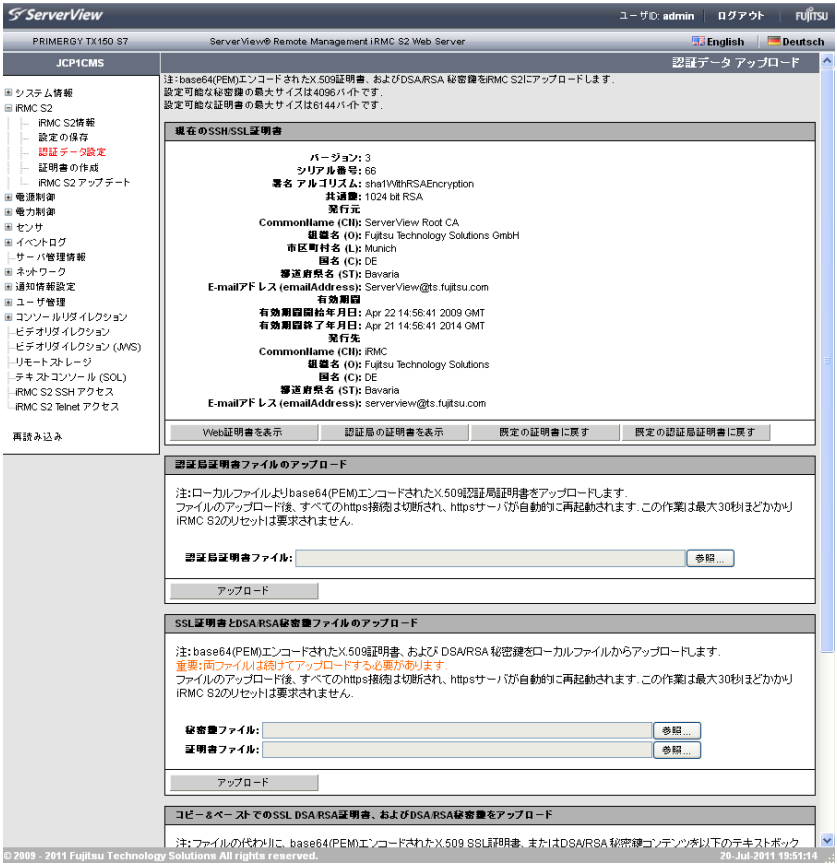


図 89: 「認証データアップロード」ページ - 現在有効な SSL/SSH 証明書の表示

規定の証明書および規定の認証局証明書のリストア

- 「*証明書の情報とリストア*」グループで「*規定の証明書に戻す*」をクリックすると、確認後に規定の証明書がファームウェアに設定されます。
- 「*証明書の情報とリストア*」グループで「*規定の認証局証明書に戻す*」をクリックすると、確認後に規定の認証局証明書がファームウェアに設定されます。

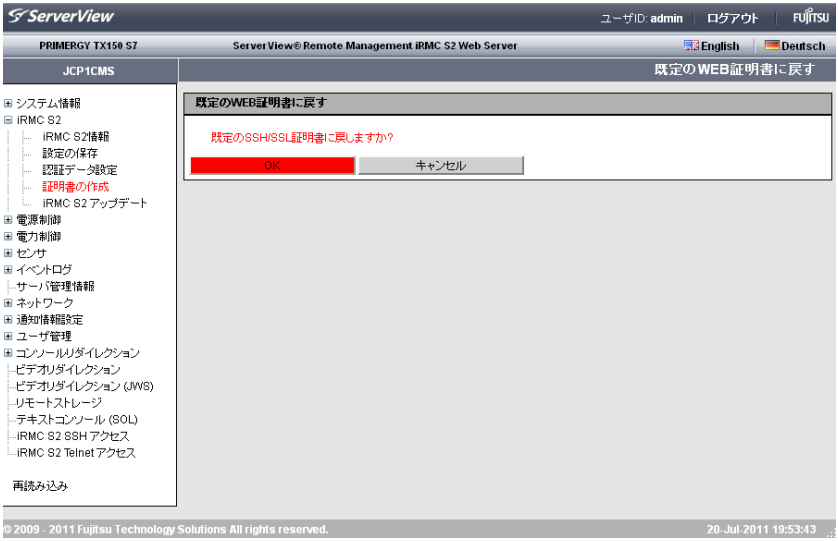


図 90: 「認証データアップロード」ページ - 規定の認証局証明書に戻す

認証局証明書のアップロード

「*認証局証明書ファイルのアップロード*」グループを使用して、認証局証明書をローカルファイルからアップロードすることができます。

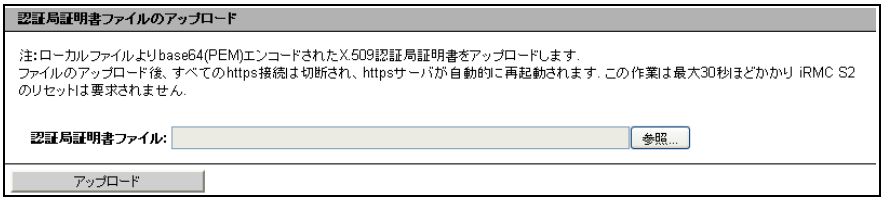


図 91: 認証局証明書のアップロード

次の手順に従います。

- 認証局証明書を管理対象サーバのローカルファイルに保存します。
- このファイルを「*認証局証明書ファイル*」で指定するには、「*参照*」ボタンをクリックして認証局証明書を含むファイルを選択します。
- 「*アップロード*」ボタンをクリックして、証明書または秘密鍵を iRMC S2/S3 にアップロードします。

  証明書また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。iRMC S2/S3 を明示的にリセットする必要はありません。
- 「*認証局証明書を表示*」ボタンをクリックして、証明書のアップロードが成功している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 秘密鍵のアップロード

「*SSL 証明書と DSA/RSA 秘密鍵ファイルのアップロード*」グループを使用してアップロードします。

秘密鍵と証明書は、iRMC S2/S3 に同時にアップロードします。

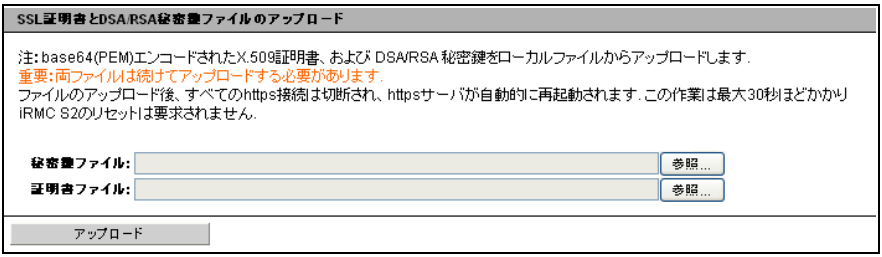


図 92: ローカルファイルからの DSA/RSA 証明書と DSA/RSA 秘密鍵のアップロード

次の手順に従います。

- 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。
- 「*秘密鍵ファイル*」と「*証明書ファイル*」を指定するには、「*参照*」ボタンをクリックして秘密鍵または証明書を含むファイルを選択します。
- 「*アップロード*」ボタンをクリックして、証明書または秘密鍵を iRMC S2/S3 にアップロードします。

  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。このプロセスは最大 30 秒ほどかかることがあります。iRMC S2/S3 を明示的にリセットする必要はありません。
- 「*Web 証明書を表示*」ボタンをクリックして、証明書のアップロードが成功している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

「*コピー&ペーストでの SSL DSA/RSA 証明書、および DSA/RSA 秘密鍵をアップロード*」グループを使用して行います。

この方法を使用して認証局証明書を iRMC S2/S3 にアップロードしないでください。認証局証明書は必ずファイルを使用してアップロードしてください（180 ページ を参照）。

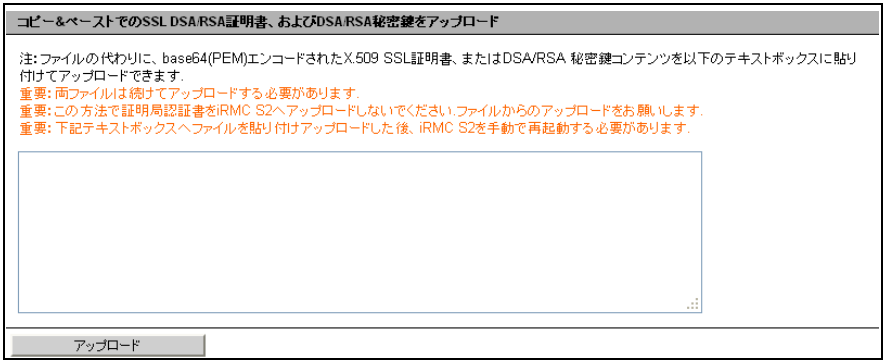


図 93: DSA/RSA 証明書 /DSARSA 秘密鍵の直接入力

次の手順に従います。

- 入力エリアに、X.509 DSA 証明書または DSA 秘密鍵をコピーします。

  同じアップロードで証明書と秘密鍵を同時に入力することはできません。

- 「*アップロード*」ボタンをクリックして、証明書または秘密鍵を iRMC S2/S3 にアップロードします。
- リモートマネジメントを使用して iRMC S2/S3 をリセットします（341 ページ の「サービスプロセッサ - IP パラメータ、識別灯、iRMC S2/S3 リセット」の項 を参照）。

  これは、iRMC S2/S3 にアップロードした証明書および秘密鍵を有効にするために必要です。

- 「*Web 証明書を表示*」ボタンをクリックして、証明書のアップロードが成功していることを確認してください。

7.6.4 自己署名証明書の作成 - 自己署名 RSA 証明書の作成

「*自己署名 RSA 証明書の作成*」ページを使用して自己署名証明書を作成できます。

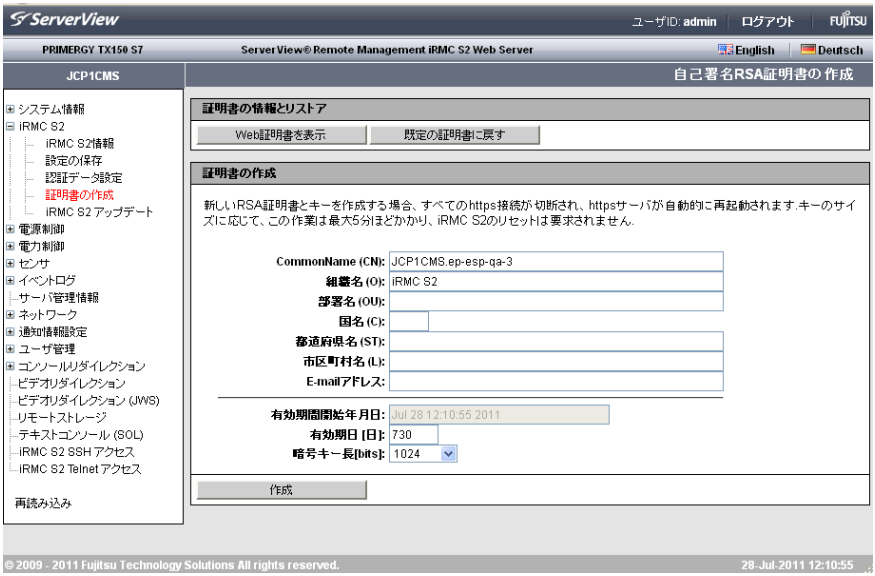


図 94: 「自己署名証明書の作成」ページ

証明書の情報とリストア

「*証明書の情報とリストア*」グループを使用して、現在有効な DSA/RSA 証明書の表示や、規定の RSA/DSA 証明書のリストアができます。

Web 証明書を表示
このボタンを使用して、現在有効な DSA/RSA 証明書を表示することができます。

規定の証明書に戻す
このボタンを使用して、確定後、ファームウェアに提供された既定の証明書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。

- ▶ 「*証明書の作成*」に詳細な必要項目を入力してください。
- ▶ 「*作成*」をクリックして、証明書を作成してください。

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ます。iRMC S2/S3 を明示的にリセットする必要はありません。

7.6.5 iRMC S2/S3 ファームウェアアップデート

「*iRMC S2/S3 ファームウェアアップデート*」ページを使用して、iRMC S2/S3 ファームウェアをオンラインでアップデートすることができます。そのためには、リモートワークステーション上、または TFTP サーバ上に更新するファームウェアイメージを用意する必要があります。

ここでは、iRMC S2/S3 ファームウェアおよびファームウェア選択に関する情報も参照してください。

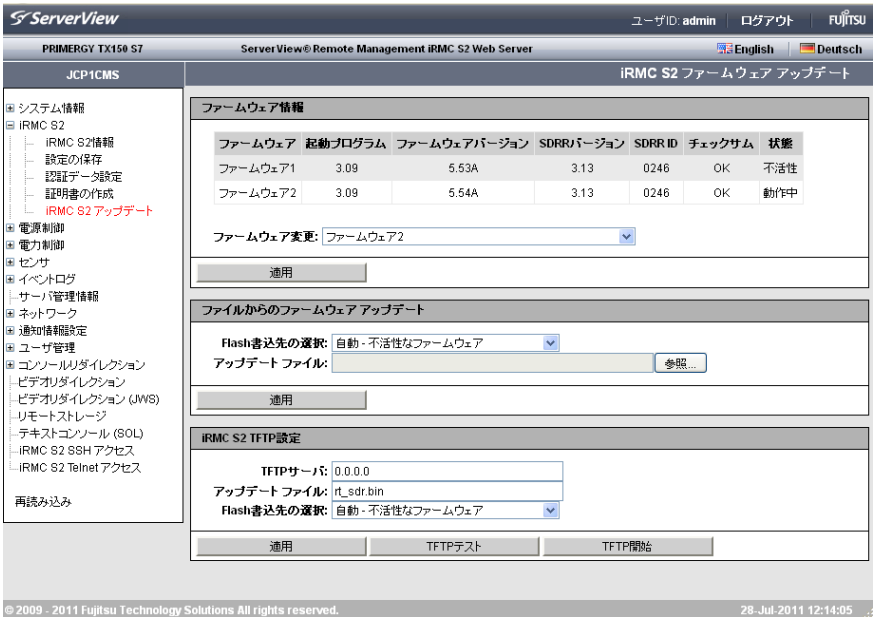


図 95: 「iRMC S2/S3 ファームウェアアップデート」ページ

ファームウェア情報

「*ファームウェア情報*」では、iRMC S2/S3 のファームウェアバージョンおよび SDRR バージョンに関する情報の表示と、ファームウェアセレクタの設定ができます。

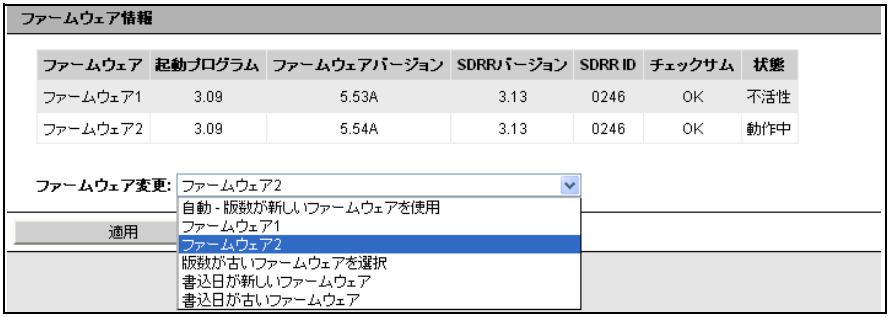


図 96: iRMC S2/S3 ファームウェアアップデート - ファームウェア情報

ファームウェア変更

ファームウェアセレクタを使用して、次回 iRMC S2/S3 を再起動したときに、有効にするファームウェアを選択します。

以下のオプションがあります。

– *自動 - 版数が新しいファームウェアを使用*

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。

– *ファームウェア 1*

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。

– *ファームウェア 2*

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。

– *版数が古いファームウェアを選択*

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。

– *書込日が新しいファームウェア*

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。

– *書込日が古いファームウェア*

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。

適用

「*適用*」をクリックして、「*ファームウェア変更*」で設定したオプションをファームウェアに設定します。

ファイルからのファームウェアアップデート

「*ファイルからのファームウェアアップデート*」ページを使用して、iRMC S2/S3 ファームウェアをオンラインでアップデートできます。そのためには、リモートワークステーション上のファイルに更新するファームウェアイメージを保存する必要があります。

適切なファームウェアは、PRIMERGY サーバの ServerView Suite DVD 1 に収録されています。また、
http://support.ts.fujitsu.com/com/support/downloads.html からダウンロードすることもできます。

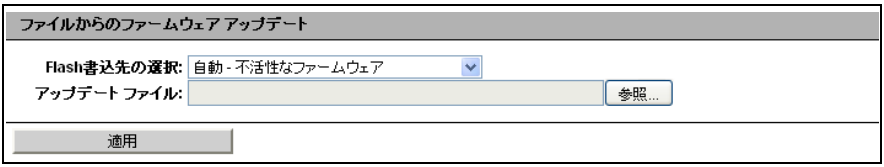


図 97: 「iRMC S2/S3 ファームウェアアップデート」- ファイルからのファームウェアアップデート

Flash 書込先の選択

アップデートする iRMC ファームウェアを指定します。

以下のオプションがあります。

– *自動－不活性なファームウェア*

アクティブでないファームウェアが自動的に選択されます。

– *ファームウェア 1*

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。

– *ファームウェア 2*

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。

アップデートファイル
ファームウェアイメージが保存されたファイルを指定します。

以下のファイルによって、アップデートを行うたびに（ランタイムファームウェアおよび SDR レコード）、iRMC S2/S3 ファームウェアのコンポーネントが 1 つアップデートされます。

rt_sdr_<D-number>_4_08g_00.bin ファイルは、PRIMERGY サーバまたはブレードサーバによっては利用可能です。これにより、iRMC S2/S3 ファームウェアのすべてコンポーネントのアップデートを一度の操作で行うことができます。

dcod<FW-Version>.bin
ランタイムファームウェアをアップデートします。

<SDR-Version>.SDR
SDR レコードをアップデートします。

参照
アップデートファイルに移動できるファイルブラウザが開きます。

- 「*適用*」ボタンをクリックして設定を有効にし、iRMC S2/S3 ファームウェアのアップデートを開始します。

iRMC S2/S3 TFTP 設定

「*ファイルからのファームウェアアップデート*」ページを使用して、iRMC S2/S3 ををオンラインでアップデートできます。そのためには、TFTP サーバ上のファイルにファームウェアイメージを保存する必要があります。

適切なファームウェアは、PRIMERGY サーバの ServerView Suite DVD 1 に収録されています。また、
http://support.ts.fujitsu.com/com/support/downloads.html からダウンロードすることもできます。

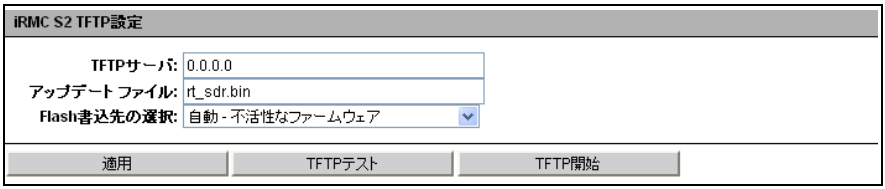


図 98: 「iRMC S2/S3 ファームウェアアップデート」ページ - iRMC S2/S3 TFTP 設定

TFTP サーバ
ファームウェアイメージのファイルが保存される TFTP サーバの IP address または DNS 名。

アップデートファイル
ファームウェアイメージが保存されたファイルを指定します。

以下のファイルによって、TFTP が開始されるたびに（ランタイムファームウェアおよび SDR レコード）、iRMC S2/S3 ファームウェアのコンポーネントが 1 つアップデートされます。

rt_sdr_<D-number>_4_08g_00.bin ファイルは、PRIMERGY サーバまたはブレードサーバによっては利用可能です。これにより、iRMC S2/S3 ファームウェアのすべてコンポーネントのアップデートを、TFTP サーバを使用して一度の操作で行うことができます。

dcod<FW-Version>.bin
ランタイムファームウェアをアップデートします。

<SDR-Version>.SDR
SDR レコードをアップデートします。

Flash 書込先の選択
アップデートする iRMC ファームウェアを指定します。

以下のオプションがあります。

– *自動－不活性なファームウェア*

アクティブでないファームウェアが自動的に選択されます。

– *ファームウェア 1*

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。

– *ファームウェア 2*

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。

- 「*適用*」ボタンをクリックして設定を有効にします。
- 「*TFTP テスト*」ボタンをクリックして、TFTP サーバとの接続をテストします。
- 「*TFTP 開始*」ボタンクリックして、TFTP サーバからファームウェアを含むファイルをダウンロードし、iRMC S2/S3 ファームウェアのアップデートを開始します。

7.7 電源制御

「*電源制御*」エントリには、PRIMERGY サーバの電源管理ページへのリンクが含まれます。

– 190 ページ の「電源投入 / 切断 −サーバの自動電源投入 / 遮断」を参照。
– 194 ページ の「電源制御オプション - サーバの電源管理の設定」を参照。
– 201 ページ の「電源装置情報 - 電源装置および FRU コンポーネントの IDPROM データ」を参照。

7.7.1 電源投入 / 切断 ーサーバの自動電源投入 / 遮断

「*Power On/Off*」ページでは、管理サーバの電源オン / オフを行います。サーバの現在の電源状態が表示され、次回の起動時のサーバの設定も行うことができます。

図 99: 「Power On/Off」ページ

電源状態概要

「*電源状態概要*」グループには、サーバの現在の電源状態の情報、および最後のサーバの電源オン / オフの理由が表示されます。また、サーバの電源が投入されてからの経過時間（月、日、分）も表示されます。

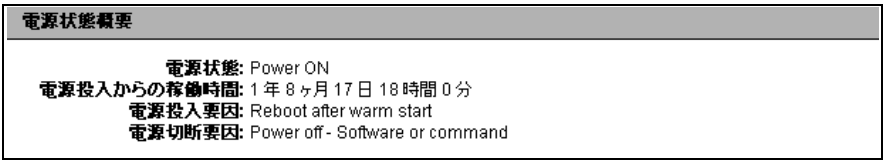


図 100: 「Power On/Off」ページ - 電源状態概要

起動オプション

「*起動オプション*」グループには、**次回**起動時のシステム構成を設定することができます。BIOS がシステムの起動プロセスに割り込んだ場合か、POST フェーズでエラーが発生した場合かを設定できます。

ここで設定するオプションは、次回起動時の 1 度のみ有効になります。

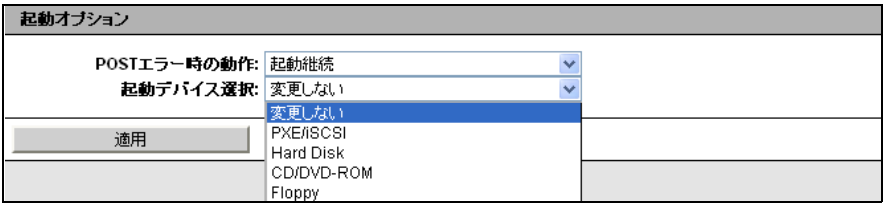


図 101: 「電源制御」ページ - 起動オプション

- 「*POST エラー時の動作*」リストから、目的の BIOS 動作を選択します。

  起動継続
  POST フェーズ中にエラーが発生しても、起動プロセスを継続します。

  起動停止
  POST フェーズ中にエラーが発生した場合、起動プロセスを停止します。

- 「*起動デバイス選択*」リストから、起動を開始するストレージメディアを選択してください。

  以下のオプションを選択できます。

  - 「*変更しない*」: システムを前回と同じストレージメディアから起動します。
  - 「*PXE/iSCSI*」: システムをネットワーク上の PXE あるいは iSCSI から起動します。
  - 「*Hard Disk*」: システムをハードディスクから起動します。
  - 「*CDROM/DVD*」: システムを CD/DVD から起動します。
  - 「*Floppy*」: システムをフロッピーディスクから起動します。

- 「*適用*」ボタンをクリックして、設定を有効にします。

電源制御 - サーバの電源投入・切断 / サーバの再起動

「*電源制御*」グループを使用して、サーバの電源投入 / 切断や、サーバの再起動を行うことができます。

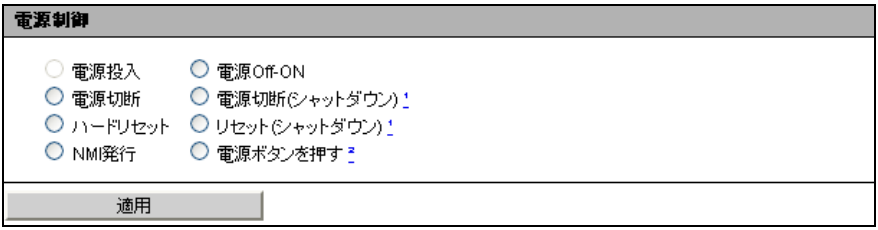


図 102: 「Power On/Off」ページ、再起動（サーバ電源投入）

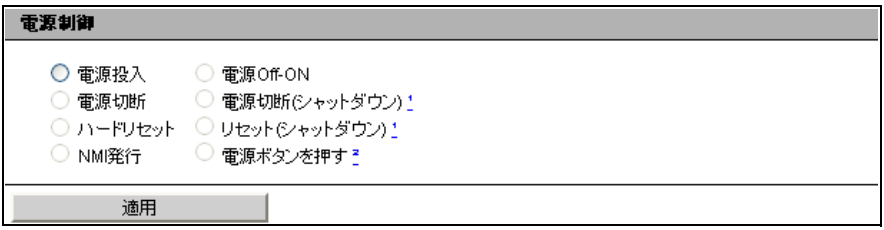


図 103: 「Power On/Off」ページ、再起動（サーバ電源切断）

電源投入
: サーバの電源を投入します。

電源切断
: オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。

ハードリセット
: オペレーティングシステムの状態にかかわらず、サーバを完全に再起動します（コールドスタート）。

NMI 発行
: マスク不可能な割り込み（NMI：Non-Maskable Interrupt）を発行します。NMI は、システムの標準の割り込みマスクテクノロジで無視できるプロセッサ割り込みです。

電源ボタンを押す
: インストールされているオペレーティングシステムと設定されている動作に依存して、電源オフボタンを短く押してさまざまな動作をトリガできます。これらの動作では、コンピュータのシャットダウンや、スタンバイモードまたはスリープモードへの切り替えができます。

電源 Off-ON
サーバの電源が完全に切断され、設定した時間の経過後、再び投入されます。この時間は、「*ASR&R オプション*」グループの「*パワー サイクル間隔*」フィールドで設定できます（237 ページを参照）。

電源切断（シャットダウン）
OS をシャットダウンして電源を切断します。
このオプションは、OS に ServerView エージェントがインストールされ、かつ、動作中であり、iRMC S2/S3 にサインオンして「接続中」の場合のみ使用できます。

リセット（シャットダウン）
OS をシャットダウンして電源を切断します。
このオプションは、OS に ServerView エージェントがインストールされ、かつ、動作中であり、iRMC S2/S3 にサインオンして「接続中」の場合のみ使用できます。

► 「*適用*」ボタンをクリックして目的の動作を開始します。

7.7.2 電源制御オプション - サーバの電源管理の設定

「*電源制御オプション*」ページを使用して、停電復旧後のサーバ動作およびサーバの電源オン / オフ時刻の設定を行うことができます。

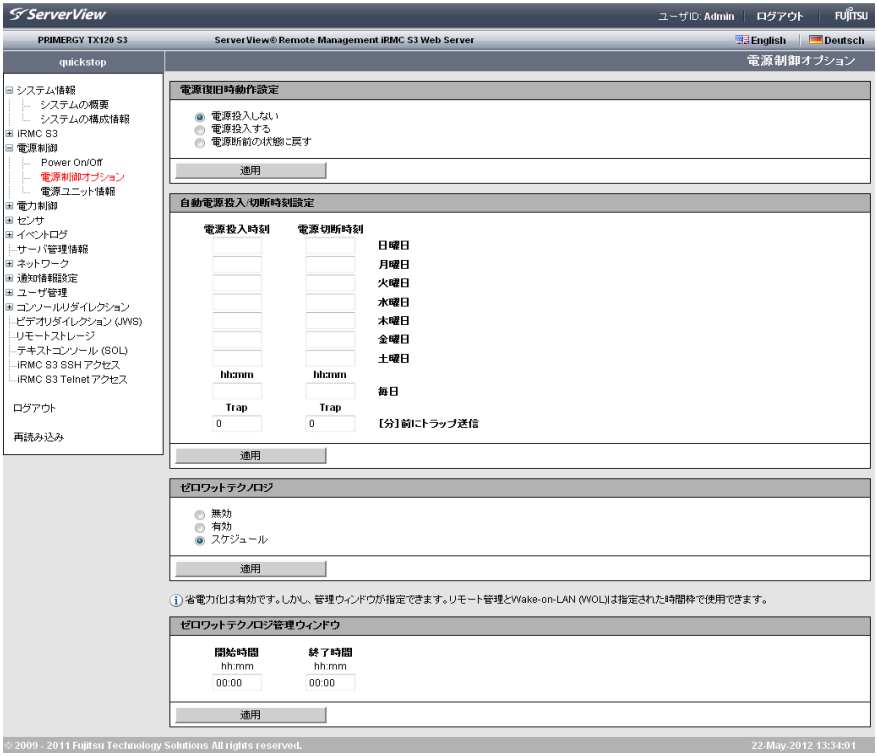


図 104: 「電源制御オプション」ページ

電源復旧時動作設定 - 停電復旧後のサーバ動作の指定

「*電源復旧時動作設定*」グループを使用して、停電復旧後のサーバの電源管理動作を指定できます。

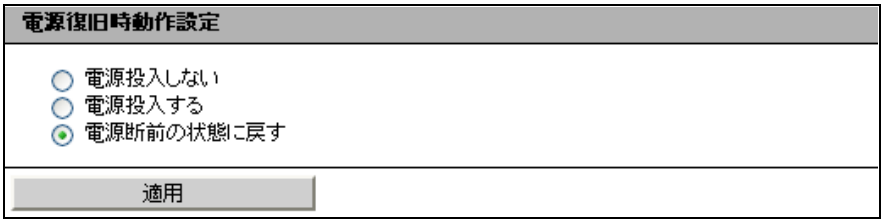


図 105: 「電源制御オプション」ページ - 電源復旧時動作設定

電源投入しない
停電復旧後、サーバの電源を常にオフのままにします。

電源投入する
停電復旧後、サーバの電源を常にオンにします。

電源断前の状態に戻す
停電前のサーバの電源状態（オンまたはオフ）に復旧します。

► 「*適用*」ボタンをクリックして、設定を有効にします。

設定した動作は、停電復旧後に実行されます。

自動電源投入 / 切断時刻設定 - サーバの自動電源投入 / 切断時刻設定

「*自動電源投入 / 切断時刻設定*」グループの入力フィールドを使用して、特定曜日の指定時間にサーバの自動電源投入 / 切断時刻を設定することができます。

「*毎日*」フィールドの指定が最優先です。

「*Trap*」フィールドを使用して、iRMC S2/S3 が予定された管理対象サーバの電源投入 / 切断前に SNMP トラップを管理コンソールに送信するかどうかを設定することもできます。その場合、このイベントの何分前に行うかを指定できます。値に「0」を設定すると、トラップは送信されません。

図 106: 「電源制御オプション」ページ - 自動電源投入 / 切断時刻設定

▶ 「*適用*」ボタンをクリックして、設定を有効にします。

ゼロワット技術

なお、次の点に注意してください。

– この機能は iRMC S3 でのみサポートされます。

– この機能は、一部の PRIMERGY サーバではサポートされていません。

「ゼロワット技術」によって、サーバのスタンバイ時の消費電力をゼロワットに削減できます。サーバの電源をオフにするたびに、サーバのスタンバイ消費電力が 0 W になります（*ゼロワット*モード）。

*ゼロワット*モードでは、サーバはリモートで管理できなくなります。「*Power*」ボタンまたは「*PSU Primary Resume*」ボタンを押さないとサーバの電源をオフにできません。

「*スケジュール*」オプションを適用すると（200 ページを参照）、PSU が*ゼロワット*モードから復帰して、リモート管理と Wake-on-LAN（WOL）の両方を使用できる時間を指定できます。

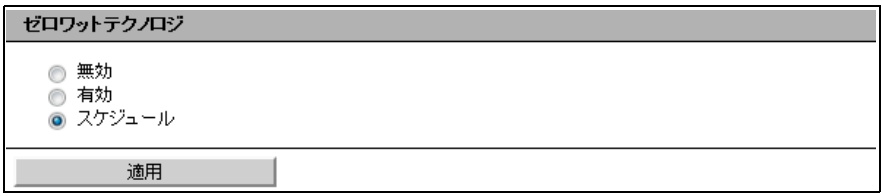


図 107: 「電源制御オプション」ページ - ゼロワット技術

無効

*ゼロワット*モードが無効になり、標準の電源投入 / 切断モードになります。サーバはいつでもリモートで管理できます。

有効

*ゼロワット*モードを無効します。

「*有効*」が設定されていても、以下の場合には*ゼロワット*モードはブロックされます。

- パワーサイクル要求 / 電源オン遅延

  パワーサイクル要求によって、*ゼロワット*モードが有効にならずにサーバの電源がオフになります。このとき、*ゼロワット*モードは、パワーサイクルの電源オフと電源オンの間の遅延時に有効になりません。

  – 遅延中に電源オン要求が発生すると、サーバは遅延終了後に電源がオンになります。

  – 遅延中に電源オン要求が発生しなかった場合、遅延期間が経過した後、iRMC S3 で*ゼロワット*モードが有効になります。

- 熱電源オンの禁止

  温度監視モード「システム熱電源オンの禁止」モードが BIOS/UEFI セットアップメニューで指定されている場合、*ゼロワット*モードは有効になりません。

- ASR&R

  現在、ASR&R アクションによってリトライカウンタがカウントダウンされている場合、*ゼロワット*モードは有効になりません。これは、リトライカウンタが 0 になった後にサーバの電源がオフに鳴った場合にも適用されます。

- 「*自動電源投入 / 切断時刻設定*」をスケジュールした場合（196 ページを参照）

  iRMC S3 の「*電源制御オプション*」ページで*自動電源投入 / 切断*タイマが設定されている場合、*ゼロワット*モードは有効にできません。

  *ゼロワット*モードは、サーバの電源がオフになっているときに*自動電源投入 / 切断*タイマが無効になった場合も、有効にできません。この場合、次に電源オフになったときのみ、*ゼロワット*モードが有効になります。スケジュールされた*自動電源投入 / 切断*タイマによって*ゼロワット*モードの有効化が妨げられることはありません。

- グローバルエラー LED

  グローバルエラー LED でシステム状態に何らかの問題があることが示される場合、iRMC S3 で *ゼロワット*モードは有効になりません。これは、サーバの電源がオフになっている場合でも、システム状態の問題を報告できなければならないからです。

- システム ID LED

  システム ID LED が点灯している間、iRMC S3 で *ゼロワット*モードは有効になりません。

- ビデオリダイレクション（AVR）

  AVR セッションが現在アクティブな場合、iRMC S3 で *ゼロワット*モードは有効になりません。すべての AVR セッションが終了したら（アクティブな AVR がない状態）、iRMC S3 で *ゼロワット*モードが有効になります。

- リモートストレージサーバ（RSS）、Telnet/SSH セッション

  RSS セッションまたは SSH/Telnet セッションが現在アクティブな場合、iRMC S3 で *ゼロワット*モードは有効になりません。これにより、iRMC S3 へのリモートインターフェース接続が失われなくなります。

- AC 電源障害

  AC 障害が発生して PSU（電源装置）が *ゼロワット*モードまたはスケジュールモードになっている場合、PSU はシステムスタンバイに戻ります。電源復旧時動作設定（195 ページを参照）に応じて、iRMC S3 はサーバの電源がオンかどうかを判断します。電源復旧時動作設定が「*常に電源切断*」に設定されている場合、AC が故障しても *ゼロワット*モードにはなりません。次回、システムの電源をオンにしたときに *ゼロワット*モードに移行できます。

スケジュールモード

ゼロワット モードを有効し、*0 Watt Technology Administration Window* を表示します。「*0 Watt Technology Administration Window*」では、PSU を *ゼロワット*モードから復帰させる間隔を指定でき、リモート管理と Wake-on-LAN（WOL）の両方を使用できます。

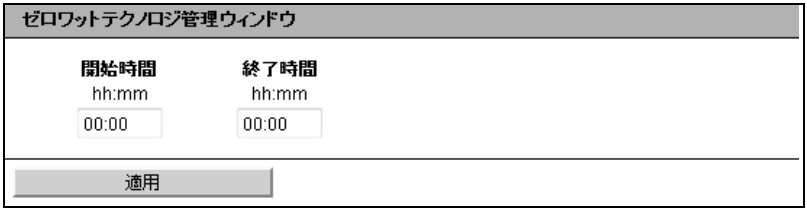


図 108: 「電源制御オプション」ページ - 0 Watt Technology Administration Window

開始時刻

時間間隔の開始を定義します（*hh:mm*）。

終了時刻

時間間隔の終了を定義します（*hh:mm*）。

► 「*適用*」をクリックすると設定が有効になります。

► 「*適用*」をクリックすると設定が有効になります。

サーバの自動電源投入/切断時刻設定をご使用時、OSの電源設定によっては、サーバのシャットダウンができない場合があります。
例）Windowsの場合
「Windowsシステムのシャットダウンの時に電源を切らない」を「有効」に設定した場合

7.7.3 電源装置情報 - 電源装置および FRU コンポーネントの IDPROM データ

「*電源装置情報*」ページには、電源装置に関する情報と、サーバの FRU の IDPROM データが表示されます。

「*CSS 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

図 109: 「電源装置情報」ページ

7.8 電源制御 - サーバの消費電力制御

「*電力制御*」エントリには、管理対象サーバの消費電力の監視と制御に関するページのリンクが含まれます。

– 203 ページ の「消費電力制御 - サーバの消費電力制御」を参照。

– 194 ページ の「電源制御オプション - サーバの電源管理の設定」を参照。（iRMC S2/S3 が搭載されるすべてのサーバに表示されるわけではありません。）

– 210 ページ の「消費電力モニタリング履歴 - サーバの消費電力の表示」（iRMC S2/S3 が搭載されるすべてのサーバに表示されるわけではありません。）

7.8.1 消費電力制御 - サーバの消費電力制御

「*消費電力制御*」ページでは、iRMC S2/S3 が PRIMERGY サーバの消費電力制御に使用するモードを指定できます。

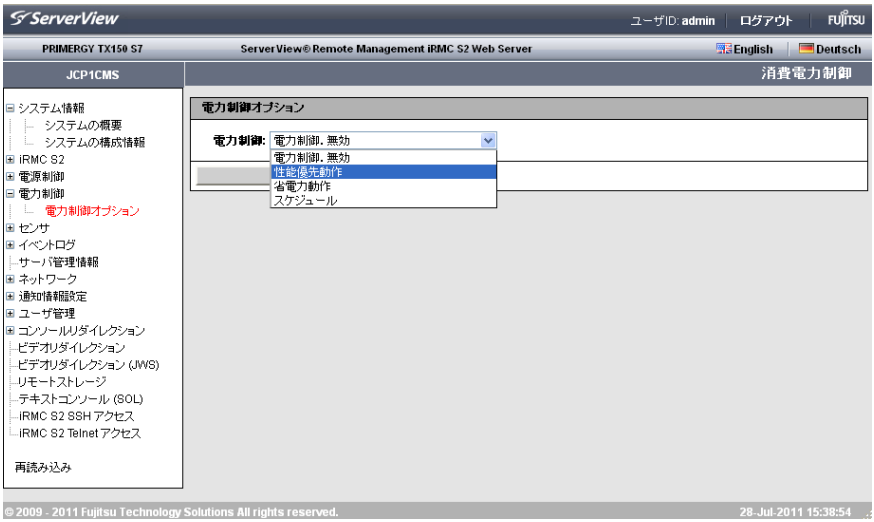


図 110: 「消費電力制御」ページ

前提条件：

消費電力制御を行うには以下の条件を満たす必要があります。

- PRIMERGY 管理対象サーバが、この機能をサポートしている必要があります。
- 「*Enhanced Speed Step*」または「*Processor Power Management*」オプションが、BIOS セットアップの「*Advanced*」メニューで有効である必要があります。

「*電源制御オプション*」グループまたは「*電力制御スケジュール*」で電力制御を「電力制限」に設定した場合、「*電力制限オプション*」グループも表示されます（205 ページを参照）。

電力制御オプション

「*電力制御オプション*」グループでは、電力制御モードを選択し、消費電力の時間的経過を監視するかどうかを指定できます。

電力制御モード

管理対象サーバの消費電力制御モードは以下の通りです。

– *電力制御. 無効* :

iRMC S2/S3 は、オペレーティングシステムに電力制御を許可します。

– *性能優先動作* :

iRMC S2/S3 は、サーバがベストパフォーマンスになるよう電力制御を行います。この場合、消費電力が増える可能性があります。

– *静音操作* （iRMC S3 のみ）:

iRMC S3 は、再低減の騒音排出を実現するようにサーバを制御します。

– *最小消費電力* :

iRMC S2/S3 は、最小消費電力を達成するようにサーバを制御します。この場合、サーバのパフォーマンスは常に理想的であるとは言えません。

– *電力制限* :

「*電力制限オプション*」グループが表示されます（207 ページ の「電力制限オプション」を参照）。

– *スケジュール* :

iRMC S2/S3 は、SCU を使用して定義可能なスケジュールに従って消費電力を制御します（205 ページ の「電力制御スケジュール」を参照）。

消費電力監視単位

消費電力を表示する単位は以下の通りです :

– *Watt*

– *BTU/h*（BTU/ 時（British Thermal Unit / 時、1 BTU / 時は、0.293 ワットに相当します。）

消費電力モニタリング有効

このオプションを有効にした場合、消費電力は連続的に監視されます。

電力監視は、バージョン 3.32 以降のファームウェアではデフォルトで有効です。

この設定は、電力監視をサポートする PRIMERGY サーバにのみ有効です。

► 「*適用*」ボタンをクリックして、設定を有効にします。

電力制御スケジュール

「*電力制御スケジュール*」グループでは、iRMC S2/S3 が管理対象サーバの消費電力を制御するために使用する詳細なスケジュールとモード（オペレーティングシステムによる制御、ベストパフォーマンス、最小電源消費）を指定できます。

「*電力制御スケジュール*」グループは、「*電力制御オプション*」グループの電力制御モードを「*スケジュール*」に設定した場合のみ表示されます。

電力制御スケジュールモードの設定は、「*エンハンススピードステップ*」オプションが BIOS セットアップで有効であることが前提です。有効でない場合、その旨のメッセージが表示されます。

「Enhanced Speed Step」オプションが有効であるにもかかわらずこのメッセージが表示される場合、以下の理由が考えられます。

– サーバの CPU （低電力 CPU）が、電力制御スケジュールをサポートしていない。

– システムが、現在 BIOS POST フェーズである。

図 111: 「消費電力制御」ページ（スケジュール）

時刻 1

iRMC S2/S3 が、「*モード 1*」で、指定する曜日に消費電力制御を開始する時刻 [hh : ss]。

時刻 2

iRMC S2/S3 が、「*モード 2*」で、指定する曜日に消費電力制御を開始する時刻 [hh : ss]。

モード 1

iRMC S2/S3 が、「*時刻 1*」で、指定する曜日に使用するよう設定された電力制御モード。

モード 2

iRMC S2/S3 が、「*時刻 2*」で、指定する曜日に使用するよう設定された電力制御モード。

「*時刻 1*」< 「*時刻 2*」となるように設定してください。そうでない場合、「*モード 2*」に指定した電力制御モードは次の週の該当する曜日の「*時刻 2*」でしか有効になりません。

「*毎日*」フィールドの指定が最優先です。

► 「*適用*」ボタンをクリックして、設定を有効にします。

Server Configuration Manager を使用して電力制御スケジュールを設定することもできます（351 ページ の「Server Configuration Manager を使用した iRMC S2/S3 の設定」の章を参照）。

電力制限オプション

「*電力制限オプション*」グループは、次の場合に表示されます。

– 電力制御モードの「*電力制限*」が選択され、「*電力制御オプション*」グループで有効である場合。

– 「*電力制御オプション*」グループで電力制御モードの「*スケジュール*」が有効の場合、「*電力制御スケジュール*」グループでの電力制御モードの「*電力制限*」が少なくともー か所以上有効である場合。

この電力制限は、この電力制御モードが「*消費電力制御スケジュール*」グループで有効なすべての期間に適用されます。

図 112: 「消費電力制御」ページ（スケジュール）

電力制限
: 最大消費電力（単位：Watt）。

警告しきい値
: 最大消費電力のパーセンテージでしきい値が、「*電力制限*」に表示されています。しきい値に達すると、「*電力制限到達時の動作*」で定義した動作が実行されます。

電力制限の据置期間

電力制限のしきい値に到達してから、電力制限到達時の動作が実行されるまでの待機時間（分）。

電力制限到達時の動作

電力制限に到達し、待機時間が経過したときの動作。

継続稼動する

動作は行われません。

電源切断（シャットダウン）

OS をシャットダウンし、電源を切断します。

このオプションは、OS に ServerView エージェントがインストールされ、かつ、動作中であり、iRMC S2/S3 にサインオンして「接続中」の場合のみサポートされます。

電源切断

オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。

動的な電力制御を有効にする

電力制限を動的に制御します。このオプションを有効にする場合、iRMC S2/S3 は電力制限の据置期間の際に直後に全体のサーバシステムの消費電力を CPU の消費電力をを抑えることで制御します。

7.8.2 現在のシステム消費電力 - 現在のシステム消費電力の表示

このビューは、iRMC S2/S3 が搭載される一部の PRIMERGY サーバではサポートされていません。

「*現在のシステム消費電力*」ページには、システムのコンポーネントおよびシステム全体の現在の消費電力が表示されます。

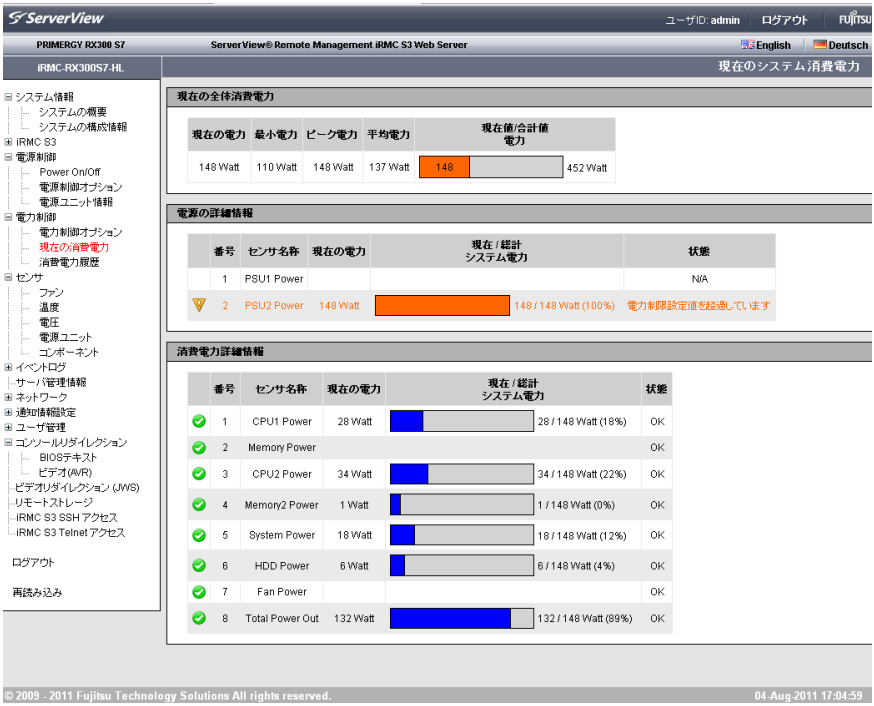


図 113: 「現在のシステム消費電力」ページ

7.8.3 消費電力モニタリング履歴 - サーバの消費電力の表示

「*消費電力モニタリング履歴*」ページには、PRIMERGY サーバの消費電力のグラフが表示されます。

このページは、iRMC S2/S3 が搭載される一部の PRIMERGY サーバでサポートされていません。

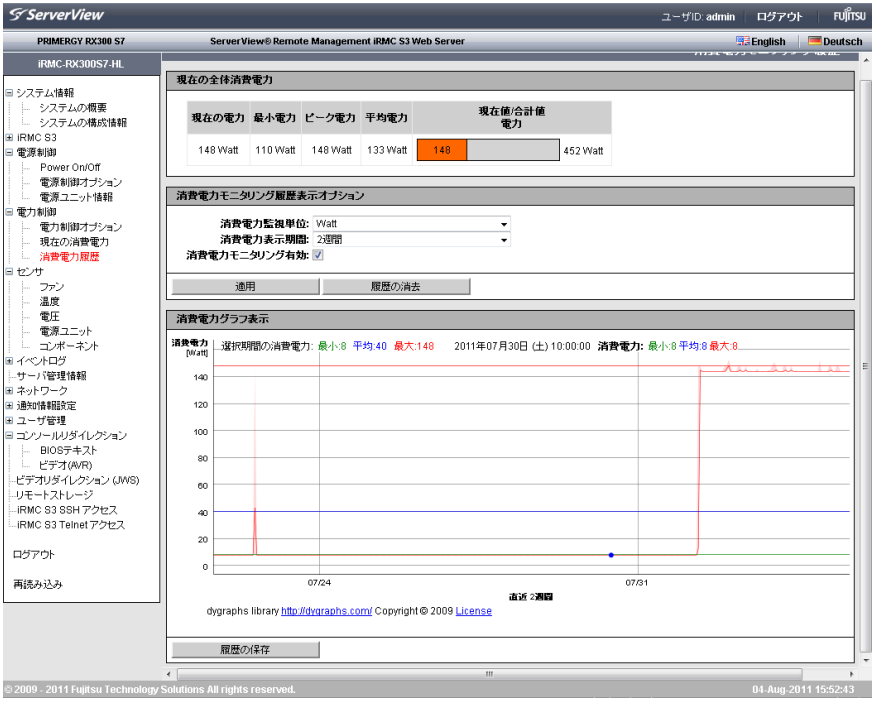


図 114: 「消費電力モニタリング履歴」ページ

現在の全体消費電力

このオプションは、一部の PRIMERGY サーバではサポートされていません。

「*現在の全体消費電力*」では、現状設定された間隔で計測したサーバの消費電力の情報が表示されています。現在の電力、最小電力、ピーク電力および平均電力が表示されます。

グラフィカルな表示でも、サーバの可能な最大消費電力量と現在の消費電力量を比較して表示しています。

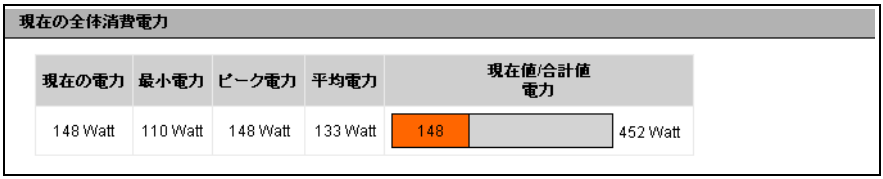


図 115: 消費電力モニタリング履歴 - 現在の全体消費電力

消費電力モニタリング履歴表示オプション

消費電力モニタリング履歴表示オプションでは、消費電力を表示するパラメータを設定することができます。

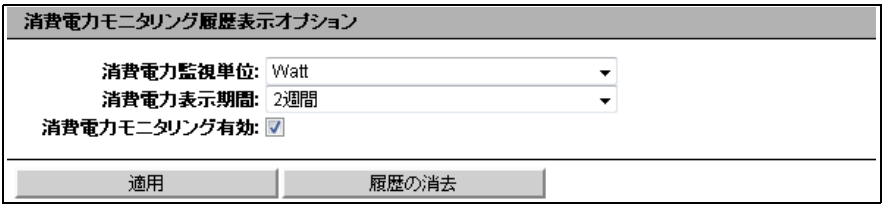


図 116: 消費電力モニタリング履歴 - 消費電力モニタリング履歴表示オプション

消費電力監視単位

電力単位：

- Watt
- *BTU/h*（BTU/ 時（British Thermal Unit/ 時、1 BTU/ 時は 0.293 ワットに相当します。）

消費電力表示期間

消費電力のグラフの表示期間。

以下の間隔を選択できます。

1 時間

デフォルトです。
最新の 1 時間を表示します（60 の値）。1 分間毎に計測が行われますので、最新の 1 時間の計測値を表示します。

12 時間

最新の 12 時間を表示します。5 分間隔での計測結果を表示します（5 番目毎の計測、全部で 144 の値）。

1 日

最新の 24 時間を表示します。10 分間隔での計測結果を表示します（10 番目毎の計測、全部で 144 の値）。

1 週間

最新の 1 週間を表示します。1 時間間隔での計測結果を表示します（60 番目毎の計測、、全部で 168 の値）。

2 週間

最新の 1 週間を表示します。およそ 4 時間間隔での計測結果を表示します（120 番目毎の計測、全部で 168 の値）。

1 ヶ月

最新の 6 ヶ月を表示します。およそ 1 日間隔での計測結果を表示します（240 番目毎の 計測、全部で 180 の値）。

1 年

最新の 12 ヶ月を表示します。2 日間隔での計測結果を表示します（2880 番目毎の 計測、全部で 180 の値）。

消費電力モニタリング有効

電力監視を実行するかどうかを指定します。

電力監視は、バージョン 3.32 以降のファームウェアではデフォルトで有効です。

この設定は、消費電力のログの記録をサポートしている PRIMERGY サーバのみに適用できます。

- ▶ 「*適用*」ボタンをクリックして、設定を有効にします。
- ▶ 「*履歴の消去*」ボタンをクリックして、表示されているデータを消去します。

消費電力グラフ表示

「*消費電力グラフ表示*」には、グラフ形式で管理対象サーバの消費電力量が表示されます（「*消費電力履歴オプション*」を使用します）。実際の消費電力と「消費電力グラフ表示」に表示される消費電力の差が、約 20% になることがあります。

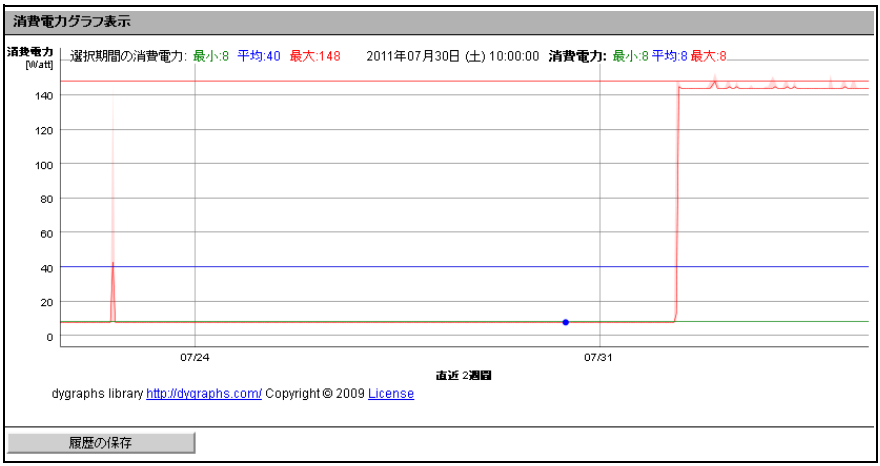


図 117: 消費電力モニタリング履歴 - 消費電力グラフ表示

7.9 センサ - センサの状態確認

「センサ」エントリには、管理対象サーバのセンサをテストするページがあります。

- 215 ページ の「ファン - ファン状態確認」を参照。
- 218 ページ の「温度 - 温度センサの状態確認」を参照。
- 220 ページ の「電圧 - 電圧センサの状態確認」を参照。
- 221 ページ の「電源ユニット - 電源ユニットの状態確認」を参照。
- 223 ページ の「センサの状態 - サーバのコンポーネントの状態確認」を参照。

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を表示するだけでなく、カラーコードと状態アイコンも使用しています。

緑 / 	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ています。 システムの稼動状態は、まだ危険な状態ではありません。
赤 / 	測定値は致命的しきい値を超えています。 システムの稼動状態は、危険な状態にある可能性があり、 データ喪失の危険があります。

表 6: センサの状態

7.9.1 ファン - ファン状態確認

「ファン」ページには、ファンおよびそれらの状態に関する情報が表示されます。

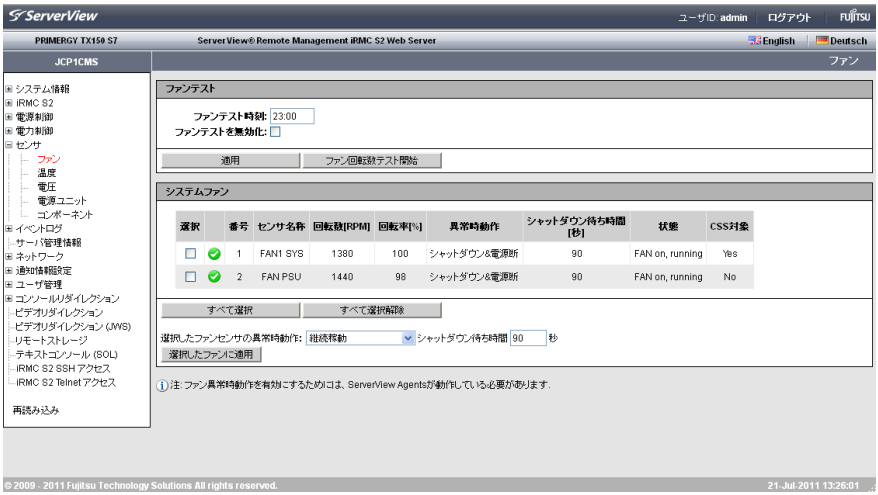


図 118: 「ファン」ページ

ファンテスト - ファンのテスト

「*ファンテスト*」グループでは、ファンのテストを自動的に開始する時刻を設定したり、手動で開始したりできます。

以前使用されていたフルスピードテストの代わりに、現在ほとんどの新しいシステムには、必要な速度に近い速度でファンテストを実行するように改良されたファンテスト機能があります。この場合、ファンテストでは音声による通知はありません。

ファンテスト時刻
ファンテストが自動的に開始される時刻を入力します。

ファンテストを無効化
このオプションを選択すると、ファンテストが行われなくなります。

- 「*適用*」ボタンをクリックして、設定を有効にします。
- 「*ファン回転数テスト開始*」ボタンをクリックして、ファンのテストを開始します。

システムファン - ファンが故障した場合のサーバ動作の設定

「*システムファン*」グループを使って、ファンの状態に関する情報を確認することができます。オプションおよびボタンを個々のファンまたはすべてのファンに対して有効にすることができます。また、ファンが故障した場合、何秒後にサーバをシャットダウンするか否かを設定することができます。

すべて選択
すべてのファンを選択します。

すべて選択解除
すべての選択を解除します。

- 故障時に特別な処置を行うファンを選択します。

► ワークエリアの下方のリストを使って、故障発生時の動作を定義します。

– 「*継続稼働*」を選択すると、選択されたすべてのファンが故障してもサーバはシャットダウンされません。

– 「*シャットダウン & 電源断*」を選択すると、選択されたファンが故障した場合、サーバはシャットダウンされ、かつ、電源が切断されます。このオプションを選択する場合、リストの右のフィールドで、ファンの故障からシャットダウンまでの時間（シャットダウン待ち時間）を設定します。

冗長ファンの場合、1 つ以上のファンが故障し、「*シャットダウン & 電源断*」がこれらのファンに設定されている場合のみ、シャットダウンが実行されます。

► 「*選択したファンに適用*」ボタンをクリックして、選択したファンへの設定を有効にしてください。

7.9.2 温度 - 温度センサの状態確認

「*温度*」ページには、CPU、FBD（FullyBuffered DIMM）および周囲の温度など、温度センサが計測したサーバのコンポーネントの温度情報が表示されます。

図 119: 「温度」ページ

選択およびボタンで、個々の温度センサあるいはすべての温度センサに対してオプションを設定することができます。また、選択されたセンサが危険温度に達した場合、サーバをシャットダウンするかどうかの設定を行うこともできます。

すべて選択
すべての温度センサを選択します。

すべて選択解除
すべての選択を解除します。

► 危険温度に達した場合の動作を定義するセンサを選択します。

► ワークエリアの下方のリストを使って、危険温度到達時の動作を定義します。

  – 「*継続稼働*」を選択すると、選択されたセンサが危険温度に達してもサーバはシャットダウンされません。

  – 「*シャットダウン & 電源断*」を選択すると、選択されたセンサが危険温度に達した場合、サーバはシャットダウンされ、かつ、電源が切断されます。

► 「*選択したセンサに適用*」ボタンをクリックして、選択した温度センサへの設定を有効にしてください。

7.9.3 電圧 - 電圧センサの状態確認

「*電圧*」ページには、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に関する情報が表示されます。

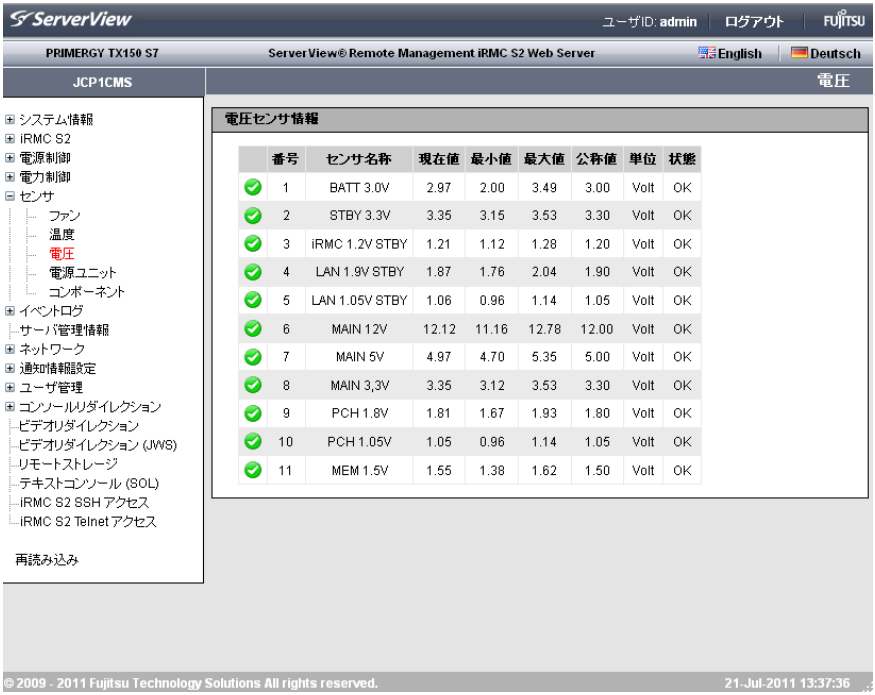


図 120: 「電圧」ページ

7.9.4 電源ユニット - 電源ユニットの状態確認

「*電源ユニット*」ページには、電源ユニットに関する情報が表示されます。一部のタイプのサーバでは、「*電源ユニット*」ページで電源ユニットの冗長設定を行うこともできます。

図 121: 「電源ユニット」ページ

電源冗長構成

この機能は一部のサーバでは使用できません。

「*電源冗長構成*」グループでは、管理対象サーバに冗長モードを設定できます。実際に使用できるオプションはサーバの機能によって異なります。

1 + 1 予備 PSU
合計 2 台の PSU の場合に、1 台の PSU が故障してもシステムの稼働が保証されます。

2 + 1 予備 PSU
合計 3 台の PSU の場合に、1 台の PSU が故障してもシステムの稼働が保証されます。

3 + 1 予備 PSU
合計 4 台の PSU の場合に、1 台の PSU が故障してもシステムの稼働が保証されます。

2 + 2（2 AC 電源）
4 台の PSU のうち 2 台がそれぞれ別個の AC ソースに接続されます。これにより、電力線や 1 台の PSU が故障しても、システムは稼働し続けることができます。

1 + 1（2 AC 電源）
（合計 2 台の PSU の）各 PSU が別個の AC ソースに接続されます。これにより、電力線や 1 台の PSU が故障しても、システムは稼働し続けることができます。

7.9.5 センサの状態 - サーバのコンポーネントの状態確認

「*センサの状態*」ページには、サーバのコンポーネントの状態に関する情報が表示されます。「*CSS 対象*」列には、各コンポーネントの CSS（**C**ustomer **S**elf **S**ervice）機能のサポートの有無が示されます。

番号	センサ名称	センサ種類ID	センサ種類別通し番号	LED点灯状況	信号状態	CSS対象
1	Ambient	External Environment	0	No	OK	No
2	CPU	Processor	0	No	OK	No
3	DIMM-1A	Memory Device	0	Yes	OK	Yes
4	DIMM-2A	Memory Device	1	Yes	OK	Yes
5	DIMM-3A	Memory Device	2	Yes	空きスロット	Yes
6	DIMM-1B	Memory Device	3	Yes	OK	Yes
7	DIMM-2B	Memory Device	4	Yes	OK	Yes
8	DIMM-3B	Memory Device	5	Yes	空きスロット	Yes
9	FAN1 SYS	Fan/Cooling Device	1	Yes	OK	Yes
10	FAN PSU	Power Supply	0	No	OK	No
11	BATT 3.0V	Battery	0	No	OK	No
12	Voltages	System Board	0	No	OK	No
13	Temp	External Environment	0	No	OK	No
14	BBU	Battery	1	No	N/A	Yes
15	PSU Connector	Cable/Interconnect	0	No	OK	No
16	PSU	Power Supply	0	No	OK	No
17	Power Level	Power Monitoring	1	No	OK	No
18	Slot1	PCI Bus	0	Yes	N/A	Yes
19	Slot2	PCI Bus	1	Yes	N/A	Yes
20	Slot3	PCI Bus	2	Yes	N/A	Yes
21	Slot4	PCI Bus	3	Yes	N/A	Yes
22	Slot5	PCI Bus	4	Yes	N/A	Yes
23	Slot6	PCI Bus	5	Yes	N/A	Yes
24	HDD	Disk Drive Bay	0	No	N/A	Yes
25	BIOS	System Firmware (BIOS/EFI)	0	No	OK	No
26	Agent	System Mgmt. Software	0	No	OK	No
27	iRMC	System Mgmt. Module	0	No	OK	No

図 122: 「センサの状態」ページ

「*センサ名称*」のエントリの「iRMC」、「Agent」、「BIOS」、「VIOM」は、iRMC S2/S3、エージェント、BIOS 、VIOM がエラーを検出したことを示します。これは、iRMC S2/S3、エージェント、BIOS、VIOM 自体が故障していることを意味するものではありません。

センサ名称「HDD」および「HDD<n>」を含むエントリ、エージェントレス HDD 監視（「アウトオブバンド」HDD 監視）

センサ名称「HDD」または「HDD<n>」（n = 1、2、...）を含むエントリは、ハードディスクドライブ（HDD）のステータスを示します：

– *センサ名称*「HDD」を含むエントリは、個々の HDD のステータスをまとめることにより、サーバの HDD 全体のステータスを示します。

  サーバの HDD 全体のステータスは、ServerView エージェントと ServerView RAID Manager によって、読み取られて iRMC S2/S3 に報告されます。

– *センサ名称*「HDD<n>」（n = 1、2、...）を含むエントリは、個々の HDD のステータスを示します。

  この機能は iRMC S3 でのみサポートされます。

  管理するサーバが「エージェントレス HDD 監視」機能（「アウトオブバンド HDD 監視」とも呼ばれます）をサポートする場合、個々の HDD の HDD<n> ステータスは、専用のライトパスステータスセンサーで直接読み取られて iRMC S3 に報告されます。

	59	HDD1	Disk Drive Bay	1	No	OK	Yes
	60	HDD2	Disk Drive Bay	2	No	Prefail	Yes
	61	**HDD3**	**Disk Drive Bay**	**3**	**No**	**Failed**	**Yes**
	62	HDD4	Disk Drive Bay	4	No	OK	Yes

図 123: 個々の HDD のステータス表示

7.10 システムイベントログ / 内部イベントログ - サーバイベントログの表示と設定

ナビゲーション領域の「*イベントログ*」エントリには、IPMI イベントログ（システムイベントログ（SEL））と iRMC S2/S3 の内部イベントログの表示および設定を行うページへのリンクが含まれます。

– 227 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」を参照。

  内部イベントログには、監査イベントに関する情報（ログオンイベント、AVR 接続イベントなど）やその他の情報（IPv6 関連の情報および LDAP ユーザ名など）を提供するエントリが含まれます。

– 230 ページ の「iRMC S2/S3 イベントログ情報 - 内部イベントログと関連するエントリに関する情報の表示」を参照。

  IPMI SEL には、オペレーティングシステムのブート / シャットダウン、ファンの故障、iRMC S2/S3 ファームウェアのフラッシュなどのイベントに関する情報を提供するエントリが含まれます。

– 233 ページ の「システムイベントログ設定 - IPMI SEL と内部イベントログの設定」を参照。

色付きのアイコンが、それぞれのイベントまたはエラーカテゴリに割り当てられています。

	危険
	重度
	軽度
	情報
	顧客自己保守（CSS）イベント

表 7: システムイベントログ / 内部イベントログの内容 - エラーカテゴリ

7.10.1 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

「*システムイベントログ内容*」ページには、IPMI SEL に関する情報と SEL エントリが表示されます。IPMI SEL には、オペレーティングシステムのブート / シャットダウン、ファンの故障、iRMC S2/S3 ファームウェアのフラッシュなどのイベントに関する情報を提供するエントリが含まれます。

「*CSS 対象*」列には、各イベントについて、イベントが CSS（**C**ustomer **S**elf **S**ervice）コンポーネントによってトリガされたかどうかを示します。

図 124: 「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

「*システムイベントログ (SEL) 情報*」グループには、IPMI SEL 内のエントリ数の情報が表示されます。最後のエントリがいつ追加または削除されたかも表示します。

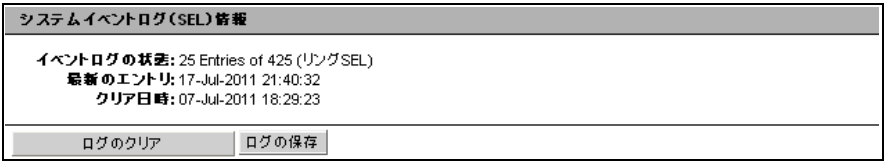


図 125: 「システムイベントログ内容」ページ - システムイベントログ情報

ログのクリア

「*ログのクリア*」ボタンをクリックすると、IPMI SEL 内のすべてのエントリを消去することが できます。

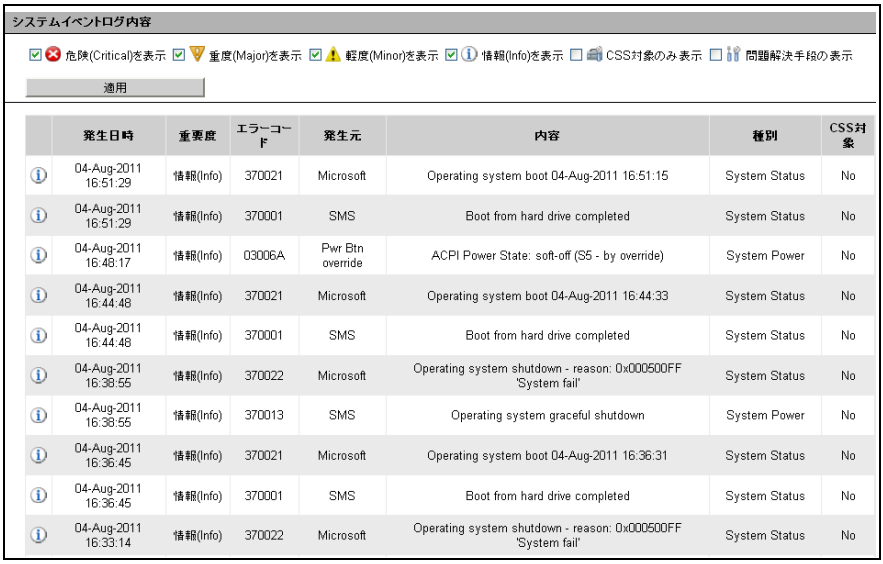
ログの保存

「*ログの保存*」ボタンをクリックした後、IPMI SEL のエントリを含む *iRMC S2/S3_EventLog.sel* ファイルをダウンロードできます。

システムイベントログ内容

「*システムイベントログ内容*」グループには、重要度によってフィルタリングされた SEL エントリが表示されます。

「*システムイベントログ内容*」グループで、現在のセッション中にフィルタ条件を変更できます。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。その後は、デフォルト設定がまた適用されます。



	発生日時	重要度	エラーコード	発生元	内容	種別	CSS対象
	04-Aug-2011 16:51:29	情報(Info)	370021	Microsoft	Operating system boot 04-Aug-2011 16:51:15	System Status	No
	04-Aug-2011 16:51:29	情報(Info)	370001	SMS	Boot from hard drive completed	System Status	No
	04-Aug-2011 16:48:17	情報(Info)	03006A	Pwr Btn override	ACPI Power State: soft-off (S5 - by override)	System Power	No
	04-Aug-2011 16:44:48	情報(Info)	370021	Microsoft	Operating system boot 04-Aug-2011 16:44:33	System Status	No
	04-Aug-2011 16:44:48	情報(Info)	370001	SMS	Boot from hard drive completed	System Status	No
	04-Aug-2011 16:38:55	情報(Info)	370022	Microsoft	Operating system shutdown - reason: 0x000500FF 'System fail'	System Status	No
	04-Aug-2011 16:38:55	情報(Info)	370013	SMS	Operating system graceful shutdown	System Power	No
	04-Aug-2011 16:36:45	情報(Info)	370021	Microsoft	Operating system boot 04-Aug-2011 16:36:31	System Status	No
	04-Aug-2011 16:36:45	情報(Info)	370001	SMS	Boot from hard drive completed	System Status	No
	04-Aug-2011 16:33:14	情報(Info)	370022	Microsoft	Operating system shutdown - reason: 0x000500FF 'System fail'	System Status	No

図 126: 「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

危険（Critical）を表示、*重度（Major）を表示*、*軽度（Minor）を表示*、*情報（Info）を表示*、*CSS 対象のみ表示*
必要に応じて、このデフォルト値以外の 1 つ以上の重要度を選択することもできます。

問題解決手段の表示
このオプションを選択すると、重要度「*Critical*」または「*Major*」の各 SEL エントリについて、推奨される問題解決手段が表示されます。

► 「*適用*」ボタンをクリックして、現在のセッション中に設定を有効にします。

7.10.2 iRMC S2/S3 イベントログ情報 - 内部イベントログと関連するエントリに関する情報の表示

「iRMC S2 イベントログ内容」ページには、内部イベントログに関する情報と、関連するエントリが表示されます。内部イベントログには、監査イベント（ログオンイベント、AVR 接続イベントなど）およびその他の情報（IPv6 関連の情報および LDAP ユーザ名など）が含まれます。

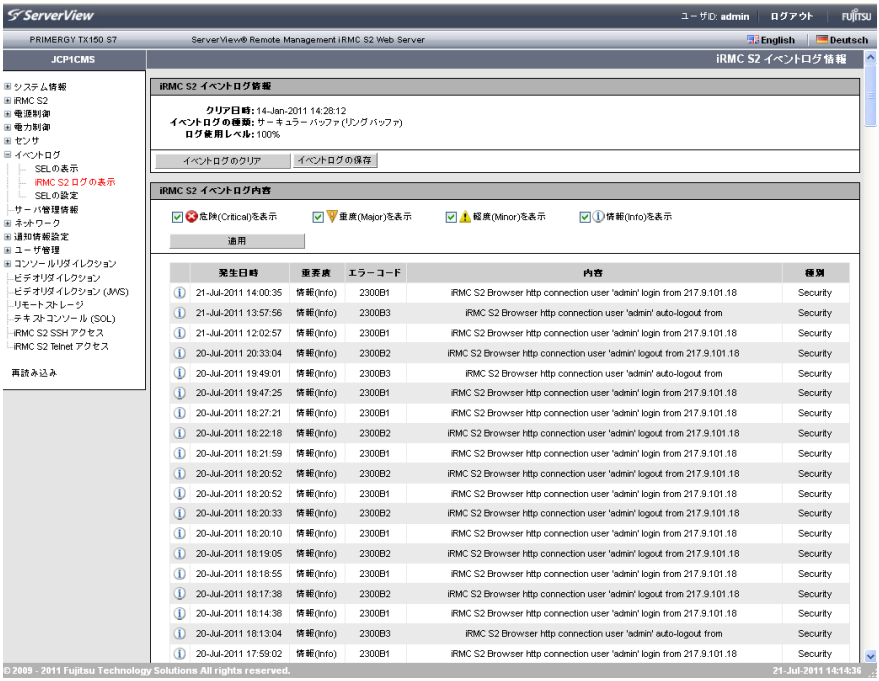


図 127: 「iRMC S2/S3 イベントログ情報」ページ

iRMC S2/S3 イベントログ情報

「*iRMC S2/S3 イベントログ情報*」グループには、内部イベントログ内のエントリ数の情報が表示されます。最後のエントリがいつ追加または削除されたかも表示します。

図 128: 「システムイベントログ情報」ページ - システムイベントログ情報

イベントログのクリア

「*イベントログのクリア*」ボタンをクリックすると、内部イベントログ内のすべてのエントリを消去することが できます。

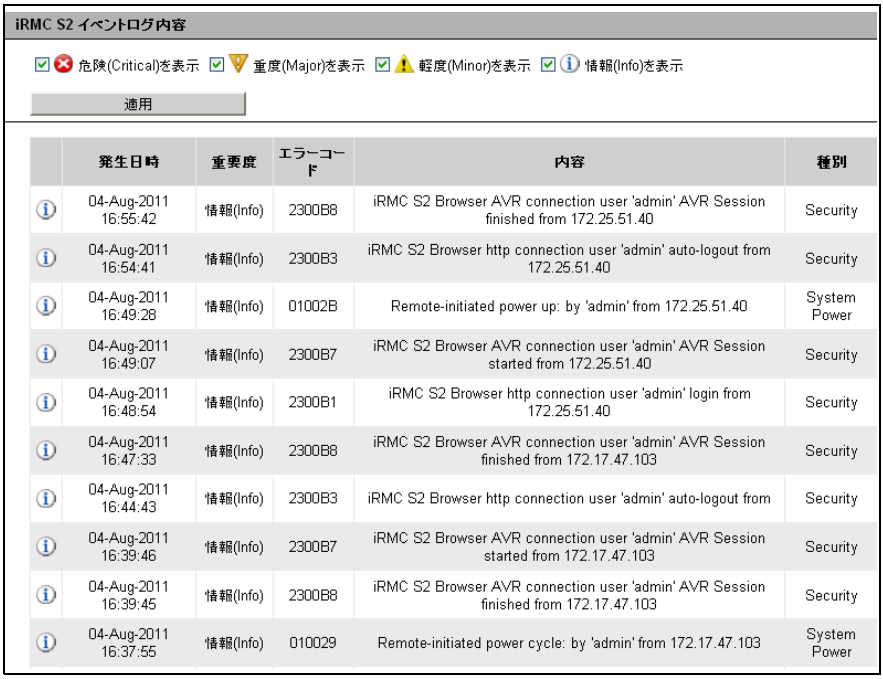
イベントログの保存

「*イベントログの保存*」ボタンをクリックした後、内部イベントログを含むファイル *iRMCS2_InternalEventLog.sel*/*iRMC S3_InternalEventLog.sel* をダウンロードできます。

iRMC S2 イベントログ内容

「*iRMC S2 イベントログ内容*」グループには、重要度によってフィルタリングされた内部イベントログエントリが表示されます。

「*iRMC S2 イベントログ内容*」グループで、現在のセッション中にフィルタ条件を変更できます。ただし、ここで行う設定はログアウトまでしか有効ではありません。次回のログイン時はデフォルト設定が適用されます。



	発生日時	重要度	エラーコード	内容	種別
ⓘ	04-Aug-2011 16:55:42	情報(Info)	2300B8	iRMC S2 Browser AVR connection user 'admin' AVR Session finished from 172.25.51.40	Security
ⓘ	04-Aug-2011 16:54:41	情報(Info)	2300B3	iRMC S2 Browser http connection user 'admin' auto-logout from 172.25.51.40	Security
ⓘ	04-Aug-2011 16:49:28	情報(Info)	01002B	Remote-initiated power up: by 'admin' from 172.25.51.40	System Power
ⓘ	04-Aug-2011 16:49:07	情報(Info)	2300B7	iRMC S2 Browser AVR connection user 'admin' AVR Session started from 172.25.51.40	Security
ⓘ	04-Aug-2011 16:48:54	情報(Info)	2300B1	iRMC S2 Browser http connection user 'admin' login from 172.25.51.40	Security
ⓘ	04-Aug-2011 16:47:33	情報(Info)	2300B8	iRMC S2 Browser AVR connection user 'admin' AVR Session finished from 172.17.47.103	Security
ⓘ	04-Aug-2011 16:44:43	情報(Info)	2300B3	iRMC S2 Browser http connection user 'admin' auto-logout from	Security
ⓘ	04-Aug-2011 16:39:46	情報(Info)	2300B7	iRMC S2 Browser AVR connection user 'admin' AVR Session started from 172.17.47.103	Security
ⓘ	04-Aug-2011 16:39:45	情報(Info)	2300B8	iRMC S2 Browser AVR connection user 'admin' AVR Session finished from 172.17.47.103	Security
ⓘ	04-Aug-2011 16:37:55	情報(Info)	010029	Remote-initiated power cycle: by 'admin' from 172.17.47.103	System Power

図 129: 「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

危険（Critical）を表示、重度（Major）を表示、軽度（Minor）を表示、情報（Info）を表示

必要に応じて、デフォルト値以外の重要度レベルを選択してください。

- 「*適用*」ボタンをクリックして、現在のセッション中に設定を有効にします。

7.10.3 システムイベントログ設定 - IPMI SEL と内部イベントログの設定

「*システムイベントログ設定*」ページでは、IPMI SEL（システムイベントログ）および内部イベントログを設定できます。

各イベントログについて以下を設定できます。

– デフォルトで「*システムイベントログ情報*」ページ（227 ページを参照）と「*iRMC S2/S3 イベントログ情報*」ページ（230 ページを参照）にそれぞれ表示されるエントリ

– IPMI SEL と内部イベントログを、リングバッファまたはリニアバッファとして構成するかどうか

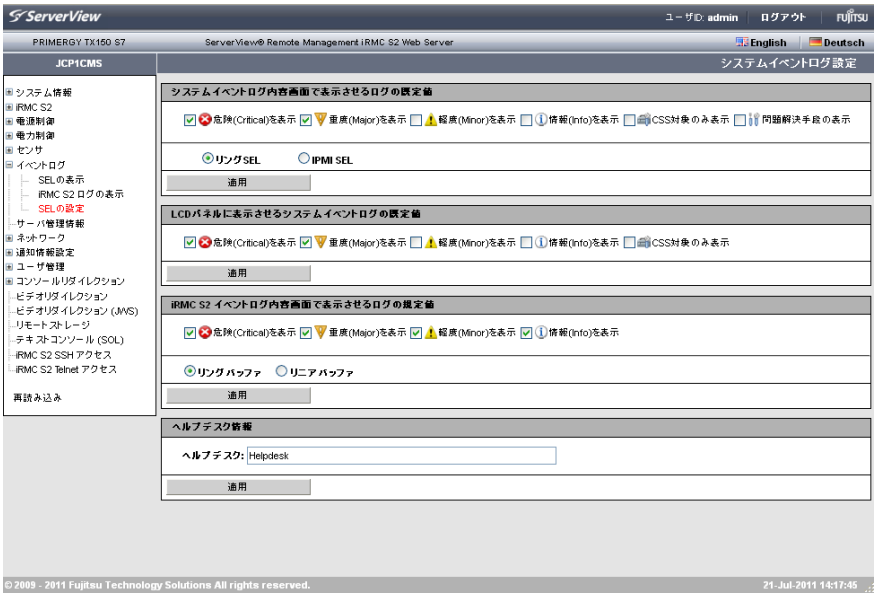


図 130: 「システムイベントログ設定」ページ

IPMI イベントログ設定

LCD パネルに表示させるシステムイベントログの既定値

ServerView Local Service Display モジュールが管理対象 PRIMERGY サーバに取り付けられている場合、重要度を選択して ServerView Local Service Display に SEL を表示することもできます。（この選択は、「*システムイベントログ内容*」ページに表示される SEL エントリに行った選択とは関係ありません。）

危険（Critical）を表示、重度（Major）を表示、軽度（Minor）を表示、情報（Info）を表示、CSS 対象のみ表示
: イベントログエントリを ServerView Local Service Display にデフォルトで表示する、1 つ以上の重要度を選択します。

システムイベントログ内容画面で表示させるログの既定値

危険（Critical）を表示、重度（Major）を表示、軽度（Minor）を表示、情報（Info）を表示、CSS 対象のみ表示
: イベントログエントリを「*システムイベントログ内容*」ページ（227 ページを参照）にデフォルトで表示する、1 つ以上の重要度を選択します。

問題解決手段の表示
: このオプションを選択すると、重要度 *Critical*」、「*Major*」、「*Minor*」の各 SEL エントリについて、エントリの理由、および推奨される問題解決手段が表示されます。

リング SEL
: イベントログはリングバッファとして構成されます。

IPMI SEL
: イベントログは IPMI SEL として構成されます。

IPMI SEL が完全にフルになると、それ以上エントリを追加できなくなります。

► 「*適用*」ボタンをクリックして、設定を有効にします。

iRMC S2/S3 イベントログ内容画面で表示させるログの規定値

危険（Critical）を表示、重度（Major）を表示、軽度（Minor）を表示、情報（Info）を表示
イベントログエントリを「*iRMC S2/S3 イベントログ情報*」ページ（230 ページを参照）にデフォルトで表示する、1 つ以上の重大度レベルを選択します。

リングバッファ
イベントログはリングバッファとして構成されます。

リニアバッファ
イベントログはリニアバッファとして構成されます。

リニアイベントログが完全にフルになると、それ以上エントリを追加できなくなります。

► 「*適用*」ボタンをクリックして、設定を有効にします。

ヘルプデスク情報

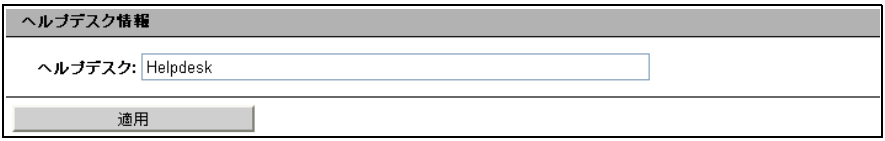


図 131: ヘルプデスク情報

ヘルプデスク
ヘルプデスクの表示に使用する文字列

► 「*適用*」ボタンをクリックして設定を有効にします。

7.11 サーバ管理情報 - サーバ設定

「*サーバ管理情報*」ページを使用して、サーバに以下の設定を行うことができます。

– サーバの ASR&R（Automatic Server Reconfiguration and Restart）設定（237 ページを参照）

– ウォッチドッグ設定（238 ページを参照）

– HP System Insight Manager（HP SIM）との連携（239 ページを参照）

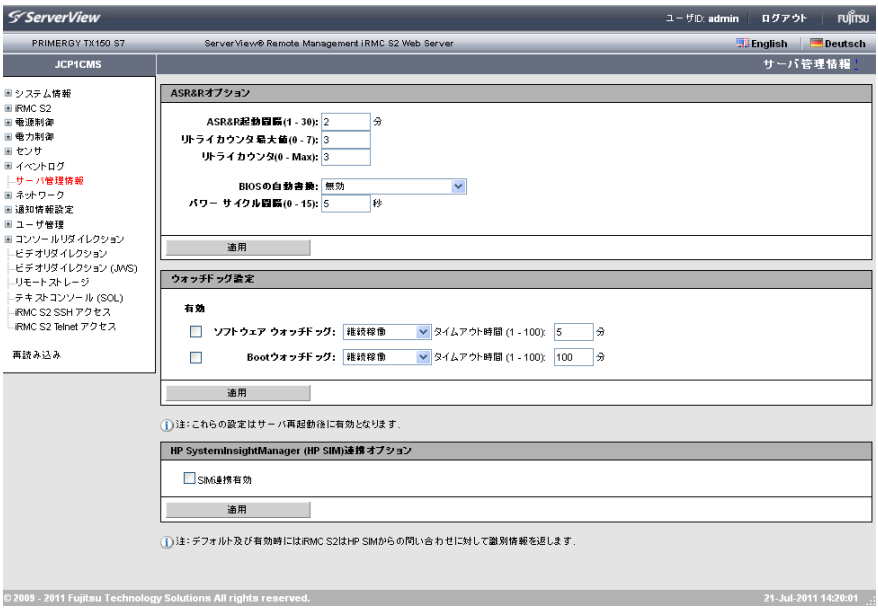


図 132: 「サーバ管理情報」ページ

ASR&R オプション - ASR&R 設定

「*ASR&R オプション*」グループを使用して、サーバの ASR&R（Automatic Server Reconfiguration and Restart）設定を行うことができます。

「*ASR&R オプション*」グループで行う設定は、管理対象サーバの次回の起動時から有効になります。

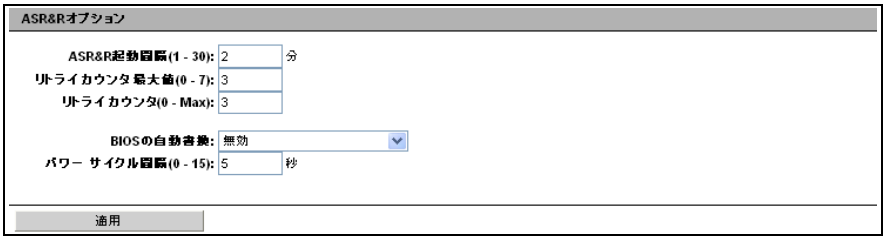


図 133: 「サーバ管理情報」ページ - ASR&R オプション

ASR&R 起動間隔（0 - 30）
重大なエラー発生後に電源断した後、自動的に電源投入するまでの時間（最大 30 分）を設定します

リトライカウンタ最大値（0 - 7）
重大なエラー発生後にサーバに許可する最大リスタート回数（最大 7 回）

リトライカウンタ（0 - Max）
重大なエラー発生後にサーバが試行するリアルタイムスタート試行回数（最大値は「*リトライカウンタ最大値*」に設定された値）

BIOS の自動書換
BIOS リカバリフラッシュビットを有効 / 無効にします。

- *有効*
  次回のシステム起動時に、BIOS を自動で書き換えます。
- *無効*
  次回のシステム起動時に、BIOS を自動で書き換えません。

この値を「*有効*」に設定すると、ファームウェアがアップデートされるまで、オペレーティングシステムは起動しません。BIOS リカバリフラッシュが、次回のシステム起動時に DOS フロッピーから（あるいは DOS フロッピーイメージから）自動で実行されます。

BIOS リカバリフラッシュが成功してから、BIOS リカバリフラッシュビットを「*無効*」に再設定してください。

パワーサイクル間隔（0 - 15）
電源オフから電源オンまでの間の間隔（秒）を設定します。

▶ 「*適用*」ボタンをクリックして設定を有効にします。

設定が保存され、適切な条件が満たされると動作が有効になります。

ウォッチドッグ設定 - ソフトウェアウォッチドッグおよび Boot ウォッチドッグの設定

「*ウォッチドッグ設定*」グループを使用して、ソフトウェアウォッチドッグおよび Boot ウォッチドッグを設定できます。

「*ASR&R オプション*」グループで行う設定は、管理対象サーバの次回の起動時から有効になります。

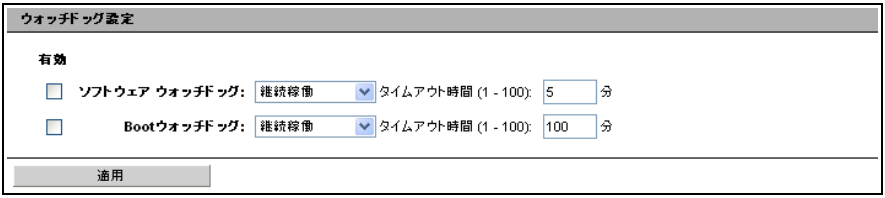


図 134: 「サーバ管理情報」ページ - ウォッチドッグオプション

ソフトウェアウォッチドッグは ServerView エージェントを使用して、システムの動作を監視します。ソフトウェアウォッチドッグは、ServerView エージェントおよびオペレーティングシステムが完全に初期化されたときに有効になります。
ServerView エージェントは、iRMC S2/S3 に定義された間隔でアクセスします。ServerView エージェントからのメッセージがない場合、システムが正しく動作していないと考えられます。
このような場合に実行される動作を設定することができます。

Boot ウォッチドッグは、システムの起動から ServerView エージェントが正常動作するまでのフェーズを監視します。
ServerView エージェントが、サーバの iRMC S2/S3 と一定時間接続を確立できない場合、ブートプロセスが正常に行われていないと考えられます。
このような場合に実行される動作を設定することができます。

次の手順に従います。

▶ 「*ソフトウェアウォッチドッグ*」および「*Boot ウォッチドッグ*」について、「*有効*」の下のチェックボックスにチェックするかチェックを外します。

- これらのチェックボックスにチェックした場合、「*ソフトウェアウォッチドッグ*」および「*Boot ウォッチドッグ*」の後ろの以下の設定ができます。

  継続稼動
  ウォッチドッグが時間切れしても、何の動作も行われず、サーバは稼動を続けます。イベントログに記録されます。

  リセット
  サーバ管理ソフトウェアが、システムリセットを行います。

  パワーサイクル
  サーバの電源が遮断され、再び直ちに電源投入されます。

- 必要に応じて、「*タイムアウト時間*」の後にこの動作を実行するまでの待機時間（分）を入力します。

  Boot ウォッチドッグは、システムが起動するまで待機します。そのため、「*タイムアウト時間（0 - 100）*」には、十分な時間を設定してください。

- 「*適用*」ボタンをクリックします。

  設定が保存され、適切な条件が満たされると動作が有効になります。

HP System Insight Manager（HP SIM ）連携オプション - HP SIM 連携設定

「*HP System Insight Manager （HP SIM) 連携オプション*」グループを使用して、iRMC S2/S3 デバイスが、HP System Insight Manager から送信される非公式の XML 問い合わせに対する応答として、ある識別情報を返すように設定することができます。

図 135: 「サーバ管理情報」ページー HP System Insight Manager（HP SIM）連携オプション

次の手順に従います。

- HP SIM との連携を無効あるいは有効にするために、「*SIM 連携無効*」チェックボックスをオンまたはオフにします。
- 「*適用*」ボタンをクリックして、設定を有効にします。

7.12 ネットワーク設定 - LAN パラメータの設定

「ネットワーク」エントリは、iRMC S2/S3 の LAN パラメータを設定するページのリンクを提供します。

- 241 ページ の「ネットワークインターフェース設定 - iRMC S2/S3 のイーサネット設定」を参照。
- 247 ページ の「ポート番号とネットワークサービス - ポート番号とネットワークサービ スの設定」を参照。
- 251 ページ の「DNS 構成 - iRMC S2/S3 の DNS の設定」を参照。

7.12.1 ネットワークインターフェース設定 - iRMC S2/S3 のイーサネット設定

「*ネットワークインターフェース*」ページでは、iRMC S2/S3 のイーサネット設定の表示および変更ができます。

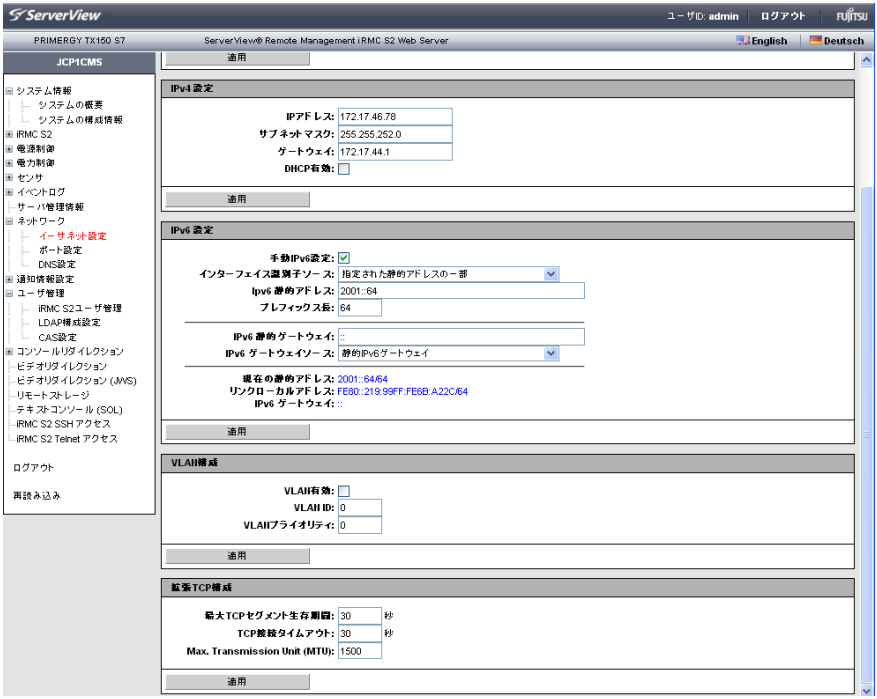


図 136: 「ネットワークインターフェース」ページ

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。

iRMC S2/S3 のイーサネット設定を誤ると、特別な設定ソフトウェア、シリアルインターフェース、または BIOS を使用しないと iRMC S2/S3 にアクセスできなくなります。

「*iRMC S2/S3 設定*」権限を持つユーザのみが、イーサネット設定を編集することができます（65 ページ の「iRMC S2/S3 のユーザー管理」の章を参照）。

ネットワークインターフェース設定

MAC アドレス
iRMC S2/S3 の MAC アドレスが表示されます。

LAN 接続速度
LAN 速度。以下のオプションを選択できます。

- 自動検出
- 1000 M Bits/s 全二重（サーバハードウェアによって異なる）
- 100 M Bits/s 全二重
- 100 M Bits/s 半二重
- 10 M Bits/s 全二重
- 10 M Bits/s 半二重

「*自動検出*」を選択すると、iRMC S2/S3 のオンボード LAN コントローラが、自動的に正しい伝送速度および全二重あるいは半二重方式の接続方法を決定します。

LAN ポート

このオプションは、一部の PRIMERGY サーバではサポートされていません。

一部の PRIMERGY サーバモデルでは、NIC（Network Interface Card）システムにインストールされた LAN インターフェースは、以下のいずれかとして設定できます。

- システムと操作を共有するための共有 LAN として

  または

- 管理 LAN として独占使用するためのサービス LAN として

IPv4 有効

iRMC S2/S3 の IPv4 アドレッシングを有効または無効にします。IPv4 アドレッシングを有効にすると「*IPv4 設定*」グループが表示されます（下記参照）。

現在 IPv4 を使用して iRMC S2/S3 にアクセスしている場合は、IPv4 アドレッシングを無効にできません。

IPv6 有効

iRMC S2/S3 の IPv6 アドレッシングを有効または無効にします。IPv6 アドレッシングを有効にすると「*IPv6 設定*」グループが表示されます（下記参照）。

現在 IPv6 を使用して iRMC S2/S3 にアクセスしている場合は、IPv6 アドレッシングを無効にできません。

IPv4 設定

「*IPv4 設定*」グループでは、iRMC S2/S3 の IPv4 設定を行うことができます。

IP アドレス

LAN 内の iRMC S2/S3 の IPv4 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 有効*」オプションが無効）を使用している場合は、ここに IP アドレスを入力できます。そうでない場合（「*DHCP 有効*」オプションが有効）、iRMC S2/S3 ではこのフィールドはアドレスの表示用に使用されます。

サブネットマスク

LAN 内の iRMC S2/S3 のサブネットマスク。

ゲートウェイ

LAN 内のデフォルトゲートウェイの IPv4 アドレス。

DHCP 有効

このオプションを有効にすると、iRMC S2/S3 は、ネットワーク上の DHCP サーバから LAN 設定を取得します。

ネットワーク上に DHCP サーバが存在しない場合は、*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てもネットワーク上に DHCP サーバが 存在しない場合、iRMC S2/S3 は検索ループを開始します（つまり、DHCP サーバが見つかるまで検索を続けます）。

（設定された）iRMC S2/S3 は、適切に設定された DHCP サーバによって、DNS サーバ に登録できます。（251 ページ の「DNS 構成 - iRMC S2/S3 の DNS の設定」を参照）

IPv6 設定

「*IPv6 設定*」グループでは、リンクローカルアドレスに加え、iRMC S2/S3 の IPv6 アドレスを手動で設定できます。これは、ステートレス自動設定を使用して、iRMC S2/S3 に常に自動的に割り当てられます。

iRMC S2/S3 の IPv6 アドレッシングを使用する場合、iRMC S2/S3 では DHCP をサポートしません。

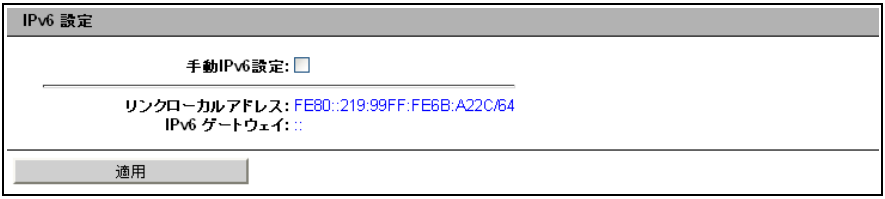


図 137: 「ネットワークインターフェース」ページ - 手動 IPv6 設定無効

手動 IPv6 設定

このオプションはデフォルトでは無効です。

「*手動 IPv6 設定*」オプションが有効な場合、「*IPv6 設定*」グループには、iRMC S2/S3 にルータブルな IPv6 アドレスを手動で設定可能な追加のパラメータが表示されます。

図 138: 「ネットワークインターフェース」ページ - 手動 IPv6 設定

インターフェイス識別子ソース

どのソースから IPv6 アドレスのインターフェース識別子部分を取得するかを指定します。

指定された静的アドレスの一部
「*IPv6 静的アドレス*」で指定された静的アドレス部分。

EUI-64（MAC アドレスベース）
iRMC S2/S3 の MAC アドレスの EUI-64 標準準拠形式。

IPv6 静的アドレス
iRMC S2/S3 の静的 IPv6 アドレス。

プレフィックス長
IPv6 プレフィックスの長さ

IPv6 静的ゲートウェイ
LAN 内のデフォルト IPv6 ゲートウェイの静的 IPv6 アドレス。

IPv6 ゲートウェイソース
iRMC S2/S3 が使用する IPv6 ゲートウェイ。

静的 IPv6 ゲートウェイ
「*IPv6 静的ゲートウェイ*」で指定したゲートウェイ。

自動（ルータ指定）
ゲートウェイがルーターによって自動的に指定されます。

VLAN 構成

VLAN 有効
このオプションで、iRMC S2/S3 の VLAN サポートを有効にします。

VLAN ID
iRMC S2/S3 が属する仮想ネットワーク（VLAN ）の VLAN ID。許容される値の範囲：1 ≦ *VLAN ID* ≦ 4094。

VLAN プライオリティ
「*VLAN ID*」で指定した VLAN における iRMC S2/S3 の VLAN プライオリティ。
許容される値の範囲：0 ≦ *VLAN プライオリティ* ≦ 7（デフォルト：0）。

拡張 TCP 構成

最大 TCP セグメント生存期間
TCP/IP パケットの最大生存期間（単位：秒）（デフォルト：32 秒）。

TCP 接続タイムアウト
TCP 接続のタイムアウト値（単位：秒）（デフォルト：32 秒）。

Max. Transmission Unit（MTU）
TCP/IP 接続で許可される TCP/IP データパッケージの最大パケットサイズ（単位：バイト）（デフォルト：3000 バイト）。

► 「*適用*」ボタンをクリックして、イーサネット設定を有効にしてください。

7.12.2 ポート番号とネットワークサービス - ポート番号とネットワークサービ スの設定

「*ポート番号とネットワークサービス*」ページでは、ポート番号およびネットワークサービスの表示および設定ができます。

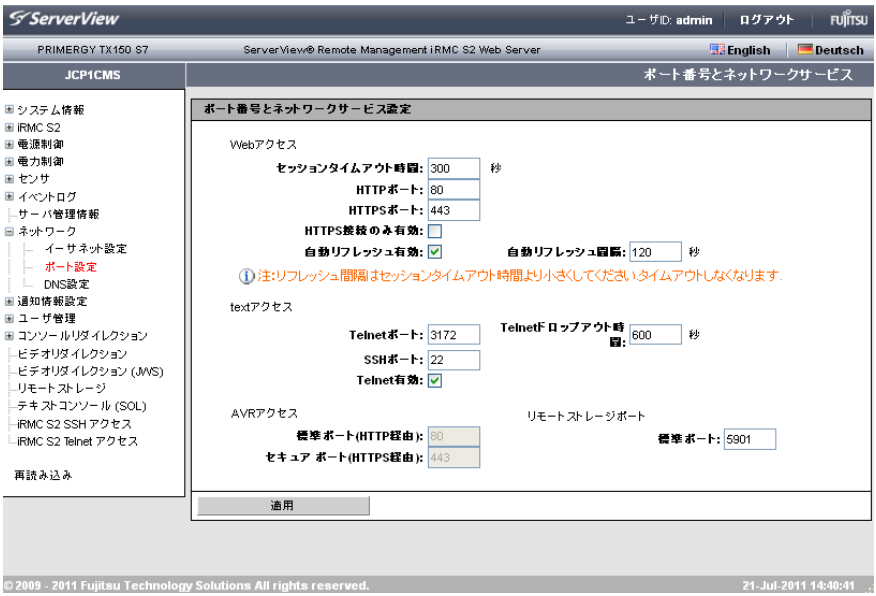


図 139: 「ポート番号およびネットワークサービス」ページ

入力フィールドが iRMC S2/S3 Web インターフェースで無効な場合、ポート番号の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

セッションタイムアウト時間
通信していない期間（秒）が設定値を経過すると自動的にセッションが閉じられます。iRMC S2/S3 Web インターフェースのログインページが表示され、再びログインするように求められます（140 ページを参照）。

「*セッションタイムアウト時間*」より短いリフレッシュ間隔を「*自動リフレッシュ間隔*」フィールドに入力した場合、「*セッションタ イムアウト*」に設定された時間が経過してもセッションは自動的に閉じません（249 ページを参照）。

HTTP ポート
iRMC S2/S3 の HTTP ポート。
デフォルトポート番号：80
変更可能：可能
デフォルト値の使用：可能
通信方向：Inbound および Outbound

HTTPS ポート
iRMC S2/S3 の HTTPS （セキュアな HTTP ）ポート。
デフォルトポート番号：443
変更可能：可能
デフォルト値の使用：可能
通信方向：Inbound および Outbound

HTTPS 接続のみ有効
「*HTTPS 接続のみ有効*」オプションを有効にした場合、入力フィールドに指定した HTTPS ポートでのみ iRMC S2/S3 へのセキュアな通信を確立することができます。

「*HTTPS 接続のみ有効*」オプションを無効にした場合、入力フィールドに指定した HTTP ポートで iRMC S2/S3 への非セキュアな通信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。

自動リフレッシュ有効
このオプションを有効にすると、iRMC S2/S3 Web インターフェースの画面は、自動的に周期的に再読み込みされます。「*自動リフレッシュ間隔*」フィールドに、再読み込みの間隔を設定します。

自動リフレッシュ間隔

iRMC S2/S3 Web インターフェースが、自動的に再読み込みする間隔（秒）を設定します。

再読み込み間隔の値に「*セッションタイムアウト時間*」（248 ページを参照））よりも短い時間を設定した場合、セッションは、「*セッションタイムアウト*」を経過しても自動的に閉じません。

テキストベースアクセス用ポート

Telnet ポート

iRMC S2/S3 の TELNET ポート。
デフォルトポート番号：3172
変更可能：可能
デフォルト値の使用：不可
通信方向：Inbound および Outbound

Telnet ドロップアウト時間

通信がなされないとき Telnet 接続が自動的に遮断されるまでの時間（秒数）。

SSH ポート

iRMC S2/S3 の SSH （セキュアなシェル）ポート。
デフォルトポート番号：22
変更可能：可能
デフォルト値の使用：可能
通信方向：Inbound および Outbound

Telnet 有効

「*Telnet 有効*」オプションを有効にした場合、ユーザは、入力フィールドに指定した TELNET ポートで、iRMC S2/S3 への接続を確立することができます。

VNC ポート

標準ポート

セキュアおよび非セキュアな AVR（Advanced Video Redirection）用の iRMC S2/S3 の VNC ポート。
ポート番号：80
ハード構成
デフォルト値の使用：可能
通信方向：Inbound

セキュアポート（SSL）

AVR の SSL セキュアなマウスおよびキーボード入力用の iRMC S2/S3 の VNC ポート。
ポート番号：443
ハード構成
デフォルト値の使用：可能
通信方向：Inbound

リモートストレージポート

標準ポート

iRMC S2/S3 の リモートストレージポートのデフォルト値。
デフォルトポート番号：5901
変更可能：可能
デフォルト値の使用：可能
通信方向：リモートワークステーションへの Outbound

iRMC S2/S3 ファームウェアバージョン 5.00 以降では、リモートストレージポートはリモートストレージサーバおよびクライアント内部の通信にのみ使用されます。統合されたリモートストレージの場合は HTTP ポートを使用します。

► 「*適用*」ボタンをクリックして、設定を保存します。

7.12.3 DNS 構成 - iRMC S2/S3 の DNS の設定

「*DNS 構成*」ページでは、iRMC S2/S3 のドメインネームサービス（DNS）を有効にして、iRMC S2/S3 のホスト名を設定できます。

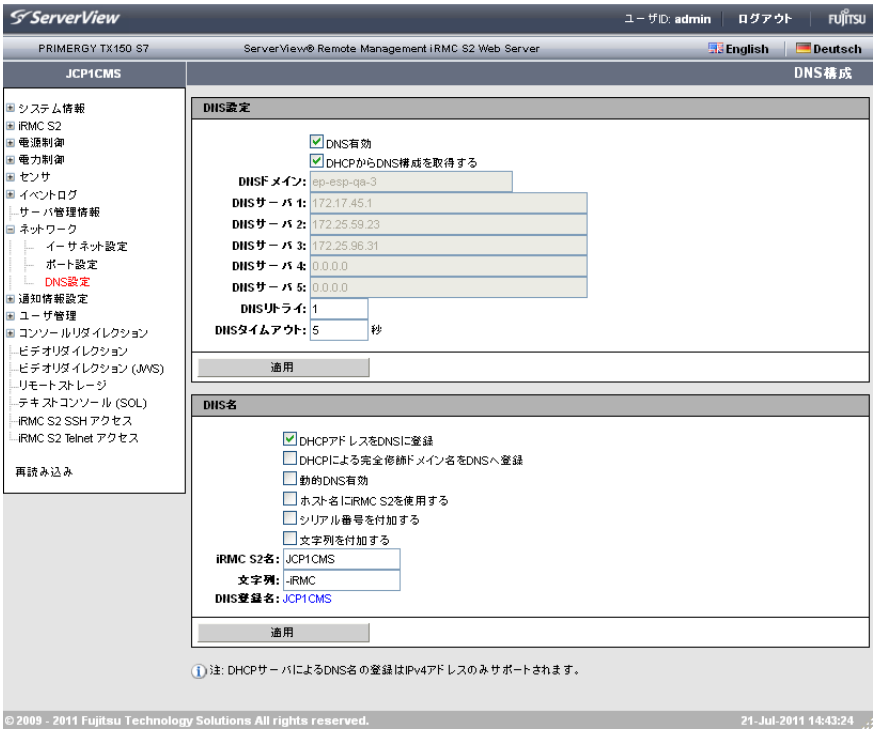


図 140: 「DNS 構成」ページ

DNS 設定

「*DNS 設定*」グループで、iRMC S2/S3 のドメインネームサービス（DNS）を有効にできます。これによって、iRMC S2/S3 の設定に IP アドレスではなく具体的な DNS 名を使用できます。

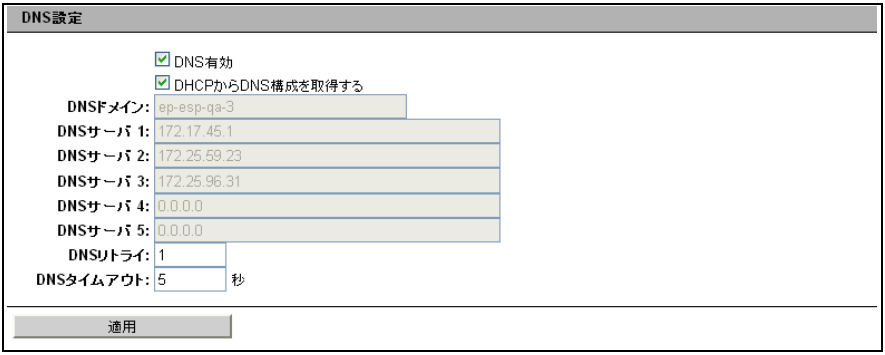


図 141: 「DNS 構成」ページ - DNS 設定

DNS 有効
: iRMC S2/S3 の DNS 使用を有効 / 無効にします。

DHCP から DNS 構成を取得する
: このオプションを有効にすると、DNS サーバの IP アドレスを DHCP サーバから自動的に 取得します。
このイベントでは、最大 5 つのサーバをサポートします。

この設定を有効にしない場合、「*DNS サーバ 1*」から「*DNS サーバ 5*」に最大 5 つの DNS サーバアドレスを入力できます。

DNS ドメイン
: 「*DHCP から DNS 構成を取得する*」オプションが無効な場合、DNS サーバのデフォルトドメインを設定するように要求されます。

DNS サーバ 1 - 5
: 「*DHCP から DNS 構成を取得する*」オプションが無効な場合、ここで、最大 5 つの DNS サーバ名を入力できます。

DNS リトライ
: DNS リトライ回数。

DNS タイムアウト
: DNS 応答のタイムアウト（秒）。

▶ 「*適用*」ボタンをクリックして、設定を保存します。

DNS 登録名

「*DNS 名*」グループでは、iRMC S2/S3 のホスト名を設定でき、「*動的 DNS*」を使用できます。動的 DNS によって、DHCP サーバは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 サーバに自動的に渡して、識別を容易にできます。

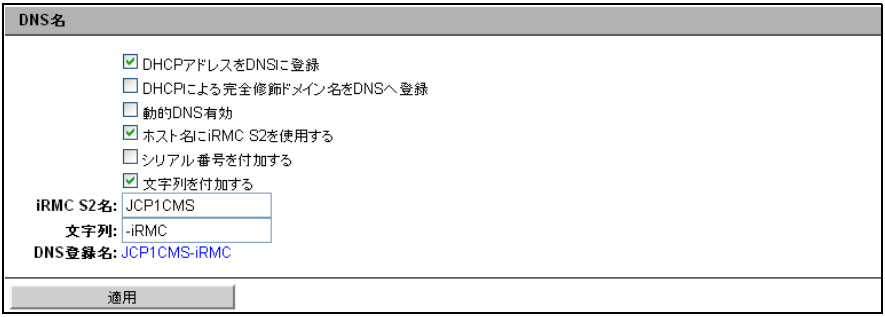


図 142: 「DNS 構成」ページ - DNS 名

DHCP アドレスを DNS に登録
このオプションは、IPv6 アドレッシングを使用する場合は無効です。DHCP サーバを使用して iRMC S2/S3 と DNS を登録するための、DHCP サーバへの DHCP 名の転送を有効または無効にします。

DHCP による完全修飾ドメイン名を DNS へ登録
このオプションは、IPv6 アドレッシングを使用する場合は無効です。DHCP サーバを使用して iRMC S2/S3 と DNS を登録するための、DHCP サーバへの FQDN（Fully Qualified Domain Name）の転送を有効または無効にします。

動的 DNS 有効
動的 DNS を使用した DNS レコードのアップデートを有効または無効にします。

ホスト名に iRMC S2/S3 を使用する
「*iRMC S2/S3 名*」入力フィールドに指定された iRMC S2/S3 名が、サーバ名の代わりに iRMC S2/S3 に使用されます。

シリアル番号を付加する
iRMC S2/S3 の MAC アドレスの最後の 3 バイトが iRMC S2/S3 の DHCP 名に付加されます。

文字列を付加する
「*文字列*」入力フィールドに指定された拡張子が、iRMC S2/S3 の DHCP 名に付加されます。

iRMC S2/S3 名
サーバ名の代わりに、iRMC 向け DHCP に渡された iRMC S2/S3 名。関連するオプションによって異なりますが、iRMC S2/S3 名が DNS 名の一部として使用されます。

文字列
iRMC S2/S3 の名前の拡張子。

DNS 登録名
iRMC S2/S3 に設定された DNS 名を表示します。

► 「*適用*」ボタンをクリックして、設定を保存します。

7.13 警告通知 - 警告通知の設定

「*通知情報設定*」エントリには、iRMC S2/S3 の警告通知の設定を行う際に利用するページのリンクがあります。

– 256 ページ の「SNMP トラップ送信設定 - SNMP トラップ通知の設定」を参照。

– 257 ページ の「シリアル / モデム通知設定 - モデム経由通知設定」を参照。

– 259 ページ の「Email 設定 - Email 送信設定」を参照。

7.13.1 SNMP トラップ送信設定 - SNMP トラップ通知の設定

「*SNMP トラップ送信設定*」ページでは、SNMP トラップ通知の設定の表示および構成ができます。

SNMP トラップを最大 7 つの SNMP サーバに送信する機能をサポートしています

図 143: 「SNMP トラップ送信設定」ページ

SNMP コミュニティ
SNMP コミュニティ名。

► 「*適用*」ボタンをクリックして、コミュニティ名を受け入れます。

「SNMP サーバ 1」 ～ 「SNMP サーバ 7」（トラップ送信先）
コミュニティに属し、「*トラップ送信先*」を設定するサーバの DNS 名または IP アドレス。

► 「*適用*」ボタンをクリックして、トラップの送信先として SNMP サーバを有効にします。

► 「*テスト*」ボタンをクリックして、SNMP サーバとの接続をテストします。

► 「*すべて適用*」ボタンをクリックすると、適切な場合、すべての設定が有効になります。

7.13.2 シリアル / モデム通知設定 - モデム経由通知設定

「*シリアル / モデム通知設定*」ページは、iRMC S2 でしか使用できません。

「*シリアル / モデム通知設定*」ページを使用して、モデム経由で送信する通知を設定できます。

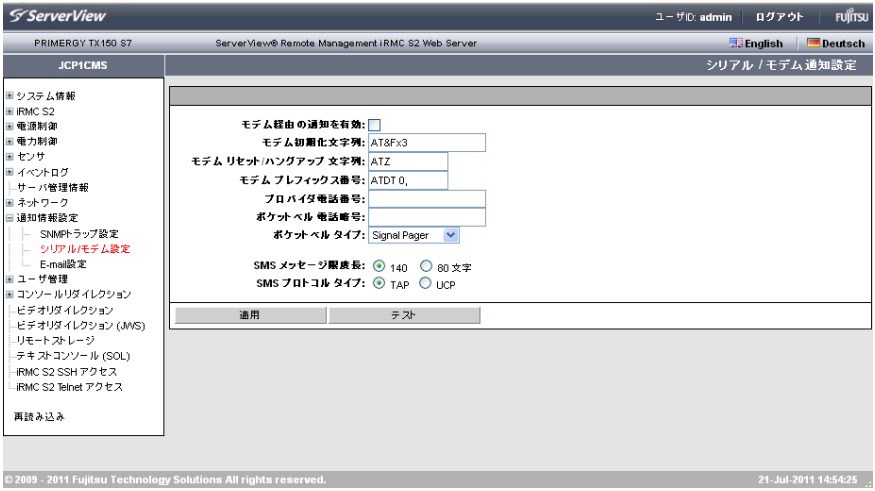


図 144: 「シリアル / モデム通知設定」ページ

モデム経由の通知を有効
: シリアル / モデム経由の通知を有効または無効にします。

モデム初期化文字列
: ここへの入力に関する詳細は、使用するモデムのユーザガイドを参照してください。

モデム リセット / ハングアップ文字列
: ここへの入力に関する詳細は、使用するモデムのユーザガイドを参照してください。

モデム プレフィックス番号
: ここへの入力は、使用する接続方式によって異なります。

プロバイダ電話番号
: SMS サーバ名を入力してください。

ポケットベル電話番号
: 携帯電話の電話番号を入力してください。

ポケットベルタイプ
次から選択することができます。

- Signal Pager
- Numeric Pager
- Alpha pager
- SMS
- DoCoMo

SMS メッセージ限度長
最大値として、80 あるいは 140 文字を選択してください。

SMS プロトコルタイプ
使用する携帯電話ネットワークに対応したオプションを選択してください。

► 「*適用*」ボタンをクリックして、設定を有効にします。

► 「*テスト*」ボタンをクリックして、テストの警告通知を送信します。

7.13.3 Email 設定 - Email 送信設定

「*E-mail 設定*」ページを使用して、Email 通知の設定を行うことができます。

2 つのメールサーバの設定がサポートされます。

Email 通知は各ユーザに個別に指定できます（268 ページ の「ユーザ “<name>” 構成 - ユーザ設定（詳細）」の項を参照）。

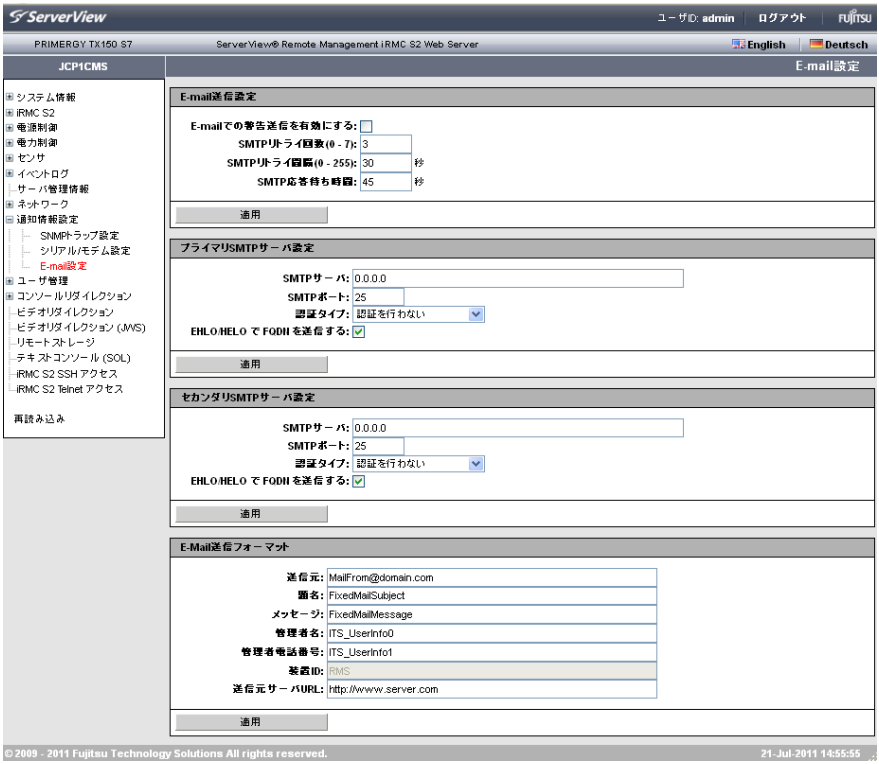


図 145: 「E-mail 設定」ページ

E-mail 送信設定 - グローバル Email 設定

「*E-mail 送信設定*」グループでは、グローバル Email 設定を設定できます。

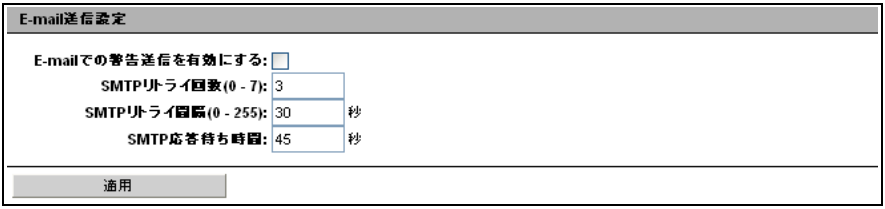


図 146: 「E-mail 設定」ページ - グローバル Email 設定

E-mail での警告送信を有効にする
　　このオプションを有効にします。

SMTP リトライ回数（0 - 7）
　　SMTP リトライ回数。

SMTP リトライ間隔（0 - 255）
　　SMTP 再試行の間隔（秒）。

SMTP 応答待ち時間
　　SMTP 応答のタイムアウト（秒）。

► 「*適用*」ボタンをクリックして、設定を有効にします。

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

「*プライマリ SMTP サーバ設定*」グループを使用して、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。

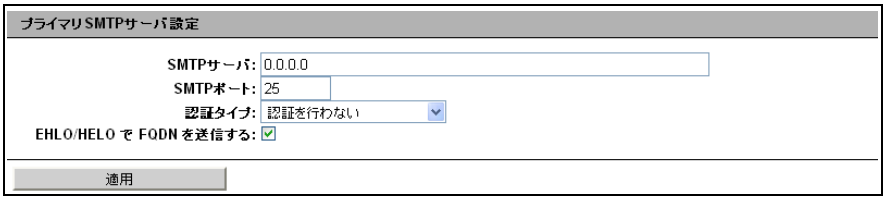


図 147: 「E-mail 設定」ページ - プライマリ SMTP サーバ設定

SMTP サーバ
プライマリメールサーバの IP アドレス。

> iRMC S2/S3 のドメインネームサービス（DNS）を利用できます（251 ページ の「DNS 構成 - iRMC S2/S3 の DNS の設定」を参照）。IP アドレスの代わりに、具体的な名前を使用できます。

SMTP ポート
メールサーバの SMTP ポート番号。

認証タイプ
iRMC S2/S3 をメールサーバに接続する際の認証方式を選択します。

- *認証を行わない*
  接続時に認証を行いません。
- *認証を行う（RFC 2554）*
  RFC 2554 に準拠した認証方式：SMTP サーバの認証方式の拡張です。

  この場合は、以下の情報が必要です。

  認証ユーザ名
  メールサーバでの認証用のユーザ名。

  認証パスワード
  メールサーバでの認証用のパスワード。

  パスワード確認
  入力したパスワードを確定します。

► 「*適用*」ボタンをクリックして、設定を有効にします。

セカンダリ SMTP サーバ設定 - セカンダリメールサーバ設定

「*セカンダリ SMTP サーバ設定*」グループを使用して、セカンダリサーバ（SMTP サーバ）の設定ができます。

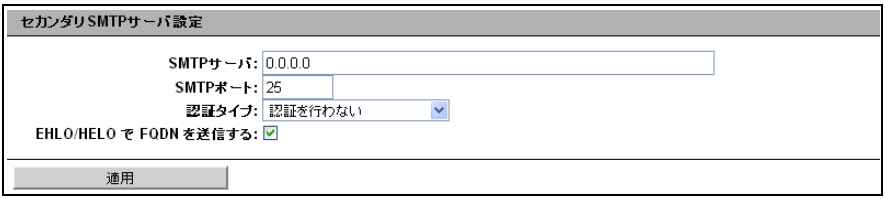


図 148: 「E-mail 設定」ページ - セカンダリ SMTP サーバ設定

SMTP サーバ
セカンダリメールサーバの IP アドレス。

iRMC S2/S3 のドメインネームサービス（DNS）を利用できます（251 ページ の「DNS 構成 - iRMC S2/S3 の DNS の設定」を参照）。IP アドレスの代わりに、具体的な名前を使用できます。

SMTP ポート
メールサーバの SMTP ポート番号。

認証タイプ
iRMC S2/S3 をメールサーバに接続する際の認証方式を選択します。

– *認証を行わない*
接続時に認証を行いません。

– *認証を行う（RFC 2554）*
RFC 2554 に準拠した認証方式：SMTP サーバの認証方式の拡張です。

この場合は、以下の情報が必要です。

認証ユーザ名
メールサーバでの認証用のユーザ名。

認証パスワード
メールサーバでの認証用のパスワード。

パスワード確認
入力したパスワードを確定します。

► 「*適用*」ボタンをクリックして、設定を有効にします。

E-mail 送信フォーマット - E-mail 送信フォーマット

「*E-mail 送信フォーマット*」グループでは、、E-mail フォーマット設定を行うことができます。個々のユーザについて「*新規ユーザの設定*」- 「*ユーザ < 名 > 設定*」- 「*E-mail 送信フォーマット*」ページを使用して E-mail フォーマットを設定できます（272 ページ参照）。

以下の Email フォーマットがサポートされています。

– 標準メール
– 題名固定
– ITS フォーマット
– Fujitsu REMCS フォーマット

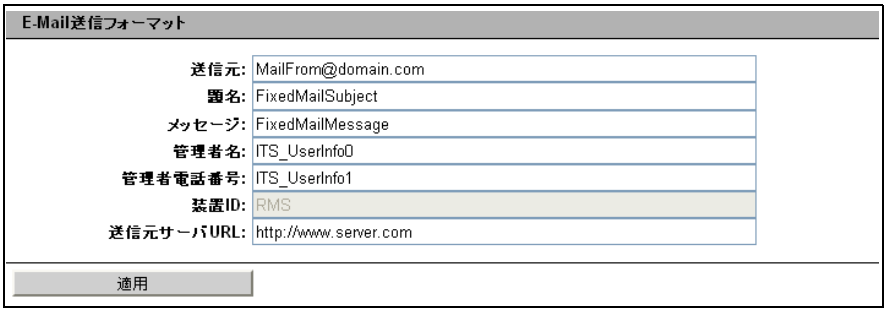


図 149: 「E-mail 設定」ページ - E-mail 送信フォーマット

E-mail フォーマットによっては、入力できない項目があります。

送信元

iRMC S2/S3 送信者を識別する情報です。
すべての E-mail フォーマットで入力可能です。

ここで入力した文字列に「@」が含まれている場合、文字列は有効な E-mail アドレスと解釈されます。そうでない場合、有効な Email アドレスとして「admin@<ip-address>」が使用されます。

題名

通知メールの固定の題名。
E-mail フォーマットとして、「*題名固定*」が有効な場合のみ入力可能です（272 ページを参照）。

メッセージ

メッセージのタイプ（E-mail）。
E-mail フォーマットとして、「*題名固定*」が有効な場合のみ入力可能です（(272 ページを参照）。

管理者名
管理責任者の名前（任意）。
E-mail フォーマットとして、「*ITS フォーマット*」が有効な場合のみ入力可能です（272 ページを参照）。

管理者電話番号
管理責任者の電話番号（任意）。
E-mail フォーマットとして、「*ITS フォーマット*」が有効な場合のみ入力可能です（272 ページを参照）。

装置 ID
この ID は、シリアル番号のような追加のサーバ ID です。
E-mail フォーマットとして、「*Fujitsu REMCS フォーマット*」が有効な場合のみ入力可能です。

送信元サーバ URL
特定の条件で、サーバがアクセスできる URL。URL を手入力する必要があります。
E-mail フォーマットとして、「*標準メール*」が有効な場合のみ入力可能です。

► 「*適用*」ボタンをクリックして設定を保存します。

7.14 ユーザ管理 - ユーザの管理

「*ユーザ管理*」エントリには、ローカルユーザ管理のページだけでなく、グローバルユーザ管理のディレクトリサービスを設定（LDAP 設定）するためのページへのリンクが含まれます。

- 265 ページ の「iRMC S2/S3 ユーザ情報 - iRMC S2/S3 のローカルユーザ管理」を参照。
- 275 ページ の「ディレクトリサービス設定（LDAP）- iRMC S2/S3 のディレクトリサービ スの設定」を参照。
- 288 ページ の「Centralized Authentication Service（CAS）設定 - CAS サービスの設定」を参照。

7.14.1 iRMC S2/S3 ユーザ情報 - iRMC S2/S3 のローカルユーザ管理

「*iRMC S2/S3 ユーザ情報*」ページには、設定されたユーザに関する情報が表示されます。各行には、設定された特定のユーザに関するデータが含まれます。ユーザ名はリンク形式で実装されています。ユーザ名をクリックして「*ユーザ “<name>” 構成*」画面を開くと（268 ページを参照）、そのユーザの設定を表示したり変更することができます。

ユーザ ID 1（“null user”）は、IPMI 標準のために予約されているため、iRMC S2/S3 のユーザ管理には使用できません。

図 150: 「ユーザ管理」ページ

削除

設定されているユーザの表には、各ユーザエントリの後に「*削除*」ボタンがあります。このボタンをクリックして、選択を確認した後に関連するユーザを削除します。

ユーザの新規作成

このボタンをクリックすると、「*新規ユーザの構成*」ページが開きます（267 ページを参照）。ここで新規ユーザの設定ができます。

7.14.1.1 新規ユーザの構成 - 新規ユーザの構成

「*新規ユーザの構成*」ページを使用して、新規ユーザの基本設定ができます。

「*新規ユーザの構成*」ページのフィールドと選択肢の一覧については、269 ページ の、「*ユーザ "<name>" 構成*」ページで説明します。

図 151 に、「User3」という名前のユーザの設定を示します。

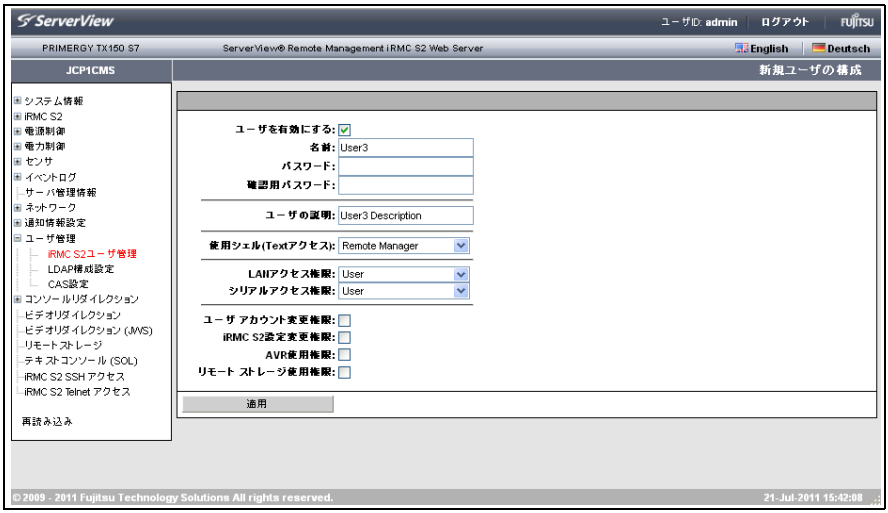


図 151: ユーザ管理 - 「新規ユーザの構成」ページ

7.14.1.2 ユーザ “<name>” 構成 - ユーザ設定（詳細）

「*ユーザ “<name>” 構成*」ページでは、ユーザ設定の表示、修正および拡張ができます。

図 152 に、図 151 で作成したユーザの設定を示します。

ユーザ名の後ろの括弧内にユーザ ID が表示されます。

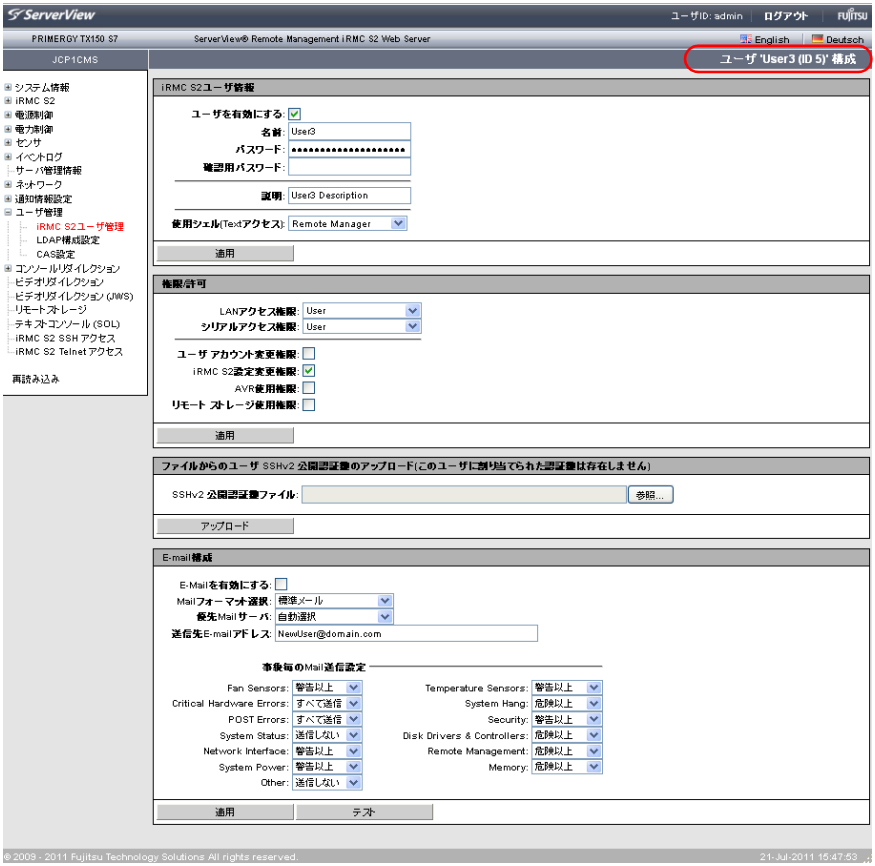


図 152: ユーザ管理 - 「ユーザ “<name>” 構成」ページ構成

ユーザ情報 - ユーザのアクセスデータの設定

「*ユーザ情報*」グループでは、ユーザのアクセスデータを設定できます。

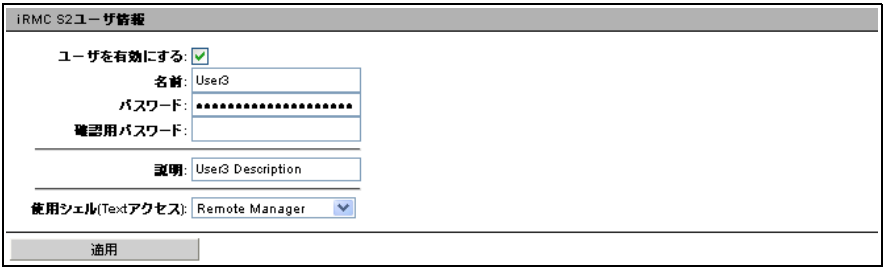


図 153: ユーザ管理 - 「ユーザ “<name>” 構成」ページ、ユーザ情報

ユーザを有効にする
このオプションを無効に設定するとユーザをロックできます。

名前
ユーザの名前を入力します。

パスワード
ユーザパスワードを入力します。

パスワード確認
パスワードを再度入力して、確認します。

説明
構成したユーザの一般的な説明を入力します。

使用シェル
目的のユーザシェルを選択します。
以下のオプションを選択できます。

- *SMASH CLP*
  (343 ページ の「コマンドラインシェルの起動 ... - SMASH CLP シェルの起動」の項を参照)。
- *Remote Manager*
  (325 ページ の「Telnet/SSH 経由の iRMC S2/S3 (リモートマネージャ)」の章を参照)。
- *IPMI Terminal Mode*
- *None*

► 「*適用*」ボタンをクリックして、設定を有効にします。

権限 / 許可 - ユーザ権限の設定

「*権限 / 許可*」グループを使用して、チャネル固有のユーザ権限を設定できます。

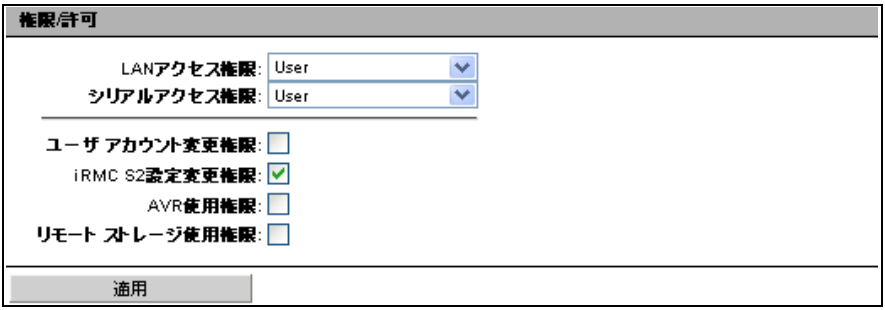


図 154: ユーザ管理 - 「ユーザ “<name>” 構成」ページ、権限 / 許可

LAN アクセス権限
ここで LAN チャネルの権限グループをユーザに割り当てます。

- *User*
- *Operator*
- *Administrator*
- *OEM*

権限グループに関連する許可に関する情報は、68 ページ の「ユーザー権限」の項 を参照してください。

シリアルアクセス権限
ユーザへのシリアルチャネルの権限グループを割り当てます。「*LAN アクセス権限*」についても同じ権限グループを使用できます。

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に割り当てることもできます。

ユーザアカウント変更権限
ローカルユーザアクセスを設定する権限。

iRMC S2/S3 設定変更権限
iRMC S2/S3 設定を行う権限。

AVR 使用権限
「ビューモード」および「フルコントロールモード」で AVR（Advanced Video Redirection）を使用する権限。

リモートストレージ使用権限
リモートストレージ機能を使用する権限。

▶ 「*適用*」ボタンをクリックして、設定を有効にします。

ファイルからのユーザ SSHv2 公開認証鍵のアップロード

「*ファイルからのユーザ SSHv2 公開認証鍵のアップロード*」グループを使用して、ローカルファイルからユーザの SSHv2 公開鍵をアップロードすることができます。

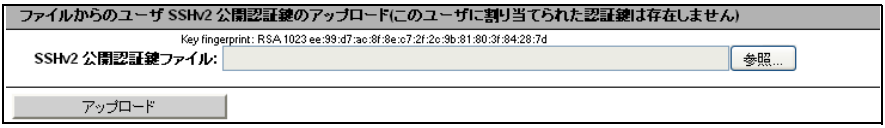


図 155: ユーザ管理 -「ユーザ “<name>” 構成」ページ、、ファイルからのユーザ SSHv2 公開認証鍵のアップロード

iRMC S2/S3 ユーザの SSHv2 公開鍵認証の詳細については、78 ページ の「SSHv2 鍵のファイルから iRMC S2/S3 へのアップロード」の項を参照してください。

E-mail 構成 - ユーザ固有の E-mail 設定

「*E-mail 構成*」グループを使用して、ユーザ固有の E-mail フォーマットを行うことができます。

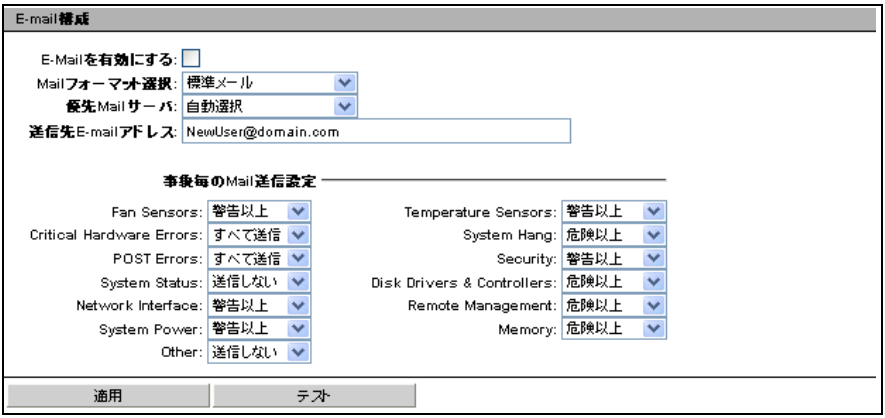


図 156: ユーザ管理 - 「ユーザ “<name>” 構成」ページ、Email 設定

E-mail を有効にする

システムステータスを Email でユーザに通知するかどうかを指定します。

Mail フォーマット選択

選択された E-mail フォーマットによって、「*E-mail 設定 – E-mail 送信フォーマット*」グループで設定を行うことができます（263 ページを参照）。

以下の E-mail フォーマットを使用できます。

- *標準メール*
- *題名固定*
- *ITS フォーマット*
- *Fujitsu REMCS フォーマット*

優先 Mail サーバ

優先 Mail サーバを選択します。
次のオプションを選択できます。

– *自動選択*

プライマリメールサーバが稼動していない場合など、電子メールが即座に正常に送信できない場合、電子メールはセカンダリメールサーバに送信されます。

– *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（261 ページ を参照）だけが、メールサーバとして使用されます。

– *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（262 ページ を参照）だけが、メールサーバとして使用されます。

Email 送信のエラーはイベントログに記録されます。

送信先 E-mail アドレス

受信者の Email アドレス。

事象毎の Mail 送信設定

iRMC S2/S3 ユーザに Email で通知するシステムイベントを設定できます。

iRMC S2/S3 のイベントログの各エントリは、特定の通知グループに割り当てられます。

各イベントグループについて、以下の設定を使用できます。

送信しない

このページンググループについては、通知機能は無効になります。

危険以上

システムイベントログに「*危険 (Critical)*」と記録されたエントリがある場合、Email で通知されます。

警告以上

システムイベントログに「*軽度 (Minor)*」、「*重度 (Major)* 」、「*危険 (Critical)*」のいずれかが記録されたエントリがある場合、Email で通知されます。

すべて送信

エントリがシステムイベントログに記録されたグループの全てのエントリが通知されます。

► 「*適用*」ボタンをクリックして、設定を有効にします。

7.14.2 ディレクトリサービス設定（LDAP）- iRMC S2/S3 のディレクトリサービ スの設定

ディレクトリサービスでグローバルユーザ管理を行うには（XX ページを参照）、「*ディレクトリサービス構成*」ページで iRMC S2/S3 を適切に設定する必要があります。

現在 iRMC S2/S3 LDAP がサポートするディレクトリサービスは、Microsoft Active Directory、Novell eDirectory および Open LDAP です。

以下の記号は、LDAP 上で文字列を検索するためのメタキャラクタとして予約されています：*、\、&、|、!、=、<、>、~、：

したがって、ユーザ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。

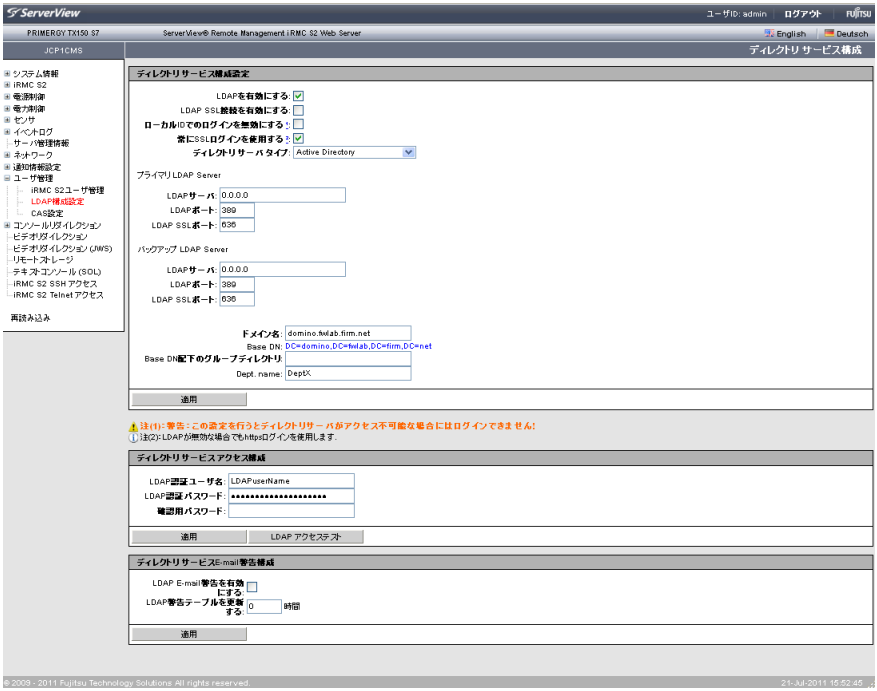


図 157: 「ディレクトリサービス構成」ページ（LDAP 構成）

LDAP を有効にする

このオプションで、iRMC S2/S3 が、LDAP を使用してディレクトリサービスにアクセスできるか否かを設定します。LDAP を使用するディレクトリサービスへのアクセスは、「*LDAP を有効にする*」が有効な場合のみ有効です。

「*LDAP を有効にする*」が有効な場合（140 ページを参照）、ログイン情報は、常に SSL 暗号化されて Web ブラウザと iRMC S2/S3 の間で送信されます。

LDAP SSL 接続を有効にする

このオプションが有効な場合、iRMC S2/S3 とディレクトリサーバ間のデータ送信は SSL 暗号化されます。

「*LDAP SSL 接続を有効にする*」は、iRMC S2/S3 Web インターフェースページが開くときに SSL 保護するかどうかには影響ありません。

「*LDAP SSL 接続を有効にする*」は、ドメインコントローラ認証がインストールされている場合のみ動作します。

ローカル ID でのログインを無効にする

このオプションを有効にした場合、iRMC S2/S3 のローカルユーザ認証はロックされ、ディレクトリサービスによるユーザ認証のみが有効になります。

注意！

「*ローカル ID でのログインを無効にする*」が有効になっていて、ディレクトリサービスへの接続が不可能な場合、iRMC S2/S3 へのログインはできなくなります。

常に SSL ログインを使用する

このオプションは LDAP が無効の場合にのみ有効です。

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、常に HTTP SSL セキュアなログインページが使用されます。「*常に SSL ログインを使用する*」を有効にせず、かつ、LDAP が無効になっている場合は、簡易ユーザ認証がログインに使用されます。

ディレクトリサーバタイプ
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
- *Open DS*

▶ 「*適用*」ボタンをクリックして、設定を有効にします。

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*」については、278 ページ の「Microsoft Active Directory 用の iRMC S2/S3 の設定」の項を参照してください。
- 「*eDirectory*」、「*Open LDAP*」、「*OpenDS*」については、282 ページ の「Novell eDirectory/OpenLDAP/OpenDS 用の iRMC S2/S3 の設定」の項を参照してください。

7.14.2.1 Microsoft Active Directory 用の iRMC S2/S3 の設定

選択した「*Active Directory*」を確定後「*適用*」をクリックすると、次の仕様の「*ディレクトリサービス構成*」ページが表示されます。

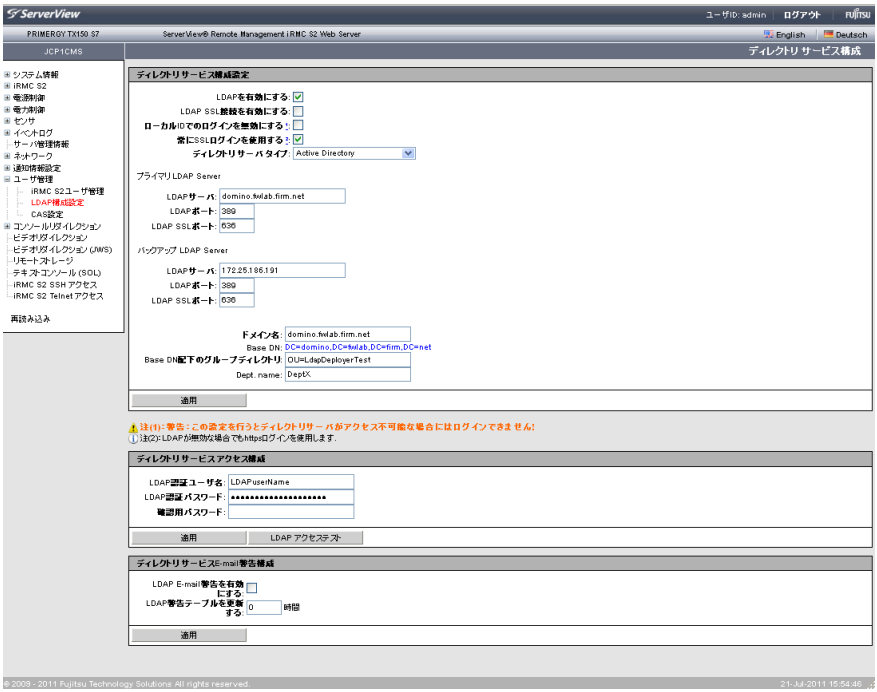


図 158: ディレクトリサービス構成：Microsoft Active Directory の仕様

図 158 で例として表示されるエントリは、『ServerView でのユーザ管理』マニュアルに示す例および図を参照しています。

次の手順に従います。

► 「*ディレクトリサービス構成設定*」グループの設定を行います。

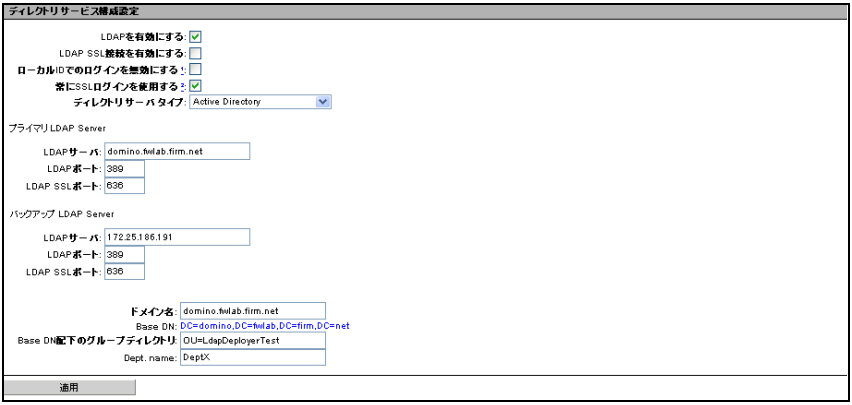


図 159: ディレクトリサービス構成設定：Microsoft Active Directory の仕様

プライマリ LDAP Server
使用する LDAP ディレクトリサーバ。

LDAP サーバ
プライマリ LDAP サーバの IP アドレスまたは DNS 名。

LDAP ポート
プライマリ LDAP サーバの LDAP ポート。

LDAP SSL ポート
プライマリ LDAP サーバのセキュアな LDAP ポート。

バックアップ LDAP Server
バックアップサーバとして運用され、「*LDAP サーバ 1*」が故障した場合のディレクトリサーバとして使用される LDAP ディレクトリサーバ。

LDAP サーバ
バックアップ LDAP サーバの IP アドレスまたは DNS 名。

LDAP ポート
バックアップ LDAP サーバの LDAP ポート。

LDAP SSL ポート
バックアップ LDAP サーバのセキュアな LDAP ポート。

ドメイン名
ディレクトリサーバの完全な DNS パス名。

Base DN
「*Base DN*」は、「*ドメイン名*」から自動的に取得されます。

Base DN 配下のグループディレクトリ
Base DN（Group DN Context）のサブツリーとして *SVS* または **iRMCgroups** を含む組織単位（OU）のパス名。

Dept. name
「Dept. name」は、ディレクトリサービスではユーザ許可と警告ロールを確認するために使用されます。Department X サーバと Department Y サーバでは、許可が異なることがあります。

► *「適用」*をクリックして設定を有効にします。

► 「*ディレクトリサービスアクセス構成*」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 ID に関連する警告通知のために必要なものです。警告通知が無効な場合、「*ディレクトリサービスアクセス構成*」は重要ではありません。

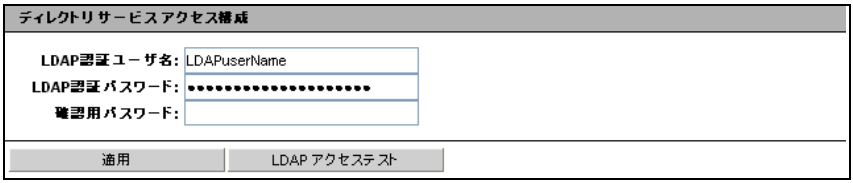


図 160: Microsoft Active Directory：ディレクトリサービスアクセス構成

LDAP 認証ユーザ名
LDAP サーバにログオンするときの iRMC S2/S3 ユーザ名。

LDAP 認証パスワード
ユーザ名に対応したパスワードを使用して、LDAP サーバでの認証を行います。

パスワード確認
「*LDAP 認証パスワード*」に入力したパスワードをもう一度入力します。

LDAP アクセステスト
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表示します（図 161 を参照）。

このテストは基本的なアクセスデータ（「LDAP サーバが存在するか」あるいは「ユーザは設定されているか」）を確認するもので、ユーザ認証のすべてを確認するものではありません。

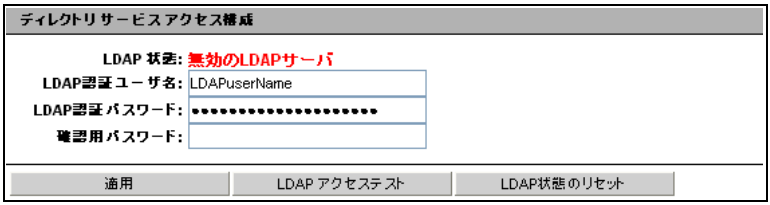


図 161: Microsoft Active Directory：LDAP サーバへの接続状況

► 「*LDAP 状態のリセット*」ボタンをクリックして、画面への表示をリセットします。

► *「適用」*をクリックして設定を有効にします。

► 「*ディレクトリサービス E-mail 警告構成*」グループを使用して、グローバル Email 警告の設定を行います。

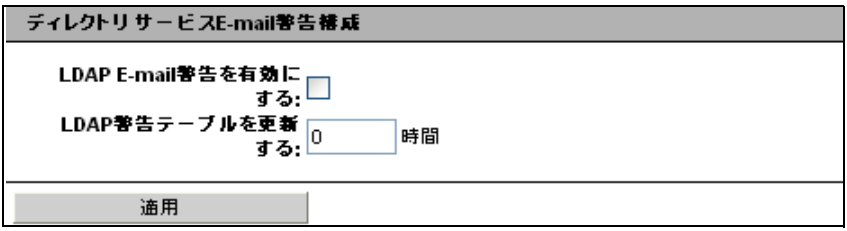


図 162: ディレクトリサービス E-mail 警告構成

LDAP E-mail 通知を有効にする
グローバル Email 通知を有効にします。

LDAP 警告テーブルを更新する（時間）
Email テーブルを定期的に更新する間隔を定義します（『ServerView でのユーザ管理』マニュアルを参照）。

0 よりも大きい値を指定することを推奨します。「0」を設定すると、テーブルは更新されなくなります。

► *「適用」*をクリックして設定を有効にします。

7.14.2.2 Novell eDirectory/OpenLDAP/OpenDS 用の iRMC S2/S3 の設定

「*Novell*」、「*OpenLDAP*」または「*OpenDS*」を選択して「*適用*」をクリックすると、「*ディレクトリサービス構成*」ページが表示されます。

「*ディレクトリサービス構成*」ページの構造は、Novell eDirectory、OpenLDAP、OpenDS では同じです。

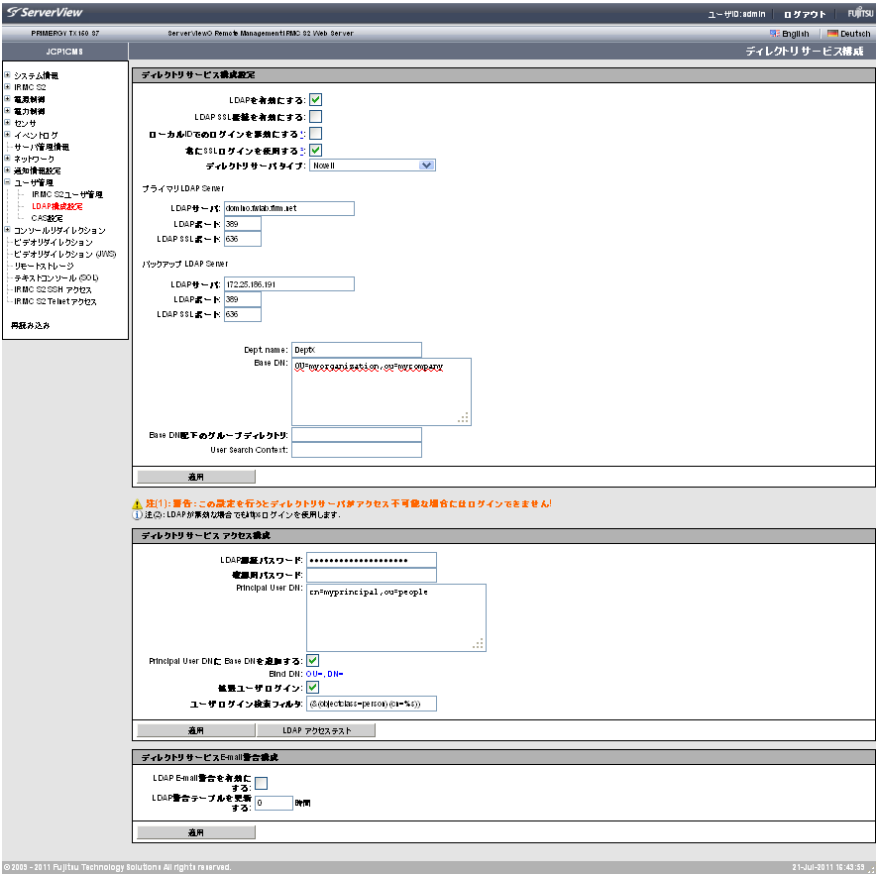


図 163: ディレクトリサービス構成設定：Novell eDirectory/ Open LDAP/OpenDS の仕様

図 163 で例として表示されるエントリは、『ServerView でのユーザ管理』マニュアルに示す例および図を参照しています。

次の手順に従います。

► 「*ディレクトリサービス構成設定*」グループの設定を行います。

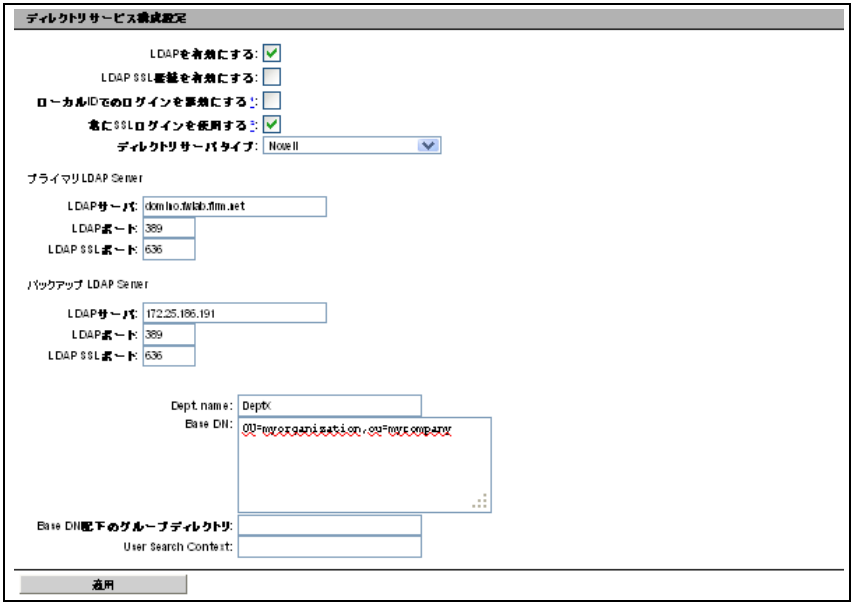


図 164: ディレクトリサービス構成設定：Novell eDirectory/Open LDAP/OpenDS の仕様

プライマリ LDAP Server
使用する LDAP ディレクトリサーバ。

LDAP サーバ
プライマリ LDAP サーバの IP アドレスまたは DNS 名。

LDAP ポート
プライマリ LDAP サーバの LDAP ポート。

LDAP SSL ポート
プライマリ LDAP サーバのセキュアな LDAP ポート。

バックアップ LDAP Server
バックアップサーバとして運用され、「*LDAP サーバ 1*」が故障した場合のディレクトリサーバとして使用される LDAP ディレクトリサーバ。

LDAP サーバ
バックアップ LDAP サーバの IP アドレスまたは DNS 名。

LDAP ポート
バックアップ LDAP サーバの LDAP ポート。

LDAP SSL ポート
バックアップ LDAP サーバのセキュアな LDAP ポート。

Dept. name
部署名。ディレクトリサービスではユーザ許可を確認するときに部署名が必要です。Department X サーバと Department Y サーバでは、許可が異なることがあります（97 ページ の図 32 も参照）。

Base DN
「*Base DN*」は、eDirectory または Open LDAP および OpenDS サーバの完全な分類名を示し、OU（組織単位）の *SVS* または **iRMCgroups** を含むツリーまたはサブツリーを表します。この DN は、LDAP 検索の開始点を示します。

Base DN 配下のグループディレクトリ
Base DN（Group DN Context）のサブツリーとして *SVS* または **iRMCgroups** を含む OU のパス名。

User Search Context
Base DN（User Search Context）のサブツリーとして OU（組織単位）の **Users** を含む OU のパス名。

► *「適用」*をクリックして設定を有効にします。

► 「*ディレクトリサービスアクセス構成*」グループで、LDAP アクセスデータを設定します。

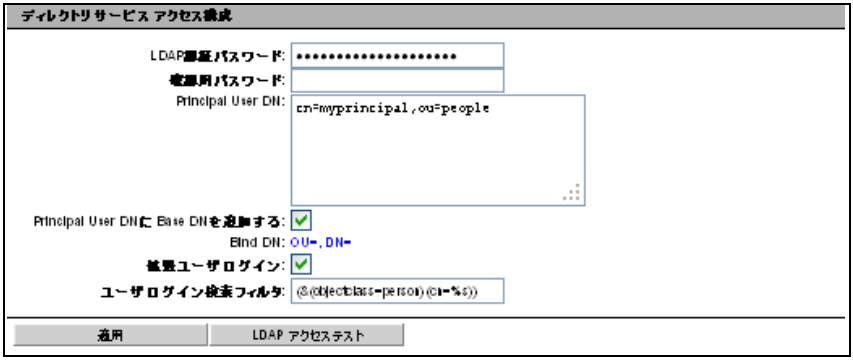


図 165: Novell eDirectory/Open LDAP：ディレクトリサービスアクセス構成

LDAP 認証パスワード

「*Principal User*」のパスワードを入力して LDAP サーバでの認証を行います。

確認用パスワード

「*LDAP 認証パスワード*」に入力したパスワードをもう一度入力します。

Principal User DN

完全な構成名。iRMC S2/S3 で使用するユーザ ID（プリンシパルユーザ）の オブジェクトパスと属性の完全な記述で、これを使用して iRMC S2/S3 は、LDAP サーバ からの iRMC S2/S3 ユーザの可を問い合わせます。

Principal User DN に Base DN を追加する

このオプションが有効な場合、「*Principal User DN*」を設定する必要はありません。この場合、「*ディレクトリサービス構成設定*」グループの「*Base DN*」で設定した Base DN が使用されます。

Bind DN

「Bind DN」には、LDAP 認証で使用されるプリンシパルユーザ DN が表示されます。

拡張ユーザログイン

ユーザがログインする際の柔軟性を拡張します。

注意！

このオプションの有効化は、LDAP 構文に詳しい方のみご利用ください。不正な検索フィルタを設定して有効にすると「*拡張ユーザログイン*」オプションが無効になるまで、グローバルログインでの iRMC S2/S3 へのログインができません。

図 166: 拡張ユーザログイン

「*拡張ユーザログイン*」を選択して「*適用*」で有効にした場合、「*ユーザログイン検索フィルタ*」フィールドが追加で表示され、標準の検索フィルタ "(&(objectclass=person)(cn=%s))" が表示されます。

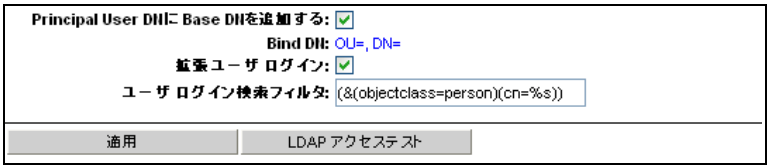


図 167: 「拡張ユーザログイン」用 LDAP 検索フィルタ

ログイン時に、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、標準フィルタを変更することができます。すべてのグローバルログインが許可され、この検索フィルタの条件を満たす場合 iRMC S2/S3 へログインします。

LDAP アクセステスト
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表示します（図 161 を参照）。

このテストは基本的なアクセスデータ（「LDAP サーバが存在するか」あるいは「ユーザは設定されているか」）を確認するもので、ユーザ認証のすべてを確認するものではありません。

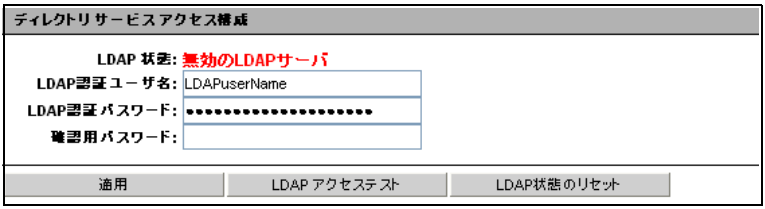


図 168: eDirectory/OpenLDAP/OpenDS: LDAP サーバへの接続状況

► 「*LDAP 状態のリセット*」ボタンをクリックして、画面への表示をリセットします。

► *「適用」*をクリックして設定を有効にします。

► 「*ディレクトリサービス E-mail 警告構成*」グループを使用して、グローバル Email 警告の設定を行います。

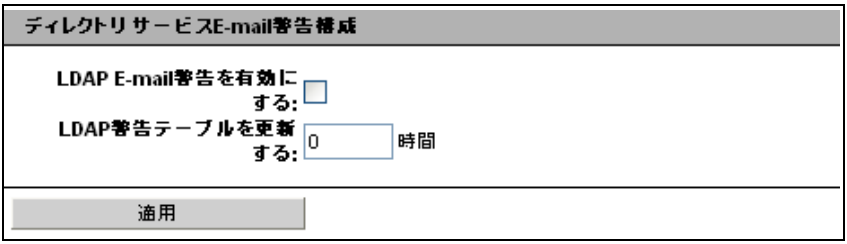


図 169: ディレクトリサービス E-mail 警告構成

LDAP E-mail 通知を有効にする
グローバル Email 通知を有効にします。

LDAP 警告テーブルを更新する（時間）
Email テーブルを定期的に更新する間隔を定義します（『ServerView でのユーザ管理』マニュアル を参照）。「0」を設定すると、テーブルは更新されなくなります。

► *「適用」*をクリックして設定を有効にします。

7.14.3 Centralized Authentication Service（CAS）設定 - CAS サービスの設定

このビューは、iRMC S2/S3 が搭載される一部の PRIMERGY サーバではサポートされていません。

SSO は、Web インターフェースを使用して iRMC S2/S3 にアクセスする場合のみサポートされます。SSO は、リモートマネージャ（Telnet/SSH）を使用して iRMC S2/S3 にアクセスする場合は**サポートされません**。

「*Centralized Authentication Service（CAS）設定*」ページでは、CAS ベースのシングルサインオン（SSO）認証用の iRMC S2/S3 Web インターフェースを設定できます。

CAS サービスの SSO ドメイン内のアプリケーションに初めてログインすると、CAS 固有のログイン画面でログイン認証情報の入力が要求されます。CAS サービスによる認証に成功すると、ユーザはログイン認証情報を再び入力せずに、iRMC Web インターフェースと SSO ドメイン内の他のサービスへのアクセスが許可されます。

図 170: Centralized Authentication Service（CAS）設定

CAS 一般設定

「*CAS 一般設定*」グループでは、CAS アクセスデータを設定できます。

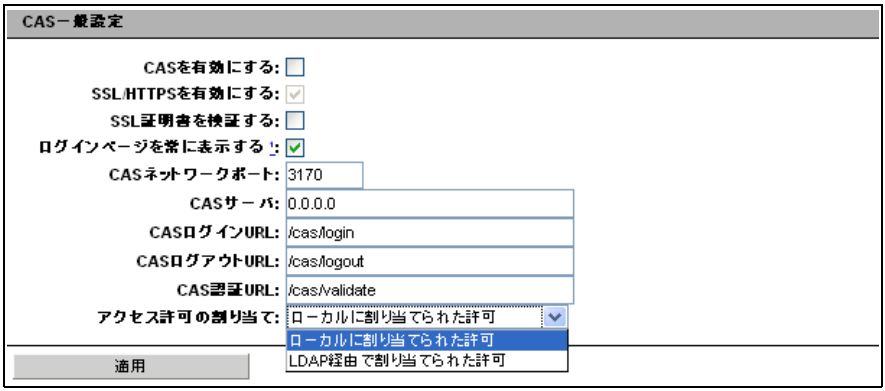


図 171: CAS 一般設定

CAS を有効にする
: 「*CAS 一般設定*」グループで指定する CAS サービスを使用して SSO を有効にします。

SSL/HTTPS を有効にする
: CAS サービスと iRMC S2/S3 間のすべての通信は SSL 暗号化されます。

SSL 証明書を検証する
: CAS サービスの SSL 証明書を CA 証明書と照らし合わせて確認します。

ログインページを常に表示する

「*ログインページを常に表示する*」が無効で CAS サービスにアクセスできない場合は、ブラウザのナビゲーションバーで、iRMC S2/S3 の IP アドレスの後に /login と入力します。

iRMC S2/S3 ログインページは常に表示されます。

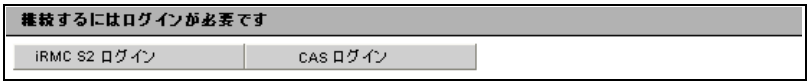


図 172: ログインページ

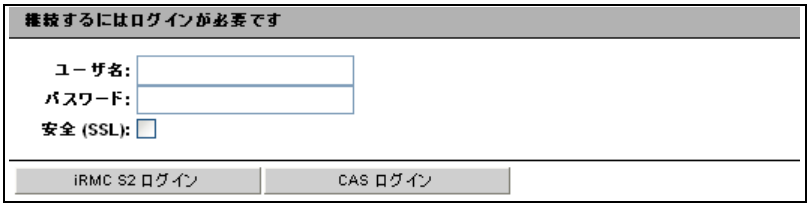


図 173: ログインページ - 明示的な認証情報の要求

これにより、「*CAS ユーザ権限と許可*」で定義した認証プロファイルとは異なる権限と許可を使用して、一時的に iRMC S2/S3 にログインできます（292 ページを参照）。

たとえば、現在 CAS サービスに「*User*」権限を持つユーザ ID でログインしているときに、「*Administrator*」権限が必要な操作を行いたいとします。ユーザは、必要な権限を持つユーザ ID で一時的に iRMC S2/S3 にログインできます。ただし、両方のユーザ ID 間で切り替えを行うことはできません。

「*iRMC S2/S3 ログイン*」および「*CAS ログイン*」ボタンには次の機能があります。

iRMC S2/S3 ログイン

「*ユーザ名*」と「*パスワード*」に指定した値を使用して、*iRMC S2/S3 Web インターフェースにログインします。*CAS サービスはバイパスされます。

CAS ログイン

SSO を使用して iRMC S2/S3 Web インターフェースにログインします。

- ユーザが CAS サービスによってまだ認証されていない場合、「*ユーザ名*」と「*パスワード*」に指定した値を使用して認証のために CAS サービスにリダイレクトされます。
- ユーザが CAS サービスによって既に認証されている場合、ユーザ名とパスワードの入力を要求されずに、iRMC S2/S3 にログインします。

CAS ネットワークポート

CAS サービスのポート。
デフォルトポート番号：3170

CAS サーバ

CAS サービスの DNS 名。

SSO ドメインに参加するすべてのシステムは、必ず同じアドレス表記を使用して中央管理用サーバ（CMS）を参照する必要があります。（SSO ドメインは、同じ CAS サービスを使用して認証を行うすべてのシステムで構成されます。）そのため、たとえば「my-cms.my-domain」という名前を使用して ServerView Operations Manager をインストールした場合、これとまったく同じ名前を使用して iRMC S2/S3 の CAS サービスを指定します。そうせずに、「my-cms」のみや my-cms の別の IP アドレスを指定しても、SSO は 2 つのシステム間で有効になりません。

CAS ログイン URL

CAS サービスのログイン URL。

CAS ログアウト URL

CAS サービスのログアウト URL。

CAS 認証 URL

CAS サービスの URL を有効にします。

アクセス許可の割り当て

SSO を使用して iRMC S2/S3 にログインするユーザの iRMC S2/S3 権限と許可を定義します。

ローカルに割り当てられた許可

「*CAS ユーザ権限と許可*」で定義した権限と許可がユーザに適用されます。

LDAP 経由で割り当てられた許可
LDAP ディレクトリサービスで定義した認証プロファイルがユーザに適用されます。

「*LDAP 経由で割り当てられた許可*」オプションは、LDAP が有効な場合のみ使用できます（オプション 276 ページ の「LDAP を有効にする」を参照）。

CAS ユーザ権限と許可

「*CAS ユーザ権限と許可*」グループでは、ユーザが SSO を使用して iRMC S2/S3 にログインする場合に、ユーザに許可する iRMC S2/S3 権限と許可を定義できます。

「*CAS ユーザ権限と許可*」グループは、「*CAS 一般設定*」グループの「*アクセス許可の割り当て*」で「*LDAP 経由で割り当てられた許可*」が選択されている場合は表示されません。

図 174: CAS ユーザ権限と許可

権限レベル
権限グループをユーザに割り当てます。

- *User*
- *Operator*
- *Administrator*
- *OEM*

権限グループに関連する許可に関する情報は、68 ページ の「ユーザー権限」の項を参照してください。

IPMI 個別許可に加えて、次のチャネル非依存許可を個別にユーザに割り当てることもできます。

ユーザアカウント変更権限
ローカルユーザアクセスデータを設定する権限。

iRMC S2/S3 設定変更権限
iRMC S2/S3 設定を行う権限。

AVR 使用権限
「ビューモード」および「フフルコントロールモード」モードで AVR（Advanced Video Redirection）を使用する権限。

リモートストレージ使用権限
リモートストレージ機能を使用する権限。

7.15 コンソールリダイレクション - コンソールのリダイレクト

次のページをコンソールリダイレクションに使用できます。

- 294 ページ の「BIOS テキストコンソール - テキストコンソールのリダイレクションの 設定と開始」を参照。
- 304 ページ の「ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の 開始」を参照。

7.15.1 BIOS テキストコンソール - テキストコンソールのリダイレクションの 設定と開始

「*BIOS テキストコンソール*」ページを使用して、テキストコンソールのリダイレクションを設定できます。

テキストコンソールのリダイレクションは、BIOS でも設定できます（52 ページ の「iRMC S3 のテキストコンソールリダイレクションの設定」の項を参照）。

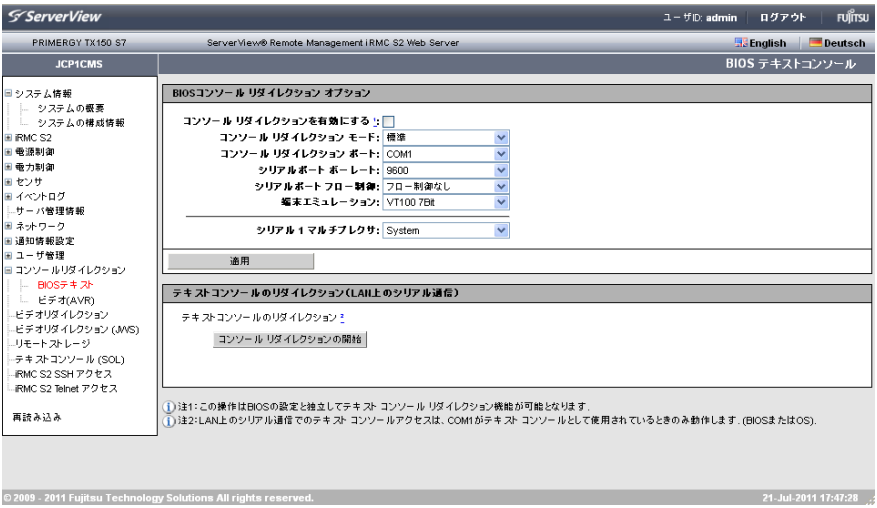


図 175: 「BIOS テキストコンソール」ページ

7.15.1.1 BIOS コンソールリダイレクションオプション - テキストコンソールのリダイレクションの設定

「*BIOS コンソールリダイレクションオプション*」を使用して、テキストコンソールのリダイレクションを設定できます。

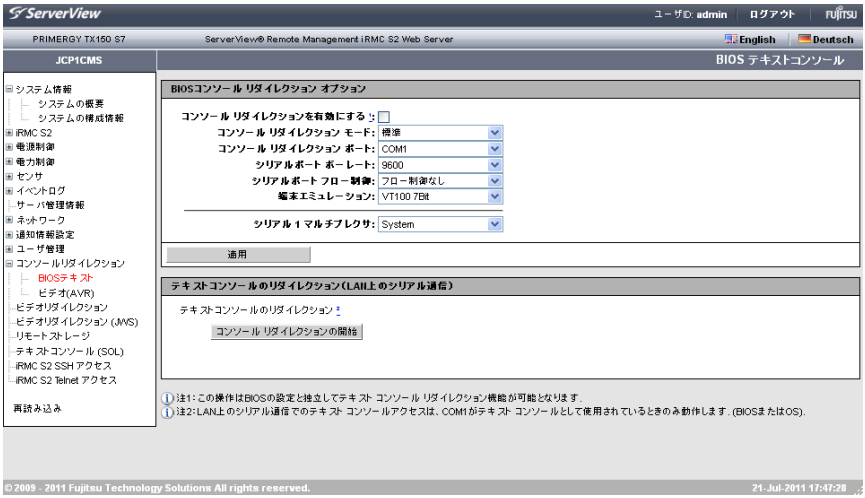


図 176: 「BIOS テキストコンソール」ページ - BIOS コンソールリダイレクションオプション

コンソールリダイレクションを有効にする

このオプションで、コンソールリダイレクションを有効 / 無効にできます。

オペレーティングシステムでも、BIOS 設定にかかわらず、テキストコンソールのリダイレクションを許可することができます。

コンソールリダイレクションモード

この設定は、オペレーティングシステムが実行中（BIOS POST フェーズ完了後）のコンソールリダイレクションの動作に影響します（302 ページ の「オペレーティングシステム実行中のテキストコンソールのリダイレクション」を参照）。

標準

コンソールリダイレクションは、BIOS POST フェーズの後、終了します。

拡張

コンソールリダイレクションは、BIOS POST フェーズが完了した後も有効になります。

コンソールリダイレクションポート
2 つのシリアルポートを使用できます（*シリアル 1*、*シリアル 2*）。

LAN を使用したコンソールリダイレクションを行う場合は、「シリアル 1」が設定されている必要があります。

「*シリアル 2*」を選択した場合、モデムケーブルを使用した接続のみ可能 です。

シリアルポートボーレート
次のボーレートが設定可能です：1200、2400、4800、9600、19200、38400、57600、115200。

シリアルポートフロー制御
次の設定が可能です。

フロー制御なし
フロー制御を行いません。

XON/XOFF（ソフトウェア）
通信制御がソフトウェアによって行われます。

CTS/RTS（ハードウェア）
通信制御がハードウェアによって行われます。

端末エミュレーション
次の端末エミュレーションを使用できます。

VT100 7Bit、*VT100 8Bit*、*PC-ANSI 7Bit*、*PC-ANSI 8 Bit*、*VT100+*、*VT-UTF8*

シリアル 1 マルチプレクサ
マルチプレクサの設定との整合性を確認します。

- シリアル：System
- LAN：iRMC S2/S3

► 「*適用*」ボタンをクリックして、設定を有効にします。

7.15.1.2 テキストコンソールのリダイレクション（LAN 上のシリアル通信） - テキストコ ンソールのリダイレクションの開始

*「テキストコンソールのリダイレクション（LAN 上のシリアル通信）」*を使用して、テキストコンソールのリダイレクションを開始できます。

「テキストコンソールリのダイレクション（LAN 上のシリアル通信）」では、オペレーティングシステムまたは BIOS が、テキストコンソールのリダイレクションに、「シリアルポート 1（COM1 ）」を使用していることを前提とします。

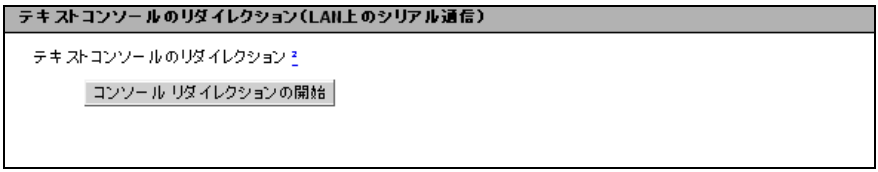


図 177: テキストコンソールのリダイレクション（LAN 上のシリアル通信）

- 「*コンソールリダイレクションの開始*」ボタンをクリックして、テキストコンソールのリダイレクションを開始します。

  テキストコンソールのリダイレクション用の Java アプレットが開始されます（298 ページ の図 178 を参照）。

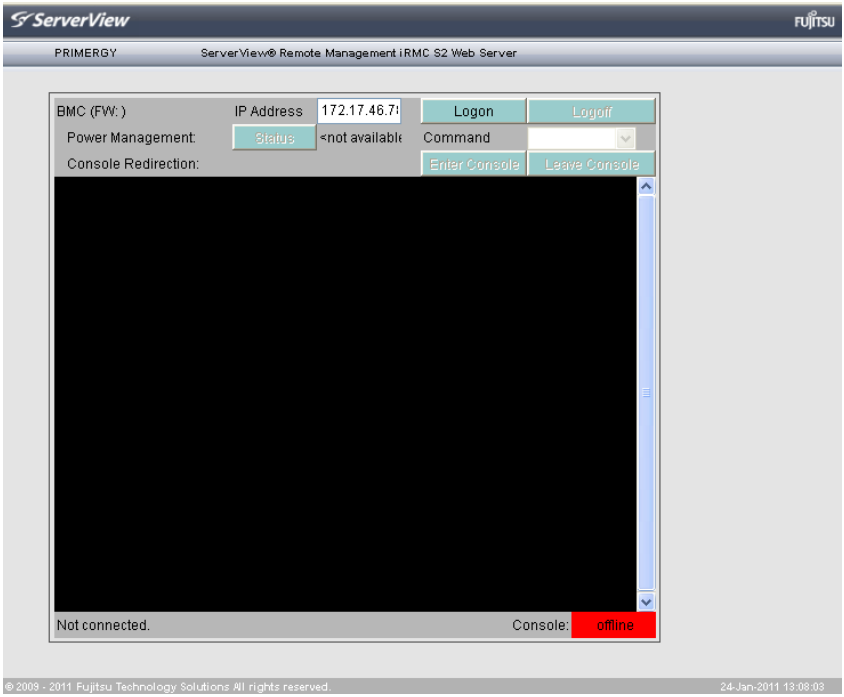


図 178: 電源管理およびテキストコンソールのリダイレクション画面（ログイン前）

► 「*Logon*」ボタンをクリックして、iRMC S2/S3 にログインします。

iRMC S2/S3 のユーザ名およびパスワードを入力するように要求されます。

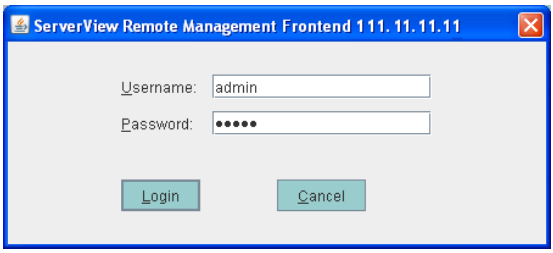


図 179: 電源管理およびテキストコンソールリのダイレクション - ログイン画面

► ユーザ名およびパスワードを入力し、「*Login*」をクリックして確定します。

電源管理およびテキストコンソールリのダイレクション画面が表示されます。

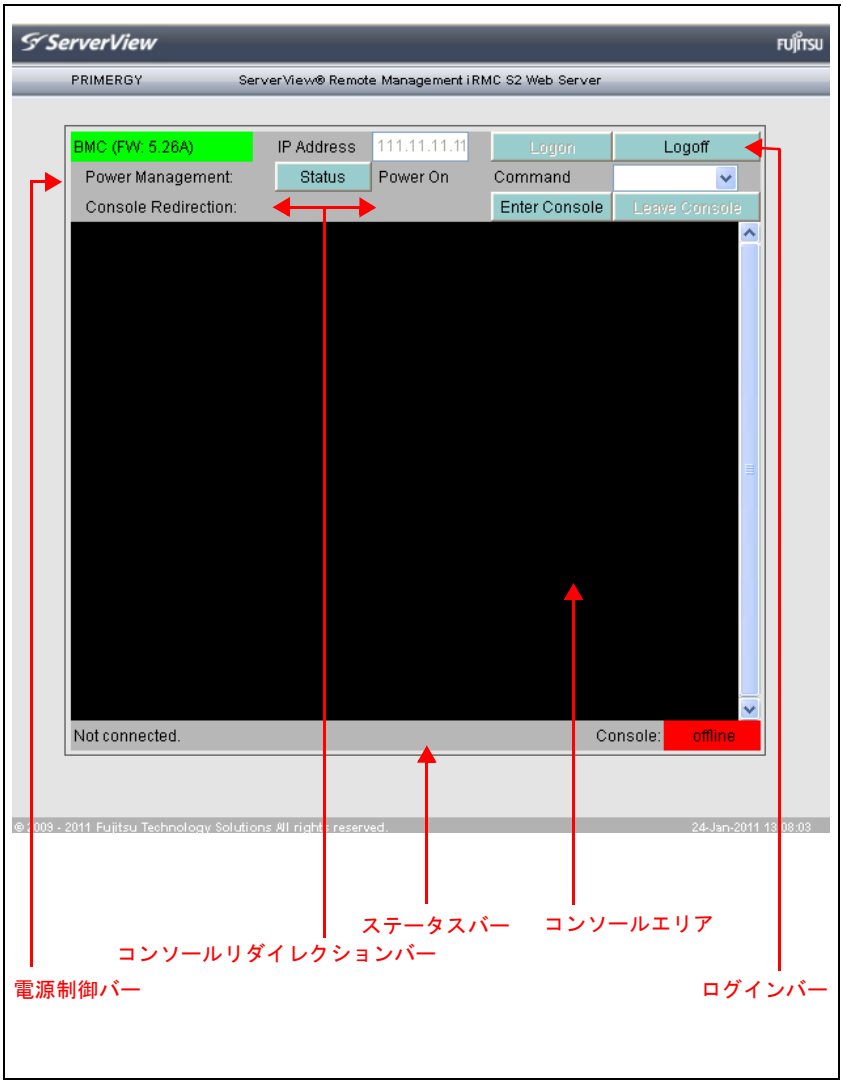


図 180: 電源管理およびテキストコンソールリのダイレクション画面

コンソールリダイレクション画面に表示される項目について以下で説明します。

ログインバー
ログインバーには、iRMC S2/S3 の IP アドレスおよび現状のファームウェアのバージョンが表示されます。「*Login*」および「*Logout*」ボタンを使用して、iRMC S2/S3 にログインあるいはログアウトできます。

電源制御バー
電源制御バーには、管理対象サーバの電源状態の情報が表示されます。「*Status* 」ボタンをクリックして表示を更新することができます。

「*Command*」ドロップダウンリストを使用して、管理サーバの IPMI コマンドの選択および実行ができます（301 ページを参照）。これを行うために、コンソールに接続する必要はありません。

コンソールリダイレクションバー
「*Enter Console*」および「*Leave Console*」ボタンを使用して、コンソールエリアを表示 / 非表示にできます。

コンソールエリア
コンソールエリアにリダイレクトされたテキストコンソールを表示します。

ステータスバー
ステータスバーに、iRMC S2/S3 の IP アドレスおよびコンソールリダイレクションのポート番号を表示します。また、ステータスバーにはコンソールリダイレクションのオンライン / オフラインの状態も表示されます。

► 「*Enter Console*」をクリックします。

コンソールに接続されたら、必要なコマンドをコンソールエリアで直接入力するか、「*Command*」ドロップダウンリストでクリックして実行できます（IPMI コマンドのみ）。

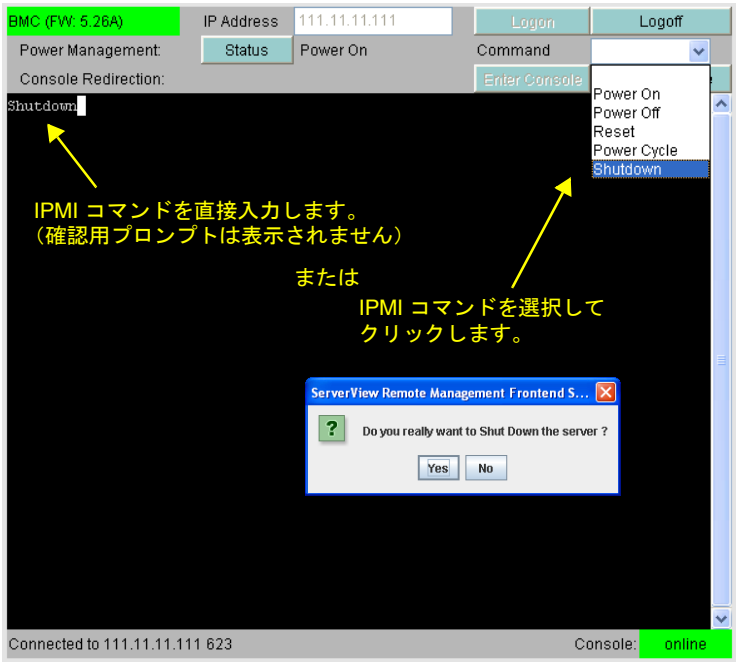


図 181: SAC あるいは IPMI コマンドをコンソールからの入力

IPMI コマンド	説明
Power On	サーバの電源を投入します。
Power Off	サーバの電源を切断します。
Reset	オペレーティングシステムの状態にかかわらず、サーバを完全に再起動します（コールドスタート）。
Power Cycle	サーバの電源切断から、およそ 5 秒経過後、電源投入を行います。
Shutdown	グレースフルシャットダウンし、電源を切断します。

► コンソールとの接続を閉じるには、「*Leave Console*」をクリックします。

7.15.1.3 オペレーティングシステム実行中のテキストコンソールのリダイレクション

管理対象サーバのオペレーティングシステムによっては、BIOS POST フェーズ後もコンソールリダイレクションの使用を継続することができます。

DOS

条件：

コンソールリダイレクションの BIOS 設定が、「*拡張*」に設定されている必要があります（294 ページ の「BIOS テキストコンソール - テキストコンソールのリダイレクションの 設定と開始」を参照）。

管理対象サーバで PRIMERGY ServerView Suite 診断ソフトウェアを起動する場合は、コンソールリダイレクションを使用して、PRIMERGY ServerView Suite 診断を操作することができます。

Windows Server 2003/2008

Windows Server 2003/2008 では、POST フェーズ後、自動的にコンソールリダイレクションを使用できます。さらに設定を行う必要はありません。オペレーティングシステムの起動中に、Windows Server 2003 SAC コンソール /Windows Server 2008 SAC コンソールに切り替わります。

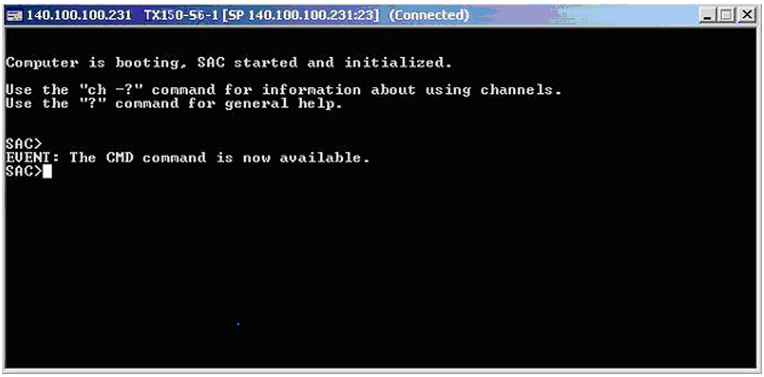


図 182: Windows Server 2003 SAC コンソール

Linux

Linux オペレーティングシステムでは、POST フェーズ後にコンソールリダイレクションを使用するために、次の設定を行う必要があります。一度設定すると、リモートアクセスも可能になります。

必要な設定

設定は、プログラムのバージョンによって異なる場合があります。

SuSe および RedHat

/etc/inittab ファイルの最後に次の行を追加します。

```
xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0
```

RedHat

/etc/grub.conf ファイルのカーネルブートパラメータに以下を追加します。

```
console=ttyS0,<baud-rate> console=tty0
```

SuSE

/boot/grub/menu.lst ファイルのカーネルブートパラメータに以下を追加します。

```
console=ttyS0,<baud-rate> console=tty0
```

7.15.2 ビデオリダイレクション（AVR）- ビデオリダイレクション（AVR）の 開始

「*ビデオリダイレクション（AVR）*」ページを使用して、グラフィカルなコンソールリダイレクションを開始できます。「ビデオリダイレクション」機能では、管理対象サーバからのグラフィカルな出力をリモートワークステーションにリダイレクトし、リモートワークステーションのキーボードおよびマウス入力を管理対象サーバへ割り当てるので、ローカルで作業しているかのようにリモートワークステーションから管理対象サーバにアクセスできます。

AVR は、同時に 2 人のユーザが使用できます。一方のユーザがサーバをフルコントロールしている場合（フルコントロールモード）、もう一方のユーザは、キーボードおよびマウスの操作を表示するだけしかできません（ビューモード）。

iRMC S2/S3 の「*ビデオリダイレクション（AVR）*」ファンクションを使用するには、ライセンスキーが必要です（169 ページ の「iRMC S2/S3 情報 - iRMC S2/S3 に関する情報」の項を参照）。

AVR 機能には、Java アプレットが使用されています。

図 183: 「ビデオリダイレクション（AVR）」ページ

ASR スクリーンショットの作成

「*スクリーンショット*」ページを使用して以下のことができます。

– 管理対象サーバの現在の VGA 画面のスクリーンショット（ビデオスクリーンショット）を取得して、それを iRMC S2/S3 のファームウェアに保存できます。

– iRMC S2/S3 ファームウェアに保存されたスクリーンショットを表示できます。

– iRMC S2/S3 ファームウェアに保存されたスクリーンショットを削除できます。

図 184: ビデオスクリーンショットの作成

ビデオスクリーンショットは ASR&R イベント発生時に自動的に作成されます。これらは、Windows では、管理対象サーバでの典型的なウォッチドッグイベントまたは「ブルースクリーン画面」です。

最大 **1 つ**のビデオスクリーンショット（作成日が最も新しいスクリーンショット）が iRMC S2/S3 ファームウェアに保存されます。

表示されるボタンをクリックして、以下の動作を行うことができます。

全画面表示

（ビデオスクリーンショットが既に保存されている場合にのみ表示されます。）
スクリーンショットは、別のブラウザ画面に表示されます。

プレビュー

（ビデオスクリーンショットが既に保存されている場合にのみ表示されます。）
「*スクリーンショット*」グループに、スクリーンショットのサムネイルが表示されます。

作成

新しいビデオスクリーンショットを取得します。

削除

（ビデオスクリーンショットが既に保存されている場合にのみ表示されます。）
iRMC S2/S3 ファームウェアに保存されたビデオスクリーンショットを、確認後に削除します。

AVR 実行中セッション - 現在の AVR セッションの表示

「*AVR 実行中セッション表*」には、現在の実行中の AVR セッションが表示されます。AVR セッションが実行されていない場合、「*AVR 実行中セッション表*」は表示されません。

2 つの AVR セッションが現在実行されている場合、「*切断*」ボタンが各セッションに表示されます。

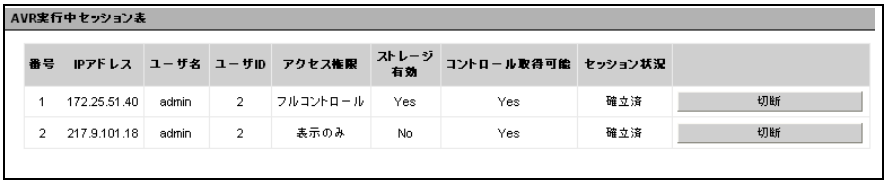


図 185: AVR 実行中セッション - （2 つの AVR セッションが実行中の場合）

切断

「*切断*」ボタンでは、確認ダイアログが表示され、左側のボタンで、AVR セッションを閉じることができます。

「*切断*」ボタンを使用してのみ、他のユーザの AVR セッションを閉じることができます。ユーザ固有のセッションを閉じるには、「*拡張機能*」メニューか ら、「*終了*」ボタンを使用します（105 ページを参照）。

ビデオリダイレクションオプション - 管理サーバ上のビデオリダイレクションセッション中の USB ポートの無効化

この機能は、一部の PRIMERGY サーバでサポートされていません。

「*ビデオリダイレクション中は USB ポートを無効化する*」を使用して、管理対象サーバで AVR セッション中に、どの USB ポートを無効にするかを設定できます。

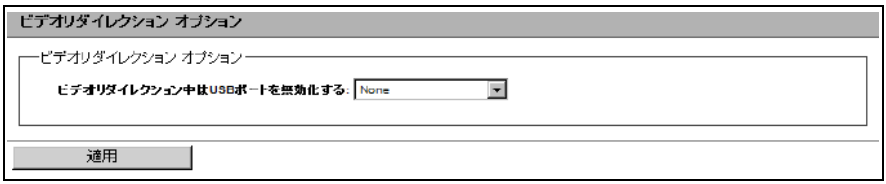


図 186: ビデオリダイレクションオプション

None
どの USB ポートも無効になりません。

前面 USB コネクタ
サーバの前面の USB ポートのみが使用不可能になります。

背面 USB コネクタ
サーバの背面の USB ポートのみが使用不可能になります。

すべて無効
サーバのすべての USB ポートが無効になります。

▶ 「*適用*」ボタンをクリックして、設定を有効にします。

サーバ側のモニタ - サーバ側モニタの電源 ON/OFF オプション

管理対象サーバ側のモニタの状態が、「*サーバ側のモニタ*」に表示されます（93 ページ の「サーバ側のモニタ ON/OFF 機能」の項を参照）。

また、以下を設定できます。

– リモートワークステーションから、サーバ側モニタの電源の ON/OFF を切り替えることができます。

– サーバ側モニタの電源を、AVR セッションの開始に合わせ、AVR セッション中は自動的にオフさせることができます。

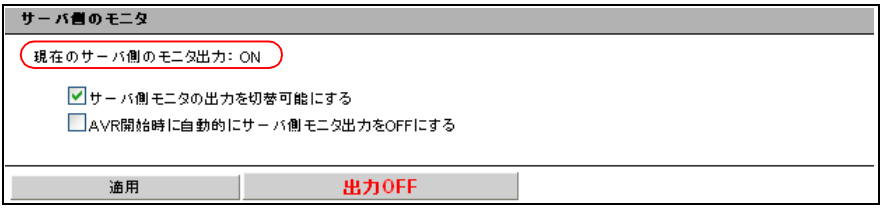


図 187: 「ビデオリダイレクション（AVR）」ページ - サーバ側のモニタ

サーバ側モニタの出力を切替可能にする

このオプションを使用して、以下のオプションを有効にすることができます。

– AVR セッションのフルコントロールモードでは、サーバ側モニタの出力の ON/OFF を切り替えることができます（AVR の「*拡張機能*」メニュー、105 ページを参照）。

– **管理者あるいは OEM 権限を持ったユーザ**は、「*出力 OFF*」/「*出力 ON*」切り替えボタンも使用できます。この方法を使用して、サーバ側モニタの電源の ON/OFF を切り替えることができます（図 188 を参照）。

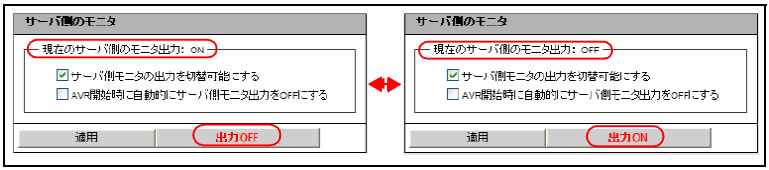


図 188: 「ビデオリダイレクション（AVR）」ページ - サーバ側のモニタの出力 ON/OFF

– AVR セッションが開始されたときに、AVR セッション中にサーバ側モニタの電源を自動的にオフにするように設定することもできます（「*AVR 開始時に自動的にサーバ側モニタ出力を OFF にする*」オプションを参照）。

サーバ側モニタオフが有効な同時セッションがない場合、AVR セッションが終了すると、サーバ側モニタの電源が自動的にオンになります。

AVR 開始時に自動的にサーバ側モニタ出力を OFF にする

このオプションは、「*サーバ側モニタの出力を切り替え可能にする*」が有効な場合のみ、有効になります。

このオプションを有効にした場合、サーバ側モニタの電源は、AVR セッションが開始されるとセッション中に自動的にオフになります。AVR セッションが終了し、サーバ側モニタオフが有効なセッションがない場合、サーバ側モニタの電源は自動的にオンになります。

同時 AVR セッション:

AVR セッション中にサーバ側モニタの電源をオンにしても（AVR メニューの「*拡張機能*」または「*出力 ON*」ボタンを使用）、新しい同時 AVR セッションが開始されると、サーバ側モニタの電源は再び自動的にオフになります。
サーバ側モニタの電源は、AVR セッションが終了すると自動的にオンになります。

► 「*適用*」ボタンをクリックして、設定を有効にします。

ビデオリダイレクション - AVR の開始

「*ビデオリダイレクションの開始*」を使用して AVR を開始します。

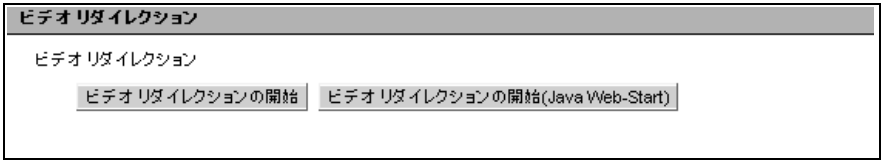


図 189: 「ビデオリダイレクション（AVR）」ページ - サーバ側のモニタ

- 再度「*ビデオリダイレクションの開始*」または「*ビデオリダイレクションの開始（Java Web-Start）*」ボタンをクリックして、2 つ目の AVR セッションを開始します。

  ビデオリダイレクションのための Java アプレットが開始されます。

  Java アプレットは、別のユーザがすでにフルコントロールモードで AVR を使用している場合、AVR 画面をビューモードで表示します。そうでない場合、Java アプレットは AVR 画面をフルコントロールモードで表示します。

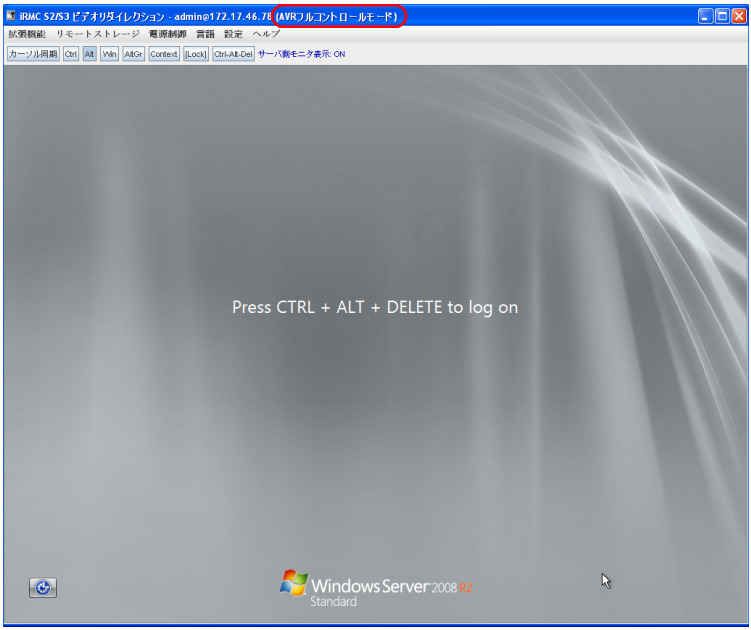


図 190: AVR 画面（ビューモード）

- AVR メニューで *「拡張機能」- 「AVR フルコントロールモード」*（詳細は 107 ページを参照）を選択し、管理対象サーバのフルコントロールを引き継ぎます。

  AVR を使用して管理対象サーバのフルコントロールを取得しようとすると、既に存在しているフルコントロールセッションがダイアログで通知されます。

  フルコントロールセッションによって、フルコントロールの取得が拒否される場合、セッションはビューモードのままになります。ユーザは、セッションでどのモードを利用するのかについて、ユーザ間で同意する必要があります。

  フルコントロールの取得に成功すると、AVR を使用するための画面が表示されるので、管理対象サーバにログインできます（312 ページ の 図 191 を参照）。

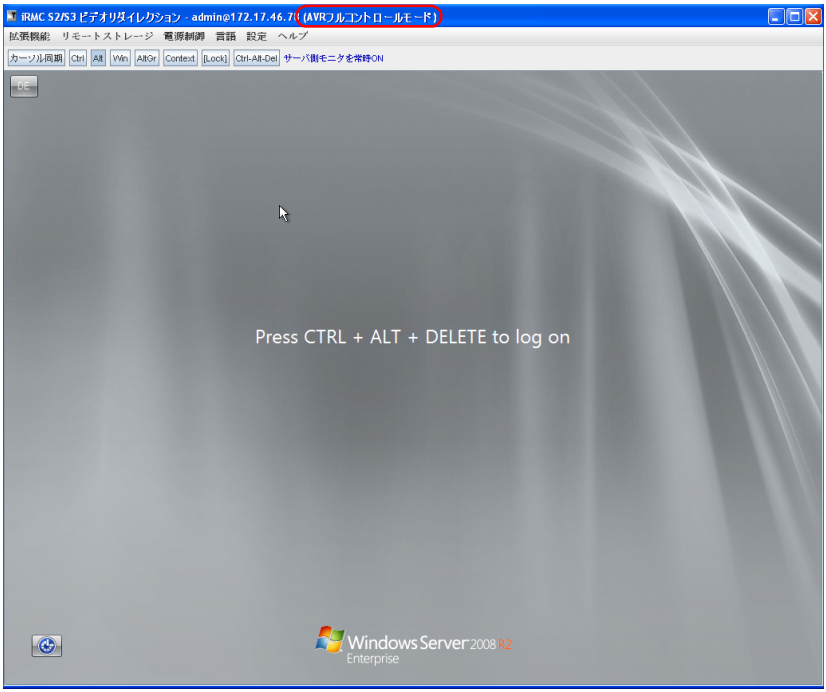


図 191: AVR 画面（フルコントロールモード）

AVR 画面のメニューと統合される特殊キーについては、87 ページ の「ビデオリダイレクション（AVR）」の章を参照してください。

2 つの有効な AVR セッションは、「*ビデオリダイレクション（AVR）*」ページで次のように表示されます。

図 192: 2 つの AVR セッションが有効な場合の AVR 画面

切断

「*切断*」ボタンをクリックすると、確認ダイアログが表示され、左側のボタンで、AVR セッションを閉じることができます。

「*切断*」ボタンでは、他のユーザの AVR セッションを閉じることができます。ユーザ固有のセッションを閉じるには、「*拡張機能*」メニューか ら、「*Exit*」ボタンを使用します（105 ページを参照）。

管理サーバの電源がオフの場合は次の画面が表示されます。

図 193: 管理サーバの電源がオフの場合の AVR 画面

7.16 リモートストレージ

「リモートストレージ」機能によって、物理的にネットワーク内の任意の場所に存在できる、仮想ドライブ（フロッピードライブまたは CD ROM）を管理対象サーバで使用できるようになります。仮想ドライブとして、物理ドライブ（フロッピーディスクドライブあるいは CD-ROM/DVD-ROM）あるいは ISO イメージ（イメージファイル）を使用することができます。

iRMC S2/S3 の「*リモートストレージ*」を使用するには、ライセンスキーが必要です（171 ページを参照）。

リモートストレージメディアとして、以下のメディアを使用できます。

– リモートワークステーション上の物理ドライブあるいはイメージファイル（115 ページを参照）。イメージファイルはネットワークドライブ（たとえば、D ドライブの場合「D:」ドライブ文字を使用）でも構いません。

– リモートストレージサーバ経由のネットワーク上のイメージファイル（130 ページを参照）。

リモートストレージ同時接続：

以下の同時接続が可能です。

– **最大 2 つ**までのリモートストレージをリモートワークステーション末の仮想ドライブとして接続できます（AVR Java アプレットを使用して接続を確立した場合）。

または

– **1 つの**リモートストレージをリモートストレージサーバに接続できます。

Java アプレットを使用したリモートストレージ接続と、リモートストレージサーバは、同時に使用できません。

「*リモートストレージ*」ページを使用して、現在のリモートストレージ接続の状態に関する情報を表示したり、リモートストレージサーバへの接続を確立することができます。

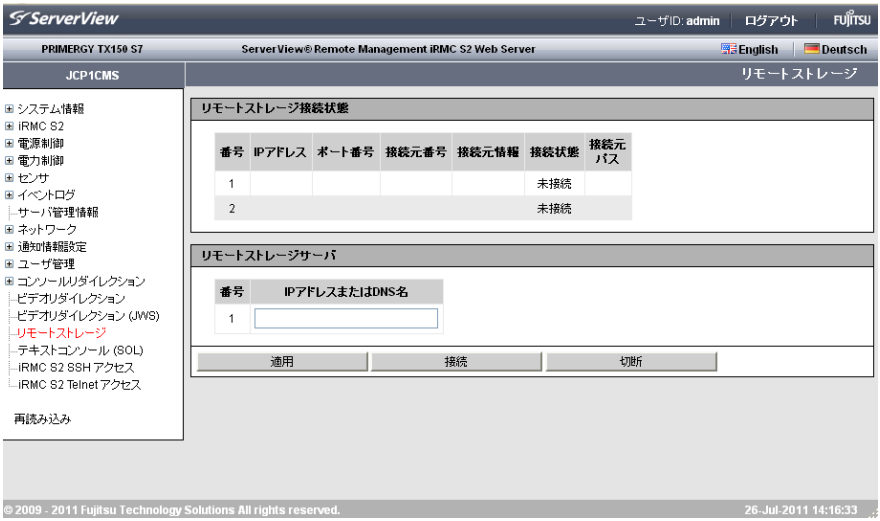


図 194: 「リモートストレージ」ページ

リモートストレージ接続状態

リモートストレージの接続状態を表示します。

番号
: リモートストレージデバイスの連番を表示します。

IP アドレス
: リモートストレージデバイスが接続されているサーバまたはワークステーションの IP アドレスが表示されます

ポート番号
: リモートストレージデバイスが接続されているサーバまたはワークステーションの IP アドレスが表示されます。

接続元番号
: リモートストレージ接続に割り当てられる番号が表示されます。

接続元情報
: サーバまたはリモートワークステーションのリモートストレージデバイスの状態が表示されます。

- *接続可能*：接続可能
- *認証を行わない*：接続不可（検出できません）

接続状態

接続の現在の状態が表示されます。

- *接続状態* : 接続中
- *未接続* : 未接続

リモートストレージサーバ

リモートストレージサーバをインストールするコンピュータを指定できます。

番号

リモートストレージサーバの連番を表示します。

IP アドレスまたは DNS 名

リモートストレージサーバがインストールされたコンピュータの IP アドレスあるいは DNS 名を入力します。

適用

「*適用*」ボタンをクリックして、リモートストレージサーバの IP アドレスまたは DNS 名を保存します。

接続

「*適用*」ボタンをクリックして、リモートストレージサーバの IP アドレスまたは DNS 名を保存し、リモートストレージサーバへの接続を確立します。

リモートストレージサーバとの接続を行う前に、リモートストレージサーバをインストールして実行させておく必要があります。

切断

「*切断*」ボタンをクリックすると、リモートストレージサーバへの接続を切断します。

7.17 Telnet/SSH（リモートマネージャ）を使用した iRMC S2/S3 の操作

iRMC S2/S3 では、Telnet/SSH ベースのインターフェースを使用できます。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。テキストコンソールのリダイレクションおよび SMASH CLP シェルを開始することもできます。

リモートマネージャは、次の手順で iRMC S2/S3 Web インターフェースから呼び出すことができます。

– 「*iRMC S2/S3 SSH アクセス*」リンクを使用して、iRMC S2/S3 への SSH（**S**ecure **Sh**ell）暗号化 Telnet 接続を開始します。

– 「*iRMC S2/S3 Telnet アクセス*」リンクを使用して、iRMC S2/S3 への 非暗号化 Telnet 接続を開始します。

iRMC S2/S3 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 Java アプレットが自動的に開始され、Telnet/SSH クライアントが実装されます。Java アプレットを使用したリモートマネージャへの Telnet/SSH アクセスは、便宜上提供されます（たとえば Windows OS には SSH クライアントは付属しません）。ただし、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 アプレットを使用して SSH 接続を確立する場合は、公開鍵認証はサポートされません。

同時セッションの最大数：

– Telnet：最大 4
– SSH：最大 4
– Telnet および SSH の合計：最大 4

リモートマネージャを使用した iRMC S2/S3 の操作については、325 ページ の「Telnet/SSH 経由の iRMC S2/S3 (リモートマネージャ)」の章を参照してください。

管理対象サーバに関する要求

Telnet を使用する iRMC S2/S3 へのアクセスを有効にする必要があります（247 ページ の「ポート番号とネットワークサービス - ポート番号とネットワークサービ スの設定」を参照）。

パスワードはプレーンテキストで送信されるので、Telnet プロトコルを使用したアクセスはデフォルトでは無効です。

SSH/Telnet 接続の確立およびリモートマネージャへのログイン

SSH と Telnet 接続の画面の違いは、各接続固有の情報が表示されるか否かです。SSH 接続の画面は下のように表示されます。

- ナビゲーションバーの「*iRMC S2/S3 SSH アクセス*」（SSH）または「*iRMC S2/S3 Telnet アクセス*」（Telnet）のリンクをクリックします。

  SSH あるいは Telnet 接続の Java アプレットが開始され、次の画面が表示されます（ここでは、SSH 接続の例を示します）。

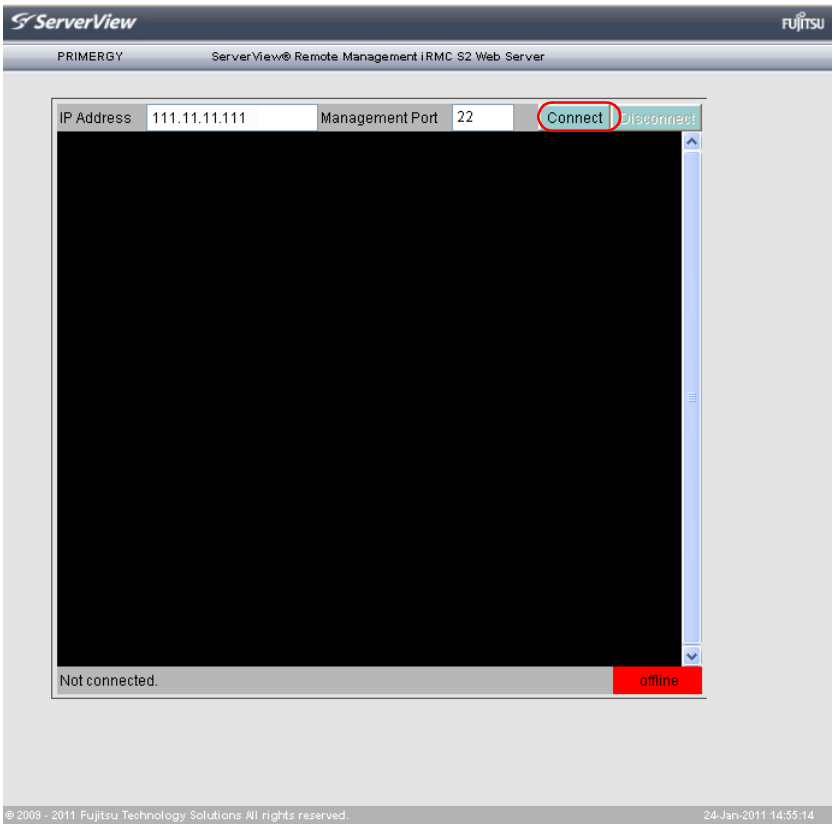


図 195: iRMC S2/S3 への SSH 接続の確立

► 接続バーの「*Connect*」ボタンをクリックします。

iRMC S2/S3 への接続が確立するとすぐに、ユーザ名とパスワードの入力が要求されます。

– *「Logging into the Remote Manager over an SSH connection」*

管理対象サーバのホストキーがまだリモートワークステーションに登録されていない場合は、SSH クライアントによってセキュリティ警告と、手順に関する指示が表示されます。

次のログイン画面が表示されます。

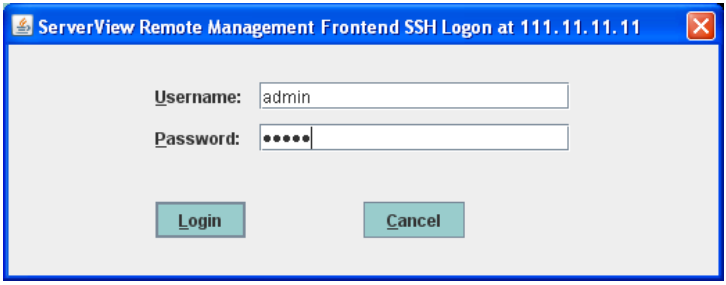


図 196: SSH 接続：リモートマネージャへのログイン

► ユーザ名とパスワードを入力し、「*Login*」ボタンをクリックして入力を確定します。

これにより、リモートマネージャのメインメニューが表示されます（323 ページ の図 198 を参照）。

– 「*Logging into the Remote Manager over a Telnet connection*」

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。

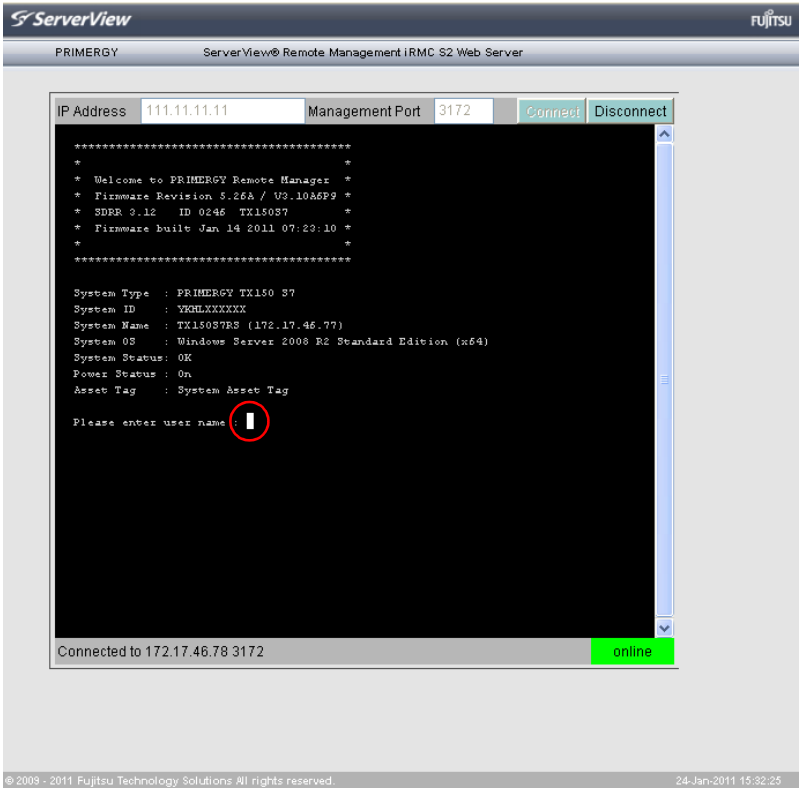


図 197: Telnet 接続：リモートマネージャへのログイン

ログインの時点で ServerView エージェントがすでにシステム上で動作しているかいないかによって、ログインウィンドウにシステム情報が表示されるか否かが異なります（329 ページを参照）。

► ユーザ名およびパスワードを入力し、Enter キーを押して、入力を確定してください。

これにより、リモートマネージャのメインメニューが表示されます（323 ページ の図 198 を参照）。

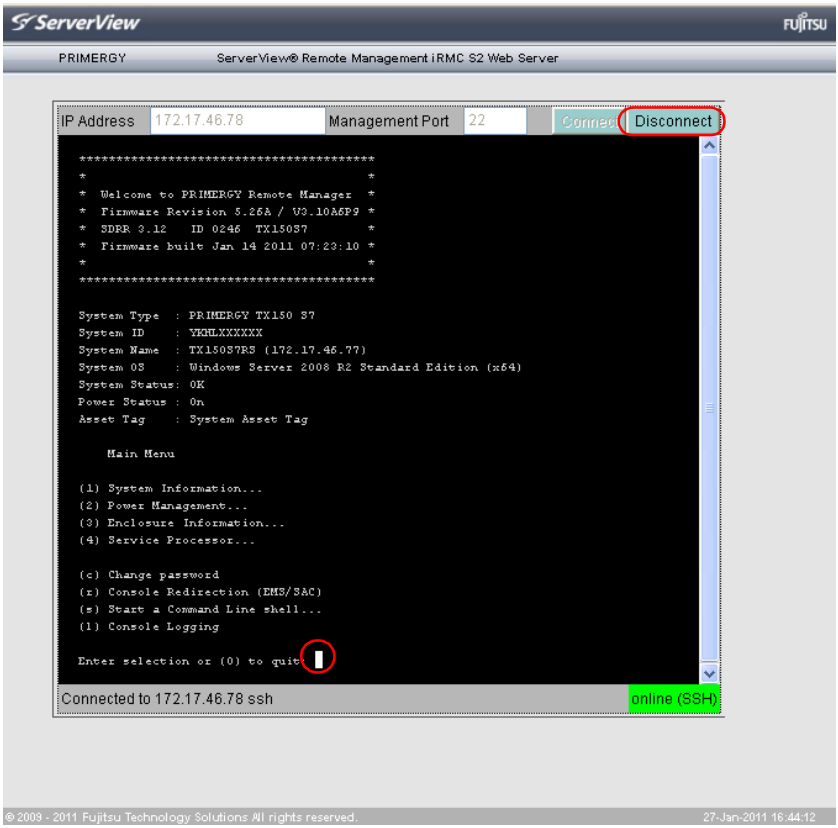


図 198: リモートマネージャのメインメニュー

Telnet/SSH 接続の切断

- リモートマネージャへの接続を切断するには、リモートマネージャ画面の の接続バーの「*Disconnect*」ボタンをクリックするか、リモートマネージャのメインメニューで 0 キーを押します（図 198 を参照）。

8 Telnet/SSH 経由の iRMC S2/S3 (リモートマネージャ)

iRMC S2/S3 では Telnet ベースのインターフェースを使用できます。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。次のインターフェースでリモートマネージャを呼び出すことができます。

– iRMC S2/S3 Web インターフェース（318 ページを参照）。
– 任意の Telnet/SSH クライアント

iRMC S2/S3 は SSH（**S**ecure **Sh**ell）によるセキュア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。原則として、VT100 シーケンスを解釈する Telnet/SSH クライアントであれば、iRMC S2/S3 へのアクセスに使用できます。ただし、iRMC S2/S3 Web インターフェースまたは ServerView Remote Management Frontend（以下では単に Remote Management Frontend と呼ぶ）の使用を推奨します。

最大パラレルセッション数

– Telnet: 最大 4
– SSH: 最大 4
– Telnet と SSH の合計 : 最大 4

管理対象サーバに関する要求条件

Telnet 経由のアクセスを iRMC S2/S3 に対して有効にする必要があります（247 ページ の「ポート番号とネットワークサービス - ポート番号とネットワークサービ スの設定」の項を参照）。

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。

ServerView Operations Manager(SVOM) ではマネジメントポートの有効／無効が認識されないため、Remote Management Frontend はデフォルト値で動作します

Remote Management Frontend が起動したときに自動的に接続は確立されないので、Remote Management Frontend が起動した後にマネジメントポートの標準以外の値を変更できます。

8.1 リモートマネージャ

この項では、リモートマネージャからの iRMC S2/S3 の操作および各種機能の詳細を説明します。末尾には、SMASH CLP の概要も示します。

8.1.1 リモートマネージャの操作

リモートビューの操作を図 199 の例に基づいて説明します。この図では、リモートマネージャのメインメニューの一部を示しています。

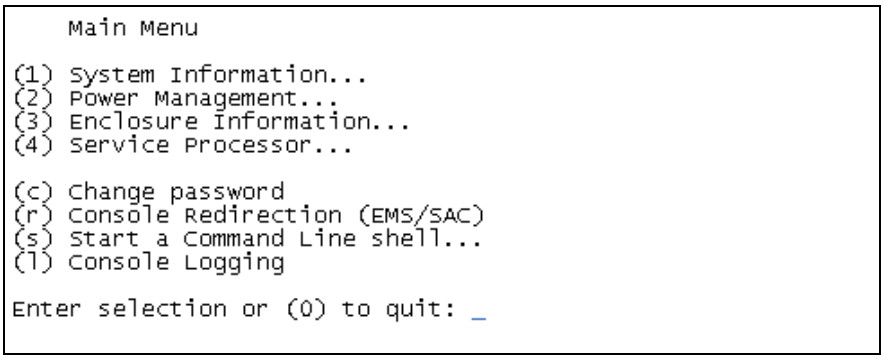


図 199: リモートマネージャの操作

- メニュー項目の先頭の文字または数字を入力して、必要なメニューを選択します。たとえば、「パスワードの変更（Change password）」の場合は「c」と入力します。

  ユーザーが使用を許されていないファンクションはハイフン (-) で、また提供されていないファンクションはアスタリスク (*) で指示してあります。

- 0 またはキーの組み合わせ Ctrl D を押してリモートマネージャを終了します。該当するイベントがイベントログに書き込まれます。

8.1.2 メニューの概要

iRMC S2/S3 のリモートマネージャメニューは、次の構造になっています。

- **System Information**
  - View Chassis Information
  - View Mainboard Information
  - View OS and SNMP Information
  - Set ASSET Tag
- **Power Management**
  - Immediate Power Off
  - Immediate Reset
  - Power Cycle
  - Power On
  - Graceful Power Off (Shutdown)
  - Graceful Reset (Reboot)
  - Raise NMI (via iRMC S2/S3)
- **Enclosure Information**
  - System Eventlog
    - View System Eventlog (text, newest first)
      システムイベントログの表示 (テキスト表示、昇順)
    - View System Eventlog (text, oldest first)
      システムイベントログの表示 (テキスト表示、降順)
    - Dump System Eventlog (raw, newest first)
      イベントログのダンプ (元データ、昇順)
    - Dump System Eventlog (raw, oldest first)
      イベントログのダンプ (元データ、降順)
    - View System Eventlog Information
      システムイベントログ情報の表示
    - Clear System Eventlog
      システムイベントログの消去

  - Internal Eventlog
    - View Internal Eventlog (text, newest last)
    - Dump Internal Eventlog (raw, newest last)
    - View Internal Eventlog Information
    - Clear Internal Eventlog
    - Change Internal Eventlog mode
  - Temperature
  - Voltages/Current
  - Fans
  - Power Supplies
  - Memory Sensor
  - Door Lock
  - CPU Sensors
  - Component Status (Lightpath)
  - List All sensors
- **Service Processor**
  - Configure IP Parameters
  - List IP Parameters (IP パラメータのリスト)
  - Toggle Identify LED
  - Reset iRMC S2/S3 (Warm reset)
  - Reset iRMC S2/S3 (Cold reset)
- **Change password**
- **Console Redirection (EMS/SAC)**
- **Start a Command Line shell**
- **Console Logging**

8.1.3 ログイン

iRMC S2/S3 に接続する際、ログイン資格情報（ユーザー名とパスワード）の入力が必要です。iRMC S2/S3 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）がリモートワークステーションのターミナルクライアントに表示されます。

ServerView エージェントが OS システム上にインストールされ、かつ起動しているか否かで、ログインウィンドウでのシステム情報表示の有無が変わります。

SSH 接続でログインした場合 : 管理対象サーバのホストキーがリモートワークステーションにまだ登録されていない場合、SSH クライアントはセキュリティ警告を発行し、推奨する続行方法を示します。

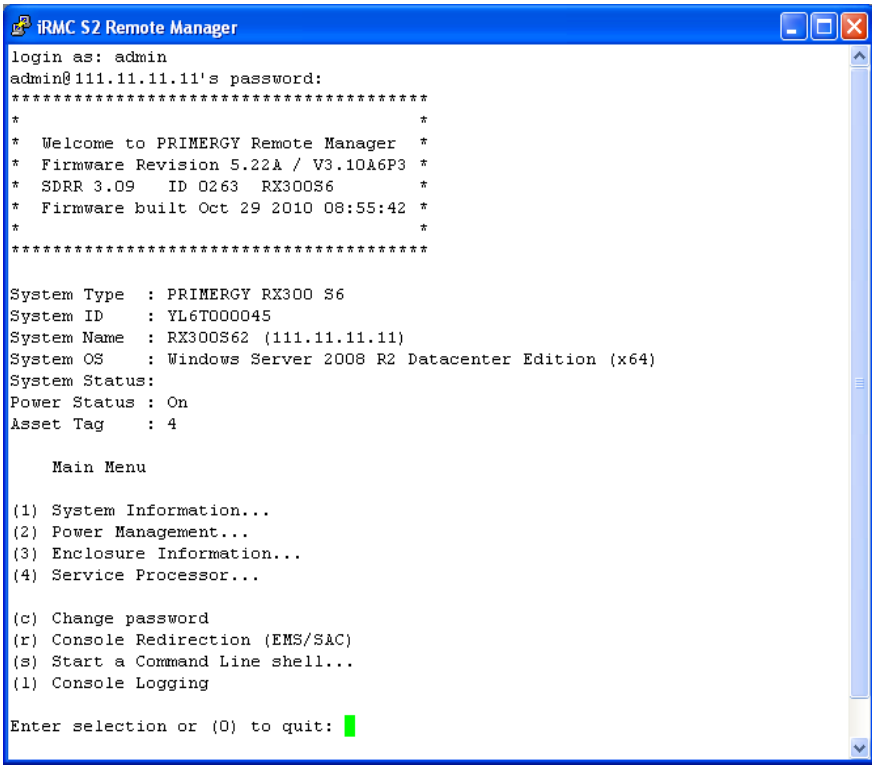


図 200: リモートマネージャ : メインメニューウィンドウ（システム情報付き）

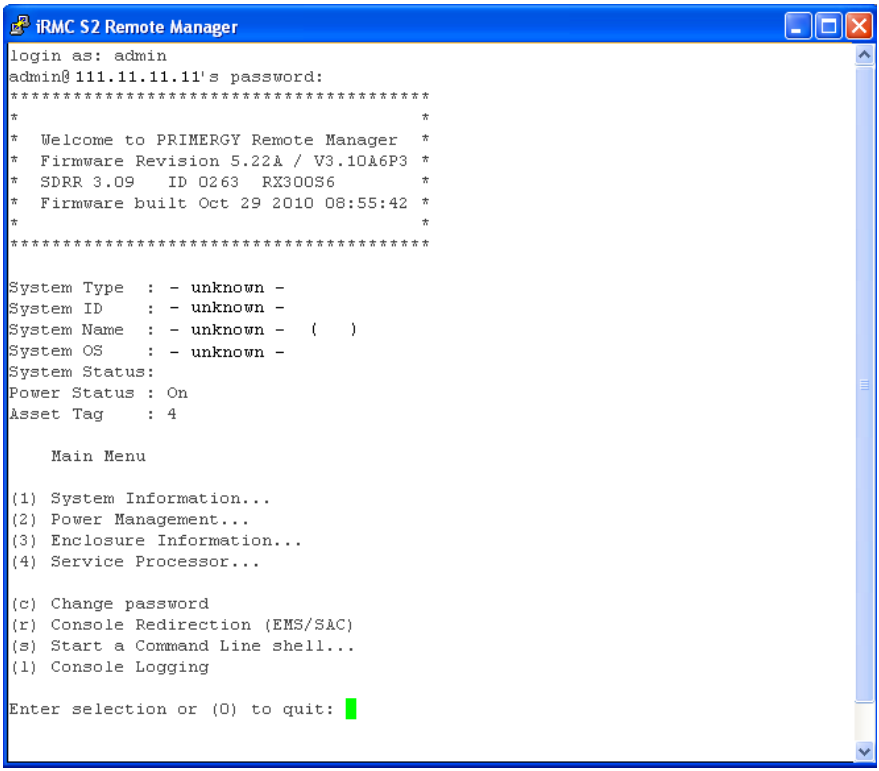


図 201: リモートマネージャ : メインメニューウィンドウ（システム情報なし）

リモートマネージャウィンドウには、対象のシステムに関する情報が表示されます。サーバの個別情報、および稼動状態 (電源状態) が表示されます。個別情報については詳細情報 (システム名など) のみ、かつ、サーバに適切に設定されている場合に限り表示されます。

- ▶ リモートマネージャを使用するには、ユーザー名とパスワードでログインする必要があります。

  ログインを行うと、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メインメニューが表示されます (331 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 を使用していつでも終了できます。

8.1.4 リモートマネージャのメインメニュー

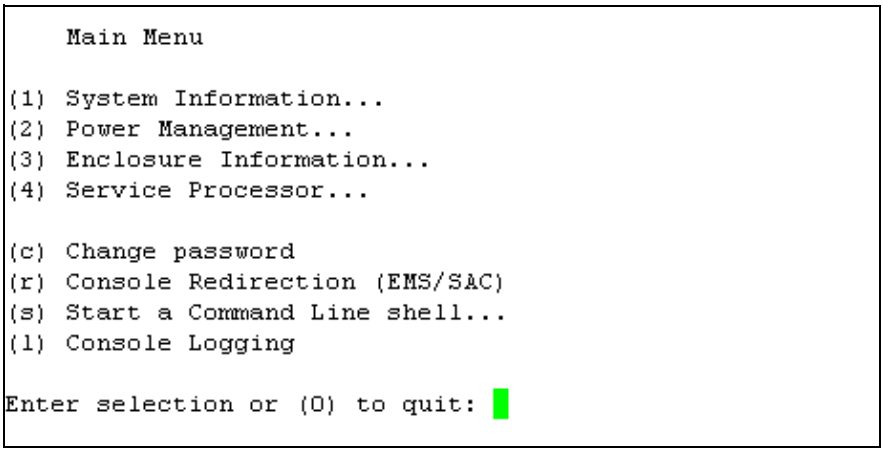


図 202: リモートマネージャ : メインメニュー

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あります。

「*System Information...*」	管理対象サーバの情報を表示し、資産タグを設定します (335 ページ の「システム情報 - 管理対象サーバの情報」の項を参照)。
「*Power Management...*」	サーバの電源をオン / オフします (336 ページ の「Power Management」の項を参照)。
「*Enclosure Information...* 」	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。 (337 ページ の「Enclosure Information - システムイベントログとセンサの状態」の項を参照)。

表 8: リモートマネージャのメインメニュー

「*Service Processor...* 」	iRMC S2/S3 を設定します（ファームウェアの更新または IP アドレスの変更など） (341 ページ の「サービスプロセッサ - IP パラメータ、識別灯、iRMC S2/S3 リセット」の項を参照)。
「*Change password* 」	パスワードの変更 (335 ページ の「パスワードの変更」の項を参照)。
「*Console Redirection (EMS/SAC)* 」	テキストコンソールリダイレクション (342 ページ の「Console Redirection (EMS/SAC) - テキストコンソールリダイレクションの開始」の項を参照)。
「*Start a Command Line shell...* 」	コマンドラインシェルの起動 (343 ページ の「コマンドラインシェルの起動 ... - SMASH CLP シェルの起動」の項を参照)。
「*Console Logging* 」	メッセージ出力をテキストコンソールにリダイレクトします (344 ページ の「Console Logging - メッセージ出力のテキストコンソールへの出力（シリアル）」の項を参照)。

表 8: リモートマネージャのメインメニュー

8.1.5 必要なユーザー許可

表 9 に、リモートマネージャの個々の機能を使用するために必要なユーザ権限の概要を示します。

リモートマネージャのメニュー項目	IPMI レベルで許可				必要な許可			
	OEM	Administrator	Operator	User	ユーザーアカウントの設定	iRMC S2/S3 設定変更権限	AVR 使用権限	リモートストレージ使用権限
View *System Information...*	X	X	X	X				
View *Chassis / Mainboard, / OS Information*						X		
Set ASSET Tag [1)]						X		
Set System Name [1)]						X		
Set System Operating System Information [1)]						X		
Set System Description [1)]						X		
Set System Location Information (SNMP) [1)]						X		
Set System Contact Information (SNMP) [1)]						X		
Power Management...	X	X	X					
View *Enclosure Information*	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					
Internal Eventlog - View/Dump Internal Eventlog	X	X	X	X				
Internal Eventlog - Clear Internal Eventlog	X	X	X	X				
Sensor overviews (システム概要 (温度、ファン ...))	X	X	X	X				
View *Service Processor...*	X	X	X	X				

表 9: リモートマネージャのメニューを使う許可

リモートマネージャのメニュー項目	IPMI レベルで許可				必要な許可			
	OEM	Administrator	Operator	User	ユーザーアカウントの設定	iRMC S2/S3 設定変更権限	AVR 使用権限	リモートストレージ使用権限
Service Processor... - *List IP Parameters*						X		
Service Processor... - *Configure IP Parameters*						X		
Service Processor... - *Toggle Identify LED*	X	X	X	X				
Service Processor... - *Reset iRMC S2 (warm/cold reset)*	X	X						
Change Password					X			
Console Redirection (EMS/SAC)	X	X	X					
Start a command Line shell... (コマンドラインシェルの起動)	X	X	X	X				
Console Logging	X	X	X					

[1] アクションは、エージェントが実行されていない場合にのみ可能です。

表 9: リモートマネージャのメニューを使う許可

8.1.6 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、「ユーザアカウントの変更権限」を持つユーザー (68 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。

8.1.7 システム情報 - 管理対象サーバの情報

メインメニューから 「*System Information...*」を選ぶと、次のメニューが表示されます。

```
    System Information Menu

(1) View Chassis Information
(2) View Mainboard Information
(3) View OS and SNMP Information

(4) Set ASSET Tag
(*) Set System Name
(*) Set System Operating System Information
(*) Set System Description
(*) Set System Location Information (SNMP)
(*) Set System Contact Information (SNMP)

Enter selection or (0) to quit:
```

図 203: リモートマネージャ : 「System Information...」メニュー

サブメニューには次のファンクションがあります。

「*View Chassis Information*」	管理対象サーバのシャーシと設定値情報。
「*View Mainboard Information*」	管理対象サーバのメインボードと設定値情報。
「*View OS and SNMP Information*」	管理対象サーバの OS、ServerView エージェント Information」バージョンの情報と、SNMP 設定情報。
「*Set ASSET Tag*」	管理対象サーバのカスタマ固有の資産タグを設定します。

表 10: システム情報メニュー

8.1.8 Power Management

メインメニューから「*Power Management...*」を選択すると、次のメニューが表示されます。

```
    Power Management Menu

(1) Immediate Power Off
(2) Immediate Reset
(3) Power Cycle
(*) Power On

(5) Graceful  Power Off (Shutdown)
(6) Graceful  Reset     (Reboot)
(n) Raise NMI (via iRMC S2)

Enter selection or (0) to quit:
```

図 204: リモートマネージャ :「Power Management」メニュー

サブメニューには次のファンクションがあります。

「*Immediate Power Off* 」	OS の状態に関係なく、サーバの電源を強制切断します。
「*Immediate Reset* 」	OS の状態に関係なく、サーバを強制再起動します（コールドスタート）。
「*Power Cycle* 」	サーバの電源を強制切断切断してから、指定時間の後、電源を投入します。
「*Power On* 」	サーバの電源を投入します。
「*Graceful Power Off (Shutdown)* 」	OS をシャットダウンして、電源を切断します。 このメニュー項目は、ServerView エージェントが OS にインストールされ、iRMC S2/S3 がその動作を認識している場合にのみ使用できます。
「*Graceful Reset (Reboot)* 」	OS をシャットダウンして、再起動します。 このメニュー項目は、ServerView エージェントが OS にインストールされ、iRMC S2/S3 がその動作を認識している場合にのみ使用できます。
「*Raise NMI (via iRMC S2/S3)*」	NMI（マスク不可能な割り込み）を iRMC S2/S3 経由で発行します。

表 11:「Power Management」メニュー

8.1.9 Enclosure Information - システムイベントログとセンサの状態

メインメニューから「*Enclosure Information...*」を選ぶと、次のメニューが表示されます。

```
    Enclosure Information Menu

(e) System Eventlog
(i) Internal Eventlog
(t) Temperature
(v) Voltages/Current
(f) Fans
(p) Power Supplies
(d) Door Lock
(m) Memory Sensors
(c) CPU Sensors
(s) Component Status
(l) List All Sensors

Enter selection or (0) to quit:
```

図 205: リモートマネージャ：「Enclosure Information」メニュー

サブメニューには次のファンクションがあります。

「*System Eventlog*」	「*System Eventlog*」メニューを呼び出します (339 ページ の「System Eventlog」の項を参照)。
「*Internal Eventlog*」	「*internal Eventlog*」メニューを呼び出します (340 ページ の「Internal Eventlog」の項を参照)。
「*Temperature*」	温度センサとその状態に関する情報を表示します。
「*Voltages/Current*」	電圧と電流センサ、およびその状態の情報を表示します。
「*Fans*」	ファンとセンサとその状態に関する情報を表示します。
「*Power Supplies*」	電源と冗長の状態の情報を表示します。
「*Door Lock*」	フロントパネルまたはハウジングが開いているかどうかを表示します。
「*Memory Sensors*」	メモリの状態に関する情報を表示します。
「*CPU Sensors*」	サーバの CPU の状態を表示します。
「*Component Status*」	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。
「*List All Sensors*」	すべてのセンサの詳細な情報を表示します。

表 12: 「Enclosure Information」メニュー

System Eventlog

「*Enclosure Information...*」サブメニューから「*System Eventlog*」を選択すると、次のメニューが表示されます。

```
    System Eventlog Menu

(1) View System Eventlog (text, newest first)
(2) View System Eventlog (text, oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)

(5) View System Eventlog Information
(6) Clear System Eventlog

Enter selection or (0) to quit:
```

図 206: リモートマネージャ：「System Eventlog」メニュー

サブメニューには次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内容がテキストに変換され、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内容がテキストに変換され、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)*」	システムイベントログの内容が時期の新しいものから順にデータのまま画面に出力されます。
「*Dump System Eventlog (raw, oldest first)*」	システムイベントログの内容が時期の古いもの から順にデータのまま画面に出力されます。
「*View System Eventlog Information*」	システムイベントログの情報を表示します。
「*Clear System Eventlog*」	システムイベントログの内容を消去します。
「*Change System Eventlog mode*」	システムイベントログのバッファモードを *Ring Buffer* モードから *Linear Buffer* モードに、またはこの逆に変更します。

表 13: 「System Eventlog」のメニュー

Internal Eventlog

「*Enclosure Information...*」サブメニューから「*Internal Eventlog*」を選択すると、次のメニューが表示されます。

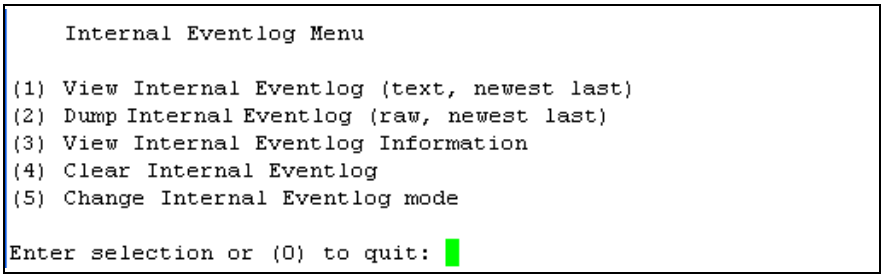


図 207: リモートマネージャ : 「Internal Eventlog」メニュー

サブメニューには次のファンクションがあります。

「*View Internal Eventlog (text, newest last)*」	内部イベントログの内容がテキストに変換され、時期の新しいものから順に画面に出力されます。
「*Dump Internal Eventlog (raw, newest last)*」	内部イベントログの内容が時期の新しいものから順にデータのまま画面に出力されます。
「*View Internal Eventlog Information*」	内部イベントログの情報を表示します。
「*Clear Internal Eventlog*」	内部イベントログの内容を消去します。
「*Change Internal Eventlog mode*」	内部イベントログのバッファモードを リング バッファモードまたは リニアバッファモードに切替えます。

表 14: 「Internal Eventlog」メニュー

8.1.10 サービスプロセッサ - IP パラメータ、識別灯、iRMC S2/S3 リセット

メインメニューから「*Service Processor...*」を選択すると、次のメニューが表示されます。

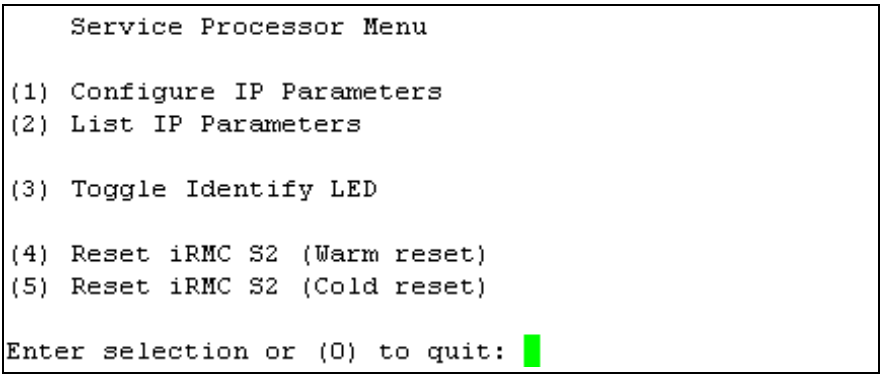


図 208: リモートマネージャ：「Service Processor」メニュー

サブメニューには次のファンクションがあります。

「*Configure IP Parameters*」	iRMC S2/S3 の IPv4 / IPv6 アドレス設定をガイド付きダイアログで設定します。個々の設定の詳細は、241 ページ の「ネットワークインターフェース設定 - iRMC S2/S3 のイーサネット設定」の項を参照してください。
「*List IP Parameters* 」	IP パラメータを表示します。
「*Toggle Identify LED*」	PRIMERGY の識別灯のオン / オフを切り替えます。
「*Reset iRMC S2/S3 (Warm reset)*」	iRMC S2/S3 をリセットします。接続は切断されます。 インターフェースだけが再初期化されます。
「*Reset iRMC S2/S3 (Cold reset)*」	iRMC S2/S3 をリセットします。接続は切断されます。 iRMC S2/S3 全体が再初期化されます。

表 15: 「Service Processor」のメニュー

「*Reset iRMC S2/S3 (Cold Reset)*」または「*Reset iRMC S2/S3 (Warm Reset)*」の後にサーバを再起動することを推奨します（192 ページを参照）。

8.1.11 Console Redirection (EMS/SAC) - テキストコンソールリダイレクションの開始

メインメニューの「*Console Redirection (EMS/SAC)*」項目からコンソールリダイレクションを開始できます。

テキストベースのコンソールリダイレクションは、シリアル 1 の LAN 上でのみ動作します。

コンソールリダイレクションを OS の実行中にも使用する場合は、「*Serial 1 Multiplexer*」を「*System*」に設定する必要があります。

キーボードショートカット "<ESC>(" または "~."（チルダ + ドット）を使用して、テキストコンソールを終了します。

使用する PRIMERGY サーバのタイプによっては、このオプションのうちの 1 つだけが機能します。

8.1.12 コマンドラインシェルの起動 ... - SMASH CLP シェルの起動

メインメニューの「*Start a Command Line shell...* 」で、SMASH CLP シェルを開始できます。SMASH CLP は、「**S**ystems **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol」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、346 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。

```
    Shell Menu

(1) Start SMASH CLP shell...


Enter selection or (0) to quit:
```

図 209: リモートマネージャ：「Start a SMASH CLP shell... 」メニュー

- *(1) Start a SMASH CLP shell...* を選ぶと、SMASH CLP シェルが起動します。

8.1.13 Console Logging - メッセージ出力のテキストコンソールへの出力（シリアル）

メインメニューの「*Console Logging*」項目では、メッセージ出力（ログ）をテキストコンソールにリダイレクトできます（シリアルインターフェース）。

メインメニューから「*(l) Console Logging*」を選択すると、次のウィンドウが表示されます。

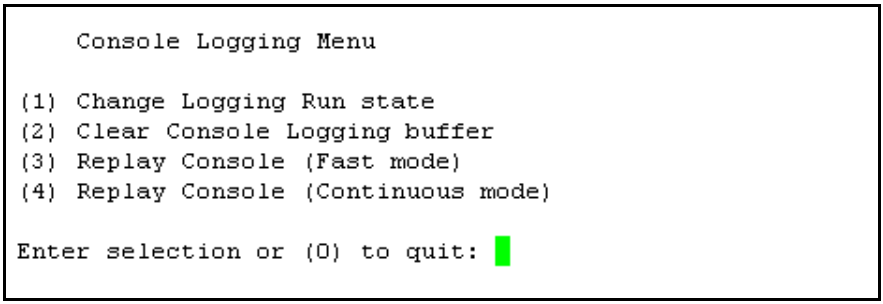


図 210: リモートマネージャ：「Console Logging」メニュー

サブメニューには次のファンクションがあります。

「*Change Logging Run state*」	ログ実行状態を表示し、変更します。詳細は、345 ページ の「「Console Logging Run State」メニュー」を参照してください。
「*Clear Console Logging buffer*」	コンソールログバッファをクリアします。
「*Replay Console (Fast mode)*」	コンソールログを表示します（高速モード）。
「*Replay Console (Continuous mode)*」	コンソールログを表示します（連続モード）。

表 16: 「Console Logging」メニュー

「Console Logging Run State」メニュー

```
    Console Logging Run State Menu
    State: STOPPED (Normal Mode)

(r) Start Console Logging
(*) Stop Console Logging

(t) Toggle to Text Mode
(*) Toggle to Normal Mode

Enter selection or (0) to quit:
```

図 211: リモートマネージャ：「Console Logging Run State」メニュー

「*Console Logging Run State Menu*」には次の機能があります。

「*Start Console Logging*」	メッセージのテキストコンソールへの出力を開始します。
「*Stop Console Logging*」	メッセージのテキストコンソールへの出力を停止します。
「*Toggle to Text Mode*」	テキストモードに切り替えます。 メッセージがコンソールに出力される前に、すべてのエスケープシーケンスは除外されます。
「*Toggle to Normal Mode*」	ノーマルモードに切り替えます。 ノーマルモードでは、メッセージがコンソールに出力される前に、次のエスケープシーケンスのみが除外されます。 <ESC>(<ESC>stop <ESC>Q <ESC>R<ESC>r<ESC>R <ESC>^ これは、色、擬似グラフィックスなどを一定の限度まで表現できることを示します。

表 17: 「Console Logging Run State」メニュー

8.1.14 コマンドラインプロトコル (CLP)

iRMC S2/S3 はユーザーシェルと呼ばれるさまざま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、これらは各ユーザー向けに設定できます。

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。

– 異なる (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 に関する詳細情報は、DMTF ドキュメント『Server Management Command Line Protocol Specification (SM CLP) DSP0214』で参照できます。

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*)。

iRMC S2/S3 システムでは、*oemfujitsu* という verb 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、<verb> 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上で <verb> 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) 自体を指定することができます。またターゲットは、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> として指定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または修正される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 212 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 /verb show が、利用可能なターゲット、プロパティ、および verb を表示します。

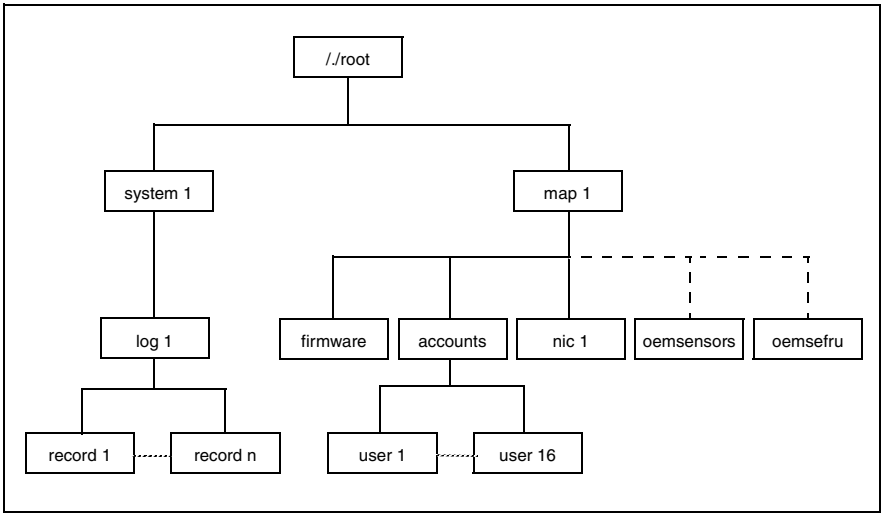


図 212: SMASH CLP 内のユーザーデータの構造

CLP コマンドの階層

CLP コマンド階層の概要を 349 ページ の表 18 に示します。

Verb / Target	Properties	Comment	cd	show	help	exit	version	set	reset	start	stop	load	oemfsc
/		Root	X	X	X	X	X						
system1													
map1													
system1	name	Host	X	X	X	X	X		System	PON	POFF		
	enabledstate	System											
...log1		Event Log (SEL)	X	X	X	X	X		iRMC				X
....record<n>	number	Single SEL entry	X	X	X	X	X		iRMC				X
	date												
	time												
	sensordescription												
	eventdescription												
	eventdirection												
map1	name	iRMC	X	X	X	X	X		iRMC				X
...firmware	version	iRMC FW	X	X	X	X	X		iRMC			X	X
...accounts		Accounts	X	X	X	X	X	X	iRMC				X
.....user<n>	username	User	X	X	X	X	X	X	iRMC				X
	password												
	group												
...nic1	networkaddress	LAN	X	X	X	X	X	X	iRMC				X
	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												
...oemfsc_sensors		OEM Sensors	X	X	X	X	X		iRMC				X
....oemfsc_sensor_num<n>lun<m>	oemfsc _reading	Single Sensor	X	X	X	X	X		iRMC				X
	oemfsc _status												
	oemfsc _sensortype												
	oemfsc _readingtype												
...oemfsc_frus		FRU	X	X	X	X	X		iRMC				X
....oemfsc_fru_devid<n>lun<m>	oemfsc _description	Single FRU	X	X	X	X	X		iRMC				X

表 18: CLP コマンドの階層

9 Server Configuration Manager を使用した iRMC S2/S3 の設定

Server Configuration Manager を使用して、次のことを実行できます。

– iRMC S2/S3 の設定

– iRMC S2/S3 でユーザー ID を設定、管理する

– iRMC S2/S3 でディレクトリサービスを設定する

– iRMC S2/S3 で CAS サービスを設定する

要件 :

管理対象サーバには最新の ServerView エージェントをインストールしておく必要があります。

次のようにして、Server Configuration Manager 機能にアクセスできます。

– ServerView Installation Manager を使用して管理対象サーバでローカルにアクセスする

– Windows のスタートメニューを使用して管理対象の Windows ベースサーバでローカルにアクセスする

  管理対象サーバに Windows 用 ServerView エージェントがインストールされているサーバでのみサポートされます

– Operations Manager のグラフィカルインターフェースを使用してリモートワークステーション上でアクセスする

  これは Windows 用 ServerView エージェントがインストールされているサーバでのみサポートされます

この章では、Server Configuration Manager を呼び出すさまざまな方法について説明します。

Configuration Manager ダイアログページの詳細は、Server Configuration Manager のオンラインヘルプを参照してください。

9.1 ServerView Installation Manager からの Server Configuration Manager の呼び出し

Server Configuration Manager は、ServerView Installation Manager（短縮して Installation Manager）から呼び出せます。サーバをインストールする際、Installation Manager からの設定が重要になります。Installation Manager によって、インストールの準備中、およびメンテナンスプログラムとして、Server Configuration Manager を使用できるようになります。Installation Manager については、『ServerView Installation Manager』マニュアルに記載されています。

9.2 Windows スタートメニューからの Server Configuration Manager の呼び出し

Windows ベースのサーバでは、Windows スタートメニューからも Server Configuration Manager を呼び出せます。

これは次の手順で行います。

- 管理対象サーバで、次のように選択します。
  スタート – すべてのプログラム – Fujitsu – ServerView – Agents – Configuration Tools – System Configuration.

  「*システム設定*」ウィンドウが開きます。

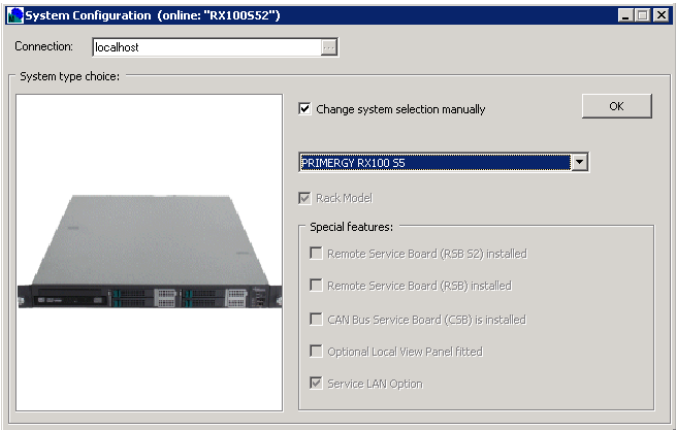


図 213: 「システム設定」ウィンドウ

► 認識している情報が表示されます。

► *OK* をクリックします。

「*システム設定*」ウィンドウのタブビューが開きます。

矢印をクリックして、左右のタブにスクロールできます。

設定の適用

個々のタブで指定した設定を適用するには、各タブで次の手順に従います。

► 「*適用*」ボタンをクリックします。

► 「*ページ保存*」ボタンをクリックします。

iRMC S2/S3 が自動的に再起動して、変更された設定が有効になります。

9.3 Operations Manager からの Server Configuration Manager の呼び出し

iRMC S2/S3 を設定する Server Configuration Manager のダイアログボックスは、Operations Manager のグラフィカルユーザーインターフェースからも使用できます。これによって、管理対象サーバの iRMC S2/S3 を Web インターフェース経由でリモートワークステーションから設定できます。

次の手順に従います。

- Operations Manager を起動します（ServerView Operations Manager のマニュアルを参照）。

  Operations Manager の開始ウィンドウが開きます。

図 214: Operations Manager: 開始ウィンドウ

► Operations Manager の開始ウィンドウの「*管理者設定*」メニューから「*サーバの設定*」を選択します。

その結果、次のウィンドウが開かれます。

図 215: Operations Manager: 「サーバの設定」- 「サーバリスト (1)」タブ

► 「*サーバリスト*」タブで、設定するタブを選択します。

その結果、次のウィンドウが開かれます。

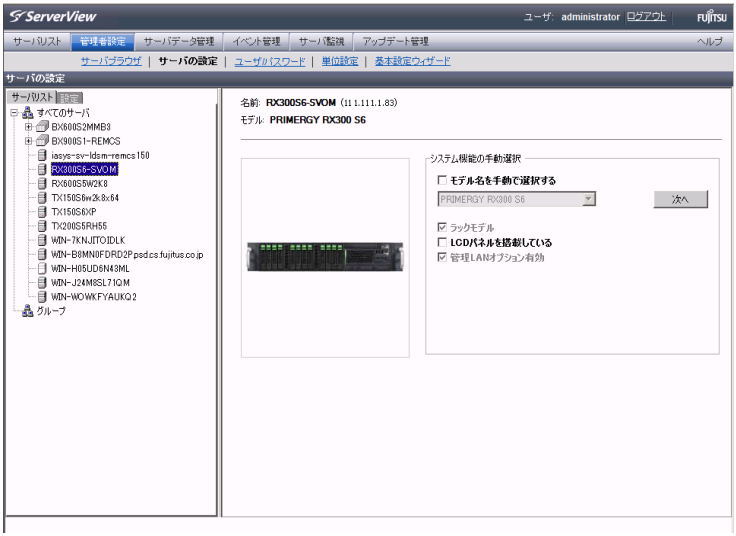


図 216: Operations Manager: 「サーバの設定」ウィンドウ - 「サーバリスト (2)」タブ

► ウィンドウの右側で、選択したサーバの詳細を指定して、「*次へ*」をクリックして入力内容を確定します。

Server Configuration Manager の最初のダイアログが表示されます。

10　ファームウェアの更新

この章では次の点について説明します。

– iRMC S2/S3 ファームウェア（概要）

– ファームウェアアップデート用メモリスティックの作成

– ファームウェアイメージのアップデート

– エマージェンシーフラッシュ

– フラッシュツール

現行バージョンのファームウェアは *ServerView Suite DVD 1* に格納されています。または 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もできます。

ServerView Suite DVD 1 の最新バージョンは 2 か月ごとに取得できます。

ファームウェアのアップデートを実行するほかに、ファームウェアを以前のバージョンにダウングレードできます。

ファームウェアをアップデートまたはダウングレードする前に、新しいファームウェアに付属の注意書き（特に Readme ファイル）をよくお読みください。

アップデートまたはダウングレードしたファームウェアを有効にするには、管理 対 象サーバを再起動する必要があります。

注意！

ファームウェアをアップデートまたはダウングレードする際、ファームウェアを正常に操作するには、ランタイムファームウェアと SDR （Sensor Data Record 、 359 ページを参照）が両方とも同じファームウェアリリースに属することを確認してください。

10.1 iRMC S2/S3 ファームウェア（概要）

iRMC S2/S3 は 2 種類の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 (低 FW イメージ)
– ファームウェアイメージ 2 (高 FW イメージ)

iRMC S2/S3 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。

ファームウェアをイメージの 1 つからロードするときにエラーが発生した場合、ファームウェアはもう 1 つのイメージから自動的にロードされます。

iRMC S2/S3 ファームウェアと EEPROM に関する情報は、次の手段で取得できます。

– iRMC S2/S3 Web インターフェースの「 *iRMC S2/S3 情報*」のページ（ 168 ページを参照）
– フラッシュツールの使用（ 372 ページを参照）

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を実行するのかは、ファームウェアセレクタで決定します (360 ページ参照) 。

iRMC S2/S3 EEPROM の構造

iRMC S2/S3 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 用の領域があります。

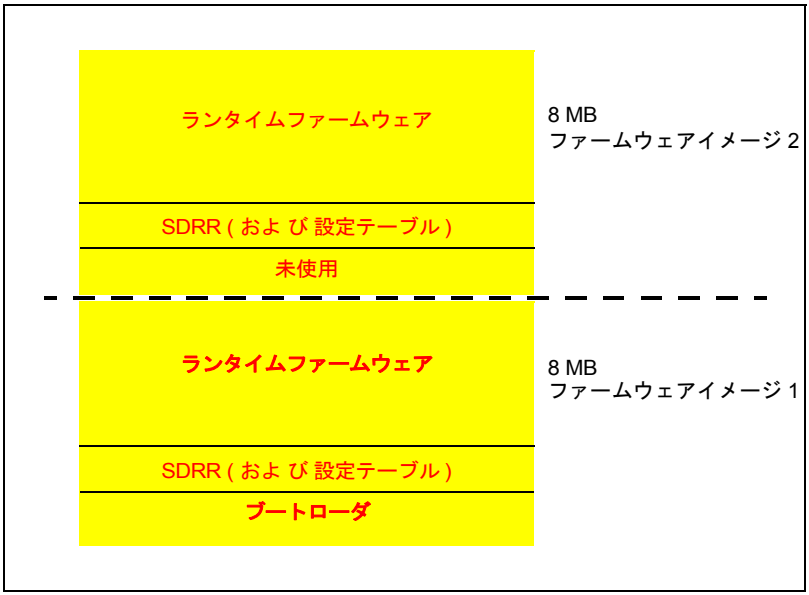


図 217: iRMC S2/S3 EEPROM の構造

– ブートローダ

  ブートローダは現在アクティブなファームウェアイメージをチェックします。ファームウェアエラーが検出されると、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 iRMC S2/S3 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 iRMC S2/S3 ファームウェアを指定します。 iRMC S2/S3 がリセットされて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ア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が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は、以下の何れかで確認できます

– iRMC S2/S3 Web インターフェースの「 *iRMC S2/S3 情報*」ページでの表示、および設定（170 ページ の「動作中ファームウェア」を参照）。

または

– フラッシュツールの使用（372 ページを参照）

10.2 USB メモリスティックでの更新準備

iRMC S2/S3 のファームウェアを次の方法でアップデートする場合は、USB メモリスティックは**不要**です。

- ServerView Update Manager を使用する
- ServerView Update Manager Express または ASP を使用する
- iRMC S2/S3 Web インターフェースと TFTP サーバを使用する

次の手順に従います。

- ファームウェア *iRMC Firmware Update for USB Stick* を Fujitsu Technology Solutions Web サーバのダウンロードセクションから、コンピュータのディレクトリにダウンロードします。

  ZIP アーカイブ *FTS_<spec>.zip* がダウンロードディレクトリに配置されます（名前の *<spec>* の部分には、システムタイプ、システムボード、ファームウェア /SDRR バージョンなどの情報が指定されます）。

  ZIP アーカイブには次のファイルが格納されています。

  - *USBImage.exe*
  - *iRMC_<Firmware-Version>.exe*
  - *iRMC_<Firmware-Version>.IMA*

- USB メモリスティックをコンピュータに接続します。
- ファイル *iRMC_<Firmware-Version>.exe* またはファイル *USBImage.exe* を起動します。

  起動したファイルに応じて、次のうちの 1 つのウィンドウが開きます（362 ページ の図 218 を参照）。

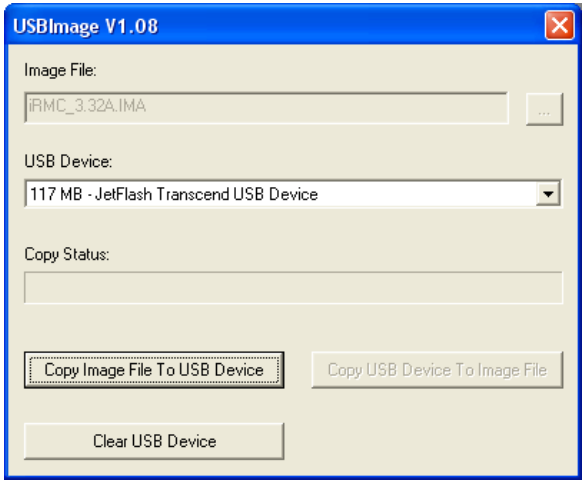


図 218: イメージファイルを USB メモリスティックにコピーする (with iRMC_<Firmware version.exe))

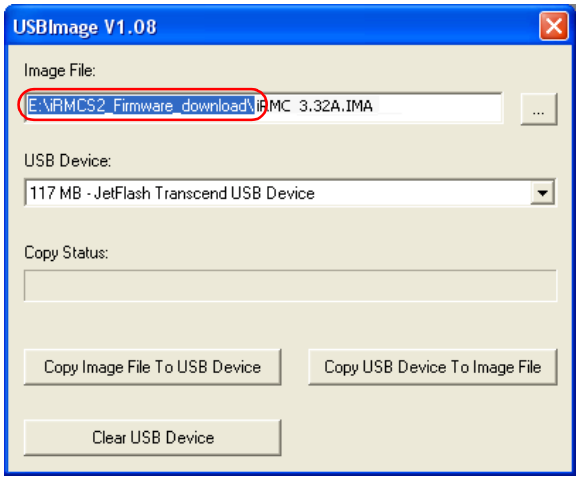


図 219: イメージファイルを USB メモリスティックにコピーする（ USBImage.exe を使用）

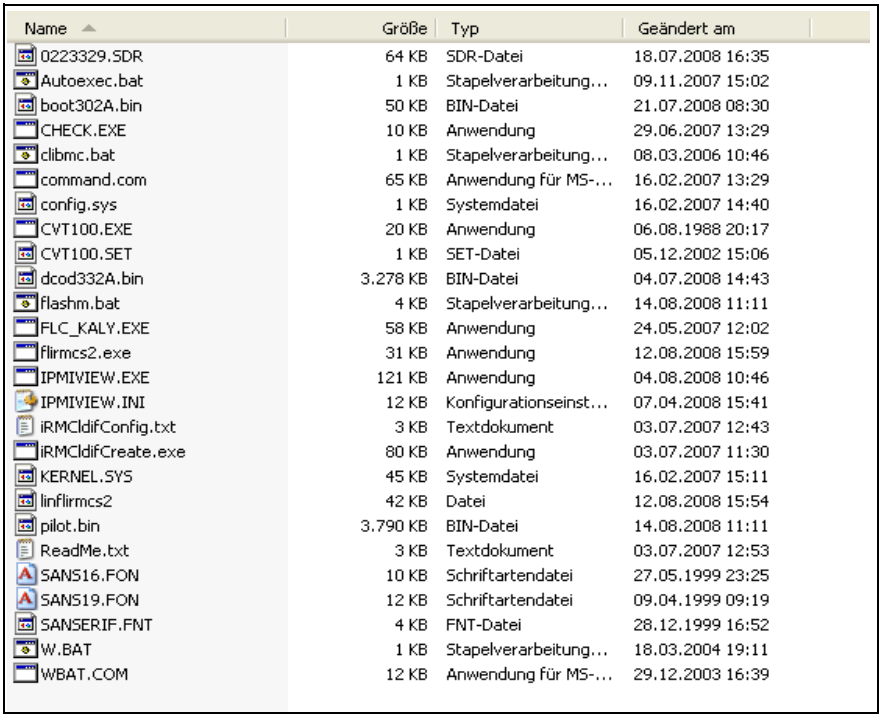
USBImage.exe を起動した場合、「*イメージファイル名*」で、ファイル *iRMC_<Firmware-Version>.IMA* を明示的に指定する必要があります。

- ► 「 *Clear USB Device* 」をクリックして、データを USB メモリスティックから削除します。
- ► 「 *Copy Image File to USB Device* 」をクリックして、ファイル *BMC_<Firmware-Version>.IMA* を USB メモリスティックにコピーして展開します。

注意！

この操作によって、 USB メモリスティックの内容が上書きされます。

コピー操作が終了したら、フラッシュツールとイメージファイルが USB メモリスティックに格納されます。



Name	Größe	Typ	Geändert am
0223329.SDR	64 KB	SDR-Datei	18.07.2008 16:35
Autoexec.bat	1 KB	Stapelverarbeitung...	09.11.2007 15:02
boot302A.bin	50 KB	BIN-Datei	21.07.2008 08:30
CHECK.EXE	10 KB	Anwendung	29.06.2007 13:29
clibmc.bat	1 KB	Stapelverarbeitung...	08.03.2006 10:46
command.com	65 KB	Anwendung für MS-...	16.02.2007 13:29
config.sys	1 KB	Systemdatei	16.02.2007 14:40
CVT100.EXE	20 KB	Anwendung	06.08.1988 20:17
CVT100.SET	1 KB	SET-Datei	05.12.2002 15:06
dcod332A.bin	3.278 KB	BIN-Datei	04.07.2008 14:43
flashm.bat	4 KB	Stapelverarbeitung...	14.08.2008 11:11
FLC_KALY.EXE	58 KB	Anwendung	24.05.2007 12:02
flirmcs2.exe	31 KB	Anwendung	12.08.2008 15:59
IPMIVIEW.EXE	121 KB	Anwendung	04.08.2008 10:46
IPMIVIEW.INI	12 KB	Konfigurationseinst...	07.04.2008 15:41
iRMCldifConfig.txt	3 KB	Textdokument	03.07.2007 12:43
iRMCldifCreate.exe	80 KB	Anwendung	03.07.2007 11:30
KERNEL.SYS	45 KB	Systemdatei	16.02.2007 15:11
linflirmcs2	42 KB	Datei	12.08.2008 15:54
pilot.bin	3.790 KB	BIN-Datei	14.08.2008 11:11
ReadMe.txt	3 KB	Textdokument	03.07.2007 12:53
SANS16.FON	10 KB	Schriftartendatei	27.05.1999 23:25
SANS19.FON	12 KB	Schriftartendatei	09.04.1999 09:19
SANSERIF.FNT	4 KB	FNT-Datei	28.12.1999 16:52
W.BAT	1 KB	Stapelverarbeitung...	18.03.2004 19:11
WBAT.COM	12 KB	Anwendung für MS-...	29.12.2003 16:39

図 220: USB メモリスティック内のイメージファイルとフラッシュツール

10.3 ファームウェアイメージのアップデート

iRMC S2/S3 ファームウェアは iRMC S2/S3 の SRAM メモリ内で実行されるため、アクティブなファームウェアとアクティブではないファームウェアの両方をオンラインで、サーバのオペレーティングシステムを実行したまま、アップデートできます。

ファームウェアイメージは、次の方法でアップデートできます。

– iRMC S2/S3 Web インターフェースを経由する
– ServerView Update Manager を使用する
– ServerView Update Manager Express または ASP を使用する
– オペレーティングシステムのフラッシュツールを使用してアップデートする

ファームウェアを以前のバージョンにダウングレードする

ファームウェアのアップデートを実行するほかに、ファームウェアを以前のバージョンにダウングレードできます。

ファームウェアをダウングレードする最も簡単な方法は、以前のバージョンのファームウェアイメージを非アクティブなファームウェアイメージとして iRMC S2/S3 の EEPROM に保存することです。この場合、ファームウェアセレクタをこの以前のバージョンイメージに設定し（185 ページを参照）、その後 iRMC S2/S3 を再起動してファームウェアを有効にするだけです。

以降の項で説明する方法を使用して、ファームウェアをダウングレードすることもできます。この場合、以前のバージョンのファームウェアに基づいてファームウェアのアップデートを実行します。以降の項では、ダウングレードを実行するための特別な要件を個別に示しています。

10.3.1 iRMC S2/S3 Web インターフェースを経由したアップデート

「*iRMC S2/S3 ファームウェアアップデート*」ページでは、ファームウェアイメージをローカルまたはリモートワークステーション、または TFTP サーバに指定して、 iRMC S2/S3 のファームウェアをアップデートできます（184 ページ の「 iRMC S2/S3 ファームウェアアップデート」の項を参照）。

10.3.2 ServerView Update Manager を使用したアップデート

ServerView Update Manager を使用して、グラフィカルユーザーインターフェース（ Windows ）またはコマンドラインインターフェース（ Windows および Linux ）を経由して、 iRMC S2/S3 ファームウェアのアップデートを開始できます。 ServerView Update Manager は、 *ServerView Suite DVD 1* または管理サーバ上のアップデートリポジトリから、アップデートデータにアクセスします。管理サーバのアップデートリポジトリは、ダウンロードマネージャを使用して、または 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して、アップデートします。

ServerView Update Manager によるファームウェアアップデートの詳細は、ServerView Update Manager のマニュアルを参照してください。

10.3.3 ServerView Update Manager Express または ASP を使用するオンラインアップデート

Windows および Linux オペレーティングシステムでは、 iRMC S2/S3 ファームウェアを ServerView Update Manager Express のグラフィカルユーザーインターフェースまたは ASP （ Autonomous Support Package ）コマンドインターフェースを使用してアップデートできます。

Windows では、 対 応する ASP-*.*exe* ファイルをダブルクリックして、 Windows エクスプローラから ASP を開始することもできます。

ファームウェアをダウンロードする際は、次のことに注意してください。

- Update Manager Express によるダウングレード :

  ファームウェアダウングレードは*エキスパート*モードでのみ実行できます。また、 *Downgrade* オプションも有効にする必要があります。

- ASP によるダウングレード :
  - Windows の場合 :

    ダウングレードは、 対 応する **.exe* ファイルをダブルクリックして ASP を開始して実行できます。 ASP を CLI から開始する場合、 *Force=yes* オプションを明示的に指定する必要があります。

  - Linux の場合 :

    オプション *-f* またはオプション *--force* を明示的に指定する必要があります。

Update Manager Express と ASP によるファームウェアアップデートの詳細は、 ServerView Suite マニュアルの「 Local System Update for PRIMERGY Servers 」を参照してください。

10.3.4 オペレーティングシステムのフラッシュツールを使用してアップデートする

オペレーティングシステムのフラッシュツールを使用したオンラインアップデートは、リカバリフラッシュとしてのみ実行され、バージョンチェックは実行されません。

前提条件

フラッシュツールとファームウェアアップデートのファイルが、管理対 象サーバのファイルシステム上にあることが必要です。

実行しているオペレーティングシステムに応じて、次のフラッシュツールの 1 つを使用します。

DOS:	flirmcs2
Windows:	winflirmcs2
	前提条件 使用している Windows オペレーティングシステム（32/64 ビット）の ServerView エージェントが管理 対 象サーバで実行している必要があります。
Windows（32 ビット）：	win32flirmcs2 （エージェントは不要）
Windows（64 ビット）：	win64flirmcs2 （エージェントは不要）
Linux:	linflirmcs2

フラッシュツールを Windows コマンドライン（ flirmcs2 、 win32flirmcs2 、 win64flirmcs2 、 winflirmcs2 ）または Linux CLI （ linflirmcs2 ）で呼 び 出します。

フラッシュツールの構文とオペランドは、372 ページ の「フラッシュツール」の項に記載されています。

次の手順に従います。

USB メモリスティックを使用したオンラインアップデートは、以下で説明されています（361 ページ の「USB メモリスティックでの更新準備」の項を参照）。

- USB メモリスティックを管理 対 象サーバに接続します。
- Windows コマンドラインまたは Linux コマンドラインインターフェース（CLI ）で、 USB メモリスティックに 対 応するドライブに移動します。
- フラッシュツールをパラメータ */s 4* で呼 び 出して、ファームウェアセレクタを値 4 に設定します。

  Windows コマンドラインでは、次のように入力します。

  ```
  WinFLIRMCS2 /s 4
  ```

- フラッシュツールを 対 応するアップデートファイルで呼 び 出して、ファームウェアと SDR データのアップデートを開始します。

  Windows コマンドラインでは、次のように入力します。

  ```
  WinFLIRMCS2 dcod< ファームウェアバージョン >.bin <nnnnnnn>.sdr /i
  ```

  ファームウェアのアップデート中、コンソールにはアップデート処理の進行状況が通知されます。エラーが発生した場合、アップデート処理は中止され、 対 応するリターンコードが報告されます（374 ページを参照）。

- 管理 対 象サーバを再起動します。これによって、アップデートされたファームウェアのファームウェアイメージが自動的に有効になります。

10.3.5 FlashDisk メニューによるアップデート

FlashDisk メニューによるアップデートの場合は、起動可能な USB メモリスティックが必要です（361 ページ の「USB メモリスティックでの更新準備」の項を参照）。

次の手順に従います。

- USB メモリスティックを管理 対 象サーバに接続します（直接、またはリモートストレージとして）。
- USB メモリスティックから起動します。

起動処理が完了した後、 USB メモリスティックのデータは自動的に RAM ディスクにコピーされます。 *autoexec.bat* ファイルが自動的に起動します。

FlashDisk メニューが開きます。

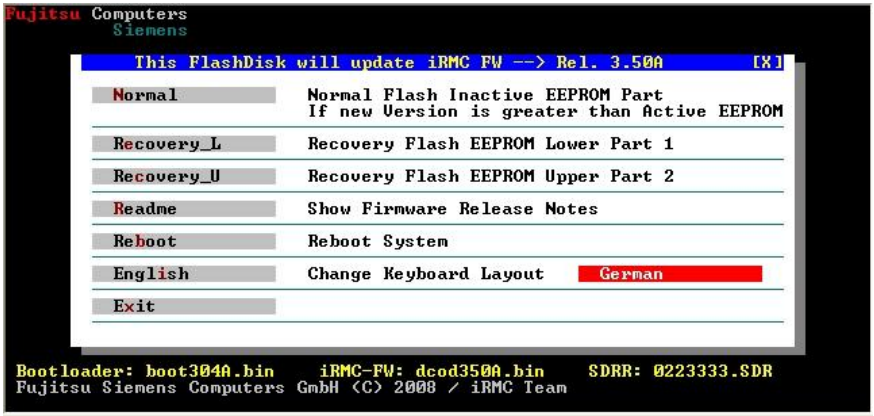


図 221: FlashDisk メニュー

ファームウェアダウングレードは、リカバリフラッシュによってのみ可能です。

「*Normal*」
*通常のフラッシュ*が実行されます。

通常のフラッシュ処理中、アクティブなファームウェアを含む EEPROM の領域が最新であるかどうかチェックされます。これらの領域で最新でないものがある場合、最新ではない、非アクティブなファームウェアに 対 応する領域がアップデートされます。

「 *Recovery _L* 」
ファームウェアイメージ 1 （低ファームウェアイメージ）の *リカバリフラッシュ*が実行されます。

リカバリフラッシュの場合、ファームウェアイメージ 1 の 3 つの領域すべてについてフラッシュが実行され、バージョンチェックは実行されません。

「 *Recovery _U* 」
ファームウェアイメージ 2 （高ファームウェアイメージ）の *リカバリフラッシュ*が実行されます。

リカバリフラッシュの場合、ファームウェアイメージ 2 の 3 つの領域すべてについてフラッシュが実行され、バージョンチェックは実行されません。

「 *Readme* 」
Readme ファイルが開きます。

「 *Reboot* 」
iRMC S2 ウォームスタートが実行されます。

「 *English* 」 ／ 「 *German* 」
キーボードレイアウトを指定します。デフォルトで「 *German* 」が設定されています。

► 対 応するボタンをクリックして、必要な種類のアップデートを開始します。

ファームウェアのアップデート中、コンソールにはアップデート処理の進行状況が通知されます。エラーが発生した場合、アップデート処理は中止されます。 対 応するリターンコードが報告されます（ 374 ページを参照 ）。

► アップデート処理が完了したら、「 *Exit* 」をクリックして FlashDisk メニューを終了します。

► USB メモリスティックを管理 対 象サーバから取り外します。

► 管理 対 象サーバを再起動します（ Ctrl + Alt + Del ）。

10.4 エマージェンシーフラッシュ

SDR にシステムとの互換性がなくなり、 iRMC S2/S3 ファームウェアが実行できなくなった場合、エマージェンシーモードを使用してファームウェアを再度実行させることができます。エマージェンシーモードでは、システムは自動的にブートローダに分岐して、ファームウェアアップデート用に準備されます。

エマージェンシーモードは、エラー LED （前面保守 LED ）（赤色）と識別灯（青色）が交互に点滅して示されます。

管理 対 象サーバをエマージェンシーモードに切り替えて iRMC S2/S3 のファームウェアをアップデートするには、次の手順に従います。

- ► 電源コネクタを取り外します。
- ► ID キーを押し下げて、コネクタをソケットに接続し直します。

  管理 対 象サーバが緊急時モードになります。
- ► サーバで DOS を起動し、リカバリフラッシュ手順を使用して iRMC S2/S3 ファームウェアをアップデートします。

  ファームウェアがアクティブではない場合、起動処理の開始までに最高 2 分かかります。この期間中に BIOS から出力されるエラーメッセージ「 iRMC S2/S3 Controller Error 」は無視してください。

10.5 フラッシュツール

以下で説明する flirmcs2 と WinFLIRMCS2 、 rFLIRMCS2 、 sFLIRMCS2 はツールの名前、およ び 使用する環境が異なるのみで動作は変わりません。従って、以下の説明は WinFLIRMCS2 、 rFLIRMCS2 、 sFLIRMCS2 にもそのまま当てはまります。

構文

```
flirmcs2 {/v|/o [/4]|/s[<íl>]}

flirmcs2 {<file1> [<file2>] [<file3>]
      [/n /l[< ログファイル >] /d /e /4 /i]}

flirmcs2 {/h|/?}
```

オプション

/v　コマンドの現在のバージョンを表示します。

/o　両方のファームウェアイメージの現在のバージョンを表示します。

/s　ファームウェアセレクタの値を表示します。

/s < 値 >

ファームウェアセレクタの値を設定します。このオプションを使用して、ファームウェアリセット後にファームウェアが開始されるファームウェアイメージを定義します。

- 0　セレクタを最新のファームウェアを持つファームウェアイメージに設定します。
- 1　セレクタをファームウェアイメージ 1 に設定します。
- 2　セレクタをファームウェアイメージ 2 に設定します。
- 3　セレクタを最も古いファームウェアを持つファームウェアイメージに設定します。
- 4　セレクタを最後にアップデートされたファームウェアを持つファームウェアイメージに設定します。
- 5　セレクタを、アップデートされてから現在までの時間が最長のファームウェアイメージに設定します。

<file1> ～ <file3>
実行するアップデートを示す 1 つ以上のファイルを指定します。次のファイルが選択されます。

boot<FW-Version>.bin
ブートローダファームウェアをアップデートします。

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 をアップデートします。

ファームウェアイメージ 2 をアップデートするには、オプション */4* も指定する必要があります（以下を参照）。

/4 ファームウェアイメージ 2 をアップデートします。

/l [< ログファイル >]
エラーメッセージを指定したログファイルに出力します。ログファイルが指定されていない場合、出力は *flbmc.log* ファイルに転送されます。

/n コンソールに出力されません。
このオプションは、 /p および */d* オプションよりも優先されます

/np フラッシュ処理中に、進行状況を示す回転するバーが表示されます。

/d 追加のデバッグ情報を出力します。

/e エミュレーションモード（デバッグ目的専用）。

/i 非アクティブなファームウェアをアップデートします。

/h または /?
ヘルプ情報を出力します。

戻り値

0	ファームウェアのアップデートに成功しました。
1	パラメータが正しくないか、指定されていません。
3	PROM タイプは指定できません
4	iRMC S2/S3 と通信できません。
5	バイナリファイルが正しくありません。
8	KCS （Keyboard Control Style interface）アクセスでエラーが発生しました。
9	ターゲット EEPROM との通信がタイムアウトしました。
10	バッファがアロケートされていません。
12	ネットワークノードが使用中です。
13	EEPROM のイレースがタイムアウトしました。
14	EEPROM のフラッシュがタイムアウトしました。
15	EEPROM のイレースでエラーが発生しました。
16	EEPROM のフラッシュでエラーが発生しました。

11 iRMC S2/S3 によるオペレーティングシステムのリモートインストール

本章では、ServerView Installation Manager （以下 Installation Manager）および iRMC S2/S3 機能の「AVR （Advanced Video Redirection : ビデオリダイレクション）」および「リモートストレージ」を使用して、リモート管理端末から管理サーバ上にオペレーティングシステムをインストールする方法を説明しています。

この章では、以下の特定のトピックについて説明します。

– リモートストレージメディアを使用したオペレーティングシステムのリモートインストールの基本手順

– ServerView DVD 1（Windows および Linux）を使用してリモートワークステーションから管理対象サーバを起動する

– 管理対象サーバに対する設定後にリモートワークステーションから Windows をインストールする

– 管理対象サーバに対する設定後にリモートワークステーションから Linux をインストールする

リモートストレージメディアの操作に主に焦点を当てて説明します。説明は Installation Manager の機能に精通していることを前提としています（『ServerView Installation Manager』マニュアルを参照）。

iRMC S2/S3 を使用したオペレーティングシステムのリモートインストールの前提条件：

– iRMC S2/S3 の LAN インターフェースが設定されている必要があります (39 ページを参照)。

– iRMC S2/S3 の「ビデオリダイレクション（AVR）」機能と「リモートストレージ」機能を使用するためのライセンスキーをインストールする必要があります（171 ページを参照）。

11.1 iRMC S2/S3 を使用したオペレーティングシステムのインストール - 基本手順

Installation Manager の場合、iRMC S2/S3 を使用したオペレーティングシステムのリモートインストールとは、リモートストレージメディアを使用して、リモートワークステーションから AVR ウィンドウを介して、管理対象サーバ上にオペレーティングシステムをローカルに設定およびインストールすることです。

Installation Manager を使用したインストールを行うには、以下の手順が必要です。

1. 起動元にするストレージメディア（DVD 1 または Installation Manager ブートイメージ）をリモートストレージとして接続します。
2. DVD 1 または Installation Manager ブートイメージを使用して、管理対象サーバを起動し、設定します。
3. リモートワークステーションの Installation Manager を使用して、管理対象サーバにオペレーティングシステムをインストールします。
4. AVR ウィンドウでマウスポインタの同期を最適化します（Linux の場合のみ必要）。

Installation Manager を使用せずに、Windows インストール CD/DVD で Windows をインストールする

リモートストレージによる Windows のリモートインストールは、Installation Manager を使用しても、Windows インストール CD/DVD のみを使用しても行えます。リモートストレージメディアの操作に関しては、この 2 つの方法はどちらも同じです。

しかし、次の理由から、Installation Manager を使用して Windows をインストールすることをお勧めします。

– Installation Manager 自身が、必要なドライバを識別してシステムにコピーします。
– インストール中に、Installation Manager のすべての機能を使用できます。つまり、たとえばサーバ管理設定も含め、システム全体を設定することができます。

– Installation Manager を使用しないインストールは、インストールプロセス中にマウスカーソルを同期できないため、キーボードで操作する必要があります。それとは対照的に、Installation Manager を使用してインストールすると、すべての設定手順およびインストール手順をマウスを使用して行うことができます。

– Installation Manager を使用しないでインストールすると、マウスカーソルの同期に必要なすべての設定を手動で行う必要があります。

– Installation Manager を使用したインストールの所要時間は、オペレーティングシステムの CD/DVD を使用したインストールと大差はありません。

Installation Manager を使用せずに、Linux インストール CD/DVD を使用して Linux をインストールする

システムが必要とするドライバがわかっている場合は、Linux インストール CD/DVD から起動して、Linux のインストールを開始できます。

インストールで、フロッピーディスクのドライバを統合する必要がある場合は、インストールを開始する前に、下記のリモートストレージ接続をセットアップする必要があります。

– 起動元にするストレージメディア（CD-ROM/DVD-ROM または ISO イメージ）

– 必要に応じて、ドライバのインストール用ストレージメディア

11.2 ストレージメディアをリモートストレージとして接続する

リモートストレージを使用すると、ネットワークの他の場所にある「仮想」ドライブを利用できるようになります。

仮想ドライブのソースには、以下を使用できます。

– リモートワークステーションの物理ドライブまたはイメージファイル。イメージファイルはネットワークドライブ（たとえば、D ドライブの場合「D:」ドライブ文字を使用）でも構いません。

– リモートストレージサーバを介してネットワークの中心に置かれているイメージファイル

パラレルリモートストレージ接続：

実行できるのは、以下のいずれかです

– **リモートワークステーションの仮想ドライブへの最大 2 つの**リモートストレージ接続（接続が AVR Java アプレットを使用して確立されている場合）

または

– **1 台のリモートストレージサーバへの 1 つの**リモートストレージ接続

アプレットとリモートストレージサーバを使用して同時リモートストレージ接続を確立することはできません。

iRMC S2/S3 Web インターフェースの「*リモートストレージ*」ページでは、現在のリモートストレージ接続の状態に関する情報を取得できます （315 ページを参照）。

リモートストレージに関する詳細は、113 ページ の「リモートストレージ」の章を参照してください。

リモートストレージワークステーションのリモートストレージとしてストレージメディアを接続する

リモートワークステーションで次の手順に従って、リモートストレージ接続を確立します。

- 「*リモート ストレージ使用権限*」で iRMC S2/S3 Web インターフェースにログインします（140 ページを参照）。
- 「*AVR（Advanced Video Redirection：ビデオリダイレクション*」ページを開き、AVR を起動します（304 ページを参照）。
- AVR ウィンドウで「リモートストレージ」を起動します（116 ページを参照）。
- リモートストレージに使用するストレージメディアを準備します（119 ページを参照）。
  - Installation Manager を使用してインストールする場合：

    ServerView Suite DVD 1 または Installation Manager ブートイメージ、およびオプションで、フォーマット済みの USB メモリスティック（ステータスバックアップメディアとして使用）を準備します。
  - ベンダーのインストール CD/DVD でインストールする場合：

    Windows または Linux インストール CD/DVD、およびオプションドライバを準備します。

    ServerView Suite DVD 1 およびオペレーティングシステムインストール CD/DVD をイメージファイル（ISO イメージ）としてフォルダに保存して、そこからリモートストレージとして接続するか、リモートストレージサーバを介して接続することをお勧めします。

  準備したストレージメディアは、「*ストレージ デバイス*」ダイアログボックスに表示されます。

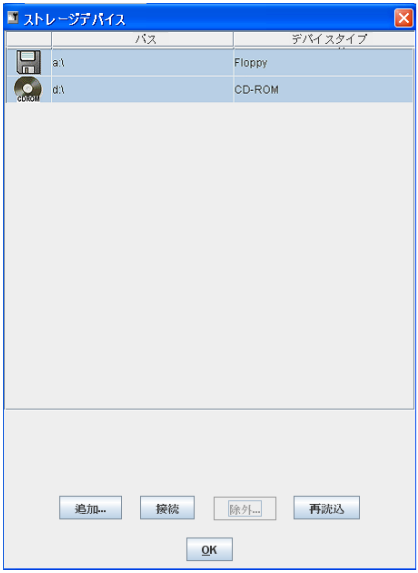


図 222: 「ストレージデバイス」ダイアログボックス：ServerView Suite DVD 1

- 「*接続*」をクリックして、DVD ROM ドライブ（DVD 1）または Installation Manager ブートイメージをリモートストレージとして接続します。

リモートストレージサーバを使用して提供される ISO イメージ（イメージファイル）をリモートストレージとして接続する

Installation Manager ブートイメージからの起動に、リモートストレージサーバを使用して提供されるイメージファイルを使用できます。

リモートストレージサーバを使用して提供される仮想ドライブを使用できるようになる前に、リモートストレージサーバをインストールして起動しておく必要があります（130 ページ の「リモートストレージサーバを経由するリモートストレージの追加」の項を参照）。

リモートストレージサーバへの接続を確立するには、リモートワークステーションで次の手順に従います。

- 「*リモートストレージ使用権限*」許可で iRMC S2/S3 Web インターフェースにログインします（140 ページを参照）。
- 「*リモートストレージ*」ページを選択します。
- リモートストレージサーバへの接続を確立します（317 ページを参照）。

11.3 管理対象サーバを ServerView Suite DVD 1 から起動して、Installation Manager で設定する

リモートワークステーションで、次の手順に従います。

- ► iRMC S2/S3 Web インターフェースを使用して、管理対象サーバを起動または再起動します（192 ページを参照）。ブートプロセスの進捗状況を AVR ウィンドウで追跡できます。

  管理対象サーバの BIOS/TrustedCore/UEFI POST フェーズでは、リモートストレージメディアは USB 2.0 デバイスとして表示されます。リモートストレージのストレージメディアは 、BIOS ブートシーケンスに次のエントリで表示されます。

  – （物理）フロッピーディスクは、別エントリの「FTS RemoteStorage FD-(USB 2.0)」と表示されます。

  – 他のすべてのリモートストレージデバイスタイプは、共有エントリ「CD-ROM DRIVE」と表示されます。

  > **i** ローカル CD-ROM/DVD-ROM ドライブと、リモートストレージとして接続されている CD-ROM/DVD-ROM ドライブの両方が管理対象サーバにある場合は、管理対象サーバはリモートストレージ CD-ROM/DVD-ROM ドライブから起動します。

- ► サーバの起動中に F2 を押します。
- ► BIOS/TrustedCore/UEFI セットアップで、ブートシーケンスを定義できる「ブート」メニューを開きます。
- ► リモートストレージとして接続されている ServerView Suite DVD 1 に対して、Boot Priority=1 （最高の優先度）を指定します。
- ► 設定を保存して、BIOS/TrustedCore/UEFI セットアップを終了します。

管理対象サーバが、リモートストレージとして接続されている ServerView Suite DVD 1 から起動します。

> **i** **システムがリモートストレージメディア（ServerView Suite DVD 1 または Installation Manager ブートイメージ）から起動しない場合は、次の手順に従います。**
>
> ► BIOS POST フェーズでストレージメディアが表示されるかどうか確認し、必要に応じてストレージメディアをリモートストレージとして接続します。

► 正しいブートシーケンスが指定されていることを確認します。

ServerView Suite DVD 1（リモートストレージメディア）からの起動には、5 分程度かかります。ブートプロセス中は、ブートの進捗状況が表示されます。ブートプロセスが完了すると、Installation Manager スタートアップにダイアログボックスが表示され、ステータスバックアップ領域のメディア（ステータスバックアップメディア）を選択するように求められます。

オペレーティングシステムのインストールを開始する前に、リモートワークステーションの AVR ウィンドウで、ローカルマウスカーソルと管理対象サーバのカーソルを同期する必要があります。AVR ウィンドウでのマウスカーソルの同期に関する詳細は、96 ページ の「マウスポインタの同期」の項 を参照してください。

► 「*Installation Manager mode*」で「*Standard mode*」を選択します。

► 設定データの保存先を、ローカルな交換可能データメディアとネットワークメディアのどちらにするか指定します。

ステータスバックアップオプションを選択しないで再起動すると、設定データがすべて失われるので注意してください。

「*Status backup medium*」

バックアップメディアは書き込み保護されません。

システムの起動時には、USB スティックが USB ポートに接続されている必要があります。USB ポートに接続されていない場合にコンフィグレーションファイルを保存するには、USB スティックを接続して、ServerView Suite DVD 1 から再起動します。

► 「*on local drive (floppy / USB stick)*」オプションを選択します。

► このオプションの右側にあるボックスで、該当ドライブを選択します。

Installation Manager ステータスディスク作成に関する詳細は、『ServerView Installation Manager』マニュアルを参照してください。

「Connecting the status medium and/or the installation media via the network」

► この目的に必要な共有を設定します。

準備したコンフィグレーションファイルを格納したメディア、およびインストールメディアをネットワーク経由で使用できるようにしている場合は、このオプションを選択する必要があります。インフラストラクチャに応じて、一時 IP アドレスを DHCP 経由で取得することも、現在の Installation Manager セッションに対して IPv4 または IPv6 アドレスを手動で設定することもできます。

► 「*次へ*」をクリックして、Installation Manager を起動します。

ローカルインストールの開始

Installation Manager を起動すると、ようこそ画面が表示されます。

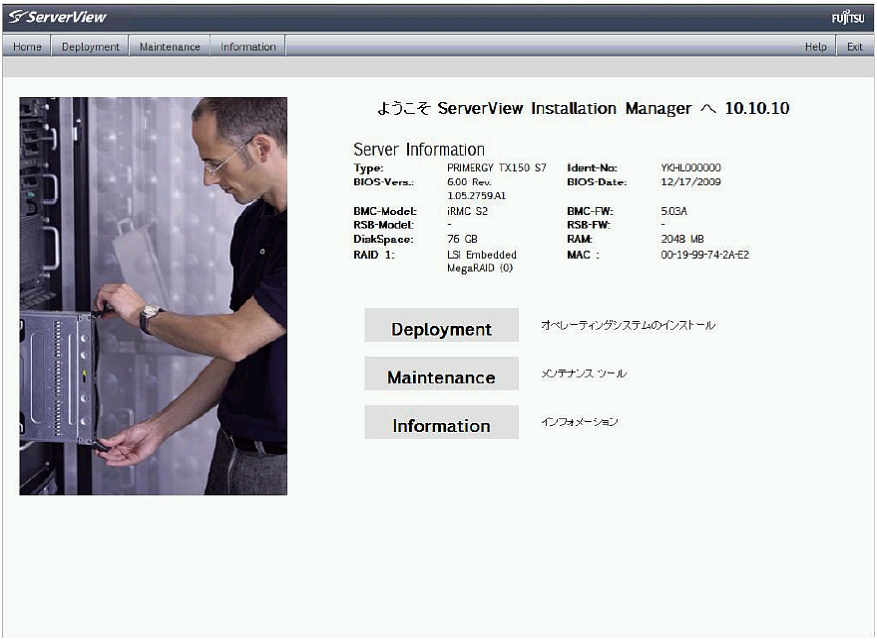


図 223: Installation Manager - ようこそ画面

- 「*Deployment*」をクリックして、ローカルインストール（デプロイメント）の準備を開始します。

  インストールの準備を行うために、システム構成、およびその後の OS の自動インストールの仕様を収集する一連のコンフィグレーションステップが Installation Manager ウィザードによって提示されます。

  管理対象サーバのローカル CD ROM/DVD ROM ドライブをインストールソースとして設定します。また、リモートワークステーションの CD ROM/DVD ROM ドライブをリモートストレージとして管理対象サーバに接続すると、そのドライブから Windows インストール CD/DVD を使用できるようになります（385 ページ の「設定完了後の管理対象サーバへの Windows のインストール」の項を参照）。

Installation Manager での設定を完了すると、Windows インストール（385 ページを参照）または Linux インストール（388 ページを参照）の「*設定内容の確認*」ダイアログページが表示されます。このダイアログページからインストールプロセスを開始できます。

11.4 設定完了後の管理対象サーバへの OS のインストール

設定を完了したら、管理対象サーバにオペレーティングシステムをインストールする必要があります。

11.4.1 設定完了後の管理対象サーバへの Windows のインストール

設定が完了すると、次のダイアログページが Installation Manager によって表示されます。

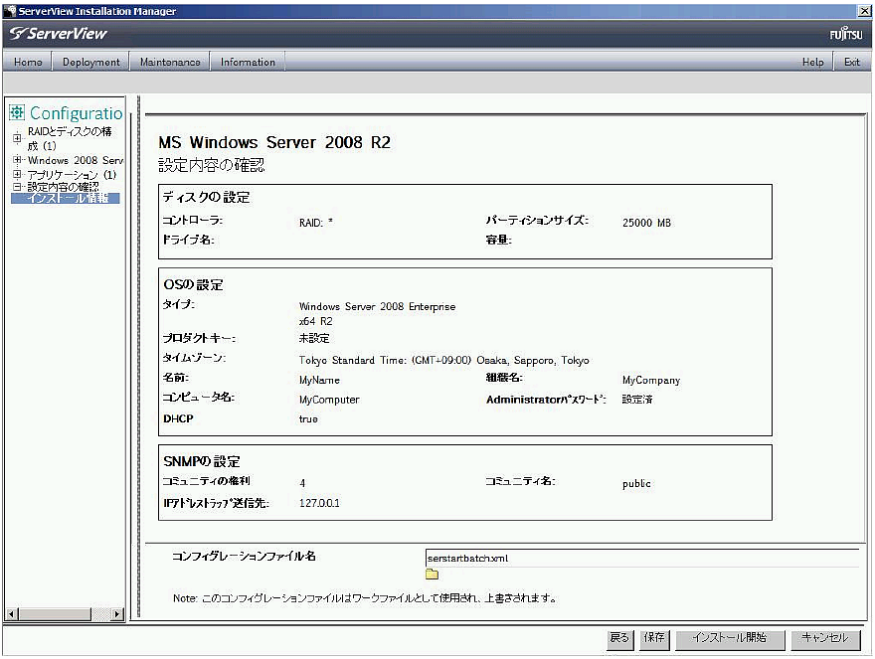


図 224: Installation Manager - 「設定内容の確認」ページ

管理対象サーバのローカル CD ROM/DVD ROM ドライブをインストールソースとして設定した場合は、リモートワークステーションで次の手順に従います。

- ► 現在アクティブなリモートストレージ接続を解除します。リモートストレージ接続の解除に関する詳細は、128 ページを参照してください。
- ► リモートワークステーションの DVD ROM ドライブから ServerView Suite DVD 1 を取り出します。
- ► この DVD ROM ドライブに、Windows インストール CD/DVD を挿入します。

  「*autostart*」がアクティブな場合は、アプリケーションを閉じてください。

- ► Windows インストール CD/DVD が入っている CD ROM/DVD ROM ドライブをリモートストレージとして接続します（124 ページを参照）。
- ► Installation Manager の「*設定内容の確認*」ページで、「*インストール開始*」をクリックします。

  すべてのインストールファイルが、管理対象サーバにコピーされます。

  コピー操作が完了すると、確認ダイアログページが Installation Manager によって開かれ、管理対象サーバを再起動する前にリムーバブルメディアドライブからすべてのストレージメディアを取り出すように求められます。

  具体的には、システムを再起動する前に、現在のリモートストレージ接続をすべてシャットダウンする必要があります。

- ► 現在のリモートストレージ接続をすべてシャットダウンするには、次の手順に従います。
  - ► 「リモートストレージ」を起動します（116 ページを参照）。

    「*ストレージデバイス*」ダイアログボックスが表示されます。このダイアログボックスには、現在接続されているストレージデバイスと、「安全な取り外し」のための指示が記載されています。
  - ► ストレージデバイスの 「安全な取り外し」を行います。つまり、ストレージデバイスにアクセスしているアプリケーションやプログラムがないことを確認してから取り外します。
  - ► 「*切断*」をクリックして、すべてのリモートストレージ接続を取り外します。

► 確認ダイアログページで、「*OK*」をクリックして管理対象サーバを再起動します。

管理対象サーバが再起動すると、AVR でインストール全体を監視できます。

Windows インストール CD/DVD から Windows をインストールする場合：

マウスカーソルの完全な同期を確実にするために、オペレーティングシステムのインストール後に管理対象サーバで次の設定を行う必要があります。

– マウスポインタの速度
– ハードウェアアクセラレーション

この設定を行う方法については、98 ページ の「管理対象 Windows サーバ：マウスポインタ同期設定の調整」の項を参照してください。

Installation Manager を使用して Windows をインストールすると、マウスポインタの問題のない同期が自動的に行われます。

11.4.2 設定完了後の管理対象サーバへの Linux のインストール

Linux のインストール中、マウスは使用できますが、同期はできません。

リモートストレージメディアを変更する場合は必ず、現在接続されているメディアのリモートストレージ接続を取り外して、新しいメディアをリモートストレージとして接続する必要があります。

設定が完了すると、次のダイアログページが Installation Manager によって表示されます。

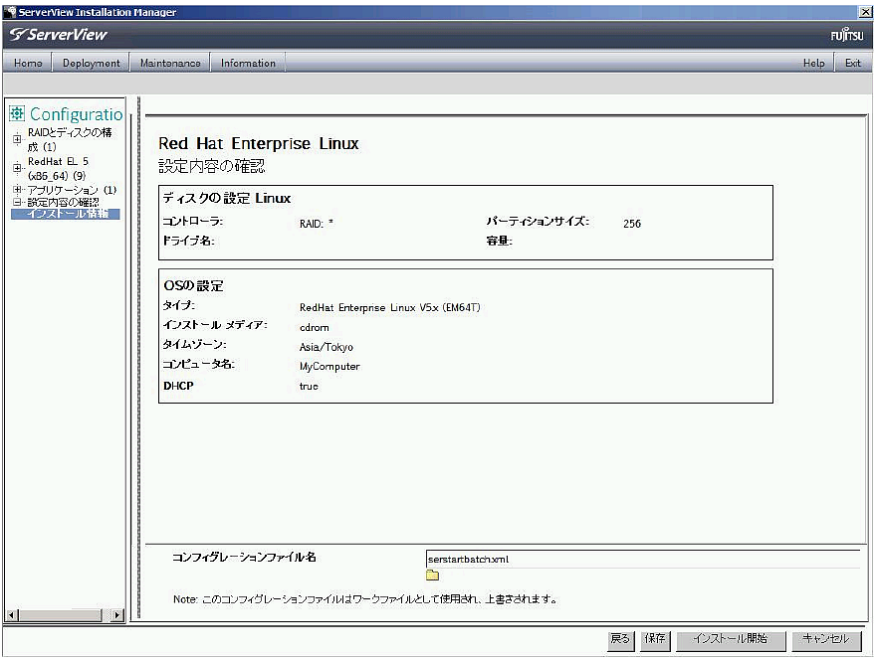


図 225: Installation Manager - 「設定内容の確認」

管理対象サーバのローカル CD ROM/DVD ROM ドライブをインストールソースとして設定した場合は、リモートワークステーションで次の手順に従います。

- ► 現在アクティブなリモートストレージ接続を解除します。リモートストレージ接続の解除に関する詳細は、128 ページを参照してください。
- ► リモートワークステーションの DVD ROM ドライブから ServerView Suite DVD 1 を取り出します。
- ► この DVD ROM ドライブに、Linux インストール CD/DVD を挿入します。

  「*autostart*」がアクティブな場合は、アプリケーションを閉じてください。
- ► Linux インストール CD/DVD が入っている CD ROM/DVD ROM ドライブをリモートストレージとして接続します（124 ページを参照）。
- ► Installation Manager の「*設定内容の確認*」ページで、「*インストール開始*」をクリックします。

  すべてのインストールファイルが、管理対象サーバにコピーされます。コピー操作が完了すると、確認ダイアログページが Installation Manager によって開かれ、管理対象サーバを再起動する前にリムーバブルメディアドライブからすべてのストレージメディアを取り出すように求められます。

  具体的には、システムを再起動する前に、現在のリモートストレージ接続をすべてシャットダウンする必要があります。
- ► システムを再起動する前に、現在のリモートストレージ接続をシャットダウンします。

  これは次の手順で行います。

  - ► 「リモートストレージ」を起動します（116 ページを参照）。

    「*ストレージデバイス*」ダイアログボックスが表示されます。このダイアログボックスには、現在接続されているストレージデバイスと、「安全な取り外し」のための指示が記載されています。
  - ► 「*切断*」をクリックして、すべてのリモートストレージ接続を取り外します。
  - ► ストレージデバイスの 「安全な取り外し」を行います。つまり、ストレージデバイスにアクセスしているアプリケーションやプログラムがないことを確認してから取り外します。
- ► 確認ダイアログページで、「*OK*」をクリックして管理対象サーバを再起動します。

管理対象サーバが再起動すると、AVR でインストール全体を監視できます。

マウスカーソルの完全な同期を確実にするために、オペレーティングシステムのインストール後に管理対象サーバで必要な設定を行う必要があります。この設定を行う方法については、101 ページ の「管理対象 Linux サーバ : マウスポインタ同期設定の調整」の項を参照してください。

12 付録

付録では次のトピックについて説明します。

12.1 iRMC S2/S3 でサポートされる IPMI OEM コマンド

本章では、iRMC S2/S3 がサポートする OEM 特有の IPMI コマンドの選択について説明します。

12.1.1 概要

iRMC S2/S3 では以下の OEM 特有の IPMI コマンドをサポートします。

- SCCI 準拠の自動電源投入／電源切断コマンド
  （SCCI：**S**erverView **C**ommon **C**ommand **I**nterface（ServerView 共通コマンドインターフェース））
  - 0115 Get Power On Source
  - 0116 Get Power Off Source
  - 011C Set Power Off Inhibit
  - 011D Get Power Off Inhibit
  - 0120 Set Next Power On Time
- **SCCI 準拠の通信コマンド**
  - 0205 System OS Shutdown Request
  - 0206 System OS Shutdown Request and Reset
  - 0208 Agent Connect Status
  - 0209 Shutdown Request Canceled

- **SCCI 準拠のシグナリングコマンド**
  - 1002 Write to System Display
- **Firmware 特有のコマンド**
  - 2004 Set Firmware Selector
  - 2005 Get Firmware Selector
  - C019 Get Remote Storage Connection
  - C01A Set Video Display on/off
- **BIOS 特有のコマンド**
  - F109 Get BIOS POST State
  - F115 Get CPU Info
- **iRMC S2/S3 特有のコマンド**
  - F510 Get System Status
  - F512 Get EEPROM Version Info
  - F542 - Get HDD lightpath status（コンポーネントステータス信号の読み取り）
  - F543 Get SEL entry long text
  - F545 Get SEL entry text
  - F5B0 Set Identify LED
  - F5B1 Get Identify LED
  - F5B3 Get Error LED
  - F5DF Set Nonvolatile Cfg Memory to Default Values
  - F5E0 Set Configuration Space to Default Values
  - F5F8 Delete User ID

12.1.2 IPMI OEM コマンドの記述

この節では、個別の OEM 特有の IPMI コマンドについて説明します。

12.1.2.1 記述形式

本章で記載する OEM 特有の IPMI コマンドは、IPMI コマンドを記述するための IPMI 標準で使用する形式によって記述されます。

IPMI 標準では、各コマンドに対する入力パラメータと出力パラメータを一覧にしたコマンド表を使用して IPMI コマンドを記述します。

IPMI 標準の情報については以下のサイトを参照してください。

http://developer.intel.com/design/servers/ipmi/index.htm

12.1.2.2 SCCI 準拠の自動電源投入／電源切断コマンド

01 15 - Get Power On Source

本コマンドは最後に行われた自動電源投入の理由を返します。理由には以下にあげるものがあります。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**01** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**15** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	3	**01** データ長
	4	電源投入原因： 最新の自動電源投入理由

電源投入原因	内容
0x00	ソフトウェアまたはコマンド
0x01	電源スイッチ（フロントパネルまたはキーボード上）
0x02	電源障害後の自動再起動
0x03	クロックまたはタイマー（ハードウェア RTC またはソフトウェアタイマー）
0x04	ファン障害によるシャットダウン後の自動再起動
0x05	臨界温度によるシャットダウン後の自動再起動
0x08	ウォッチドックタイムアウト後の再起動
0x09	リモートオン（モデム RI ライン、SCSI ターミネーションパワー、LAN、IC カード リーダー・・・）
0x0C	CPU エラー後の再起動
0x15	ハードウェアリセットによる再起動
0x16	ウォームスタート後の再起動
0x1A	PCI バス電源管理イベントによる電源投入
0x1D	リモートマネージャ経由のリモート制御による電源投入
0x1E	リモートマネージャ経由のリモート制御による再起動／リセット

01 16 - Get Power Off Source

本コマンドは最後に行われた自動電源切断の理由を返します。理由には以下にあげるものがあります。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**01** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**16** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	3	**01** データ長
	4	電源切断原因： 最後の自動電源切断理由

電源切断原因	内容
0x00	ソフトウェア（SWOFF、コマンドによる電源切断）
0x01	電源スイッチ（フロントパネルまたはキーボード上）
0x02	AC 電源障害
0x03	クロックまたはタイマー（ハードウェア RTC またはソフトウェアタイマー）
0x04	ファン障害
0x05	臨界温度
0x08	ウォッチドッグタイムアウト繰り返し後の電源切断
0x0C	CPU エラー繰り返し後の電源切断
0x1D	リモートマネージャ経由のリモート制御による電源切断

01 1C - Set Power Off Inhibit

本コマンドは*電源切断防止*フラグを設定します。

この設定により、正当な理由なくサーバの電源をオフにしようとした場合に一時的に電源切断が防止されます。電源切断防止フラグが設定されていると、サーバの「Power Off」、「Power Cycle」または再起動を実行しようとした理由がファームウェアによって保存されますが、動作は実行されません。最後に実行したサーバの「Power Off」、「Power Cycle」または再起動の理由が常時保存されます。保存された動作は*電源切断防止*フラグをリセットしたときのみ実行されます。

*電源切断防止*フラグは、電源障害後、またはリセットボタンの押下時に自動的にリセットされます。

*電源切断防止*フラグには、メインメモリダンプを作成する際に使用するダンプフラグと同じ効果があります。この場合、ダンプを作成する前にイニシエーターで必ずフラグを設定し、ダンプが完了したときにリセットします。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**01** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**1C** コマンド指定子
	5	**00** オブジェクト ID
	6:7	**00 00** 値 ID
	8	**01** データ長
	9	電源切断防止フラグ：0 = 防止しない、1 = 防止する
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

01 1D - Get Power Off Inhibit

本コマンドは*電源切断防止*フラグの値を取得します。

*電源切断防止*フラグの詳細については、396 ページ の「01 1C - Set Power Off Inhibit」の説明を参照してください。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**01** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**1D** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**01** 応答データ長
	6	電源切断防止フラグ：0 = 防止しない、1 = 防止する

01 20 - Set Next Power On Time

本コマンドは、設定スペースに保存されている電源投入／切断時刻とは別に所定の時間でシステムの電源を投入します。

コマンドは 1 回のみ有効です。

設定した「電源投入」時刻をキャンセルするには、再度 01 20 コマンドで「0 」を「電源投入」時刻に指定してください。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**01** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**20** コマンド指定子
	5	**00** オブジェクト ID
	6:7	**00 00** 値 ID
	8	**04** データ長
	9:12	時刻（LSB ファースト）（下記参照）
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

時刻（LSB ファースト）

システムの電源を再度投入した時刻（UNIX 特有の形式）です。時刻は不揮発メモリに保存されません。設定単位は 1 分毎です。設定単位は 1 分毎です。システムの電源を投入した後、内部で時刻が 0 に 設定されます。

「電源投入」時刻に 「0 」を指定した場合、システムの電源は投入されません。

12.1.2.3 SCCI 準拠の通信コマンド

SCCI 準拠の通信コマンドには、エージェントサービスが OS で起動していることが必要です。コマンドを実行するは、iRMC S2/S3 と通信するエージェントが最終的に動作を行います。

02 05 - System OS Shutdown Request

本コマンドはサーバのオペレーティングシステムのシャットダウンを開始します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**02** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**05** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

02 06 - System OS Shutdown Request and Reset

本コマンドはサーバのオペレーティングシステムのシャットダウンを開始した後にシステムを再起動します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**02** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**06** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

02 08 - Agent Connect Status

本コマンドはエージェントがアクティブであるかどうかを確認します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**02** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**08** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**01** データ長
	6	**接続状態**： 00 ＝接続が切断された、エージェントが接続されていない 01 ＝接続が再確立された、エージェントが接続されている

02 09 Shutdown Request Cancelled

本コマンドは発行されたシャットダウン要求をキャンセルします。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**02** Cmd ：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**09** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

12.1.2.4 SCCI 準拠のシグナリングコマンド

10 02 - Write to System Display

本コマンドは、LocalView ディスプレイ（接続されている場合）に文字を書き込むために使用します。

要求データ	-	**B8**　NetFnlLUN：OEM/ グループ
	-	**10**　Cmd ：コマンドグループファンテスト
	1:3	**80 28 00**　IANA-Enterprise-Number FTS、LSB ファースト
	4	**02**　コマンド指定子
	5	**オブジェクトインデックス**：：書き込みを行うディスプレイの線
	6:7	**値 ID**（未使用）
	8	**長さ**　1 ずつ増加する書き込む文字数（文字列がヌル終端である必要はありません。ディスプレイの長さを超える文字列は切り捨てます。）
	9	**属性** 0 ＝文字列を左詰めで書き込みます 1 ＝文字列を右詰めで書き込みます
	10:10+n	ディスプレイに書き込む**文字**（文字列がヌル終端である必要はありません。）
応答データ	-	**BC**
	-	**10**
	1	完了コード
	2:4	**80 28 00**　IANA-Enterprise-Number FTS、LSB ファースト

12.1.2.5 Firmware 特有のコマンド

20 04 - Set Firmware Selector

本コマンドは、ファームウェアのリセット後にアクティブになる IRMC S2/S3 のファームウェアイメージを設定します。

要求データ	-	**20** NetFnlLUN：ファームウェアファームウェア
	-	**04** CMD ：コマンドグループファームウェア
	1	セレクタ： 0 = Auto（版数が新しいファームウェアを選択します。） 1 = Low Firmware Image 2 = High Firmware Image 3 = Auto oldest version（版数が古いファームウェアを選択します。） 4 = MRP（書込日が新しいファームウェアを選択します。） 5 = LRP（書込日が古いファームウェアを選択します。）
応答データ	-	**24**
	-	**04**
	1	完了コード

20 05 - Get Firmware Selector

本コマンドは現在のファームウェアセレクタ設定を返します。

要求データ	-	**20** NetFnlLUN：ファームウェアファームウェア
	-	**05** CMD ：コマンドグループファームウェア
応答データ	-	**24**
	-	**05**
	1	完了コード
	2	次回のブートセレクタ： 0 = Auto（最新のファームウェアバージョンの EEPROM を選択します。） 1 = Low EEPROM 2 = High EEPROM 3 = Auto oldest version（最も古いファームウェアバージョンの EEPROM を選択します。） 4 = MRP（最後に更新したファームウェアを選択します。） 5 = LRP（最初に更新したファームウェアを選択します。）
	3	動作中のセレクタ：どのファームウェアが現在動作中であるかを示します。 1 = Low EEPROM 2 = High EEPROM

C0 19 - Get Remote Storage Connection or Status

本コマンドは、渡されたパラメータに応じて、以下に関する情報を返します。

– 使用できるリモートストレージ接続があるか
– リモートストレージ接続の状態および種類

要求データ 1 が「1」に設定された場合、コマンドはストレージメディアがリモートストレージとして接続されているかどうかの情報を返します。

要求データ	-	**C0** NetFnlLUN：OEM
	-	**19** CMD ：コマンドグループファームウェア
	1	01
	2	00
	3	00
応答データ	-	**C4**
	-	**19**
	1	完了コード
	2	**01**
	3	**00：No** **01：接続されている**
	4	**00**
	5	**00**

要求データ 1 が「2」に設定された場合、コマンドは任意のリモートストレージ接続の状態および種類に関する情報を返します。

要求データ	-	**C0** NetFnlLUN：OEM
	-	**19** CMD ：コマンドグループファームウェア
	1	02
	2	00
	3	00 ＝接続 0 01 ＝接続 2
応答データ	-	**C4**
	-	**19**
	1	完了コード
	2	**02**
	3	**00**
	4	**00**
	5	**00 ＝無効／未知** **01 ＝アイドル** **02 ＝接続試行中** **03 ＝接続済み** **04 ＝接続再試行に失敗または試行回数の終了** **05** = **＝接続切断** **06** = **＝切断中**
	6	00 **＝無効／未知** **01 ＝ストレージサーバ／ IPMI** **02 ＝アプレット** **03 ＝なし／未接続**

C0 1A - Set Video Display On/Off

本コマンドは、ローカルコンソールの有効／無効を切り替えることができます。

要求データ	-	**C0** NetFnlLUN：OEM
	-	**1A** Cmd ：コマンドグループファンテスト
	1	00 ＝ビデオ表示を有効に設定します 01 ＝ビデオ表示を無効に設定します
応答データ	-	**C4**
	-	**1A**
	1	完了コード

12.1.2.6 BIOS 特有のコマンド

F1 09 - Get BIOS POST State

本コマンドは BIOS が POST 中であるかどうかの情報を提供します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F1** Cmd ：コマンドグループ BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**09** コマンド指定子
応答データ	-	**BC**
	-	**F1**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	[7:1] – 予備 [0] - Get BIOS POST State：0 ＝ BIOS が POST 状態ではない 1 ＝ BIOS が POST 状態

F1 15 - Get CPU Info

本コマンドは CPU 内部情報を返します。iRMC S2/S3 では、POST フェーズ中に BIOS から本情報を取得します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F1** Cmd ：コマンドグループ BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**15** コマンド指定子
	5	CPU のソケット番号（0 ベース）
応答データ	-	**BC**
	-	**F1**
	1	**完了コード** 01 ＝未実装の CPU ソケット
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	CPU ID、LSB ファースト
	7	プラットフォーム ID
	8	ブランド ID
	9:10	CPU の最大コアスピード [MHz]、LSB ファースト
	11:12	Intel QuickPath インターコネクト [MT/s]、LSB ファースト
	13	熱制御オフセット
	14	熱ダイオードオフセット
	15	CPU データ予備
	16:17	記録 ID CPU 情報 SDR、LSB ファースト
	18:19	記録 ID CPU ファン制御 SDR、LSB ファースト
	20:21	CPU ID ハイワード、LSB ファースト（なければ 0）

12.1.2.7 iRMC S2/S3 特有のコマンド

F5 10 - Get System Status

本コマンドは、電源状態、エラーステータス等のシステムの各種内部情報を返します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループメモリ
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**10** コマンド指定子
	5:8	**タイムスタンプ**
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**システムステータス**（詳細は、以下に参照してください。）
	6	**シグナリング**（詳細は、以下に参照してください。）
	7	**通知**（詳細は、以下に参照してください。）
	8	**POST コード**

タイムスタンプは、*通知*バイトの評価のみに適用されます。

システム LED

Bit 7 - System ON

Bit 6 -

Bit 5 -

Bit 4 - SEL entries available

Bit 3 -

Bit 2 - Watchdog active

Bit 1 - Agent connected

Bit 0 - Post State

シグナリング

Bit 7 - Localize LED

Bit 6 -

Bit 5 -

Bit 4 -

Bit 3 - CSS LED

Bit 2 - CSS LED

Bit 1 - グローバルエラー LED

Bit 0 - グローバルエラー LED

通知

Bit 7 - SEL Modified （New SEL Entry）

Bit 6 - SEL Modified （SEL Cleared）

Bit 5 - SDR Modified

Bit 4 - Nonvolatile IPMI Variable Modified

Bit 3 - ConfigSpace Modified

Bit 2 -

Bit 1 -

Bit 0 - New Output on LocalView display

F5 12 - Get EEPROM Version Info

本コマンドは、EEPROM に保存されている現在のバージョン（bootloader、ファームウェアおよび SDR）に関する情報を返します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループメモリ
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**12** コマンド指定子
	5	EEPROM# 00 ＝ EEPROM 1、01 ＝ EEPROM 2
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**ステータス** 00 ＝チェックサムエラーランタイム FW、01 ＝ OK
	6	**メジャー FW リビジョン** バイナリコード
	7	**マイナー FW リビジョン** BCD コード
	8:10	**Aux.FW Revision** バイナリコード（メジャー／マイナー／ Aux）
	11	**メジャー FW リビジョン** ASCII コード
	12	**メジャー SDRR リビジョン** BCD コード
	13	**マイナー SDRR リビジョン** BCD コード
	14	**SDRR リビジョン文字** ASCII コード
	15	**SDRR-ID** LSB バイナリコード
	16	**SDRR-ID** MSB バイナリコード
	17	**メジャー Booter リビジョン** バイナリコード
	18	**メジャー Booter リビジョン** BCD コード
	19:20	*Aux.*Booter Revision バイナリコード（メジャー／マイナー）

F5 42 - Get HDD lightpath status（コンポーネントステータス信号の読み取り）

このコマンドは、Hard Disk Drive（HDD）スロットの状態に関する情報を返します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**42** コマンド指定子
	5	ステータス信号が読み取られるコンポーネントの**エントリ ID**（IPMI 1.5 Spec. の*表 37-12*）。
	6	ステータス信号が読み取られるコンポーネントの**エントリインスタンス**（0 ベース）。
	7	ステータス信号が関連するコンポーネントのステータスを報告するセンサの**センサタイプ**（IPMISpec. の*表 36-3*）。
	[8]	オプション（オプション） Bit 7:2 - 予約 Bit 1 ：完了コード 0x02 が削除される Bit 0 - 1 ：コンポーネントステータスセンサのリターン ID 文字列
応答データ	-	**BC**
	-	**F5**
	1	**完了コード** 01 = ステータス信号を取得できません 02 = コンポーネントがありません
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**信号状態：** 00 = OK 01 = 確認 02 = 故障前警告 03 = 故障
	6	**CSS と 物理 LED を使用可能：** Bit 6:0 - 0 = 物理 LED を使用不可 Bit 6:0 > 00 = 物理 LED を使用可能、単一または複数の色、コード Bit 7 = 0：CSS コンポーネントなし Bit 7 = 1：CSS コンポーネントあり

[7]	コンポーネントステータスセンサの ID 文字列の長さ （リクエストバイト 8 の Bit 0 が設定されている場合のみ存在）
(8 ～ m)	コンポーネントステータスセンサの ID 文字列（ASCII 文字）の長さ （リクエストバイト 8 の Bit 0 が設定されている場合のみ存在）

F5 43 - Get SEL entry long text

本コマンドは任意の SEL エントリをロングテキストに変換します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**43** コマンド指定子
	5:6	**レコード ID** SEL レコード 、LSB ファースト 0x0000: 最初のレコードを取得します。 0xFFFF: 最後のレコードを取得します。
	7	応答 SEL テキストの**オフセット**
	8	**MaxResponseDataSize** 応答の*変換済み SEL データ* サイズ（16:n）
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	次のレコード ID
	7:8	**実際の ID**
	9	**レコードタイプ**
	10:13	**タイムスタンプ**
	14	**重要度:** Bit 7: 0＝CSS コンポーネントなし 1 ＝ CSS コンポーネントあり Bit 6-4： 000 = INFORMATIONAL 001 ＝ MINOR 010 ＝ MAJOR 011 ＝ CRITICAL 1xx ＝ Unknown Bit 3-0： 0000 予備
	15	テキスト全体の**データ長**
	16:n	**変換済み SEL データ** 要求された部分 (n=16+ MaxResponseDataSize - 1)
	n + 1	**文字列終了** 「\0」という文字をつける

F5 45 - Get SEL Entry Text

本コマンドは任意のシステムイベントログ SEL エントリを ASCII テキストに変換します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**45** コマンド指定子
	5:6	SDR の**レコード ID**、LSB ファースト
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	**次のレコード ID**
	7:8	**実際の ID**
	9	**レコードタイプ**
	10:13	**タイムスタンプ**
	14	**重要度:** Bit7: 0=CSSコンポーネントなし 1 = CSS コンポーネントあり Bit 6-4： 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown Bit 3-0： 0000 予備
	15	**データ長**
	16:35	**変換済み SEL データ**

F5 B0 - Set Identify LED

本コマンドにより、サーバオン／オフの識別灯（青色）を切り替えることが可能です。さらに、識別灯に直接接続された GPIO の設定および読み込みが可能になります。

サーバ上の識別切り替えを使用して識別灯を切り替えることも可能です。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B0** コマンド指定子
	5	**識別灯：** 0：識別灯オフ 1：識別灯オン
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 B1 - Get Identify LED

本コマンドは、サーバの識別灯（青色）の状態に関する情報を返します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B1** コマンド指定子
応答データ	-	**BC**
	-	F5
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	識別灯の状態（ビット 0 のみが該当します。）

F5 B3 - Get Error LED

本コマンドは、サーバの Error LED（赤色）および CSS LED（黄色）の状態に関する情報を返します。Error LED はコンポーネントの最も重大なエラー状態を示します。CSS LED は、ユーザ自身が障害を修復できるかどうかを示します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B3** コマンド指定子
応答データ	-	BC
	-	F5
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**Error LED の状態：** 0：CSS off ／ GEL off 1：CSS off ／ GEL on 2：CSS off ／ GEL blink 3：CSS on ／ GEL off 4：CSS on ／ GEL on 5：CSS on ／ GEL blink 6：CSS blink ／ GEL off 7：CSS blink ／ GEL on 8：CSS blink ／ GEL blink

F5 DF - Reset Nonvolatile Cfg Variables to Default

本コマンドは、すべての不揮発性 IPMI 設定をデフォルト値に強制的に設定します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**DF** コマンド指定子
	5:8	43 4C 52 AA ＝ 'CLR'0xaa：セキュリティコード
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 E0 - Reset ConfigSpace variables to default

本コマンドは、すべての設定スペース変数をデフォルトに強制的に設定します。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**E0** コマンド指定子
	5:8	43 4C 52 AA ＝ 'CLR'0xaa：セキュリティコード
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 F8 - Delete User ID

システムでは最大 16 人のユーザがサポートされます。本コマンドは、iRMC S2/S3 ユーザを個別に削除することができます。

注意！

すべての iRMC S2/S3 ユーザを削除するとシステムを管理することができなくなります。

要求データ	-	**B8** NetFnlLUN：OEM/ グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**F8** コマンド指定子
	5:8	ユーザ ID（1 ～ 16）
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

12.2 SCCI およびスクリプト設定を使用した iRMC S2/S3 の設定

この節では以下について説明します。

– SCCI（**S**erverView **C**ommon **C**ommand **I**nterface）対応インターフェースを使用して iRMC S2/S3 を設定する方法

– iRMC S2/S3 のスクリプト設定

12.2.1 iRMC S2/S3 の設定データ

以下で説明するインターフェースは主にリモート設定を行うためおもので、SCCI 実装では**ありません**。SCCI コマンドと設定の定義、および SCCI ファイルフォーマットのみ使用します。

12.2.1.1 概要

iRMC S2/S3 は、NVRAM（不揮発性 RAM）の次の 2 つの個別のセクションにある内部設定データを保存します。

– FTS 固有の ConfigSpace データ。ファームウェアが固定の内部記述テーブルを使用してアドレス指定します。

– 製造メーカー固有のオリジナルの NVCFG データ。オフセット定義でアクセスします。

オリジナルの NVCFG データの設定データには、ConfigSpace アクセス手法でアクセスできるように、ファームウェアが内でマッピングされているものがあります。たとえば、iRMC S2/S3 の DNS サーバと DNS 設定に、IPMI OEM LAN 設定パラメータおよび ConfigSpace を使用してアクセスできます。どちらの手法も、オリジナルの NVCFG 領域内の下位レベルの同じ構造にアクセスします。

iRMC S2/S3 固有でない ServerView ソフトウェアコンポーネント（ServerView エージェントまたは Server Configuration Manager）は、標準の IPMI 関連のコマンド、および標準の IPMI ユーザ設定や IPv4 ネットワーク設定などの設定項目などをマッピングすることもあります。これにより、IPMI BMC 層と上位のソフトウェアレベル間に抽象化レベルを実装します。

SCCI は、Fujitsu が定義したジェネリックなアプリケーションプログラミングインターフェース（API）で、Server Management Controller ハードウェアおよび Server Management ソフトウェア（ServerView エージェントなど）に対応します。容易に拡張して、新しいコマンドや新しい設定項目に対応させることができます。SCCI のアーキテクチャの概要については、ServerView エージェントのオンラインヘルプを参照してください。

iRMC S2 ファームウェア 5.20A（IPv6 バージョン）より、iRMC S2/S3 は、iRMC S2/S3 内の */config URL* を使用したリモート設定と制限付きスクリプティングをサポートしています。

Web ベースのアクセスによる iRMC S2/S3 のリモート設定の利点

Web ベースのアクセスによるリモート iRMC S2/S3 設定には、次の利点があります。

– HTTP POST オペレーションを使用して、ファイルを iRMC S2/S3 にアップロードできます。特別なツールは必要ありません。認証された HTTP POST オペレーションをサポートする任意のジェネリックツールやスクリプティング環境を使用できます。サンプルスクリプトが ServerView Suite DVD 1 に収録されています。

– iRMC S2/S3 Web サーバのビルトイン認証と認証手法を使用できます。

– ローカル iRMC S2/S3 ユーザアカウントを使用する、RFC 2617 ベースの HTTP 1.1 Basic および Digest 認証をサポートします。

– 標準の HTTPS ベースのアクセスによるオプションの強力なビルトイン暗号化機能を装備しています。

– グローバルユーザアカウント（LDAP ディレクトリサーバによって管理されます）および HTTP 1.1 Basic 認証で使用できます。

  HTTP 1.1 Basic 認証を使用する場合、暗号化と機密保持上の理由から、HTTPS プロトコルを使用してユーザ名とパスワードの組み合わせを保護するようにしてください。

– XML ベースの設定ファイルフォーマットを使用できます。手作業でファイルを編集するか、リファレンスインストールまたは Server Configuration Manager からファイルをエクスポートするかを選択できます。

  SCCI ベースのインストール手法（Server Configuration Manager など）で設定ファイルを再利用できます。

– 新しい設定項目と新しくサポートされる SCCI コマンドを容易に拡張できます。

12.2.1.2 SCCI ファイルフォーマット

使用する XML 設定ファイル（*.pre*）のフォーマットは、Windows プラットフォームの ServerView エージェントと共にインストールされる、セットアップ設定ヘルプファイルから取得されます。この説明と iRMC S2/S3 固有の注意事項のコピーを以下に示します。

設定ファイルは、次の XML 構文がベースとなります。

– 各構成設定は、「<CMD>」で始まるシンプルな XML フラグメントで構成されます。

– 構成設定の完全なシーケンスは、「<CMDSEQ> および </CMDSEQ>」というタグのペアで囲まれます。

以下に、2 つの構成設定で構成される典型的なコマンドシーケンスの例を示します。

```
<CMDSEQ>
<CMD Context="SCCI" OC="ConfigSpace" OE="3800" OI="0" Type=
"SET">
<DATA Type="xsd::hexBinary" Len="1">04</DATA>
<CMD Context="SCCI" OC="ConfigSpace" OE="3801" OI="0" Type=
"SET">
<DATA Type="xsd::hexBinary" Len="1">00</DATA> </CMD>
</CMDSEQ>
```

Context を内部で使用して、オペレーションプロバイダを選択します。現在、サポートされるプロバイダは SCCI のみです。

SCCI プロバイダ固有のコマンドのパラメータ

以下の SCCI プロバイダ固有のコマンドを使用できます。

Operation Code（OC）
: コマンド／オペレーションコードを指定する 16 進値または文字列。

  iRMC S2/S3 は、制限された SCCI コマンドセットのみサポートします。サポートされるコマンドの一覧は、427 ページ の 表「iRMC S2/S3 でサポートされる SCCI コマンド」を参照してください。

Operation Code Extension（OE）
: 拡張されたオペレーションコードの 16 進値。デフォルト：OE=0

  ConfigSpace 読み書きオペレーションには、この値で ConfigSpace ID を定義します。

Object Index（OI）
: オブジェクトのインスタンスを選択する 16 進値。Default:OI=0"

Operation Code Type（Type）
: 構成設定の場合、値 GET（読み取りオペレーション）および SET（書き込みオペレーション）がサポートされます。デフォルト：Type= GET

  SET にはデータが必要です。適切なデータタイプを指定するには、下記の *Data（DATA）* パラメータを使用します。

Cabinet Identifier（CA）
: 拡張キャビネットを選択して、そのキャビネット ID 番号を使用できます。

  このパラメータをシステムキャビネットのリクエストに対して使用**しないでください**。

Data (DATA)

SET パラメータ（書き込みオペレーション）を指定する場合、データタイプ（Type パラメータ）と、場合によってはデータ長（LEN パラメータ）が必要です。

現在、以下のデータタイプがサポートされます。

– xsd::integer

整数値

例

```
<DATA Type="xsd::integer">1234</DATA>
```

– xsd::hexBinary

バイトストリーム。各バイトは 2 つの ASCII 文字でコード化されます。下記の例で示すように Len パラメータを使用して、ストリームの長さ（バイト数）を指定します。

データタイプ xsd::hexBinary は、制約なく使用できます。

例

4 バイト 0x00 0x01 0x02 0x04 のストリームは、以下の ASCII ストリームとしてコード化されます。

```
<DATA Type="xsd::hexBinary" Len="4">0001020304</DATA>
```

– xsd::string

通常、文字列の転送に使用されます。また、string タイプは、IPv4 アドレスおよび MD5 ベースのユーザパスワードに使用できます。この場合、文字列データは、受け付けられるターゲットフォーマットに内部で変換されます。

暗号化データの転送

Fujitsu 専用のデータ暗号化は、ユーザまたはサービス（LDAP/SMTP）アクセスパスワードや、iRMC S2/S3 の AVR ライセンスキーなどの機密データでサポートされます。*iRMC_PWD.exe* プログラムを使用して、パスワードデータを暗号化することができます（431 ページ の「iRMC_PWD.exe プログラムでの暗号化パスワードの生成」の項を参照）。

Encrypted="1" を <DATA> タグで設定して、書き込むデータを暗号化することを示す必要があります。

例

「Hello World」という文字列を転送する場合：

```
<DATA Type="xsd::string">Hello World</DATA>
```

claer（読み取り可能）テキストとしてパスワードを転送する場合：

```
<DATA Type="xsd::string">My Readable Password</DATA>
```

暗号化されたパスワードを転送する場合：

```
<DATA Type="xsd::string" Encrypted=
"1">TpVlTJwCyHEIsC8tk24ci83JuR9l</DATA>
```

IPv4 アドレス「192.23.2.4」を転送する場合：

```
<DATA Type="xsd::string">192.23.2.4</DATA>
```

注意！

`xsd::string` データタイプの使用は、読み込み可能な文字列、IP アドレス、MD5 ベースのユーザパスワードに限定されます。

その他のすべてのデータには、`xsd::hexbinary` データタイプを使用してください。

ä、ö、ü などの文字は、使用しているアプリケーションで実際に必要でない限り、文字列に直接指定しないでください。

SCCI および ConfigSpace インターフェースは、どちらも文字の暗号化情報を保存しません。つまり、US-ASCII 以外の文字は使用しているアプリケーションによって内部で解釈されるので、使用しないようにしてください。

特殊文字を実際に指定する必要がある場合、適切な BOM を含む UTF-8 フォーマットでファイルの編集と保存を行ってください。

Command Status（`Status`）

構成設定を転送すると、`Status` にオペレーションの結果が含まれます。オペレーションが正常終了した場合、値 `0` が返されます。

パブリックなすべての構成設定の仕様（ConfigSpace）については、*SCCI_CS.pdf* ファイルを参照してください。このファイルは、ServerView エージェントのインストールパッケージの *Help* フォルダの中にあります。また、*SCCI_CS.pdf* PRIMERGY Scripting Toolkit でも配布されます。

12.2.1.3 注意事項

.pre ファイルに指定されるすべてのコマンドは、通常順次に実行されます。以下については、このルールが除外されます。

– 壊れたネットワーク接続を回避するには、IPv4 および VLAN ネットワーク設定のコマンドをコマンドシーケンスの最後に実行します。

– 現在、IPv6 構成パラメータは、不揮発性の IPv6 構成パラメータの設定に限定されます。

  回避策として、次の手順を行うことができます。

  1. スクリプトを次のように調整します。

     a) スクリプトの開始時：IPv6 を無効にします。

     b) IPv6 パラメータを設定します。

     c) スクリプトの終了時：IPv6 を有効にします。

  2. IPv4 アドレスからスクリプトを実行します。

– SSL 証明書と関連の一致するプライベートキーは、コマンドシーケンスの最後に実行されます。両方のコンポーネントは、同じ *.pre* ファイルに保存されている必要があり、互いに一致することが確認されます。

– 管理対象サーバのパワーマネジメントオペレーション、または iRMC S2/S3 の再起動が必要な場合。

  個々のコマンドファイルでこれらのコマンドを実行するようにします（ただし、必須ではありません）。これを実現するには、設定オペレーションとパワーマネジメントオペレーションを別個のタスクに分割します。

– 連続するコマンドの実行間のオプションの時間遅延は、スクリプトの外部で実装します。

  たとえば、次の手順で実現することができます。

  1. スクリプトを別個のスクリプトに適切に分割します。

  2. クライアントの機能範囲を使用して、個々のファイルの送信間の時間遅延を挿入します。

12.2.1.4 iRMC S2/S3 からのエクスポート／iRMC S2/S3 へのインポート

iRMC S2/S3 Web インターフェースの「*iRMC S3 ファームウェア設定の保存*」ページで、現在の iRMC S2/S3 の設定データを設定ファイル（*.pre*）に保存（エクスポート）できます。また、既存の設定ファイル（*.pre*）の iRMC S2/S3 設定データをインポートできます。つまり、iRMC S2/S3 に設定データをロードできます（詳細は、173 ページ の「iRMC S2/S3 ファームウェア設定の保存 - ファームウェア設定の保存」の項を参照）。

あるいは、iRMC S2/S3 設定をインポートするために、HTTP POST オペレーションを使用して、該当する SCCI コマンドファイルを iRMC S2/S3 の */config URI* に送信することもできます。

12.2.2 iRMC S2/S3 のスクリプト設定

この節では、以下のトピックについて説明します。

– iRMC S2/S3 でサポートされる SCCI コマンド。

– iRMC S2/S3 のスクリプト設定用のさまざまなスクリプト言語の使い方。

– *iRMC_PWD.exe* プログラムを使用した、暗号化パスワードの生成手順。

12.2.2.1 iRMC S2/S3 でサポートされる SCCI コマンドの一覧

iRMC S2/S3 でサポートされる SCCI コマンドを 表 19 に示します。

SCCI OpCode	SCCI コマンド文字列	内容
0xE002	ConfigSpace	ConfigSpace 書き込み
0x0111	PowerOnCabinet	サーバの電源オン
0x0112	PowerOffCabinet	サーバの電源オフ
0x0113	PowerOffOnCabinet	サーバのパワーサイクル
0x0204	ResetServer	サーバのハードリセット
0x020C	RaiseNMI	NMI パルス（マスク不可割り込み）
0x0205	RequestShutdownAndOff	グレースフルシャットダウン、実行中のエージェントが必要
0x0206	RequestShutdownAndReset	グレースフルリブート、実行中のエージェントが必要
0x0209	ShutdownRequestCancelled	シャットダウンリクエストのキャンセル
0x0203	ResetFirmware	BMC リセットの実行
0x0250	ConnectRemoteStorageServer	スタンドアロンのリモートストレージサーバの接続または接続解除

Table 19: iRMC S2/S3 でサポートされる SCCI コマンド

12.2.2.2 cURL でのスクリプティング

オープンソースコマンドラインツール Curl で、URL 構文で指定したデータを転送できます。ソースコードの最新バージョンと、オペレーティングシステムのプリコンパイルバージョンは、*http://curl.haxx.se/* からダウンロードできます。

以下に、curl を使用して設定ファイルを iRMC S2/S3 に送信する方法についていくつかの例を示します。

curl コマンドラインオプションの詳細は、curl のマニュアルを参照してください。

– Basic 認証（デフォルト）とデフォルトの iRMC S2/S3 admin アカウントでの HTTP Access

```
curl --basic -u admin:admin --data @Config.pre
http://<iRMC S2/S3 IP address>/config
```

– Digest 認証とデフォルトの iRMC admin アカウントでの HTTP Access

```
curl --digest -u ad<iRMC S2/S3 IP address>min:admin --data
@Config.pre http://<iRMC S2/S3 IP address>/config
```

– 認証チェックなし（-k）で、Digest 認証とデフォルトの iRMC admin アカウントでの HTTPS Access

```
curl --digest -k -u admin:admin --data @Config.pre
https://<iRMC S2/S3 IP address>/config
```

– LDAP ユーザアカウントでの HTTPS Access

LDAP ユーザには Basic 認証を指定する必要があることにご注意ください。

```
curl --basic -k -u LDAPuser:LDAPpassword --data @Config.pre
https://<iRMC S2/S3 IP address>/config
```

12.2.2.3 Visual Basic（VB）スクリプトでのスクリプティング

次の VB スクリプトでは、設定ファイルを iRMC S2/S3 に送信します。

```
IP_ADDRESS = "<iRMC S2/S3 IP address>"
USER_NAME  = "admin"
PASSWORD   = "admin"

FILE_NAME  = ".\\ConfigFile.pre"

Const ForReading = 1
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile(FILE_NAME, ForReading)

' ------------------------------------------------------------
On Error Resume Next

Set xmlHttp = CreateObject("Microsoft.XMLHTTP")
xmlHttp.Open "POST", "http://"& IP_ADDRESS & "/config", False,
USER_NAME, PASSWORD
xmlhttp.setRequestHeader "Content-Type", "application/x-www-
form-urlencoded"
xmlHttp.Send objFile.ReadAll

Wscript.Echo xmlhttp.responsexml.xml
```

12.2.2.4 Python でのスクリプティング

```
#!/usr/bin/python3
import sys
import httplib2
from urllib.parse import urlencode

# ============================================================
# iRMC

USER = 'admin'
PWD  = 'admin'
IP_ADDR =  '192.168.1.100'
# ============================================================

h = httplib2.Http()

# Basic/Digest authentication
h.add_credentials(USER, PWD)

def doit(data,ausgabe=sys.stdout):
  try:
    resp, content = h.request("http://%s/config" % IP_ADDR,
    "POST", data)
    if resp['status'] == '200'
      data = content.decode('utf-8')
      print(data,file=ausgabe)
      else:
      print('STATUS:',resp['status'],file=ausgabe)
      print(str(resp),file=ausgabe)
  except Exception as err:
    print('ERROR:',str(err),file=ausgabe)
  print()


# Example 1 - send a configuration file to the iRMC S2/S3
try:
  data = open('ConfigFile.pre').read()
  doit(data)
except Exception as err:
  print('ERROR:',str(err),file=ausgabe)


# Example 2 - Set Config Space Values
# 0x200 (ConfCabinetLocation) and
# 0x204 (ConfSystemContact) direct from the script
#
LocationContact = '''<?xml version="1.0" encoding="UTF-8"
standalone="yes" ?>
```

```
<CMDSEQ>
  <!-- ConfCabinetLocation -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="200" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
  <!-- ConfSystemContact -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="204" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
</CMDSEQ>
'''

doit(LocationContact % ("Ostsee","Kiel"))
```

12.2.2.5 iRMC_PWD.exe プログラムでの暗号化パスワードの生成

Fujitsu Technology Solutions iRMC パスワード暗号化および確認ユーティリティ *iRMC_PWD.exe* は、SCCI スクリプティングで使用するための暗号化パスワードを生成できる Win32 プログラムです。*iRMC_PWD.exe* を使用して、シングルパスワードの暗号化と、スクリプト設定用の SCCI バッチファイルの生成の両方を行うことができます。

iRMC_PWD 標準コマンドオプション

[-h] [-?]
: このヘルプ。

[-v]
: 暗号化されたパスワード文字列を確認します。

[-o] <oid>
: 暗号化するデータのオブジェクト ID。

[-u] <username>
: 指定したオブジェクト ID のユーザ名（オプション）。

[-p] <password>
: 指定したオブジェクト ID のパスワード / / 確認する暗号化パスワード文字列。

[-x] <opCodeExt>
: 暗号化する ConfigSpace データの Opcode 拡張。

[-p] <password>
指定したオブジェクト ID のパスワード。
デフォルト：1452 (ConfBMCAcctUserPassword)

サポートされる値：

1273 - ConfAlarmEmailSMTPAuthPassword

[-p] <password>
指定したオブジェクト ID のパスワード。
デフォルト：1452（ConfBMCAcctUserPassword）

サポートされる値：

1452 - ConfBMCAcctUserPassword

1273 - ConfAlarmEmailSMTPAuthPassword

197A - ConfLdapiRMCgroupsUserPasswd

1980 - ConfBMCLicenseKey

iRMC_PWD コマンドライン出力オプション

[-b]
出力ファイルを WinSCU BATCH ファイルとして作成します。

[-f] <Output File>
出力ファイルの名前を指定します。
デフォルト：*iRMC_pwd.txt*
バッチモードのデフォルト：*iRMC_pwd.pre*

例

oid *2* を使用して、ユーザ名を `admin` に、パスワードを `SecretPassword` に設定／変更する `.pre` ファイルを生成するとします。

これを実現するには、以下のコマンドを入力します。

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b
```

iRMC_PWD が、433 ページ の図 226 に示される内容を使用して、*.pre* ファイルを生成します。

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b


<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CMDSEQ>
<!-- "ConfBMCAcctUserName" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1451" OI="2" Type="SET">
  <DATA Type="xsd::string">admin</DATA>
  <STATUS>0</STATUS>
</CMD>
<!-- "ConfBMCAcctUserPassword" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1452" OI="2" Type="SET">
  <DATA Type="xsd::string"
Encrypted="1">N2BZd3oLHAgc11pnHCAV9P/ItwRue4qBB3IU7Xsh</DATA>
  <STATUS>0</STATUS>
</CMD>
</CMDSEQ>
```

Figure 226: 生成される .pre ファイルの内容