ユーザガイド - 日本語

Fujitsu Server PRIMEQUEST 4000 Series

iRMC S6

コンフィグレーションとメンテナンス

2024 年 11 月版
CA92344-5407-05

DIN 9001 および ISO 27001 に準拠したドキュメントの作成

高い品質と情報セキュリティ基準に確保されるように、
このマニュアルは、ISO 9001 および ISO 27001
に準拠した Etteplan の品質管理システムの規定と情報
セキュリティマネジメントシステムを満たすように作成されました。
Etteplan Germany GmbH ¦ www.etteplan.com

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。

目次

1 はじめに **7**
1.1 目的と対象ユーザ 8
1.2 iRMC のマニュアル 8
1.3 本書の表記 9
2 iRMC の機能の概要 **11**
2.1 Embedded Lifecycle Management（eLCM） 19
2.2 ユーザインターフェース 23
2.3 アプリケーションプログラミングインターフェース（API） 24
2.4 使用される通信プロトコル 25
2.5 システム構成 27
2.5.1 OPL 28
2.5.2 システムボード（SB） 28
2.5.2.1 SB の電源のオン/オフ 30
2.5.2.2 SB の再起動 30
2.5.2.3 Home SB 31
2.5.2.4 非Home SB 31
2.5.2.5 Reserved SB 32
2.5.2.6 構成 32
2.5.3 パーティション 34
2.5.4 ネットワークの設定 35
2.5.4.1 外部通信 36
2.5.4.2 内部通信 37
2.5.5 電源 39
2.5.6 時間の設定 40
2.6 SB と iRMC のステータス LED 41
3 最初の手順 **43**
3.1 LAN インターフェースの設定 43
3.1.1 要件 43

3.1.2 LAN インターフェースのテスト 43
3.2 iRMC S6 への初回ログイン 44
3.2.1 要件 44
3.2.2 iRMC の工場出荷時のデフォルト 45
3.2.3 初回ログイン 46
3.2.4 ログアウト 49
4 証明書 **50**
4.1 サーバ証明書 51
4.1.1 セキュアな通信の証明書のインポート 51
4.1.2 証明書の生成 52
4.2 iRMC の CA 証明書 53
4.3 eLCM の CA 証明書 54
4.4 メール暗号化の S/MIME 証明書 55
5 ユーザ管理 **57**
5.1 「ユーザ管理」概念 57
5.2 ユーザ権限 60
5.3 ローカルユーザ管理 62
5.3.1 二要素認証（2FA） 63
5.3.1.1 ユーザアカウントの 2FA の有効化 64
5.3.1.2 2FA のセットアップ 64
5.3.1.3 エマージェンシーコードの使用 68
5.3.1.4 ユーザアカウントの 2FA の再構成 70
5.3.2 SSHv2 によるセキュアな認証 70
5.3.2.1 SSHv2 公開鍵と秘密キーの作成 71
5.3.2.2 SSHv2 公開鍵をアップロードする 75
5.3.2.3 SSHv2 公開鍵の使用 76
5.3.2.4 例: SSHv2 公開鍵 80
5.3.3 ローカル iRMC ユーザへの E メール警告の設定 80
5.4 グローバルユーザ管理 81
5.4.1 LDAP ディレクトリサービスを使用するユーザ管理の概念 82
5.4.1.1 ユーザロール 82
5.4.1.2 組織単位（OU）SVS 83

5.4.1.3 多部門サーバー、グローバルアクセス権限 85
5.4.1.4 SVS: ロールにより定義される許可プロファイル 86
5.4.2 コラボレーションの構成ステップ 88
5.4.3 SVS_LdapDeployer ユーティリティ 89
5.4.3.1 SVS_LdapDeployer の構文 89
5.4.3.2 SVS_LdapDeployer の起動 91
5.4.3.3 例 92
5.4.4 Microsoft Active Directory による iRMC ユーザ管理 93
5.4.4.1 Active Directory サーバ上の iRMC LDAP/SSL アクセスの設定 93
5.4.4.2 iRMC ユーザへのユーザロールの割り当て 97
5.4.5 Novell eDirectory によるグローバル iRMC ユーザ管理 103
5.4.5.1 iRMC ユーザ管理の Novell eDirectory への統合 103
5.4.5.2 iRMC ユーザの許可グループへの割り当て 107
5.4.5.3 Novell eDirectory 管理のためのヒント 110
5.4.6 OpenLDAP によるグローバル iRMC ユーザの管理 112
5.4.6.1 新しい iRMC ユーザの作成 113
5.4.6.2 プリンシパルユーザの作成 114
5.4.6.3 OpenLDAP 管理のヒント 115
5.4.7 グローバル iRMC ユーザへの Eメール警告の設定 116
5.4.7.1 グローバル Eメール警告送信 116
5.4.7.2 警告ロールの表示 119
5.4.7.3 iRMC ユーザへの警告ロール割り当て 121
5.4.8 LDAP 認証の iRMC の設定 121
5.4.9 ユーザ許可の設定 124
6 OS のリモートインストール 127
6.1 OS のインストールの一般的な手順 127
6.2 バーチャルメディアとしてのストレージメディアの接続 129
6.3 管理対象サーバのブート 131
6.4 管理対象サーバへの Windows のインストール 134
6.5 管理対象サーバへの Linux のインストール 135
6.6 管理対象サーバへの ESXi のインストール 137

7 ファームウェアのアップデート 140
7.1 ファームウェアセレクタ 141
7.2 ゴールデンイメージ 141
7.3 Web インターフェースを使用したファームウェアアップデート 143
7.4 ファームウェアダウングレード 144
7.5 ファームウェアの整合 145
7.6 ファームウェアのバックアップ 146
8 RAID 構成 148
8.1 ハードウェア RAID 148
8.1.1 サポートされる RAID レベル 149
8.1.2 完全性チェック 151
8.1.3 RAID コントローラ 152
8.1.3.1 物理ディスク 154
8.1.3.2 論理ドライブ 156
8.1.4 論理ドライブの作成 157
8.1.5 論理ドライブの削除 158
8.2 ソフトウェア RAID 158
9 トラブルシューティング 159
9.1 正常性情報の詳細確認 160
9.2 ログ情報 162

1 はじめに

最近のサーバシステムはますます複雑化しており、それに従ってこのようなサーバの管理に関する要件も拡大しています。

iRMC（integrated Remote Management Controller）は、統合された LAN 接続と拡張機能を持つ BMC を表します。このように、iRMC は PRIMEQUEST サーバをシステムの状態に関係なく包括的に制御する機能を提供します。特に、iRMC では、PRIMEQUEST サーバの Out-Of-Band 管理（Lights Out Management - LOM）が可能です。Out-Of-Band 管理では、サーバの電源がオンになっているかどうかに関係なくシステム管理者がリモート制御を使用してサーバを監視および管理できるようにする専用の管理チャネルを使用します。

図 1: PRIMEQUEST サーバのシステムボード上の iRMC S6

PRIMERGY または PRIMEQUEST サーバのシステムボードにある自律型のシステムとして、iRMC は独自の OS、独自の Web サーバ、分離されたユーザ管理、および独立した警告管理を備えています。サーバが電源オフまたはスタンバイモードになっていても、iRMC の電源は入った状態で維持されます。通信は LAN 接続経由で行われ、Fujitsu PRIMEQUEST サーバで共有したり、システム管理専用に使用したりできます。

PRIMEQUEST サーバの Out-Of-Band 管理が可能なほかに、内蔵 SD カードを搭載した iRMC の拡張機能により、PRIMEQUEST サーバのライフサイクルを包括的に管理することができます。ライフサイクル管理は、大部分が iRMC に統合され（embedded）、iRMC によって完全に制御されるため、「embedded Life Cycle Management（eLCM）」と呼ばれます。

eLCM の一部の機能では、iRMC が管理対象サーバで実行中の ServerView Agentless Service（およびオプションの ServerView PrimeUp）と通信して連携

する必要があります。また、ServerView Agentless Service と通信することにより、iRMC に追加の in-band 情報が提供されます。

1.1 目的と対象ユーザ

この取扱説明書は、ハードウェアとソフトウェアについて十分な知識を持っているシステム管理者、ネットワーク管理者、およびサービス専門家を対象とします。IPMI の設定に関する基本的な情報と、以下の事項について詳しく扱います。

- 「**概要**」では、iRMC の機能の基本的事項を取り扱います。
- 「**最初の手順**」では、LAN 接続の情報と、iRMC へのログイン方法について説明します。
- 「**証明書**」では、iRMC で証明書を使用する理由と方法を説明します。
- 「**ユーザ管理**」では、iRMC 関連のユーザ管理について説明します。
- 「**リモートインストール**」では、iRMC によるオペレーティングシステムのインストール方法について説明します。
- 「**ファームウェアのアップデート**」では、iRMC のファームウェアをアップデートする方法について説明します。
- 「**RAID 構成**」では、HW RAID の一般的な原理と、それを iRMC で実装する方法について、大まかに説明します。
- 「**トラブルシューティングで**」は、HW エラーが発生したときの主要な問題を説明します。

1.2 iRMC のマニュアル

取扱説明書は、Fujitsu PRIMEQUEST 4000 シリーズの iRMC S6 ファームウェアについて記述するマニュアルセットの一部です。iRMC S6 のマニュアルセットには、以下の取扱説明書が含まれています。

- 『iRMC S6 コンセプトとインターフェース』（CA92344-5402）
- 『iRMC S6 Web インターフェース』（CA92344-5404）
- 『iRMC S6 コンフィグレーションとメンテナンス』（CA92344-5406）

本 iRMC バージョンを実行するターゲットシステムは、PRIMEQUEST 4000 マシンです。

関連資料

iRMC Redfish API の仕様書では、Fujitsu Redfish API のコマンドとパラメータの詳細情報を記載しています。

iRMC『Redfish API』のホワイトペーパーでは、iRMC Redfish API の一般的な処理方法を説明しています。

iRMC RESTful API の仕様書では、iRMC RESTful API のコマンドとパラメータの詳細情報を記載しています。

『PRIMEQUEST 4000 シリーズ REMCS サービスインストールマニュアル』では、リモートカスタマーサポートシステム（REMCS）のインストールおよび通信の設定方法について説明します。

PRIMEQUEST ハードウェアおよび ServerView ソフトウェアのすべてのドキュメントは、Fujitsu サポートページからオンラインで入手できます。

PRIMEQUEST のドキュメント一式は、DVD ISO イメージとしてダウンロードすることもできます。

1.3 本書の表記

以下の表記規定を使用します。

表記	説明
	健康上のリスク、データの損失やデバイスの損傷の可能性があるさまざまな種類のリスクを示します。
	追加関連情報とヒントを示します。
太字のテキストおよびかぎ括弧（「」）	インターフェース要素の名前を示します。
等間隔表示	パスおよびファイル名など、テキストブロック内で出力やシステム要素を示します。
等間隔表示	テキストブロックの外側にキーボードを使用して入力するコマンド、システム出力、構文および命令文を示します。
monospace semibold(太字の等間隔表示)	キーボードを使用して入力する命令文の処理例を示します。
青字の文字列	関連するトピックへのリンクを示します。

テーブル 1: 本書の表記

表記	説明
ピンクの文字列	すでに表示したリンクを示します。
<文字>	実際の値に置き換える必要のある変数を示します。
[文字]	オプション（構文）を示します。
[key]	キーボード上のキーを示します。大文字のテキストを入力する場合、[Shift] キーを指定します。たとえば、A を入力する場合 [Shift] + [A] キーを押します。2 つのキーを同時に押す場合は、2 つのキーをプラス記号で連結して示します。
かぎ括弧（「」）二重かぎ括弧（『』）	かぎ括弧（「」）は、章の名前を示します。 二重かぎ括弧（『』）は、他のマニュアル名などを示しています。

テーブル 1: 本書の表記

画面

いくつかの画面はシステムに依存しているため、表示される詳細はシステムによって異なります。メニューオプションとコマンドには、システム固有の違いがある場合もあります。

2 iRMC の機能の概要

iRMC では、提供される広範囲の機能をデフォルトでサポートしています。Advanced Video Redirection（AVR）、バーチャルメディア、embedded Lifecycle Management を使用すると、iRMCでは、PRIMEQUEST サーバのリモート管理に高度な追加機能も提供されます。

以下の機能には特殊なライセンスキーは不要です。

アカウントのロック

ログインに指定した回数失敗すると、ユーザアカウントを指定した期間または永久にロックすることができます。

Advanced Video Redirection (AVR)

iRMC は HTML5、Java または VNC を介してビデオリダイレクションをサポートします。

Java または HTML5 を使用した AVR により、以下の利点があります。

- 標準的な Web ブラウザ上での操作。管理用サーバにその他のソフトウェアをインストールする必要はありません。ただし、Java アプレットを使用する場合は、Java Runtime Environment が必要です。また、Web ブラウザが HTML5 に対応している必要があります。
- システムに依存しないグラフィカルおよびテキストコンソールリダイレクション（マウスおよびキーボードを含む）
- ブート監視、BIOS 管理、および OS の操作のためのリモートアクセス。
- AVR は、他の場所からパーティションを操作するための最大 2 つの同時「仮想接続」をサポートしています。また、ハードウェアビデオ圧縮を使用してネットワーク上の負荷を削減します。
- Java を使用した AVR セッション中に、ISO イメージはマウントできません。
- ローカルモニタの電源切断のサポート: AVR セッション中にローカル SB 画面で実行されるユーザ入力およびアクションを権限のない者が見ることができないようにするために、AVR セッション中に監視対象 SB のローカル画面の電源を切断することが可能です。
- 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。

警告管理

iRMC の警告管理機能は、警告転送のために以下のオプションを提供しています。

- SNMP を使用して PET（Platform Event Trap）が送信されます。
- Eメールで直接警告を送信します。

また、iRMC は、関連するすべての情報を ServerView Agentless Service に供給します。

BMC の基本的な機能

iRMC は、電圧監視、イベントログ、リカバリ制御など、BMC の基本的な機能をサポートしています。

ブラウザによるアクセス

iRMC は、管理サーバによって標準的な Web ブラウザからアクセスできる独自の Web サーバを備えています。

CAS ベースのシングルサインオン（SSO）認証

iRMC は CAS（Centralized Authentication Service）設定をサポートしており、CAS ベースの SSO 認証用の iRMC 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 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 は、自動ネットワーク設定をサポートしています。これにはデフォルトの名前があり、DHCP サポートは iRMC が DHCP サーバから IP アドレスを取得するようにデフォルトで設定されています。iRMC 名は、DNS（Domain Name System）によって登録されます。最大 3 つの DNS サーバがサポートされています。DNS/DHCP が使用できない場合、iRMC は静的 IP アドレスもサポートしています。

保守ランプ

保守 LED は、常に監視対象パーティションの状態を示します。

ディレクトリサービスを使用するグローバルユーザ管理

iRMC のグローバルユーザ ID は、ディレクトリサービスのディレクトリに保管されています。これにより、ユーザ ID を中央サーバで管理できます。そのため、 ネットワークでこのサーバに接続されているすべての iRMC で、ユーザ ID を使用することができます。

iRMC ユーザ管理では、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、Open DJ、Apache DS

「ヘッドレス」のシステム動作

監視対象 SB にマウス、モニタ、キーボードを接続する必要はありません。これには、コストが削減され、ケーブル配線がシンプルになり、セキュリティが向上するなどのメリットがあります。

ID LED

たとえば、フル装備のラックに取り付けられた場合に、システムの識別を容易にするために、iRMC Web インターフェースから ID ランプ を有効にすることができます。

iRMC 間の監視

2 つの SB 上の iRMC はプライベート LAN と GPIO の 2 つのインターフェースを介して接続されます。プライベート LAN を使用するソケット通信（TCP/UDP）を介して、1 つの iRMC がパートナー iRMC のサバイバル状態を常に監視します。パートナー iRMC が 180 秒以上応答しない場合、エントリが SEL に書き込まれます。

LAN

監視対象 SB の Management LAN ユニット（MLANU）には 3 つのポートがあります。

- Management LAN はユーザポートとも呼ばれ、関連するパーティションの iRMC の IP アドレスを示します。
- Maintenance LAN は CE ポートとも呼ばれ、フィールドエンジニアがメンテナンスタスクに使用するポートです。
- RECMS ポートは、REMCS センタに送信されるレポートに使用されます。

スパナのマークが付いているポートが iRMC に割り当てられています。ユーザポートは 2 つの MLANU で冗長にすることができます。いずれかの MLANU のユーザポートは、各パーティションの iRMC Web インターフェースにアクセスできます。

LAN over USB

LAN over USB で呼び出されたインターフェースにより、監視対象 SB と iRMC との間でインバンド通信が可能になります。この通信により、監視対象 SB から iRMC へのインターフェースが追加され、Redfish インターフェースや SSH によるアクセスに使用されます。また、監視対象 SB から iRMC への Redfish アクセスなど、Management LAN と業務 LAN との間のショートカットを防ぎます。詳細は、『iRMC S6 - コンセプトとインターフェース』取扱説明書を参照してください。

ローカルユーザ管理

iRMC には、固有のユーザ管理方法があり、最大 16 人のユーザをパスワード付きで作成し、それぞれが属するユーザ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。

ネットワークボンディング

iRMC のネットワークボンディングは、Ethernet ネットワークアダプタの故障時の冗長を目的として設計されています。そのため、iRMC ネットワーク管理トラフィックは、単一物理リンクの故障により発生するサービスロスから保護されます。

iRMC はアクティブバックアップモデルのみサポートします。つまり、リンクが故障するまで 1 つのポートがアクティブで、もう 1 つのポートは MAC を引き継いでアクティブになります。

パスワードポリシー

セキュリティ上の理由から、パスワードポリシーは慎重に練られています。パスワードは 12 文字以上で、英数字と特殊文字を組み合わせる必要があります。

プラットフォームファームウェアの復元（PFR）

BIOS または iRMC ファームウェアのイメージファイルが破損しているか、変更されている場合は、iRMC が破損または変更されたイメージファイルをゴールデンイメージで自動的に修復します。

消費電力制御

iRMC では、監視対象 SB に対する包括的な消費電力制御を行うことができます。また、iRMC が監視対象 SB に対して電力消費を制御するために使用するモードを指定できます。これらのモードは必要に応じて切り替えることができます。

電源 LED

電源 LED は、SB のスイッチが現在オンになっているか、オフになっているかを知らせます。ServerView Agentless Service がインストールされ、実行されている場合、電源の現在の状態に応じて複数の電源動作が可能になります。

電源制御

システムの状態に関係なく、リモートワークステーションから監視対象 SB の電源オン/オフを以下の方法で切り替えることができます。

- iRMC Web インターフェースを使用する
- AVR ウィンドウの「**電源**」メニュー
- Remote Manager またはコマンドラインインターフェースを使用する
- スクリプトで行う

電源

PRIMEQUEST 4000 には最大 4 台のホットプラグ電源ユニットがあり、主電源 100 V - 127 V または 200 V - 240 V で 2200 W（DPS-2200AB）またはr 2600 W（DPS-2600DB）です。

1 台の電源ユニットが故障しても、残りの電源ユニットが操作を停止せずに継続します。故障した電源ユニットは操作中に交換できます。

RAID 設定

次のレベルの RAID 構成の設定および管理ができます。

- RAID-0
- RAID-1
- RAID-1E
- RAID-5
- RAID-6
- RAID-10
- RAID-50
- RAID-60

システムイベントログ（SEL）のの表示、フィルタリングおよび保存

次のインターフェースから選択して、SEL の内容を表示、保存、削除できます。

- iRMC Web インターフェース
- iRMC の Telnet/SSH ベースのインターフェース（Remote Manager）
- Redfish API を使用してスクリプトで行う

内部イベントログ（IEL）の表示、フィルタリングおよび保存

次のインターフェースを使用して、IEL の内容を表示、保存、削除できます。

- iRMC Web インターフェース
- iRMC の Telnet/SSH ベースのインターフェース（Remote Manager）
- Redfish API を使用してスクリプトで行う

REMCS

REMCS（リモートカスタマーサポートシステム）は、サーバのハードウェア構成情報を収集し、サーバの問題を監視し、設定されている場合は REMCS センタにレポートします。REMCS センタとの通信は iRMC で処理されます。iRMC は各パーティションからの情報をまとめて、REMCS センタに送信します。

E-mail による REMCS 通報はできません。REMCS リンクの詳細については、『PRIMEQUEST 4000 series REMCS 導入マニュアル』を参照してください。

セキュリティ（TLS、SSH）

Web サーバへのセキュアな通信と、マウスやキーボードを含む安全なグラフィカルコンソールリダイレクションを、 HTTPSを使用して提供します。Remote Manager を使用して iRMC にアクセスするように、SSH メカニズムを使用して保護され、暗号化された接続を設定できます。Remote Manager は、iRMC のテキストベースのユーザインターフェースです。

シンプルな設定 - インタラクティブ/スクリプトベース

iRMC の設定には、以下のツールが使用できます。

- iRMC Web インターフェース
- プロファイル管理
- Redfish API
- Remote Manager
- RESTful API
- ServerView Operations Manager
- SCCI API
- UEFI BIOS セットアップ

IPMIVIEW でスクリプトを使用して設定を行うこともできます。これは、SB がまず ServerView Installation Manager を介して設定されるときに iRMC を設定することが可能なことを意味します。スクリプトおよびプロファイルに基づいて多数の SB を設定することも可能です。

SNMPv1/v2c/v3 のサポート

SNMP サービスを、IPMI を介して SNMP SC2 MIB（Sc2.mib）、SNMP MIB-2、SNMP OS.MIB、SNMP RAID.MIB、SNMP STATUS.MIB 上の SNMPv1/v2c/v3 GET 要求をサポートする iRMC に設定できます。

SNMP サービスが有効になっている場合、ファンや温度センサーなどのデバイスの情報を SNMP プロトコル経由で取得でき、SNMP Manager を実行する任意のシステムで表示できます。

さらに SNMP トラップを、トラップの宛先設定で指定された受信先に送信できます。詳細は、『iRMC S6 - コンセプトとインターフェース』取扱説明書を参照してください。

テキストコンソールリダイレクション

Telnet/SSH クライアントを使用して iRMC への Telnet/SSH セッションを確立して、テキストベースの Remote Manager にアクセスできます。Remote Manager では、iRMC への限定的なメニュー ベースのインターフェースがあります。Telnet のほかに、SOL（serial over LAN）および SSH（Secure Shell）のサポートもあります。

二要素認証

ローカル iRMC ユーザアカウントは、TOTP を介した二要素認証を使用するように設定できます。TOTP は Time-based One-Time Password の訳語で、二要素認証（2FA）の共通フォームです。現在の時刻を入力として使用する標準化されたアルゴリズムにより、一意の数値パスワードを生成します。時間ベースのパスワードはオフラインで使用でき、ユーザにとってわかりやすく、2 番目の要素として使用するとアカウントのセキュリティが向上します。

バーチャルメディア

バーチャルメディア機能により、リモートのワークステーションに存在しているか、Remote Image Mount 機能を使用したネットワークで一元的に使用可能な「仮想」ドライブが使用できます。

バーチャルメディアで使用可能な「仮想」ドライブは、ローカルドライブとほぼ同じ方法で管理され、以下の選択肢を提供します。

- データの読み取りおよび書き込み
- バーチャルメディアからのブート
- ドライバおよびアプリケーションのインストール

バーチャルメディアは、以下の種類のデバイスをサポートして、リモートワークステーション上の「バーチャルドライブ」を提供します。

- CD/DVD ドライブ
- CD/DVD イメージ
- HDD/USB 物理および論理ドライブ（サポートされる Web ブラウザを Windows の管理者として実行する必要があります）
- HDD/USB イメージ
- バーチャルメディアウィザード経由で使用される共有フォルダ

リモートイメージマウント機能により、イメージは「バーチャルドライブ」という形態でネットワーク共有に一元的に提供されます。

Virtual Network Computing（VNC）

監視対象 SB にリダイレクトするために、VNC ビューワを使用することもできます。VNC はオープンソースでプラットフォームに依存しません。GUI ベースのオペレーティングシステム用および Java 用の数多くのクライアントとサーバがあります。同時に 2 つのクライアントを VNC サーバに接続できます。コントロールのリダイレクトには最初のセッションのみ使用できます。他のセッションは読み取り専用モードでのみ動作します。

- iRMC に実装される VNC サーバは、監視対象 SB のいくつかの画面を共有し、クライアントでそのコントロールを共有させることができます。
- VNC クライアント（またはビューワ）は、SB から発生する画面のデータを表示するプログラムで、サーバからアップデートを受け取り、収集したローカル入力を VNC サーバに報告することによってサーバを制御します。
- VNC プロトコル（RFB プロトコル）は、サーバからクライアントへの 1 つのグラフィック プリミティブの送信と、クライアントからサーバへのイベントメッセージの送信に基づく、シンプルなプロトコルです。

VNC セッションを使用するには、マシンに、TightVNC や RealVNC などのサードパーティの VNC クライアントソフトウェアが必要です。TightVNC などの一部の VNC クライアントは、初回サインイン段階を過ぎると接続を暗号化しません。セキュアな接続を行うには、SSH（Secure Shell）トンネルを使用して VNC 接続をトンネリングします。

SSH を通じて VNCをトンネリングする場合は、PuTTY を使用して iRMC に接続することを推奨します。

2.1 Embedded Lifecycle Management（eLCM）

標準的な機能とは別に、iRMC は embedded Lifecycle Management（eLCM）もサポートしています。この拡張機能には有効なライセンスキーが必要で、別途購入できます。

Fujitsu PRIMEQUEST 4000 サーバの embedded Lifecycle Management（eLCM）は、一般的なルーチン管理タスクをサポートしています。システム管理者は、サーバ管理のプロセスを簡素化し、高度に統合し、自動化することができます。

eLCMは、USB、CD、DVD などの外部メディアを使用する必要なく、サーバ内で直接使用可能な（組み込まれた）管理機能を拡張します。ユーザは、組み込まれた下記の ServerView 機能にアクセスできます。

- embedded Installation Management（eIM）は、ServerView Installation Manager に相当する eLCM です。eIM とリポジトリは iRMC S6 SD カードに保存されるので、Fujitsu PRIMEQUEST システムをインストールするために外部の ServerView メディアをセットアップする必要はありません。

- embedded RAID Management（eRM）は、ServerView RAID Manager に相当する eLCM として使用することができ、RAID 管理に関して eIM を補完します。
- 埋め込みオフラインおよびオンラインアップデート（eUM）は、ServerView Update Manager モジュールの eLCM エディションです。オンラインアップデートでは、サーバ OS（およびオプションの ServerView PrimeUp）の実行中に BIOS およびコントローラファームウェアをアップデートできます。オフラインアップデートでは、管理対象サーバで、ネットワークやストレージのコントローラファームウェアなどのシステムコンポーネントをアップデートできます。
- 高度に自動化されたオフラインおよびオンラインアップデートに対して、eLCM シンプルアップデートでは個々のコンポーネントを必要なバージョンにアップデートできます。コンポーネントに応じて、オンラインまたはオフラインモードを利用できます。
- 埋め込みカスタムイメージでは、iRMC SD カードに ISO イメージをダウンロードできる URL を指定できます。
- eLCM PrimeCollect は、サーバ誤動作時のエラー情報などの、Fujitsu PRIMEQUEST サーバのハードウェアおよびソフトウェアに関する詳細情報を収集して保存します。収集された情報は、ZIP ファイル形式で iRMC S6 SD カードに保存されます。

アップデートリポジトリ

eLCM アップデート管理およびデプロイメントは、リポジトリサーバを使用して、ダウンロード用の関連パッケージを提供します。

デフォルトのアップデートリポジトリ：https://support.ts.fujitsu.com

効率的なアクセスを行うために、デプロイメントリポジトリのコンテンツが以下の地域にミラーリングされます。

- フランス : https://webdownloads.ts.fujitsu.com
- オーストリア : https://webdownloads1.ts.fujitsu.com
- ドイツ : https://webdownloads2.ts.fujitsu.com
- USA : https://webdownloads3.ts.fujitsu.com

セキュリティ上の理由で、iRMC をインターネットに直接接続することはできません。ただし、ServerView Update Repository ソフトウェアを使用して、現地データセンターやネットワークの最も近いリポジトリをミラーリングすることができます。

VMware HCL のサポート

VMware ESXi OS を搭載した管理対象サーバのアップデート準備中に、インベントリデータは HCL ファイルと比較されます。HCL ファイルはアップデートリポジトリ

からダウンロードされます。このリストは、VMware が発行する認定サーバ設定の情報に基づいています。比較結果に応じて、以下の処理が実行されます。

- コンポーネントにエントリがない: 最も新しいバージョンがアップデートリストに追加されます。
- コンポーネントにエントリがある: 最も新しい認定済みバージョンがアップデートリストに追加されます。

「アップデート」設定の VMware HCL 検証をスキップできます。この設定は ESXi および ServerView CIM プロバイダがインストールされているシステムにのみ影響します。

パフォーマンスの向上

eLCM は、サーバの OS で実行中のエージェントタイプや管理ソフトウェアを必要とする従来のサーバ管理をバイパスします。管理ソフトウェアを iRMC に変更すると、管理対象サーバのパフォーマンスが向上します。

eLCM がサーバの OS で実行中でなければならない可能性のあるソフトウェアは、ServerView Agentless Service コンポーネントのみです。Agentless Service は、HTI（High-Speed Transfer Interface）を使用して iRMC S6 とのみ通信するため、サーバ OS のフットプリントは非常に小さく、システム全体のパフォーマンスにほとんど影響を及ぼしません。

ServerView Service Platform（SV SP）が embedded Lifecycle Management 内で使用されます。これは、PRIMEQUEST サーバ内部の内蔵 eLCM SD カードに保存され、eLCM によって管理される、ISO イメージです。

これらの機能には、他の運用シナリオもサポートされています。

コンソールを使用する対話的運用（物理的またはリダイレクション）

1. ターゲットシステムの電源を入れます。
2. POST（Power-On Self-Test）中に、[F5] を押します。
3. 表示される eLCM メニューで、使用する機能を選択します。
    - システム構成とインストール
    - RAID 構成
4. プラットフォームが起動されたら、コンソールに表示される手順に従います。

iRMC Web インターフェースによる無人運用

1. 目的のシステム構成および OS インストールを指定するプロファイルファイルを作成します。プロファイルの処理は、『FUJITSU Server PRIMEQUEST 4000 Series Business Model iRMC S6 - Concepts and Interfaces』取扱説明書に記載されています。
2. iRMC Web インターフェースを起動して、「**デプロイメント**」ページを開きます。
3. 目的の起動モードとして、「Extensible Firmware Interface ブート (EFI)」または「レガシシーブート（PC 互換）」を設定します。
4. プロファイルファイルをアップロードします。
5. 「**デプロイメントの開始**」を選択して、デプロイメントプロセスを開始します。

Redfish API による無人運用

1. 目的のシステム構成および OS インストールを指定するプロファイルファイルを作成します。プロファイル処理については、『iRMC S6 - コンセプトとインターフェース』取扱説明書を参照してください。
2. Redfish のアクション `/redfish/v1/Systems/0/Oem/ts_fujitsu/ProfileManagement/Actions/FTSProfileManagement.ApplyProfile` を使用してプロファイルを適用します。詳細については、iRMC Redfish API の仕様書を参照してください。

RESTful API による無人プロセス “SysRollOut Service”

詳細については、RESTful API のホワイトペーパーを参照してください

2.2 ユーザインターフェース

iRMC は以下のようなユーザインターフェースを提供します。

- iRMC Web インターフェース（Web インターフェース）

  iRMC Web サーバへの接続は、標準的な Web ブラウザ（Microsoft Edge、Mozilla Firefox、Google Chrome など）を使用して確立します。

  特に、iRMC の Web インターフェースにより、すべてのシステム情報およびファン速度、電圧などのセンサからのデータにアクセスできます。テキストベースのコンソールリダイレクションおよびグラフィカルコンソールリダイレクション（ビデオリダイレクション - AVR）を設定することもできます。また、管理者は Web インターフェースを使用して iRMC 全体を設定できます。

  HTTPSで iRMC Web サーバへのセキュアなアクセスを実現します。Web インターフェースは HTTPS 接続をサポートします。HTTP リンクは HTTPS にリダイレクトされ、セキュアなアクセスを保証します。

  Web インターフェースを使用した iRMC の操作は、『iRMC S6 - Web インターフェース』取扱説明書に記載されています。

- Remote Manager: LAN を使用したテキストベースの Telnet/SSH インターフェース

  リモートマネージャは、Telnet/SSH クライアントから直接呼び出すことができます。

  リモートマネージャのテキストベース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リダイレクションを開始することもできます。SSH（Secure Shell）を使用してリモートマネージャを呼び出した場合、リモートマネージャと管理対象サーバの間の接続は暗号化されます。

  Remote Manager を使用した iRMC の操作は、『iRMC S6 - コンセプトとインターフェース』取扱説明書に記載されています。

2.3 アプリケーションプログラミングインターフェース（API）

iRMC S6 はスクリプト設定で APIs（アプリケーションプログラミングインターフェース）をサポートしています。スクリプトでは、環境の要件に従って、設定する必要がある iRMC は 1 つだけです。この設定は、サーバに 1 台ずつアクセスしなくても、その他のすべての PRIMEQUEST サーバにアップロードできます。

- Redfish

  Redfish は DMTF 規格仕様およびスキーマで、RESTful インターフェースを規定しています。広く普及していることを考慮して選択した、さまざまな IT テクノロジーを利用しています。これらのテクノロジーは、Python、Java、PowerShell、C などの一般的なプログラミングおよびスクリプト言語を使用してサーバを管理できる、新たな基盤を較正します。

- RESTful

  Representational state transfer は、インターネット上のコンピュータシステムの相互運用性を実現する方法です。REST 準拠の Web サービスでは、均一で定義済みのステートレス操作を使用して、要求側のシステムは Web リソースのテキスト表現にアクセスし、操作できます。

- SCCI

  Server Control Command Interface は、Fujitsu が各種のサーバ管理コントローラハードウェアおよびソフトウェアに対して定義した、汎用 API です。新しいコマンドや新しい構成アイテムを含むよう、簡単に拡大できます。

詳細は、『iRMC S6 - コンセプトとインターフェース』取扱説明書を参照してください。

2.4 使用される通信プロトコル

iRMC では、通信に以下のプロトコルおよびデフォルトポートを使用します。

接続のリモート側	通信方向	接続の iRMC 側（ポート番号/プロトコル）	設定可能	デフォルトで有効
CAS/シングルサインオン	↔	3170/TCP	はい	はい
Email/SMTP	↔	25/TCP	はい	いいえ
LDAP	↔	389/TCP/UDP	はい	いいえ
HTTPS（Web インターフェース、Redfish API、RESTful API など）	↔	443/TCP	はい	はい
RFB（VNC を使用した AVR）	↔	5900/TCP	はい	いいえ
RMCP	↔	623/UDP	はい	はい
SNMP	↔	161/UDP	はい	いいえ
SNMP トラップ	→	162/UDP	いいえ	はい
SSH	↔	22/TCP	はい	はい
Telnet	↔	3172/TCP	はい	いいえ
TFTP /repository	↔	69/UDP	いいえ	いいえ

テーブル 2: 通信プロトコル

次の表に、iRMC および SMTP サーバ間の接続と、両サイドの設定に応じた接続の確立およびセキュアの可否について示します。

iRMC SNMP ポート番号	iRMC SMTP SSL	メールサーバ SMTP ポートセキュリティ	接続
465	はい	なし	確立されない
465	はい	STARTTLS 任意	確立されない
465	はい	STARTTLS 必須	確立されない
465	はい	SSL/TLS	セキュア
465	いいえ	なし	非セキュア
465	いいえ	STARTTLS 任意	非セキュア
465	いいえ	STARTTLS 必須	確立されない
465	いいえ	SSL/TLS	確立されない
他の任意のポート番号	はい	なし	非セキュア
他の任意のポート番号	はい	STARTTLS 任意	セキュア
他の任意のポート番号	はい	STARTTLS 必須	セキュア
他の任意のポート番号	はい	SSL/TLS	セキュア
他の任意のポート番号	いいえ	なし	非セキュア
他の任意のポート番号	いいえ	STARTTLS 任意	非セキュア
他の任意のポート番号	いいえ	STARTTLS 必須	確立されない
他の任意のポート番号	いいえ	SSL/TLS	確立されない

テーブル 3: SMTP サーバとの通信モード

2.5 システム構成

PRIMEQUEST 4000 サーバの前面では、以下のコンポーネントにアクセスできます。

図 2: PRIMEQUEST 4000 サーバの前面

1 ID カード

2 2 台目のディスクユニット（DU#1）、SAS HDD/SSD または PCIe SSD SFF ベイを搭載（オプション）

3 操作パネルユニット（OPU）と操作パネル（OPL）

4 2 台目の SB ユニット（SB#1）

5 1 台目の SB ユニット（SB#0）

6 1 台目のディスクユニット（DU#0）、SAS HDD/SSD または PCIe SSD SFF ベイを搭載

PRIMEQUEST 4000 サーバには電源ボタンがありません。サーバの電源のオン/オフは、iRMC Web インターフェースで切り替えます（30 ページの SB の電源のオン/オフを参照）。

2.5.1 OPL

操作パネル（OPL）は OPU の一部で、LED でシステムの状態を表示します。キャビネットを使用しない 1 つの OPU になります。

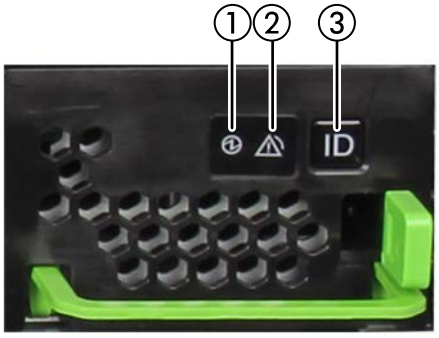


図 3: OPL のボタンと表示ランプ

1 システム電力 LED

2 システムアラーム LED

3 システムの場所 LED および識別灯ボタン

表示機能に加え、以下の機能もあります。

- 環境温度センサ
- システムの基準時間としてのシステム RTC。iRMC はシステム RTC 時刻をシステム（キャビネット）時刻として使用します
- RAID コントローラの記憶領域（IOU の FBU）

2.5.2 システムボード（SB）

システムボードは、最大 2 つの CPU を搭載できるメインボードです。キャビネット内に最大 2 つのシステムボード（SB）を搭載できます。各システムボードには iRMC が提供されます。つまり、1 つのキャビネットには 2 つの iRMC を搭載でき、どちらも関連する SB に接続されたハードウェアを監視します。

SB の表示ランプ

表示ランプは、SB と関連する iRMC の現在のステータスを示します（詳細については、「41 ページの SB と iRMC のステータス LED」を参照）。

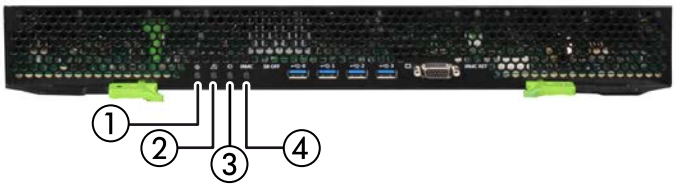


図 4: SB の表示ランプ

1 電源 LED

2 アラーム LED

3 識別灯 LED

4 iRMC ステータス LED

SB のボタン

関連する iRMC をリセットできるため、各 SB は個別にリセットできます。

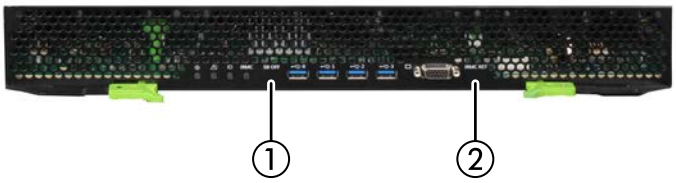


図 5: SB 前面のボタン

1 強制電源オフボタン

2 iRMC リセットボタン

関連する iRMC が故障した場合、**強制電源オフ**ボタンで SB の電源を強制的にオフにします。**iRMC リセット**ボタンでは、OS を停止せずに iRMC をリセットできます。iRMC がハングアップした場合は、このボタンを使用して iRMC をリカバリします。

特殊用途向けの SB にはさまざまなタイプがあります。

- Home SB（「31 ページの Home SB」を参照）
- 非Home SB（「31 ページの 非Home SB」を参照）
- Reserved SB（「32 ページの Reserved SB」を参照）

SB とパーティションは、Web インターフェースの「**管理**」メニューの「**詳細**」ページを使用します。

2.5.2.1 SB の電源のオン/オフ

SB には電源ボタンがありません。代わりに、iRMC メインウィンドウに電源アイコンが実装されています。

図 6: メインウィンドウの電源アイコン

この電源アイコンは、SB のステータスを以下のように色分けして表示します。

赤色: パーティションの電源がオフ

緑色パーティションの電源がオン

さらに、電源のオンとオフを、「**設定**」メニューの「**電源制御**」ページでスケジュールすることもできます。

SB がパーティションの一部の場合、同じ方法でパーティションの電源のオン/オフを切り替えられます。

2.5.2.2 SB の再起動

メインウィンドウの電源のアイコンは、SB のさまざまな再起動方法を提供します。緑の電源のアイコンにマウスポインタを合わせると、コンテキストメニューに特に次のコマンドが表示されます。

通常リセット
グレースフルシャットダウン後にリセットします。

即時リセット
OS の状態にかかわらず、SB を完全に再起動します（コールドスタート）。

パワーサイクル
SB 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、「**自動システム回復および再起動(ASR&R)**」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。

2.5.2.3 Home SB

Home SB はパーティション内のシステムボードで、CPU と PCH の レガシーの PCI インターフェースを有効にします。各パーティションには必ず Home SB が含まれます。パーティションに SB が 2 つある場合、デフォルトでは SB#0 が Home SB です。Home SB をパーティションから削除すると、残りの SB が Home SB になります。

Home SB を手動で変更したり、iRMC で新しいパーティションの Home SB を指定したりできます。

以下の機能は Home SB でのみ有効です。

- レガシー IO が有効であり、USB ポートと VGA ポートはこの SB でのみ使用できます。
- Home SB のクロックソースは、パーティションのクロックソースになります。

Home SB の iRMC は、関連するパーティションを監視しています。iRMC 間のパーティションの監視は、SB が 2 つ取り付けられている場合でも、冗長ではありません。ただし、iRMC 間の生存監視は実行されます。

iRMC が故障した場合、もう一方の SB の iRMC に情報を提供できます。この場合、SB の縮退と Reserved SB の切り替えは実行されません。

2.5.2.4 非Home SB

1パーティションに2SBを含む場合、Home SB以外は非Home SBとなります。

非Home SBのiRMCは限られたサービスのみを提供します。

非Home SBでサポートされる唯一の機能は、レポートです。

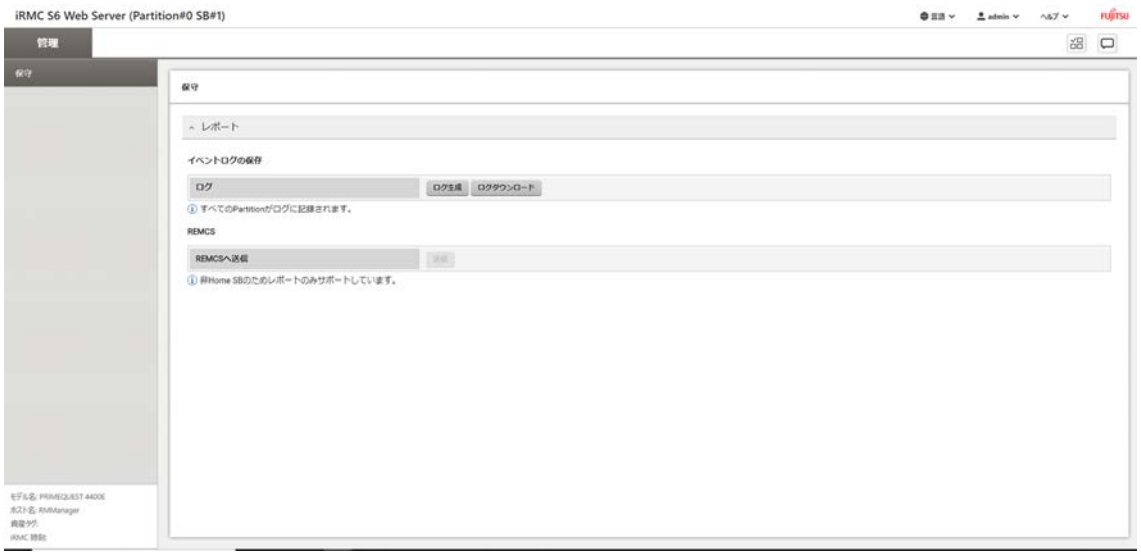


図 7: ホームSB以外でiRMCにログインした後のメインウィンドウ

2.5.2.5 Reserved SB

Reserved SB は、割り当てられた SB が故障した場合に使用される冗長 SB です。これがシームレスに動作するように、Reserved SB を故障する前にインストールして構成しておく必要があります。前提条件を満たす場合、Reserved SB 機能は SB が故障すると次のように動作します。

1. 故障した SB を自動的にパーティションから削除します。
2. Reserved SB をパーティションに追加します。
3. パーティションをリブートし、Reserved SB を有効にします。

Reserved SB を構成する場合は次のルールが適用されます。

- Reserved SB の CPU および DIMM 取り付けルールは、デフォルトに従います。
- SB#0 を SB#1 の Reserved SB として定義します。または、SB#1 を SB#0 の Reserved SB として設定できます。ただし、両方の SB を同時に Reserved SB として定義することはできません。Reserved SB が取り付けられている場合は、各パーティションに SB が 2 つ設定されることはありません。
- Reserved SB として定義される SB は、手動でどのパーティションにも適用できます。この場合、このパーティションの Reserved SB の定義は失われますが、もう一方のパーティションの Reserved SB の定義は維持されます。
- パーティションと Reserved SB の DIMM の構成によっては、Reserved SB が有効になった後、メモリモードが変わる可能性があります。
- 切り替え後に実行する時間同期には、NTP を使用します。
- デバイスが Home SB 上の外部ポート（VGA と USB）に接続されている場合に Home SB を交換した場合は、デバイスを新しく交換した Home SB に接続する必要があります。

パーティションで使用されている SB は、Reserved SB として定義することもできます。これで、有効な Reserved SB と呼ばれます。

- Reserved SB を含むパーティションの状態が電源オフの場合、パーティションの SB は Reserved SB として使用されます。
- Reserved SB を含むパーティションの状態が電源オンの場合、iRMC によってパーティションの状態が電源オフに変わり、その後パーティションの SB は Reserved SB として使用されます。

2.5.2.6 構成

PQ4000 には最大 2 つの SB を搭載できるため、次のパーティション構成でのみ Reserved SB 制御ができます。

- Home SB と 非Home SB による 1 つのパーティション
- SB 1 つずつの 2 つのパーティション

Reserved SB を切り替えられないため、SB が 1 つのみのデバイスでは、Reserved SB 制御は使用できません。

また、SB 2つのパーティションの場合、Reserved の SB はありません (同じパーティションに組み込まれているため、Reserved SB 制御がありません）。

Home SB は、次のいずれの場合も必ず SB 設定で構成する必要があります。

- 1 つのパーティションに SB 1 つのみ
- 1 つのパーティションに 2 つの SB のうちの 1 つ

パーティションの電源がオンの場合に、SB および IOU の設定を変更することはできません。SB の設定に応じて、Home SB/Reserved SB で設定できる、または自動的に設定される値は、以下のとおりです。

SB #0	SB #1	Home SB	Reserved SB
Partition #0	Partition #1	SB #0*1 SB #1	なし*2 SB #0 SB #1
Partition #1	Partition #0	SB #0*1 SB #1	なし*2 SB #0 SB #1
Partition #0	Partition #0	SB #0*2 SB #1	なし*1
Partition #1	Partition #1	SB #0*2 SB #1	なし*1
*1：自動的に適用されます。 *2：デフォルトで設定されています。			

テーブル 4: 有効な構成

SB #0 と SB #1 の電源状態により、変更できるパーティション設定は一部のみになります。次の表に、関連する SB の電源状態の依存関係と設定変更の可否の概要を示します。

SB#0 の電源	オフ	オン	オフ	オン
SB#1 電源	オフ	オフ	オン	オン
SB #0	はい	いいえ	いいえ	いいえ
SB #1	はい	いいえ	いいえ	いいえ
Home SB	はい	いいえ	いいえ	いいえ
IOU #0	はい	いいえ	いいえ	いいえ
IOU #1	はい	いいえ	いいえ	いいえ
Reserved SB	はい	いいえ	いいえ	いいえ
Reserved SB 強制電源オフ待ち	はい	はい	はい	はい
SB #0 メモリモード	はい	いいえ	はい	いいえ
SB #0 ロックステップモード	はい	いいえ	はい	いいえ
SB #1 メモリモード	はい	はい	いいえ	いいえ
SB #1 ロックステップモード	はい	はい	いいえ	いいえ

テーブル 5: 電源の依存関係

2.5.3 パーティション

PRIMEQUEST 4000 シリーズは、パーティション機能を使用して、キャビネットのハードウェアリソースを複数の論理システムに分割し、各システムを個別に動作させます。

パーティションには以下のメリットがあります。

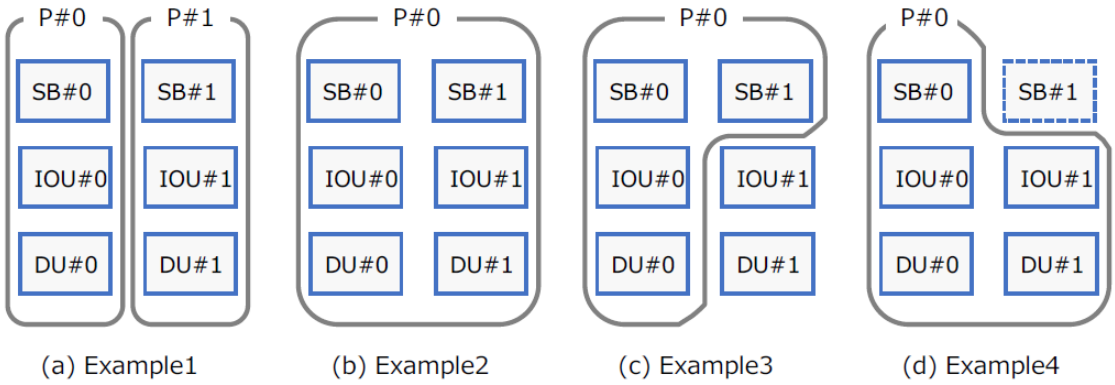
- 各パーティションで異なる OS を使用できます。
- 他のパーティションと区別して、1 つのパーティションの OS をリブートしたり、シャットダウンすることができます。
- 柔軟な I/O と Reserved SB を使用してパーティションを構成することができます。
- 複数の構成を 1 つのキャビネットで操作でき、互いに個別に操作される複数のサーバをキャビネットに統合することもできます。
- パーティションで故障が発生した場合、ハードウェアで他のパーティションが影響を受けないように保護できます。

キャビネット内にはパーティションが 2 つ存在できます。パーティションには、以下のコンポーネントを割り当てることができます。

- 物理 SB 1 つ
- 物理 IOU 1 つ
- 物理 DU_SAS 1 つ
- 物理 DU_NVMe 1 つ
- 物理 DU_SAS_NVMe 1 つ
- 物理 PCI_Box 半分（6 スロット）

パーティションには少なくとも SB と IOU を 1 つずつ含める必要があります。
Home SB の iRMC でパーティションの電源のオンとオフを切り替えます。

パーティションの有効な構成:



（a） パーティション構成例 1: パーティションを 2 つ作成する。

（b） パーティション構成例 2: 1 つのパーティションに SB#0 と SB#1 を搭載する

（c） パーティション構成例 3: 1 つのパーティションに SB を 2 つと IOU を 1 つ搭載する

（d） パーティション構成例 4: 1 つのパーティションに SB を 1 つと IOU を 2 つ搭載する

Home iRMC は、Home SB で実行している iRMC で、パーティションの制御を実行します。

2.5.4 ネットワークの設定

LAN 接続のインターフェースは、各 SB のオンボード LAN コントローラで提供されます。LAN コントローラは、PRIMEQUEST 4000 サーバの背面にあります。

MLANU は 3 つの LAN インターフェースを提供します。スパナのマークが付いているポートが、保守機能のために iRMC に割り当てられています。

図 8: 外部通信用ポート

アイコン	ラベル	意味
		Management LAN（ユーザポートとも呼ばれます）：PRIMEQUEST サーバの関連するパーティションの IP アドレス。
	ローカル	Maintenance LAN（iRMC と CE操作端末間の通信専用ポート）
	リモート	Maintenance LAN (iRMCとFujitsu REMCSセンター間の専用通信ポート)

これらの 3 つの LAN ポートは、以下の通信タイプで使用されます。

- 36 ページの 外部通信
- 37 ページの 内部通信

2.5.4.1 外部通信

iRMC の外部通信は、3 つのすべての LAN ポートを経由して処理されます。

パーティション IP アドレス

各パーティションの iRMC Web インターフェースには、Home SB に対応する MLANU を気にせずに、いずれかの MLANU のユーザポートを経由してアクセスできます。パーティションが 2 つある場合は、各パーティションに IP アドレスを割り当てる必要があります。各パーティションの管理には、独自の iRMC Web インターフェースを使用します。

各パーティションの iRMC Web インターフェースでは、SEL のチェックも行われます。パーティションの 1 つの iRMC が故障した場合、他のパーティションの iRMC によって SEL にメッセージが入力されます。パーティション IP アドレスは、Reserved SB スイッチの前後に継承されます。

REMCS および CE ポートの IP アドレス

MLANU#0 の CE ポートと REMCS ポートは SB#0 の iRMC とのみ通信でき、MLANU#1 の CE ポートと REMCS ポートは SB#1 の iRMC とのみ通信できます。保守作業の場合は、CE 操作ターミナル（FST とも呼びます）を Home SB 側の MLANU の CE ポートに接続します。

CE ポート

CE ポートは、担当保守員専用の Management LAN ポートです。保守を行う場合は、担当保守員が FST（担当保守員が使用する PC）を保守対象システム Maintenance LAN ポートに接続します。

REMCS ポート

REMCS は、サーバ全体のハードウェア構成情報を収集し、サーバに異常がないか監視して、Fujitsu REMCS センタに通知します。REMCS センタとの通信は iRMC で処理されます。iRMC は各パーティションからの情報をまとめて、REMCS ポート経由で REMCS センタに送信します。

初期化ステップで、CE および REMCS ポートの IP アドレスが固定され、次のデフォルト値が割り当てられます。

- SB # 0 の CE/REMCS ポート: 192.168.1.100
- SB # 1 の CE/REMCS ポート: 192.168.1.101

これらのアドレスを変更するには、Web インターフェースの「**管理**」メニューの「**詳細設定**」ページを使用します。Maintenance LAN のサブネットは、Management LAN、業務 LAN などのサブネットのような、他のサブネットと区別する必要があります。担当保守員は、システムのインストール時に Maintenance LAN と REMCS LAN を構成します。

リモートワ保守ターミナルが、DHCP を使用しないでマネージド SB の iRMC に別の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。

Maintenance IP は、Maintenance IP の項目を設定する際に、SMTP アドレスで指定されたアドレスを使用して、1 つのゲートウェイにのみ渡すことができます。REMCS への通信確認応答は、IP アドレスを **SMTP アドレス**を使用して指定したサーバでのみ確認できます。REMCS ポートは、指定した SMTP アドレス以外の IP アドレスからの通信には応答しません。

E-mail による REMCS 通報はできません。REMCS リンクの詳細については、『PRIMEQUEST 4000 series REMCS 導入マニュアル』を参照してください。

2.5.4.2 内部通信

iRMC は、次のインターフェースを使用してシステム全体を監視して制御します。

- I2C（Inter-Integrated Circuit）
- PECI（Platform Environment Control Interface）

2 つの iRMC を搭載した PRIMEQUEST 4000 サーバ内に SB が 2 つあるので、関連する MLANU のユーザポートは、iRMC 間の通信にも使用されます。iRMC のいずれかが 180 秒後に故障と見なされた場合、REMCS ポートが検証用に使用されます。

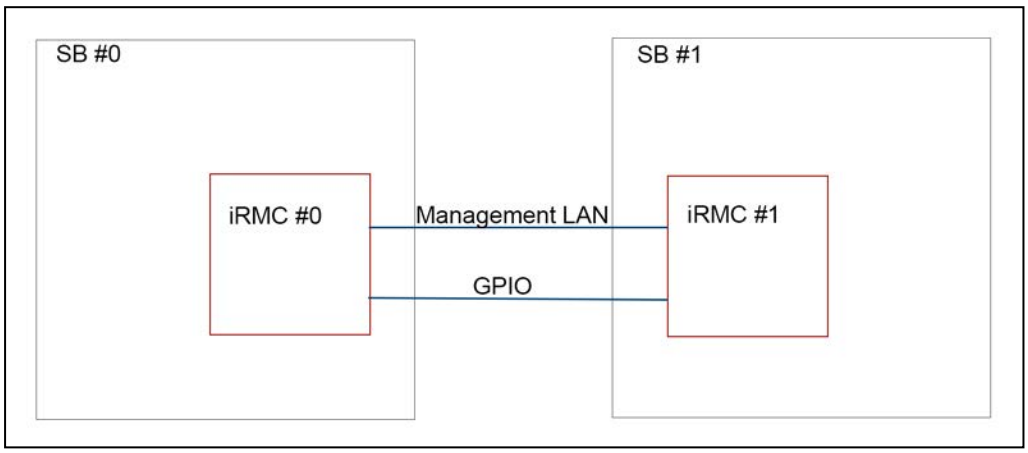


図 9: iRMC 間の通信

iRMC — iRMC LAN は、iRMC#0 と iRMC#1 との間の内部通信用の LAN です。このネットワークは、iRMC 間のデータ同期に使用されます。

iRMC 間の通信では、汎用入出力（GPIO）インターフェースが、この LAN に加えて他の iRMC の死活監視用に提供されます。

2.5.5 電源

6 台の電源ユニット（PSU）をパーティションに取り付けることができます。必要な PSU の数は、サーバモデルと、サーバを実行する国で使用する入力電圧によって異なります。

消費の監視

消費電力監視は、PRIMEQUEST 4000 キャビネット、PCI _ Box、パーティション全体の消費電力の表示と提供を行う機能です。

iRMC は、iRMC Web インターフェースで瞬時に消費電力の値（現在の電力、最小電力、最大電力、平均電力）とグラフを表示します。

パーティション電力の値として返される値は、このパーティションの SB および IOU で使用される電力の合計です。

消費電力監視機能は、iRMC Web インターフェースの「**電源制御**」で有効または無効にできます。

消費の制御

消費電力制御は、iRMC の独自の電力制御モードに従ってキャビネットの消費電力を制御する機能です。

PRIMEQUEST 4000 は、OS で制御される、省電力動作、スケジュール、電力制限（省電力）、低ノイズなどを、電力制御モードとして提供します。

冗長構成

PRIMEQUEST 4000 は、電源の冗長構成をサポートしています。最初に電源を入れると、iRMC では、取り付けた PSU の数に基づいて自動的に冗長値を設定します。

- PSU が 2 台取り付けられている場合: PSU 2+0 構成
- PSU が 3 台取り付けられている場合: PSU 2+1 構成
- PSU が 4 台取り付けられている場合: PSU 2+2 構成

電源冗長モードは、iRMC Web インターフェースの「**詳細設定**」ページで設定できます。

2.5.6 時間の設定

PRIMEQUEST 4000 には、リアルタイムクロック（RTC）が OPL と SB にインストールされます。

- OPL の RTC は、システムクロック（System_RTC）として使用されます。OPL のシステムクロックは、iRMC Web インターフェースの「**詳細設定**」ページで設定できます。
- SB の RTC はパーティションクロックとして使用され、OS で変更できます。OS は、ブート中にプラットフォームコントローラハブ（PCH）に構築された RTC を読み取り、独自の時間を管理します。

iRMC には内部時刻があります。iRMC の時刻はシステムクロックと同期され、協定世界時（UTC）で管理されます。iRMC の時刻設定は、Web インターフェースの「**管理**」ページで変更できます。

iRMC 時刻は、SB を取り付けて電源をオンにすると即座に同期されます。SB バッテリーは、iRMC 時刻を維持しません。iRMC の時刻は、3 時間おきにシステム時刻と同期されます。システム時刻を手動で変更すると、iRMC 時刻も変更されます。

iRMC は、以下の場合にパーティションクロックを読み取ります。

- パーティションの電源が完全にオフになったとき
- Home SB が切り替えられたとき

システム時刻とパーティション時刻に時間差がある場合、iRMC では、OPL の不揮発性領域にその差を維持します。たとえば、パーティション時刻が元々 iRMC 時刻の 30 分前に設定されている場合、iRMC では、OPL の不揮発性領域に 30 分の差を維持します。システム時刻を手動で変更した場合、iRMC によって、パーティション時刻とシステム時刻の差が更新されます。

BIOS 時刻

次の場合に、BIOS は、iRMC からシステム時刻を取得して、Home SB のパーティション時刻に書き込みます。

- Home SB が交換されたとき
- Home SB が切り替えられた後

システム時刻とパーティション時刻の差も、iRMC から取得され、その差も反映されます。

NTP

iRMC 設定で、OPL のシステム時刻を、PRIMEQUEST 4000 システムの外部のより高精度な NTP サーバと同期させることができます。外部ネットワークに接続でき

ない場合は、外部クロックデバイスを使用して NTP サーバデバイスを使用することをお勧めします。

つまり、iRMC と OS（BIOS）の時刻は個別に管理されます。iRMC は、OS と iRMC の時間差のみを管理します。

2.6 SB と iRMC のステータス LED

PRIMEQUEST 4000 サーバに組み込まれた各コンポーネントには、独自の LED セットが搭載されています。

LED	色	意味
電源状態	緑色	関連するコンポーネントの電源状態を表示します。
アラーム状態	オレンジ色	関連するコンポーネントにエラーが発生しているかどうかを表示します。
場所情報	青色	関連するコンポーンネントが、iRMC Web インターフェースでチェックされたかどうかを識別します。

iRMC 状態 LED は白色で、関連する SB の状態によって変わります。そのため、iRMC 状態 LED は、関連する SB のインジケータセットに配置され、以下を示します。

SB のステータス	電源 LED	アラーム LED	識別灯 LED	iRMC ステータス LED
AC 入力オフおよびすべてのパーティション電源オフ	オフ	オフ	オフ	オフ
AC 入力オン、パーティション電源オフ、iRMC ファームウェアブート中	オフ	-	-	点滅（白色）
AC 入力オン、パーティション電源オフ、iRMC ファームウェアのブート完了	オフ	-	-	オン（白色）

SB のステータス	電源 LED	アラーム LED	識別灯 LED	iRMC ステータス LED
SB を含むパーティション電源オン	オン（緑色）	-	-	-
SB エラー	-	オン（オレンジ色）	-	-
SB の識別	-	-	オン（青色）	-
iRMC ファームウェアのリブート	-	-	-	点滅（白色）
iRMC PFR リカバリ	-	-	-	点滅（白色）
iRMC PFR リカバリが失敗した	-	-	-	点滅（白色）

3 最初の手順

iRMC を操作するための最初の手順は、以下のとおりです。

- LAN 接続を確立します。
- iRMC Web インターフェースのログイン

3.1 LAN インターフェースの設定

PRIMEQUEST 4000 サーバは、最初はローカルポートの IP アドレスで構成されます。そのため、iRMC Web-GUI を Management LAN に設定できます。これにより、最初のログオンのために iRMC LAN 接続を構成する必要がなくなりました。

その後、ユーザーのニーズに合わせて、Web インターフェースを使用して LAN 接続パラメータを含む iRMC を構成できます。

iRMC 接続の「スパニングツリー」のツリーは、無効にしておきます。（例: Port Fast=enabled; Fast Forwarding=enabled）

また、LAN over USB でインバンド通信を設定することもできます。詳細は、『iRMC S6 - コンセプトとインターフェース』取扱説明書を参照してください。

3.1.1 要件

iRMC Web-GUI にログオンする前に、次の要件を満たす必要があります。

- LAN ケーブルが正しいポートに接続されていること。
- キャビネット内の各 iRMC に 2 つの IP が必要です。
- 別のサブネットからアクセスするため、ゲートウェイを設定すること

3.1.2 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。

1. Web ブラウザから、iRMC Web-GUI 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。
2. Ping コマンドで、iRMC 接続をテストしてください。

3.2 iRMC S6 への初回ログイン

iRMC の工場出荷時のデフォルト設定を使用して、設定作業を一切行わずに iRMC に初回ログインできます。

3.2.1 要件

接続を機能するには、以下の要件を満たす必要があります。

リモートワークステーションでは、Web インターフェースを使用して接続するために以下のブラウザのいずれかが必要です。

- Microsoft Edge ブラウザ
- Google Chrome バージョン 50 以降
- Mozilla Firefox バージョン 50 以降

2 要素認証がアカウントに有効されている場合は、以下が必要です。

- NTP サービスが構成され、iRMC で使用されている。
- MS Authenticator や Fast 2FA などの TOTP ベースの承認アプリケーションを使用して、ワンタイムパスワードを生成している。

コンソールリダイレクションの必要条件は、使用する接続タイプによって異なります。

- Java: Java Runtime Environment
- HTML5: Web ブラウザ
- VNC: 選択した VNC ビューア

ネットワーク内

- 静的 IP アドレスを使用していない場合、ネットワークに DHCP サーバがあります。
- IP アドレスの代わりに具体的な名前を使用して iRMC Web インターフェースにログインする場合、ネットワークの DHCP サーバを動的 DNS に設定する必要があります。
- DNS を設定する必要があります。設定しない場合は、IP アドレスを要求する必要があります。

3.2.2 iRMC の工場出荷時のデフォルト

iRMC のファームウェアには、デフォルトの 管理者 ID と iRMC のデフォルトの DCHP 名が用意されています。

デフォルトの 管理者 ID

管理者 ID とパスワードは、大文字小文字を区別します。

管理者 ID　admin

パスワード マシンのパスワードはシステム ID カードに記載されています。

セキュリティ上の理由により、初回ログオン時に admin ユーザのパスワードを変更する必要があります。

パスワードは、大文字小文字を区別しないユーザ名ごとに異なり、12 文字以上である必要があります。空白文字は使用できません。パスワードには、以下の 3 つの種類の文字を含める必要があります。

- 小文字
- 大文字
- 特殊文字（"+" を除く）
- 数字（0 ～ 9）

iRMC のデフォルト DHCP 名

iRMC のデフォルトの DCHP 名は次の形式です：

`iRMC<シリアル番 号>`

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

ログイン後、iRMC の MAC アドレスは、「**ネットワーク制御**」ページの「**ネットワークインターフェース**」グループに読み取り専用フィールドとして表示されます。

3.2.3 初回ログイン

初回ログインの場合は、管理者認証情報を使用して管理者としてログインして、エンドユーザライセンス契約に同意する必要があります。

ユーザ名 : admin

パスワード: マシンのパスワードはシステム ID カードに記載されています。

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ようにお勧めします。少なくとも管理者アカウントのパスワードを変更するようにお勧めします（「57 ページの ユーザ管理」）。

1. リモートワークステーションから Web ブラウザを開きます。
2. iRMC の（設定済みの）DNS 名または IP アドレスを入力します。
   ログインダイアログボックスが開きます。

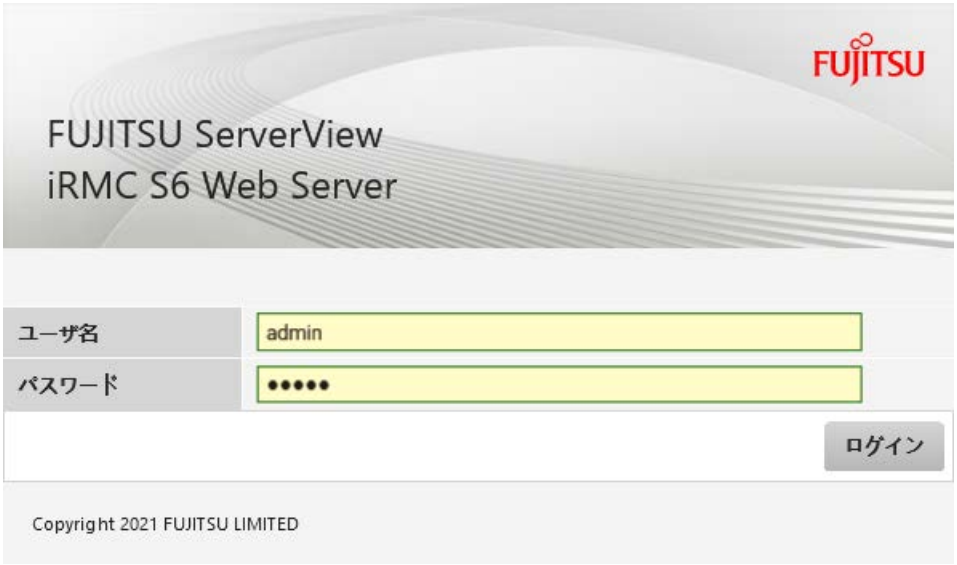


図 10:「ログイン」ダイアログボックス

3. ログインダイアログボックスが表示されない場合は、LAN 接続を確認してください。
4. デフォルトの管理者アカウントのデータを入力します。
5. 「**ログイン**」をクリックして、ログインを確定します。

6. セキュリティ上の理由から、最初のログイン時に管理者ユーザのパスワードの変更を求められます。新しいパスワードを入力し、もう一度入力してください。

パスワードは、大文字小文字を区別しないユーザ名ごとに異なり、12 文字以上である必要があります。空白文字は使用できません。パスワードには、以下の 3 つの種類の文字を含める必要があります。

- 小文字
- 大文字
- 特殊文字（"+" を除く）
- 数字（0 ～ 9）

2 要素認証がアカウントに指定されている場合は、以下のダイアログボックスが開きます。

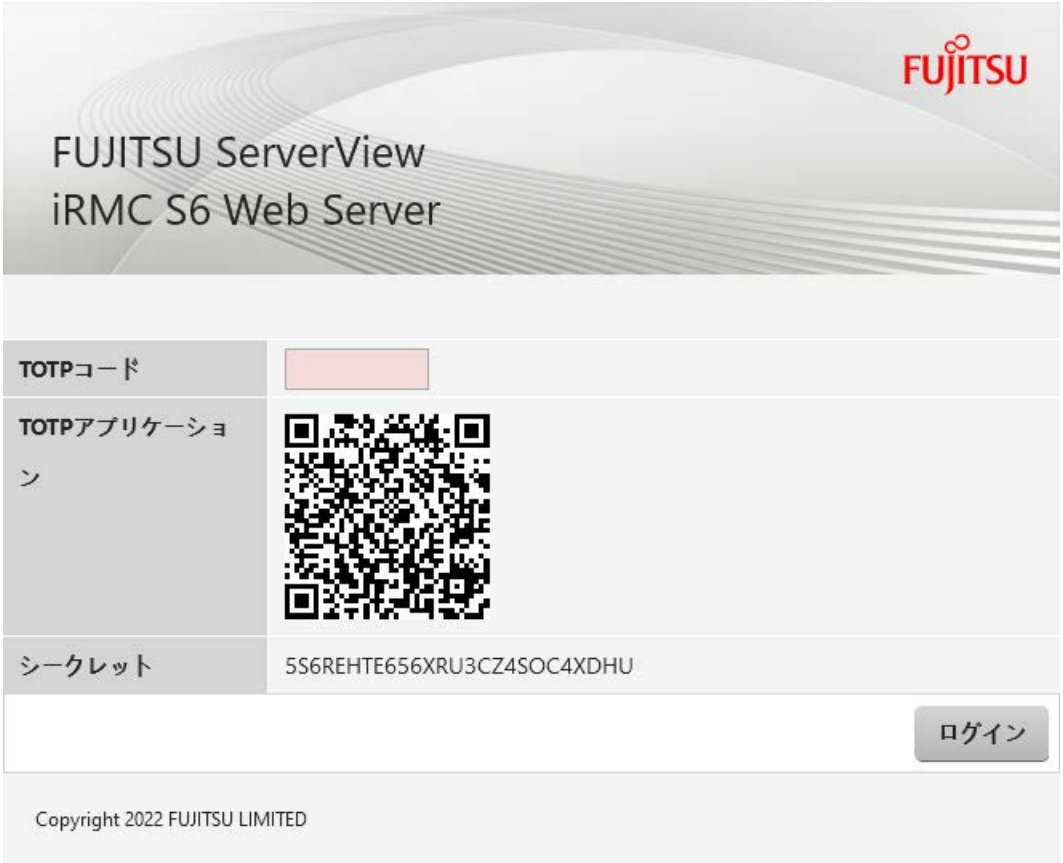


図 11: 2FA の「ログイン」ダイアログボックス

7. QR コードまたは「**シークレット**」フィールドに表示されたコードを使用して、TOTP ベースの承認アプリケーションでワンタイムパスワードを生成します。
8. ワンタイムパスワードを「**TOTP コード**」入力フィールドに入力します。

9. 「**ログイン**」をクリックします。

   ログインに成功すると、使用する TOTP ベースの承認アプリケーションが iRMC によって受理され、エマージェンシーコードでダイアログボックスが開きます。

図 12:「ワンタイムエマージェンシーコード」ダイアログボックス

   これらのエマージェンシーコードは 1 回だけ表示されます。このコードは、2 要素認証を使用してログインできなくなった場合に使用できます。たとえば、TOTP ベースの承認アプリケーションを持つデバイスを紛失した場合や、デバイスやアプリケーションが破損した場合です。

10. スクリーンショットを取るなどして、エマージェンシーコードを保存します。
11. 「**確認**」をクリックします。

    エンドユーザライセンス契約（EULA）が開きます。

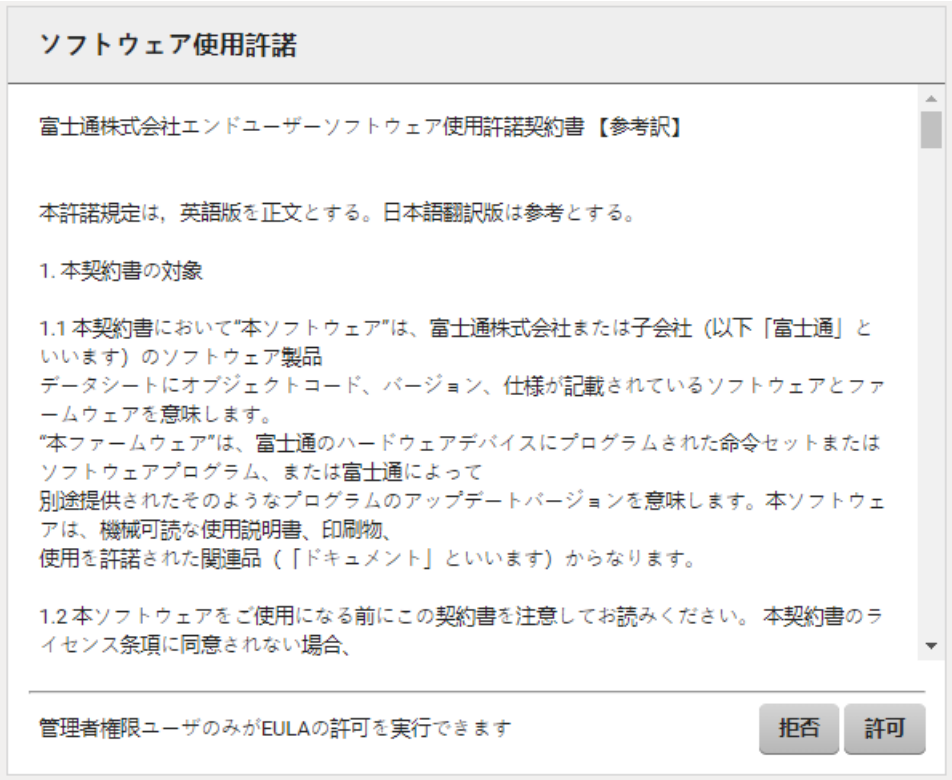


図 13:「ソフトウェア使用許諾」ダイアログボックス

12. 契約内容をよく読んで、「**許可**」をクリックして同意します。
    iRMC Web インターフェースが開き、「**システム概要**」ページが表示されます。

3.2.4 ログアウト

ログアウトすると、iRMC セッションを終了できます。

1. タイトルバーで、「**<ユーザ>**」メニューを開きます。
2. 「**ログアウト**」をクリックします。
   ユーザはログアウトし、ログインダイアログボックスが再び開きます。必要に応じて、再びログインできます。

4 証明書

セキュアな通信を実現するために、公開キー証明書が使用されます。公開キー証明書を使用して、メッセージ、ソフトウェア、デジタルドキュメントの信頼性と整合性を検証します。

公開キーの最も一般的な形式は、X.509.[2] で定義されています。iRMC は、base64（PEM）エンコード形式の X.509 証明書を受け入れます。

iRMC は、次の目的で証明書を使用します。

証明書タイプ	目的	ストア	方法
サーバ証明書	iRMC への Web ベースのセキュアなアクセス（Web インターフェース / RESTful API / Redfish など）	キーストア	51 ページの セキュアな通信の証明書のインポート
CA 証明書	iRMC と CAS / SMTP サーバ間のセキュアな通信	トラストストア	53 ページの CAS/SMTP 検証の CA 証明書のインポート
CA 証明書	iRMC および eLCM リポジトリ間のセキュアな通信	eLCM のトラストストア	54 ページの eLCM 検証の証明書のインポート
S/MIME 証明書	メールの暗号化	ユーザストア	56 ページの S/MIME 証明書のアップロード

テーブル 6: iRMC 内で使用される証明書

インストール後に使用可能な証明書は、下記と交換できます。

- 自己署名証明書
- 内部 CA によって署名された証明書
- 外部 CA によって署名された証明書、通常は商用 CA

SSL/TLS セキュア通信を iRMC で使用することを推奨します。そのため、できるだけ早く、生成された自己署名証明書を、信頼できる CA、所有者または商用 CA によって署名された有効な証明書に置き換えてください。

4.1 サーバ証明書

iRMC には、一意の自己署名サーバ証明書（デフォルトの証明書）が付属します。この証明書を使用して、HTTPS によるセキュアな通信を有効にします。HTTP プロトコルでは、セキュアな通信は提供されません。

自己署名証明書は、すぐに使える暗号化された iRMC への初期接続を提供しますが、信頼はできません。

HTTPS から iRMC Web インターフェースにアクセスすると、自己署名証明書に関する警告がブラウザに表示されます。

セキュリティ上の理由により、生成された自己署名証明書を、信頼できる所有者または商用 CA によって署名された有効な証明書に置き換えることを推奨します。

Web ブラウザから iRMC にアクセスする場合に、ブラウザのセキュリティ警告を回避するには、HTTPS 経由でサーバにアクセスするすべてのシステムのトラストストアに、CA 証明書をインポートする必要があります。

Firefox は独自の Certification Authorities ストアを使用しますが、Edge および Chrome は、オペレーティングシステムの Trusted Certification Authorities ストアを使用します。

証明書は、iRMC の Web インターフェースを使用して交換されます。次の手順に従います。

- SSL 証明書を iRMC のキーストアにインポートします。
- プライベートキーを iRMC のキーストアにインポートします。

iRMC でのすべてのサーバ証明書関連の操作は、iRMC Web インターフェースの「**証明書**」ページで開始できます。

4.1.1 セキュアな通信の証明書のインポート

初回に作成した自己署名証明書を信頼される CA の証明書に交換して、iRMC のキーストアにインポートするには、次の手順を行います。

1. iRMC Web インターフェースを起動して、「**ツール**」メニューの「**証明書**」ページを開きます。
2. 「**現在の SSL/TLS 証明書**」グループを開いて「**ファイルから読み込み**」をクリックします。

   「**SSL/TLS 証明書のアップロード**」ダイアログボックスが開きます。
3. SSL 証明書とプライベートキーを iRMC のキーストアにインポートするには、以下を指定します。

- 「**SSL/TLS 公開キー**」フィールドに `publickey.pem` を指定します。
- 「**SSL/TLS 秘密キー**」フィールドに `privkey.pem` を指定します。

これを行うには、関連する「**選択**」ボタンをクリックして、管理対象サーバの対応するローカルファイルに移動します。秘密鍵または公開鍵を含むファイルのサイズは 4 KB までです。

SSL 証明書とプライベートキーをローカルファイルから iRMC のキーストアに読み込む場合は、SSL 証明書とプライベートキーをを同時に読み込む必要があります。

4. 「**アップロード**」ボタンをクリックして、SSL 証明書または秘密鍵を iRMC にアップロードします。
5. iRMC をリブートします。

4.1.2 証明書の生成

iRMC Web インターフェースで「**ツール**」メニューの「**証明書**」ページを使用して自己署名証明書を作成できます。

1. 「**ツール**」メニューの「**証明書**」ページを開きます。
2. 「**現在の SSL/TLS 証明書**」グループを開いて「**生成**」をクリックします。

   「**証明書の生成**」ダイアログボックスが開きます。
3. 必要な詳細を入力します。
4. 「**生成**」をクリックして、証明書を作成します。

新しい証明書を生成すると、既存の HTTPS 接続がすべて切断され、HTTPS サーバが自動的に再起動します。鍵の長さによって、最大 2 分ほどかかることがあります。

iRMC を明示的にリセットする必要はありません。

4.2 iRMC の CA 証明書

CA 証明書は、iRMC と下記との SSL/TLS セキュア通信に使用されます。

- CAS（シングルサインオンのための中央認証サービス）サーバ
- SMTP（E-mail 設定）サーバ

iRMC と CAS または SMTP間のセキュアな通信を有効にするために、CAS / SMTP サーバのサーバ証明書への署名に使用した CA 証明書を iRMC の eLCM トラストストアにアップロードすることができます。

ただし、CAS と SMTP のどちらも、対応する「**SSL 証明書を検証**」オプションが無効な場合、SSL/TLS セキュアですが信頼できない通信を許可することができます。セキュリティ上の理由により、事前に定義された CA 証明書を、CAS および SMTP サーバのサーバ証明書への署名に使用した CA 証明書に交換し、「**SSL 証明書を検証**」オプションを有効にするようにしてください。

CAS/SMTP 検証の CA 証明書のインポート

デフォルトの CA 証明書を、CAS および SMTP サーバのサーバ証明書の検証に使用可能な CA 証明書に交換するには、iRMC で次の手順が必要です。

1. iRMC Web インターフェースを起動して、「**ツール**」メニューの「**証明書**」ページを開きます。
2. 「**CAS と SMTP の現在の CA 証明書**」グループを開きます。
3. グループの末尾にある「**ファイルから読み込み**」をクリックして、「**CAS と SMTP の CA 証明書のアップロード**」ダイアログボックスを開きます。
4. CA 証明書を iRMC のトラストストアにインポートするには、「**選択**」をクリックして「**ファイルを開く**」ダイアログボックスの CA 証明書に移動します。
5. 「**アップロード**」をクリックして、CA 証明書を iRMC のトラストストアにアップロードします。

4.3 eLCM の CA 証明書

iRMC の embedded Lifecycle Management（eLCM）機能を使用すると、物理デバイスを操作せずにマウスを数回クリックするだけで、iRMC から一元的に PRIMEQUEST サーバのライフサイクル管理を行うことができます。

eLCM 機能を使用するには、内蔵 iRMC SD カードと共に購入する有効な eLCM ライセンスキーが必要です。

次の eLCM 機能には、HTTP（非セキュア）または HTTPS（セキュア）でのダウンロードに必要なパッケージを提供する Web リポジトリへの接続が必要です。

- オンラインアップデート
- オフラインアップデート
- デプロイメント

これらの機能のための Fujitsu のデフォルトパブリックリポジトリでは、HTTPS を使用します。サーバ証明書の署名に使用された CA 証明書は、iRMC の eLCM トラストストアに含まれ、信頼されるセキュアな接続を許可します。

ただし、Fujitsu のパブリックリポジトリの代わりに、カスタムリポジトリ（内部のミラーリポジトリなど）を使用する場合もあります。

HTTPS を使用した iRMC とカスタムリポジトリ間のセキュアな通信を有効にするために、リポジトリのサーバ証明書への署名に使用した CA 証明書を iRMC の eLCM トラストストアにアップロードすることができます。

eLCM 検証の証明書のインポート

eLCM リポジトリ検証の最大 5 個の CA 証明書を、eLCM のトラストストアにアップロードするには、iRMC で次の手順が必要です。

1. iRMC Web インターフェースを起動して、「**ツール**」メニューの「**証明書**」ページを開きます。
2. CA 証明書を eLCM のトラストストアにインポートするには、「**CA 証明書**」グループで「**追加**」をクリックします。

   「**CA 証明書のアップロード**」ダイアログボックスが開きます。
3. 「**選択**」をクリックして、「**ファイルを開く**」ダイアログボックスの CA 証明書に移動します。
4. 「**アップロード**」をクリックして、CA 証明書を eLCM のトラストストアにアップロードします。
5. ダイアログボックスを閉じます。

4.4 メール暗号化の S/MIME 証明書

メール暗号化の S/MIME 証明書は、「**ローカルユーザアカウントの編集**」ダイアログボックスの「**証明書**」タブの「**S/MIME 証明書**」サブタブでアップロードできます。

図 14: S/MIME 証明書のアップロード

S/MIME 証明書をアップロードする場合に、「**Email 設定**」グループの「**暗号化を有効にする**」オプションを有効にして、暗号化したメールを送信することができます。

S/MIME 証明書のアップロード

S/MIME 証明書をファイルから iRMC へアップロードするには、以下の手順に従います。

1. iRMC Web インターフェースのログイン
2. 「**設定**」メニューで「**ユーザ管理**」ページを開きます。
3. 「**iRMC ローカルユーザアカウント**」のテーブルで、「**編集**」をクリックして関連するユーザ設定を編集します。
4. 「**ローカルユーザアカウントの編集**」ダイアログボックスで、「**証明書**」タブを開きます。
5. 「**証明書**」タブで「**S/MIME 証明書**」サブタブを開きます。
6. 「**選択**」をクリックして、必要な証明書を含むファイルに移動します。
7. 「**アップロード**」ボタンをクリックして S/MIME 証明書を iRMC にアップロードします。

   S/MIME 証明書のアップロードが成功した後、ユーザ設定の「**E メール設定**」タブで「**暗号化を有効にする**」オプションを有効にできます。

5 ユーザ管理

iRMC によるユーザ管理には 2 種類の異なるユーザ ID を使用します。

- **ローカル**ユーザーID はiRMC 内部の不揮発性記憶装置に保存され、iRMC のユーザ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 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 S6 ユーザ管理では、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、OpenDS、ApacheDS などのオープンディレクトリサービス

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の詳細については、『ServerView でのユーザ管理』取扱説明書を参照してください。

5.1 「ユーザ管理」概念

iRMC によるユーザ管理は、ローカルとグローバルのユーザ ID を並列に管理することができます。

ユーザがいずれかの iRMC 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（ユーザ名、パスワード）を検証する際には、iRMC は以下のように処理します。

iRMC はユーザ名とパスワードを内部に保存されたユーザ ID と照合します。

- ユーザは、認証に成功すれば（ユーザ名とパスワードおよび 2 要素認証が有効）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 は次のステップ の検証手順を継続します。

iRMC は、LDAP 経由でユーザ名とパスワードを使用してディレクトリサービスで自己認証します。

LDAP 構成設定に従って、iRMC は以下のように処理を進めます。

- LDAP サーバの ServerView Suite 構造に認証設定がある ServerView 固有の LDAP グループが使用される場合、iRMC は、LDAP クエリを使用してユーザの権限を判定し、ユーザが iRMC での処理について認証されているかどうかを確認

します。

次の特性があります。

- ディレクトリサーバ構造の拡張が必要です。
- 特権と権限はディレクトリサーバで一元的に設定されます。

- LDAP 標準グループが iRMC にローカルに配置された認証設定で使用される場合、iRMC は以下のように処理を進めます。
  1. iRMC は LDAP クエリを使用して、ディレクトリサーバ上のどの標準 LDAP グループにユーザが属しているか、判定します。
  2. iRMC はこの名前のユーザグループが iRMC でローカルに設定されているかどうかも確認します。この場合、iRMC はこのローカルグループを使用してユーザの権限を決定します。

  次の特性があります。

  - ディレクトリサーバ構造の拡張は不要です。
  - 特権と権限はそれぞれ個別に iRMC で設定されます。

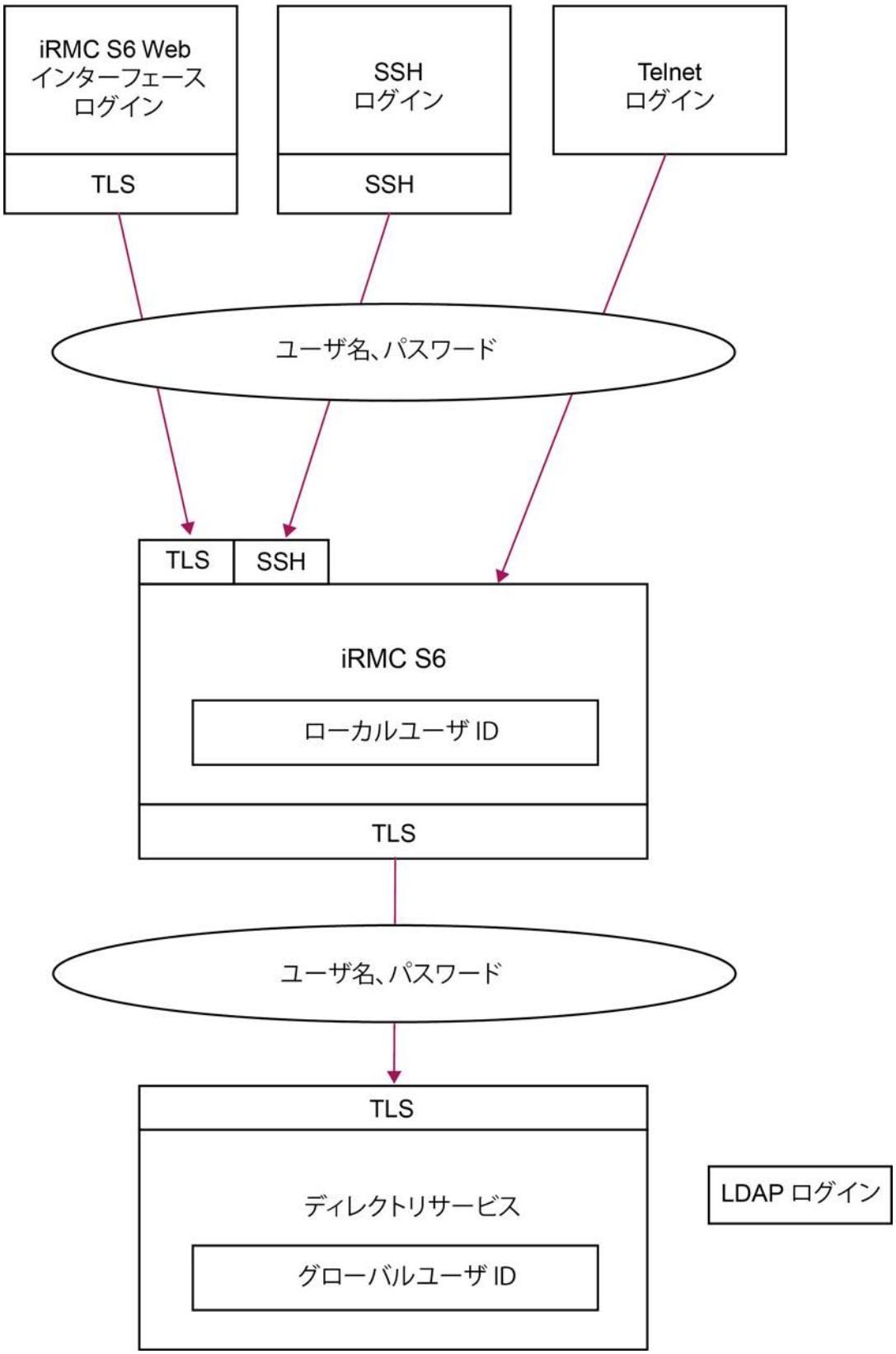


図 15: iRMC S6 経由のログイン認証

iRMC とディレクトリサービスの間の LDAP 接続には、HTTPS を使用することを推奨します。HTTPS で保護された iRMC 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、特にユーザ名とパスワードのデータの送信が安全にできます。

5.2 ユーザ権限

iRMC は以下の 2 つの相互補完的なユーザ権限を区別します。

- ロールに割り当てられたチャネル権限
- 明示的に割り当てられた権限

チャネル権限は通信に使用されるプロトコルに結びつけられます。

Redfish チャネル固有の権限

Redfish API 経由の Web インターフェースとスクリプトは、ロールと呼ばれる、Redfish で定義された権限を使用します。3 種類のロールが定義されています。

- 制限のない、管理者
- システム関連の設定は変更できるが、ユーザや iRMC 設定を管理できない、オペレーター
- 読み取り専用で、情報の読み取りと自分のパスワード変更のみが可能なオペレーター

IPMI チャネル固有の権限

IPMI 権限は、RESTful API、プロファイル、リモート管理など、残りのiRMC インターフェースに使用されます。

iRMC は各々のユーザ 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。

- ユーザ
- オペレーター
- 管理者
- OEM

iRMC 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、ユーザは、iRMC に LAN インターフェースを経由して接続したにより、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。

グループ許可に加えて、ユーザに次の許可を個別に割り当てることもできます。

ユーザアカウント変更 - ローカルユーザ ID を設定する許可

iRMC 設定変更 - iRMC 設定を行うための許可

iRMC 独自の機能による IPMI アクセス許可

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

権限	意味
AVR使用権限	「View Only」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 ストレージ有効	バーチャルメディア機能を使用する権限

個々の iRMC 機能を使用するために必要な特権と許可は、次のマニュアルに記載されています。

- iRMC Web インターフェースについては、『iRMC S6 - Web インターフェース』取扱説明書と Redfish API 仕様書
- Remote Manager については、『iRMC S6 - コンセプトとインターフェース』取扱説明書

5.3 ローカルユーザ管理

iRMC には固有のローカルユーザ管理方法があります。最大 16 人のユーザをパスワード付きで設定し、それぞれが属するユーザ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 ID は iRMC S6 の不揮発性ストレージに、ローカルで保存されます。

iRMC は、ローカルユーザ向けの以下のセキュリティ機能もサポートしています。

- TOTP ベースの承認アプリケーションを使用する 2 要素認証
- 公開キーと秘密キーのペアを使用した、SSHv2 ベースの公開キー認証（70 ページの SSHv2 によるセキュアな認証）

Web インターフェースで、設定された iRMC ユーザのリストが表示されます。新しいユーザの設定、既存ユーザの設定変更、または、ユーザのリストからの削除が可能です。

iRMC でのユーザ管理には「ユーザアカウント変更権限」が必要です。

設定されたユーザのリスト表示

設定済みのユーザのリストが、「**設定**」メニューの「**ユーザ管理**」ページにある「**iRMC ローカルユーザアカウント**」グループに表示されます。

このリストで、ユーザの削除と、ダイアログボックスを開いて新しいユーザの設定ができます。

新しいユーザの設定

設定されたユーザのリストの下にある「**追加**」ボタンで、新しいユーザを設定できます。

「**ローカルユーザアカウントの追加**」ダイアログボックスで、新規ユーザの基本設定ができます。

ユーザの設定変更

ユーザアカウントの設定を変更するには、設定されたユーザのリストで該当するユーザの横にある「**編集**」ボタンをクリックします。

「**ローカルユーザアカウントの編集**」ダイアログボックスで、既存ユーザの設定を変更できます。

ユーザの削除

ユーザアカウントを削除するには、設定されたユーザのリストで該当するユーザの横にある「**削除**」ボタンをクリックします。

iRMC Web インターフェースの「**情報通知設定**」ページの詳細は、『iRMC S6 - Web インターフェース』取扱説明書を参照してください。

5.3.1 二要素認証（2FA）

二要素認証（2FA）は、ID およびアクセス管理セキュリティ手法で、リソースとデータにアクセスするために 2 段階の身元識別を必要とします。

一般に、認証の第一要素では、ユーザ名とパスワードを使用します。第二要素は、ソフトウェアベースの認証器から生成されたコードです。2FA を有効にした場合、iRMC Web インターフェースを使用するには、これに加えてワンタイムパスワード（コード）を生成する必要があります。

コードは TOTP ベースの承認アプリケーションで生成できます。スマートフォンのアプリ（Google Play および App Store）、デスクトップまたはインターネット上で広く提供されている Web ベースのアプリケーションから選択できます。この TOTP ベースの承認アプリケーションは、最初のログインのセットアップ手順で導入されます。

2FA を有効にする前に、NTP サーバ経由で iRMC で時刻同期を有効にすることを強く推奨します。適切に動作させるには、iRMC の時刻設定を、TOTP ベースの承認アプリケーションの設定と同一にする必要があります。

時刻が一致していないと、iRMC で 2FA を利用できません。TOTP ベースの承認アプリケーションで生成された時刻コードとの同期がずれてくると、入力されたコードが iRMC で受理されなくなります。

ユーザアカウントで 2FA を有効にするには、以下の手順が必要です。

- 管理者：64 ページの ユーザアカウントの 2FA の有効化
- iRMC ユーザ：64 ページの 2FA のセットアップ

2FA を有効にしてセットアップすると、ユーザアカウントでログインするたびに動作するようになります。2FA アクセスが付与されていないと、iRMC Web インターフェースへのアクセスはブロックされます。

iRMC Web インターフェースへのアクセスは、以下の条件が満たされるまで付与されます。

- 新しい IP アドレスから同じユーザアカウントへのアクセスが発生した
- 猶予期間が経過した
- iRMC リブートが発生した

猶予期間中、ワンタイムパスワードを再度入力する必要はなく、ユーザ資格情報でログインできます。

TOTP ベースの認証器アプリケーションが失われたり破損したりした場合は、以下のステップが新しいセットアップに適用されます。

- 68 ページの エマージェンシーコードの使用
- 70 ページの ユーザアカウントの 2FA の再構成

5.3.1.1 ユーザアカウントの 2FA の有効化

1. iRMC に管理者としてログインします。
2. 「**設定**」メニューで「**ユーザ管理**」ページを開きます。
3. 「**iRMC ローカルユーザアカウント**」グループを開きます。
4. 新しい iRMC ユーザを作成するか、既存のユーザを編集します。
5. 「**ローカルユーザアカウントの追加**」または「**ローカルユーザアカウントの編集**」ダイアログボックスで、「**アクセス設定**」タブを開きます。
6. 「**二要素認証**」タブを開きます。
7. 「**二要素認証を有効にする**」オプションを有効にします。
8. 「**OK**」をクリックします。

   2 要素認証がユーザアカウントで有効になります。

ユーザが次回 iRMC にログインしたときに、ユーザアカウントで 2 要素認証をセットアップする必要があります。

5.3.1.2 2FA のセットアップ

2FA では、iRMC ユーザには、ワンタイムパスワードの生成に使用される TOTP ベースの承認アプリケーションが必要です。このパスワードは iRMC によってセットアップ時に提供されるコードに基づいて作成されます。

2FA をセットアップするには、次の手順に従います。

1. リモートワークステーションから Web ブラウザを開きます。
2. iRMC の（設定済みの）DNS 名または IP アドレスを入力します。

   ログインダイアログボックスが開きます。

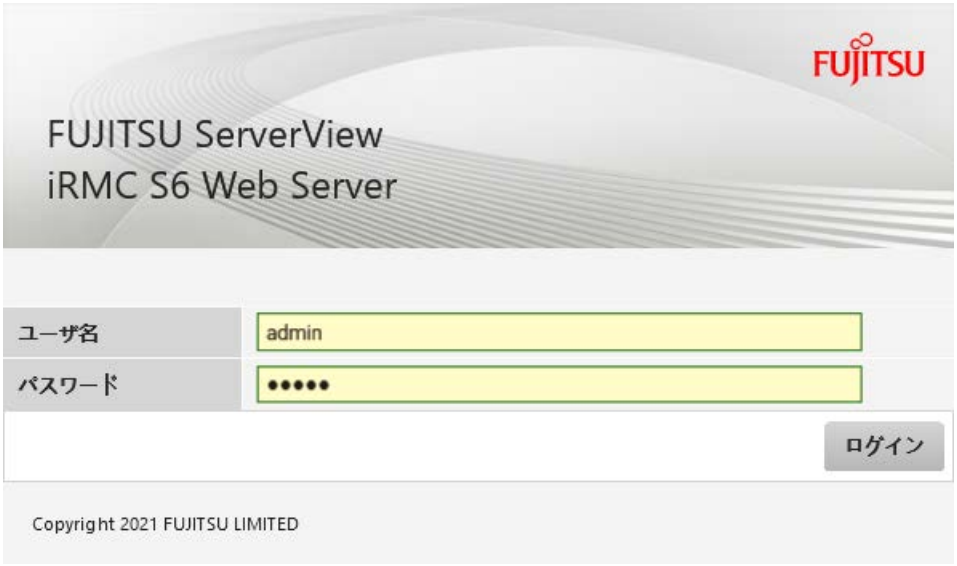


図 16:「ログイン」ダイアログボックス

3. 資格情報（ユーザ名とパスワード）を入力します。
4. 「**ログイン**」をクリックして、ログインを確定します。
   次のダイアログボックスが開きます。

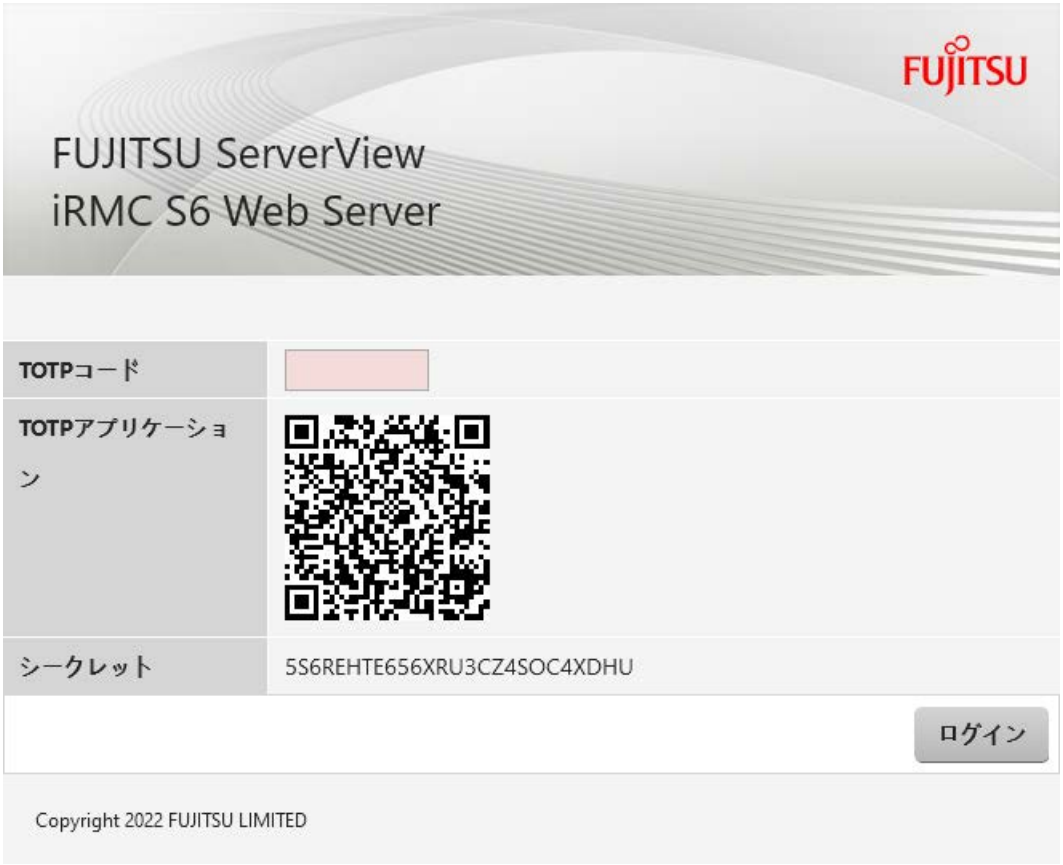


図 17: 2FA の「ログイン」ダイアログボックス

5. QR コードまたは「**シークレット**」フィールドに表示されたコードを使用して、今後使用する TOTP ベースの承認アプリケーションでワンタイムパスワードを生成します。
6. ワンタイムパスワードを「**TOTP コード**」入力フィールドに入力します。
7. 「**ログイン**」をクリックします。

   ログインに成功すると、使用する TOTP ベースの承認アプリケーションが iRMC によって受理され、エマージェンシーコードでダイアログボックスが開きます。

図 18:「ワンタイムエマージェンシーコード」ダイアログボックス

これらのエマージェンシーコードは 1 回だけ表示されます。このコードは、2 要素認証を使用してログインできなくなった場合に使用できます。たとえば、TOTP ベースの承認アプリケーションを持つデバイスを紛失した場合や、デバイスやアプリケーションが破損した場合です。

8. スクリーンショットを取るなどして、エマージェンシーコードを保存します。
9. 「**確認**」をクリックします。

   iRMC Web インターフェースが開き、「**システム概要**」ページが表示されます。

   セットアップの手順の後、ログインすると、最初のログイン時に使用した TOTP ベースの認証アプリケーションにリンクされます。以降のすべてのログインについては、2 番目の認証ダイアログボックスには「**TOTP コード**」入力フィールドのみが含まれます。

   ユーザアカウントの 2 要素認証設定のステータスは、「有効 - 構成済み」に変更されます。

図 19:「ローカルユーザーアカウントの編集」ダイアログボックス

承認アプリケーションを使用できなくなった場合は、iRMC Web インターフェースにログインできなくなり、ユーザアカウントの 2FA を再設定する必要があります。

5.3.1.3 エマージェンシーコードの使用

エマージェンシーコードは、iRMC Web インターフェースへの無制限の 2FA アクセスを得るために、1 回のみ使用できます。

使用する TOTP ベースの承認アプリケーションを持つデバイスが紛失または破損した場合、次の手順に従って iRMC にログインします。

1. リモートワークステーションから Web ブラウザを開きます。
2. iRMC の（設定済みの）DNS 名または IP アドレスを入力します。

   ログインダイアログボックスが開きます。

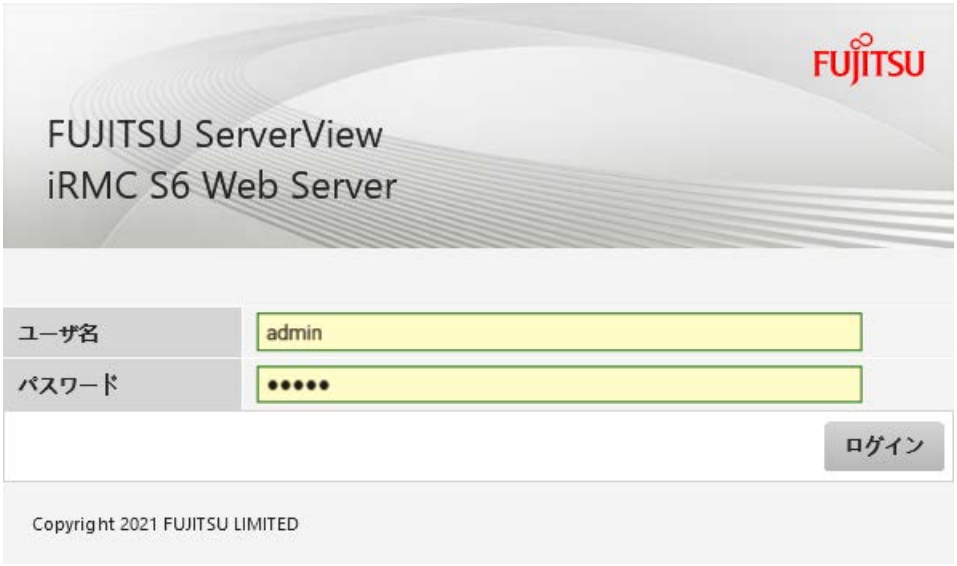


図 20:「ログイン」ダイアログボックス

3. 資格情報（ユーザ名とパスワード）を入力します。
4. 「**ログイン**」をクリックして、ログインを確定します。

   次のダイアログボックスが開きます。

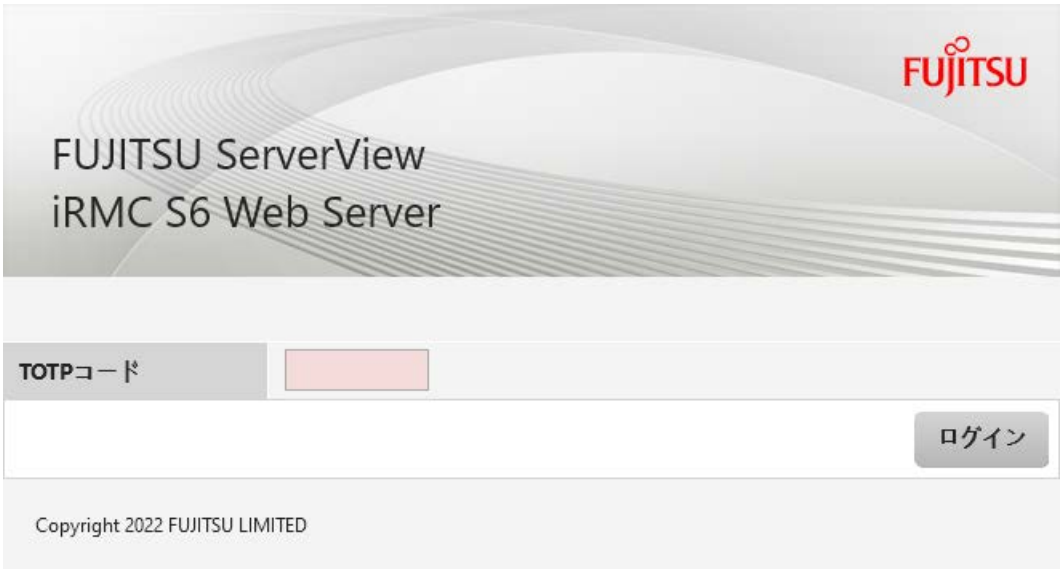


図 21: 2FA の「ログイン」ダイアログボックス

5. エマージェンシーコードの 1 つを「**TOTP コード**」入力フィールドに入力します。
6. 「**ログイン**」をクリックします。

   iRMC Web インターフェースが開き、「**システム概要**」ページが表示されます。

5.3.1.4 ユーザアカウントの 2FA の再構成

すべてのエマージェンシーコードが使用され、使用していた TOTP ベースの承認アプリケーションが利用できなくなった場合、2 要素認証を別のアプリケーションでセットアップする必要があります。この場合、管理者は古い構成をクリアして、新しい構成を用意する必要があります。

1. iRMC Web インターフェースに管理者としてログインします。
2. 「**設定**」メニューで「**ユーザ管理**」ページを開きます。
3. 「**iRMC ローカルユーザアカウント**」グループを開きます。
4. 既存の iRMC ユーザで「**編集**」をクリックします。
5. 「**ローカルユーザアカウントの編集**」ダイアログボックスで、「**アクセス設定**」タブを開きます。
6. 「**二要素認証**」タブを開きます。
7. 「**強制再構成**」オプションをオンにします。
8. 「**OK**」をクリックします。

   ユーザアカウントの 2 要素認証設定がクリアされます。ユーザは別の TOTP ベースの承認アプリケーションを iRMC に導入する必要があります。

5.3.2 SSHv2 によるセキュアな認証

ユーザ名とパスワードによる認証方法に加えて、iRMC は SSHv2 に基づくローカルユーザの公開キーと秘密キーのペアを使用する公開キー認証もサポートしています。SSHv2 公開キー認証を実装するため、iRMC ユーザの SSHv2 キーを iRMC にアップロードします。iRMC ユーザは自分の秘密キーをプログラム PuTTY または OpenSSH クライアントプログラムなどと一緒に使用します。

iRMC は SSH RSA 公開キーをサポートしています。iRMC へアップロードする SSHv2 公開キーは、RFC4716 フォーマットでも OpenSSH フォーマットでも使用可能です（80 ページの 例: SSHv2 公開鍵）。

公開キー認証

iRMC の公開キー認証は、基本的に以下のように処理されます。

iRMC にログインするユーザが鍵のペアを作成します。

- 秘密キーは読み取り保護され、ユーザのコンピュータ内に保存されます。
- ユーザ（または管理者）は公開キーを iRMC にアップロードします。

設定が正しければ、ユーザはパスワードを入力しなくても安全に iRMC にログインできるようになります。ユーザの責任は秘密キーの機密保護のみです。

秘密キー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 の公開キーと秘密キーを作成して、別々のファイルに保存します（71 ページの SSHv2 公開鍵と秘密キーの作成）。
2. SSHv2 公開キーをファイルから iRMC にアップロードします（75 ページの SSHv2 公開鍵をアップロードする）。
3. プログラム PuTTY または ssh を iRMC への SSHv2 アクセス用に設定します（76 ページの SSHv2 公開鍵の使用）。

5.3.2.1 SSHv2 公開鍵と秘密キーの作成

SSHv2 公開鍵と秘密キーは以下の方法で作成することができます。

PuTTYgen プログラムを使用する

1. ユーザの Windows コンピュータで PuTTYgen を起動します。

   PuTTYgen のメインウィンドウが開きます。

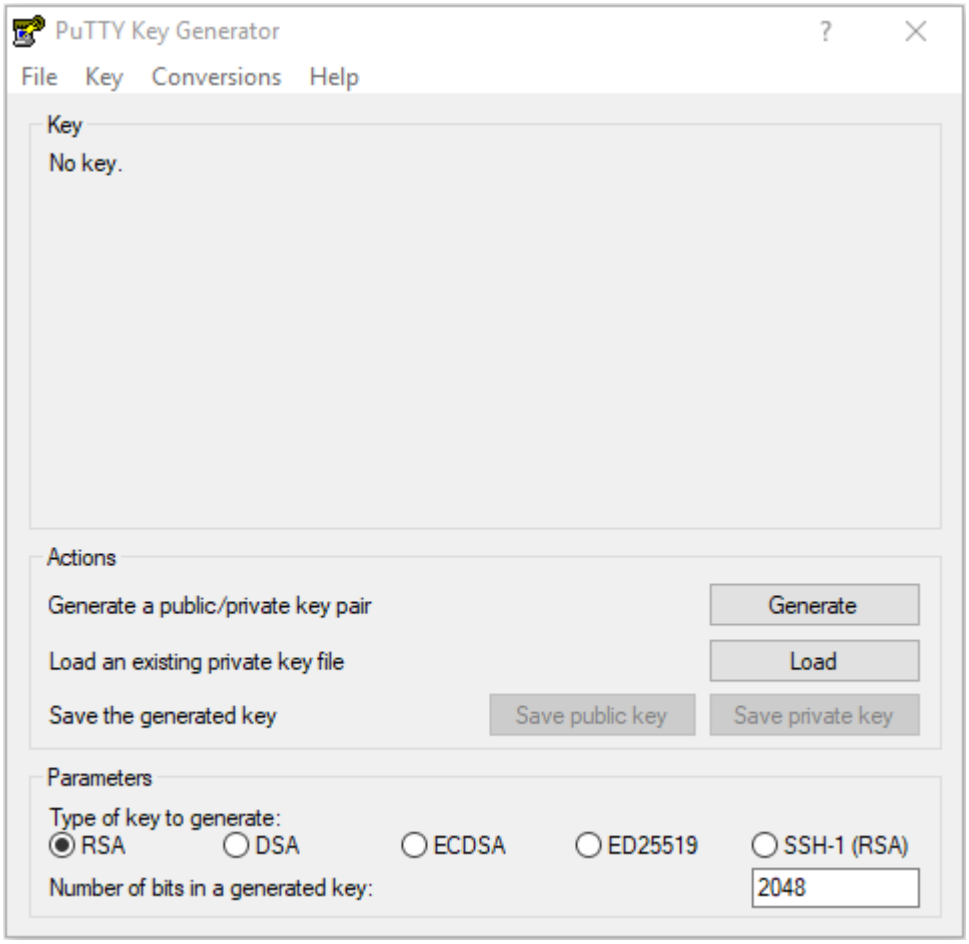


図 22: PuTTYgen: 新しい SSHv2 公開鍵と秘密キーの作成

2. 「Parameters」グループで「RSA」キータイプを選択します。
3. 「Generate」をクリックして、鍵の生成を開始します。

   プログレスバーに生成の進行状況が表示されます。
4. プログレスバー上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SSHv2 公開鍵のフィンガープリントを表示します。

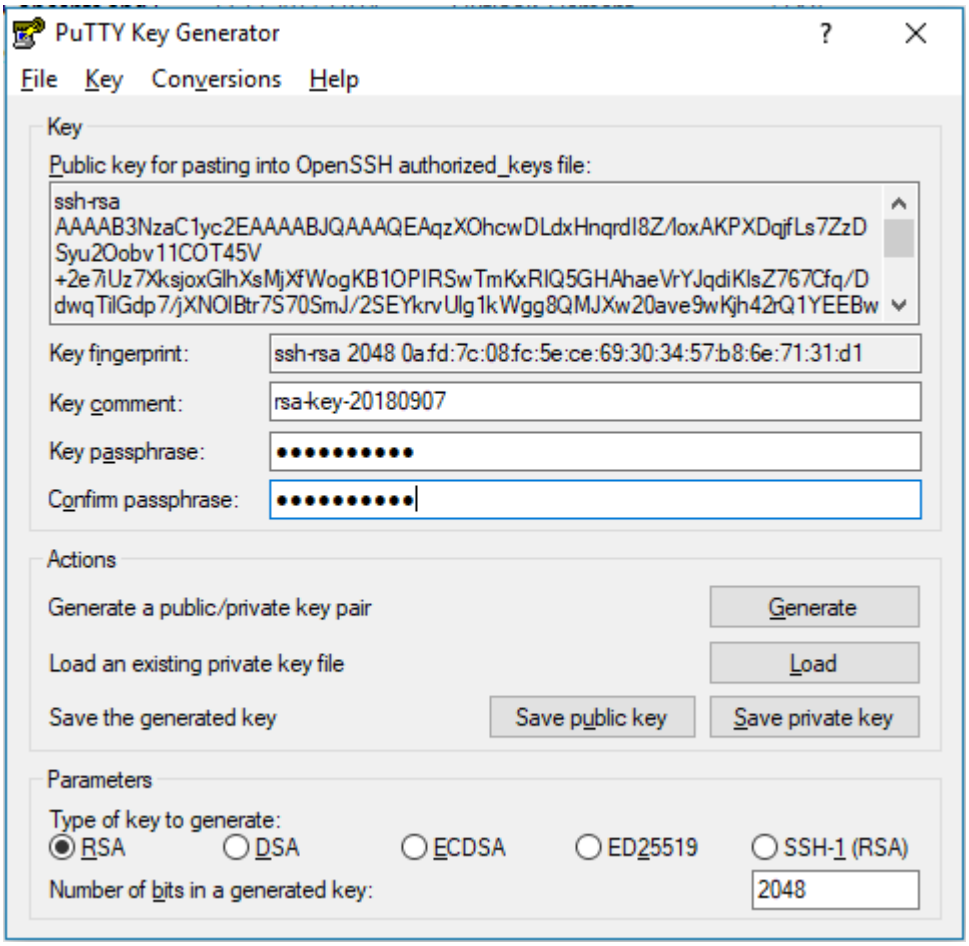


図 23: PuTTYgen: 生成された秘密 SSHv2 キー

5. 「Save public key」をクリックして、SSHv2 公開鍵をファイルに保存します。公開鍵をこのファイルから iRMC にアップロードできます（75 ページの SSHv2 公開鍵をアップロードする）。
6. 「Save private key」をクリックして、PuTTY に使用する秘密 SSHv2 キーを保存します。

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

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 のパラメータの詳しい説明は、http://www.openssh.org/manual.html で OpenSSH ユーザガイドを参照してください。

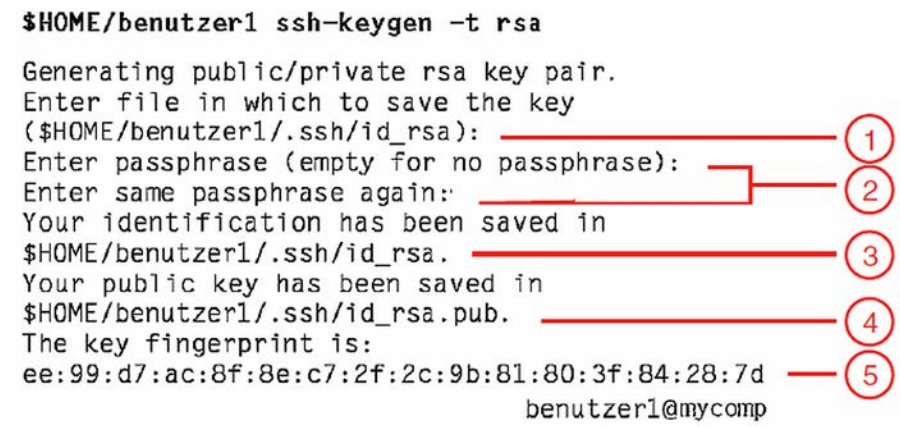
次の手順に従います。

1. コマンドウィンドウを開きます。
2. 「ssh-keygen」を呼び出して RSA キーのペアを生成させます。

   `ssh-keygen -t rsa`

   ssh-keygen は、鍵生成処理の進行状況をログに記録します。ssh-keygen は、ユーザに秘密キーが保存されるファイル名および秘密キーのパスフレーズを要求します。ssh-keygen は、生成された SSHv2 公開鍵と秘密キーを別のファイルに保存し、公開キーのフィンガープリントを表示します。

例:「ssh -keygen」による RSA キーペアの生成



説明

1. ssh-keygen はSSHv2 キー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 は、ユーザに秘密キーの暗号化に使用するパスフレーズの入力（およびその確定）を要求します。パスフレーズを入力せずに［Enter］を押して確定しても、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 キーが `/.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SSHv2 公開鍵が `/.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SSHv2 公開鍵のフィンガープリントと公開鍵が属するローカルのログインを表示します。

5.3.2.2 SSHv2 公開鍵をアップロードする

SSHv2 公開キーをファイルから iRMC へアップロードするには、以下の手順に従います。

1. iRMC Web インターフェースのログイン
2. 「**設定**」メニューで「**ユーザ管理**」ページを開きます。
3. 設定されたユーザのリストで、対応するユーザの横の「**編集**」をクリックします。
4. 「**ローカルユーザアカウントの編集**」ダイアログボックスで、「**証明書**」タブを開きます。
5. 「**SSHv2 公開キー**」サブタブを開きます。
6. 「**アップロード**」グループで「**選択**」をクリックして、必要な公開キーを含むファイルに移動します。
7. 「**アップロード**」ボタンをクリックして公開キーを iRMC 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 は「**フィンガープリント**」グループに鍵のフィンガープリントを表示します。

図 24: キーフィンガープリントの表示

8. セキュリティ上の理由から、ここに示すフィンガープリントが PuTTYgenの「Key fingerprint」フィールドに表示されるものと一致することを確認してください（71 ページの SSHv2 公開鍵と秘密キーの作成）。

5.3.2.3 SSHv2 公開鍵の使用

SSHv2公開キーを使用するには、適切なツールを設定する必要があります。

SSHv2 公開キーを使用する PuTTY の設定

PuTTY プログラムでは、iRMC への公開キー認証接続のセットアップと、自身のユーザ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SSHv2公開キー/秘密キーのペアに基づいて、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。

1. ユーザの Windows コンピュータで PuTTY を起動します。

   PuTTY のメインウィンドウが開きます。

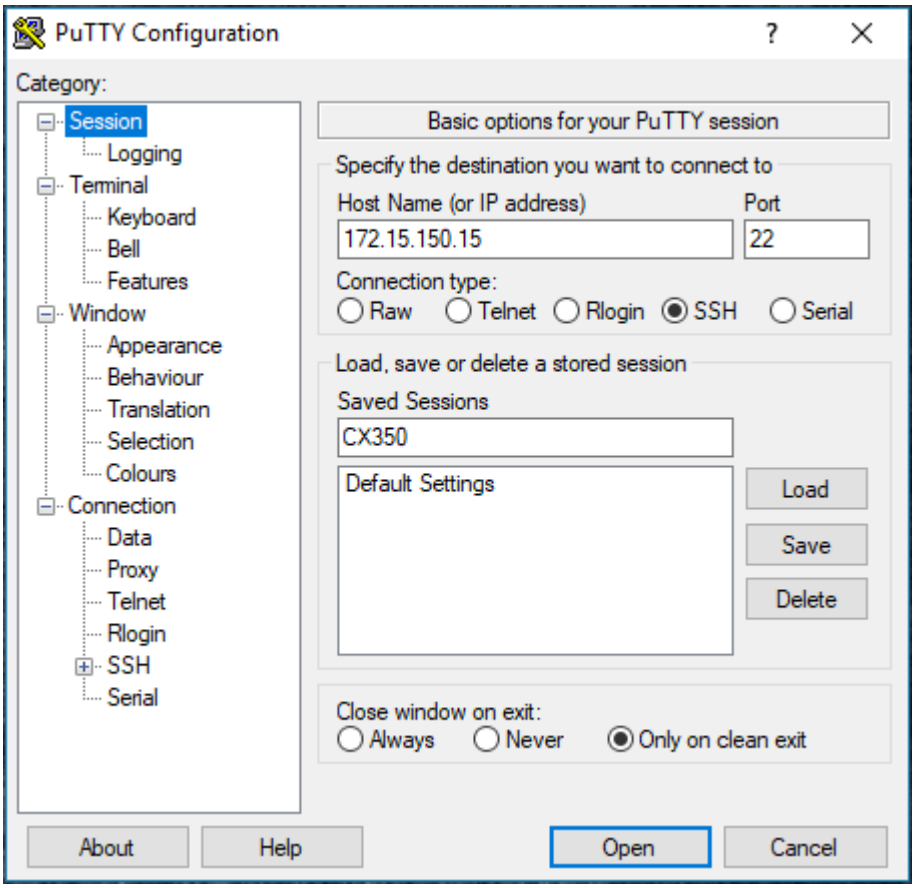


図 25: SSH セッションの選択とロード

2. 「**Saved Sessions**」リストで、SSHv2 キーを使用する iRMC S6 との SSH セッションを選択します。新しいセッションを作成することもできます。
3. 「**Load**」をクリックして選択した SSH セッションのパラメータをロードします。
4. 「**Category**」ツリーで、「**SSH/Auth**」を選択して SSH 認証オプションを設定します。

   認証パラメータが表示されます。

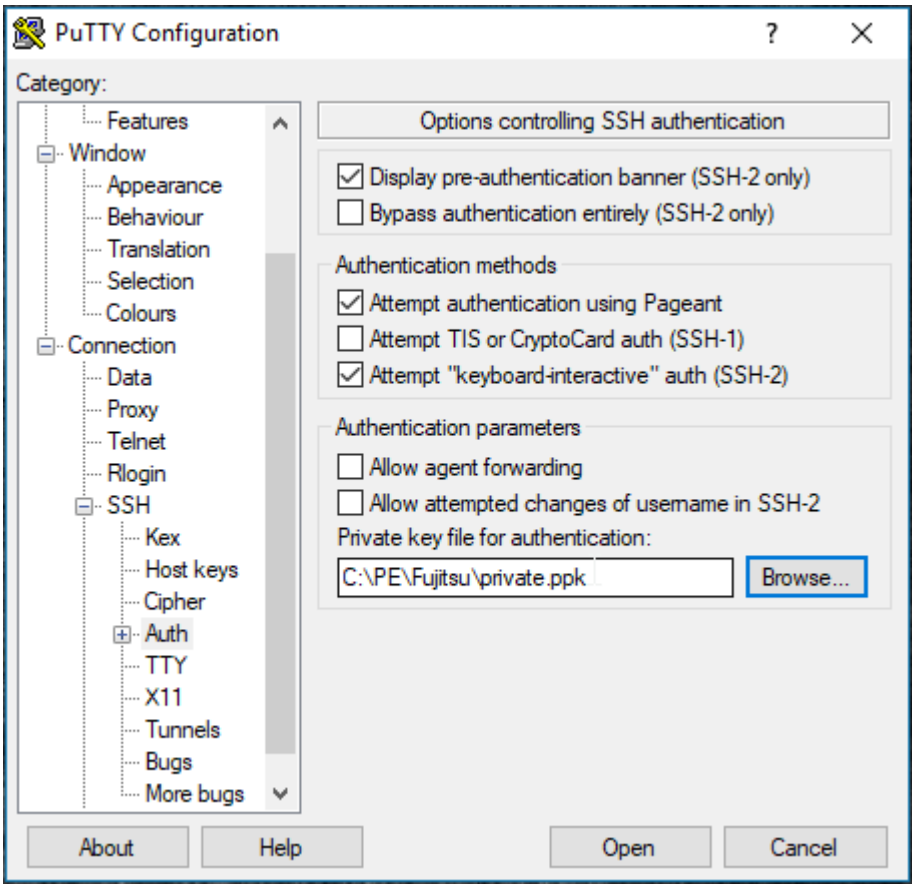


図 26: SSH 認証のオプションの設定

5. iRMC S6 で使用する秘密キーが入ったファイルを選択します。

   この時点で、iRMC にアップロードした公開キーではなく、秘密キー（71 ページの SSHv2 公開鍵と秘密キーの作成）が必要です。

6. 「**Category**」ツリーで「**Connection/Data**」を選択して、iRMC への自動ログインに使用するユーザ名をさらに指定します。

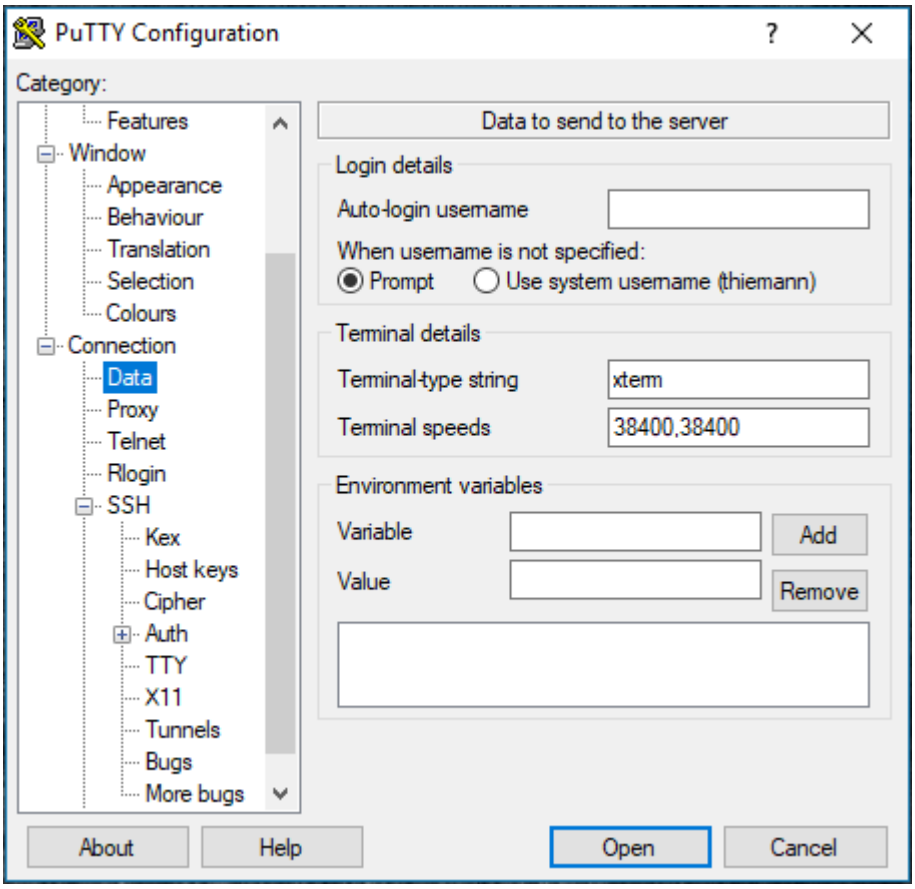


図 27: PuTTY: iRMC に自動ログインするユーザ名の指定

SSHv2 公開キーに使用する 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 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 S6 上のローカルログインとして設定され、関連する SSHv2 キーは iRMC 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。

- 「ssh」を呼び出すときに使用したコマンドライン引数
- ユーザごとの設定ファイル（`$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。ほかのどのユーザに対しても、アクセスを拒否してください。

- 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。

  - ユーザごとの設定ファイルがない。
  - ユーザ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 の設定とそのパラメータ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。

1. コマンドウィンドウを開きます。
2. 「ssh」を起動して、SSHv2 認証により iRMC にログインします。

   ```
   ssh -l [<ユーザ>] <iRMC_S6>
   ```
   または
   ```
   ssh [<ユーザ>@]<iRMC_S6>
   ```

<ユーザ>
: iRMC へのログインに使用するユーザ名。<ユーザ> を指定しない場合は、ssh は、ローカルコンピュータにログインしているユーザ名を使用します。

<iRMC_S6>
: ユーザがログインしようとする iRMC 名または、iRMC の IP アドレス。

例：iRMC への SSHv2 認証ログイン

次の ssh 呼び出しでは、公開キーと秘密キーのペアの生成に ssh-keygen が使用されたこと（71 ページの SSHv2 公開鍵と秘密キーの作成）と、公開キー User1/.ssh/id_rsa.pub が iRMC ユーザ user4 のために iRMC にロードされたこと（75 ページの SSHv2 公開鍵をアップロードする）を前提としています。

ユーザは自身のローカルコンピュータから、「$HOME/User1」でユーザ名「user4」を使用して、以下のように iRMC "RX300_S82-iRMC" にログインすることができます。

```
ssh user4@RX300_S82-iRMC
```

5.3.2.4 例: SSHv2 公開鍵

同じSSHv2 公開鍵を、種類のフォーマットで以下に示します。

RFC4716 フォーマット

```
---- BEGIN SSH2 PUBLIC KEY ----
コメント : "rsa-key-20090401"
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US6/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH フォーマット

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+\
AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US6/9ArJxj
lhXUzlPPVzuBtPaRB7+\
bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+FpGJ2iw== rsa-key-
20090401
```

5.3.3 ローカル iRMC ユーザへの E メール警告の設定

ローカル iRMC ユーザへの E メール警告が、iRMC ユーザ管理システムに組み込まれています。このため、E メール警告を管理対象サーバで設定して処理できます。ローカル iRMC ユーザへの Eメール警告により、異常なコンポーネント状態やコンポーネント故障が特定された場合、管理対象サーバでメッセージを生成して転送できます。

Eメール警告を関連する iRMC の Web インターフェースで個別に指定するには、「**ローカルユーザアカウントの追加**」または「**ローカルユーザアカウントの編集**」ダイアログボックスでユーザのプロパティを設定します。

一般的な情報と Fujitsu サポートへの警告送信については、36 ページの 外部通信および116 ページの グローバル Eメール警告送信の項を参照してください。

5.4 グローバルユーザ管理

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

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

グローバルユーザ管理は現在 iRMC の以下の機能ではサポートされていません。

- IPMI-over-LAN 経由のログイン
- SOL 経由のコンソールリダイレクション

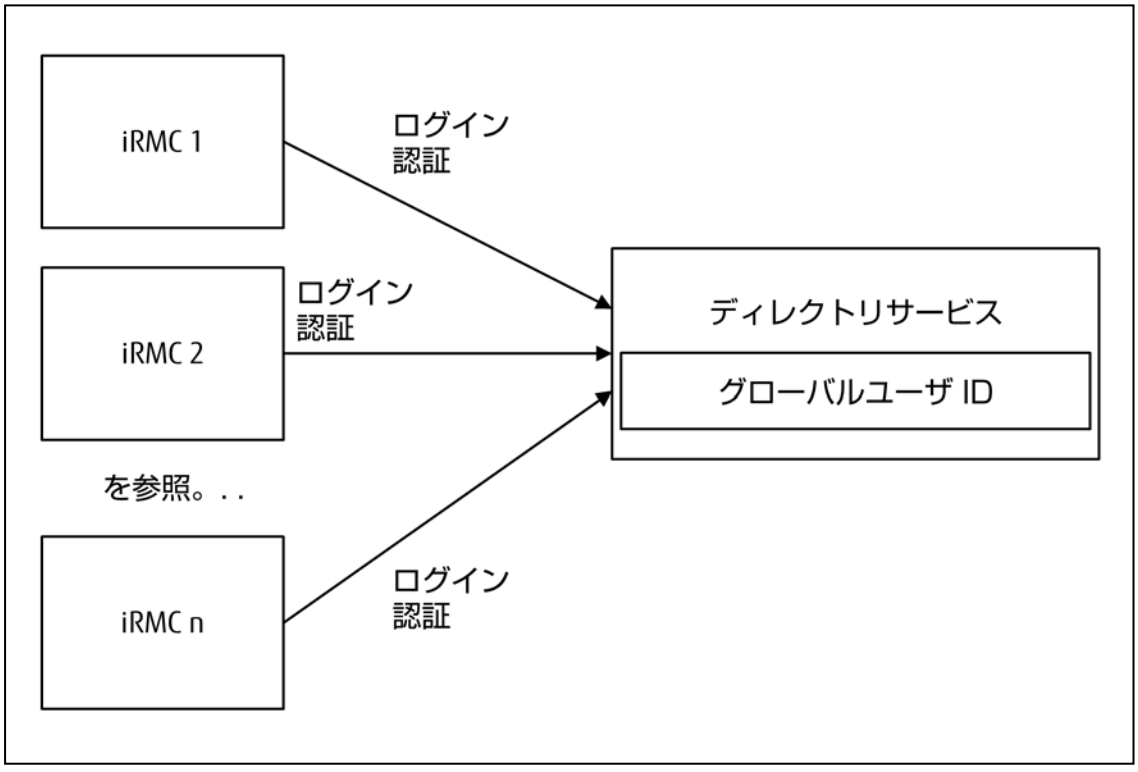


図 28: 複数の iRMC によるグローバルユーザ ID の共用

個々の iRMC と中央ディレクトリサービスの間の通信は TCP/IP プロトコル LDAP（Lightweight Directory Access Protocol）経由で実行されます。LDAP によって、ディレクトリサービスにアクセスする方法が最もよく使われ、ユーザ管理に最も

適しています。オプションで、LDAP 経由の通信は、SSL によってセキュリティを確保することができます。

グローバル iRMC ユーザ管理の設定を行うには、使用するディレクトリサービスに関して熟知している必要があります。ディレクトリサービスを熟知した管理者以外は作業を行わないでください。

5.4.1 LDAP ディレクトリサービスを使用するユーザ管理の概念

ディレクトリサービスベースの、グローバルなユーザ管理の概念は、以下のディレクトリサービスにも同様に適用されます。

- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP、OpenDJ、OpenDS、ApacheDS などのオープンディレクトリサービス

図は、Microsoft Active Directory ユーザインターフェースの **Active Directory Users and Computers** コンソールの例に基づいています。

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。

5.4.1.1 ユーザロール

LDAP ディレクトリサーバ経由のグローバル iRMC ユーザ管理では、標準のディレクトリサーバのスキーマを拡張する必要はありません。その代わりに、ディレクトリサーバに関連するすべての情報は、ユーザ権限も含めて、追加 LDAP グループと組織単位（OU）を使用して提供されます。これらの OU は、LDAP ディレクトリサーバのドメイン内の別々の OU で結合されたものです（図83 ページの 組織単位（OU）SVSを参照）。

iRMC ユーザは、組織単位（OU）**SVS** で宣言された役割（ユーザロール）を割り当てられることで、権限を取得します。

ユーザロール（略称: ロール）による許可の割り当て

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

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

図は、Administrator、Maintenance、Observer および UserKVM の各ロールによるユーザ権限の、ロールに基づく割り当ての概念を図解したものです。

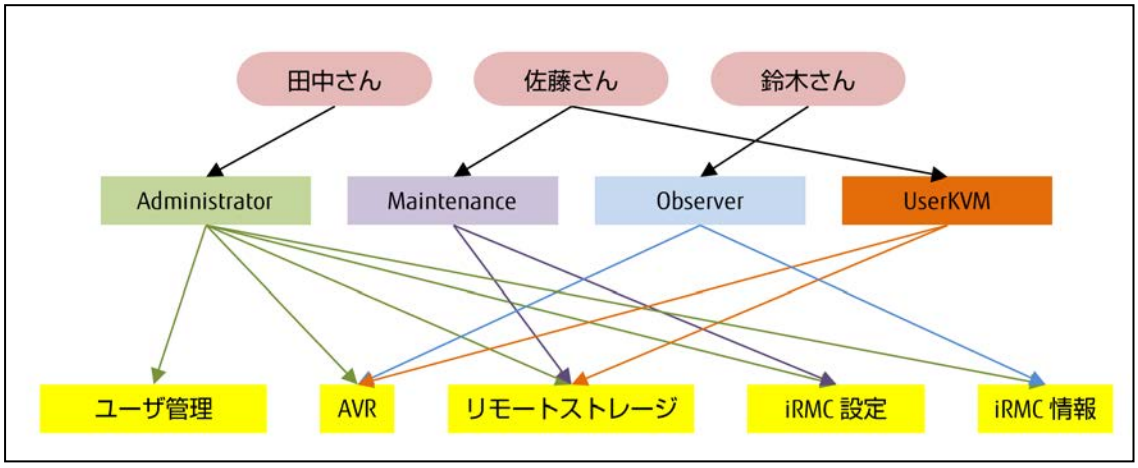


図 29: ロールに基づくユーザ権限の割り当て

ユーザロールの概念には、以下のような重要な利点があります。

- 各々のユーザまたはユーザグループに、個別に許可を割り当てる必要がない。その代わりに、許可はユーザロールに従って割り当てられる。
- 許可のストラクチャが変更になった場合にユーザロールによる許可を適合させるのみでよい。

5.4.1.2 組織単位（OU）SVS

iRMC ファームウェアは、OU「SVS」に保存されている LDAP v2 ストラクチャをサポートします。LDAP v2 ストラクチャはすべて今後の機能拡張に向けて設定されています。

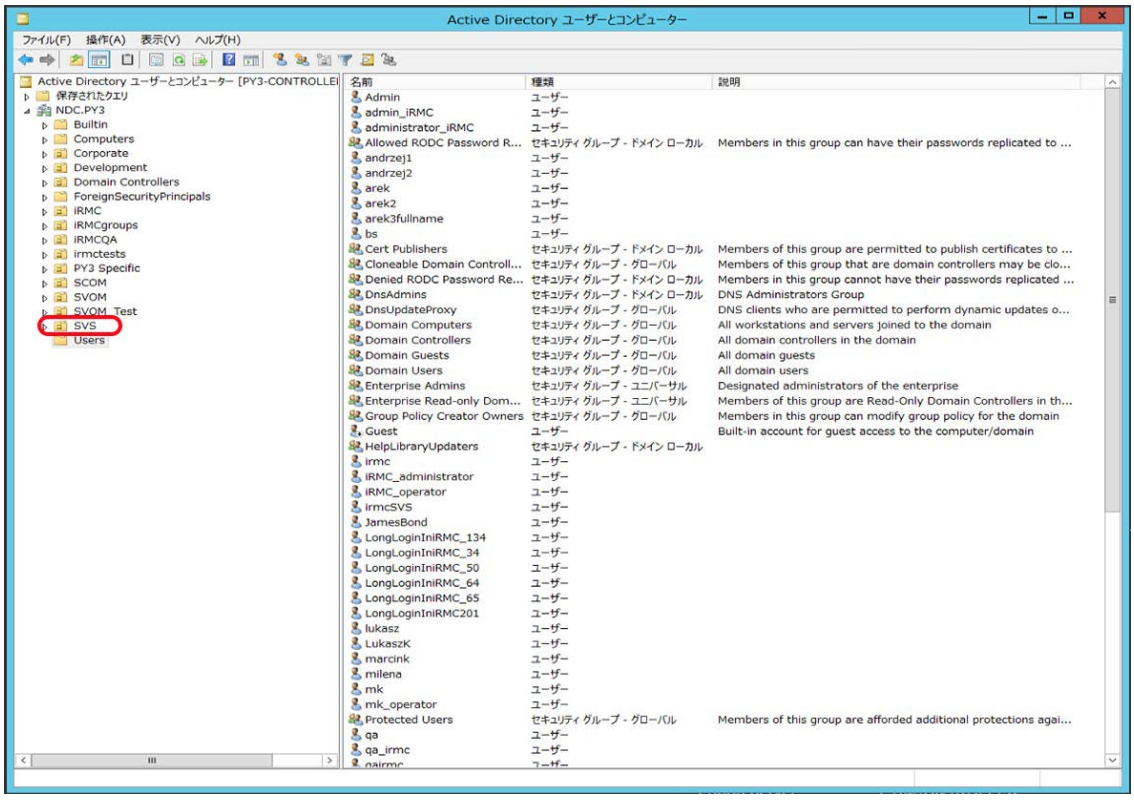


図 30: NDC.PY3 ドメインの OU SVS

SVS には、OU Declarations、Departments および User Settings が含まれています。

- Declarations には、定義されたロールのリストと定義済みの iRMC ユーザ権限のリストが含まれています。
- Departments には、ユーザ権限のためのグループが含まれています。
- User Settings には、メールフォーマット（警告メールに使用します）などのユーザまたはユーザグループ固有の詳細情報と、ユーザシェルのためのグループが含まれています。

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

たとえば、Microsoft Active Directory の場合には、iRMC ユーザのエントリは標準 OU である Users に納められています。ただし、iRMC ユーザは標準ユーザとは異なり、OU SVS の 1 つまたは複数のグループのメンバーにもなっています。

ServerView ユーザ管理と iRMC グローバルユーザ管理の両方を同じ組織単位（OU）SVS で動作させるには、iRMC ユーザ管理が DEFAULT 部門に属するように設定する必要があります。

5.4.1.3 多部門サーバー、グローバルアクセス権限

大規模な企業では、iRMC によって管理されるサーバは通常さまざまな部門に割り当てられます。また、管理対象サーバの管理者権限も、多くの場合部門独自の方法で割り当てられます。

OU **Departments** は、iRMC によって管理されるサーバを結合し、多数のグループを形成します。これらのグループは、同じユーザ ID と許可が適用される部門に対応します。図ではこれらは、**CMS**、**DEFAULT**、**irmctests**、**Others** および **PY3irmc** 部門などです。

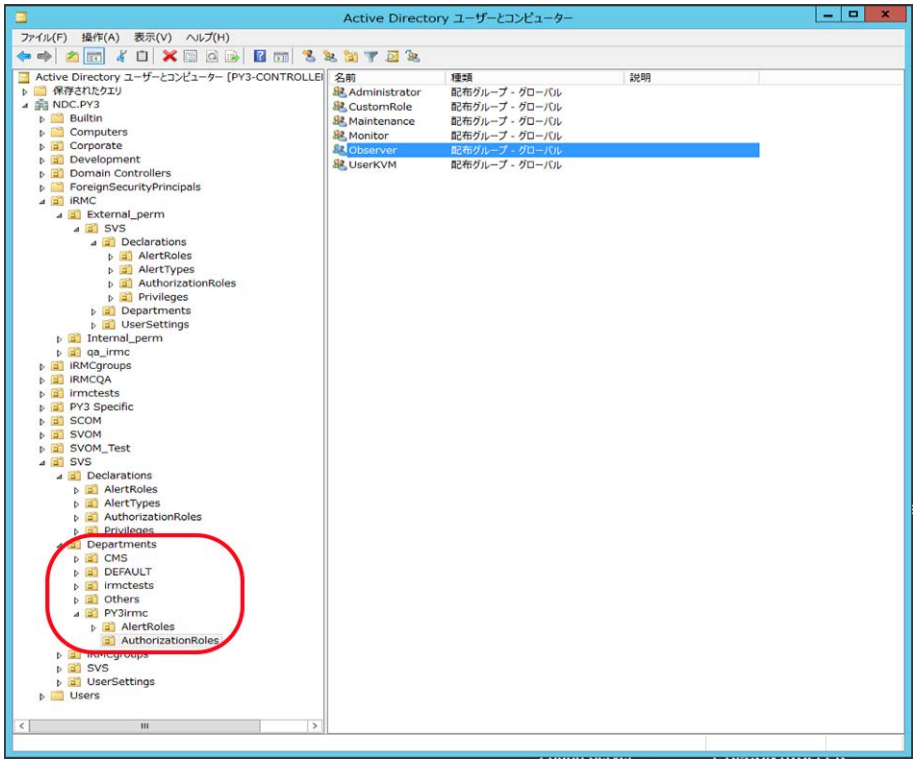


図 31: **NDC.PY3** ドメインの組織構造

Others というエントリは任意ですが推奨します。**Others** は、これらのサーバすべてに内包される予め定義された部門名で、他の部門に属することはありません。**Departments** の下にリストされる部門（OU）の数に関しては、制限はありません。

iRMC Web インターフェースを使用してディレクトリサービスを設定する場合は、関連する iRMC が属する管理対象サーバの部門名を指定します。LDAP ディレクトリにその名前の部門がない場合には、**Others** 部門にある権限を使用します。

5.4.1.4 SVS: ロールにより定義される許可プロファイル

要求される関連ユーザロール（認証ロール）は各部門の直下にリストされます。ここにリストされるロールはすべて OU Declarations で定義されます。それ以外にロールの数に関する制限はありません。ロールの名前は必要に応じて選ぶことができますが、運用するディレクトリサービスに賦課された特定のシンタックス要件に合わなければなりません。各認証ロールは、iRMC 上の処理のためにタスクに基づく許可プロファイルを個々に定義します。

認証ロールと同様に警告ロールもリストされます。各警告ロールには Eメール警告用の特定の警告プロファイルを定義します（「116 ページの グローバル iRMC ユーザへの Eメール警告の設定」の項を参照）。

ユーザロールの表示

「Active Directory ユーザとコンピュータ」の構造ツリーの SVS の下で部門（PY3irmc など）を選択して関連ノード PY3irmc - Authorization Roles にマークした場合、この部門に定義されたユーザロール（ここでは PY3irmc）が右側の領域に表示されます。

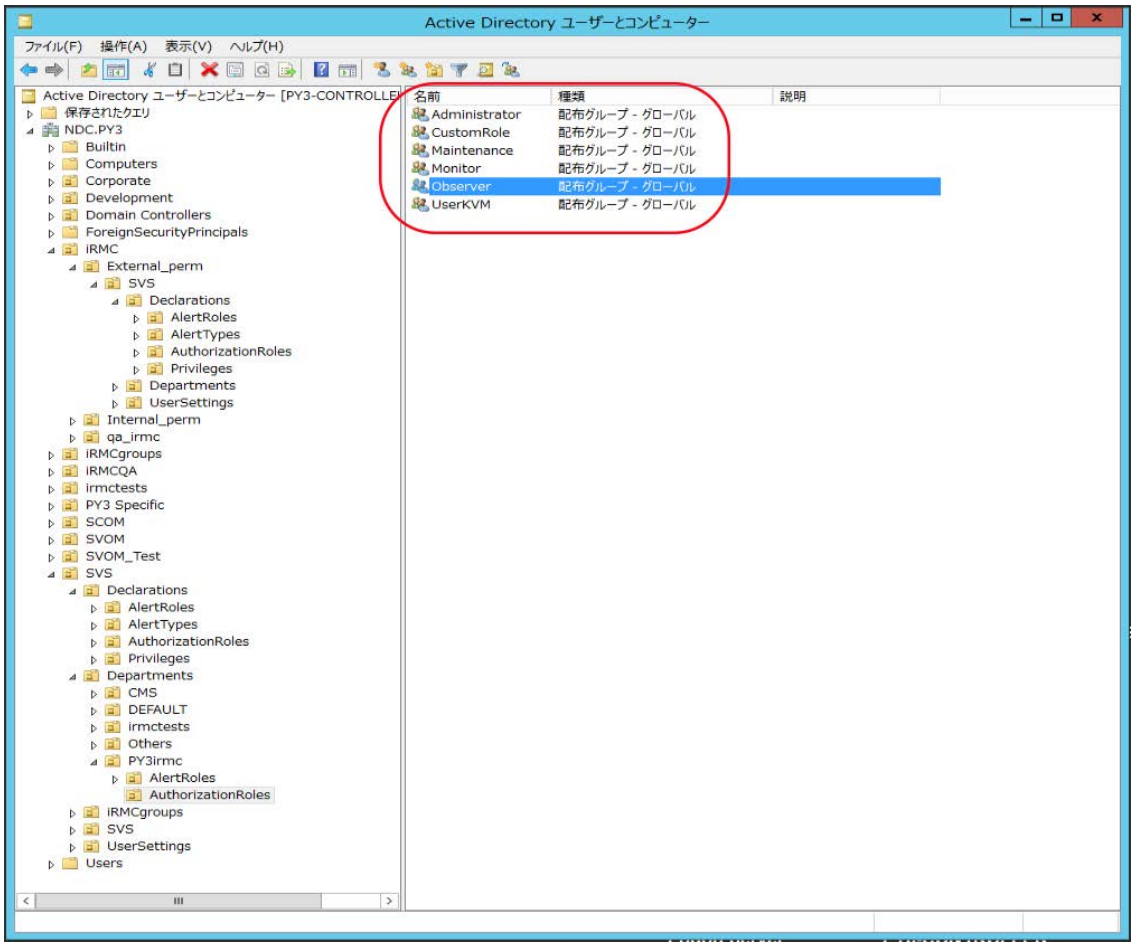


図 32: 「**ユーザとコンピュータ**」スナップインでのユーザロールの表示

ユーザがメンバーとなっている Active Directory フォルダの表示

「**Active Directory ユーザとコンピュータ**」の構造ツリーの「**Users**」の下にあるユーザ（例: **kvms4**）を選択し（1）、コンテキストメニューから「**プロパティ- - メンバ**」を選択してこのユーザの「**プロパティ**」ダイアログボックスを開くと、ユーザが所属する許可グループ（ここでは「**kvms4**」）が「**メンバ**」タブの中に表示されます（2）。

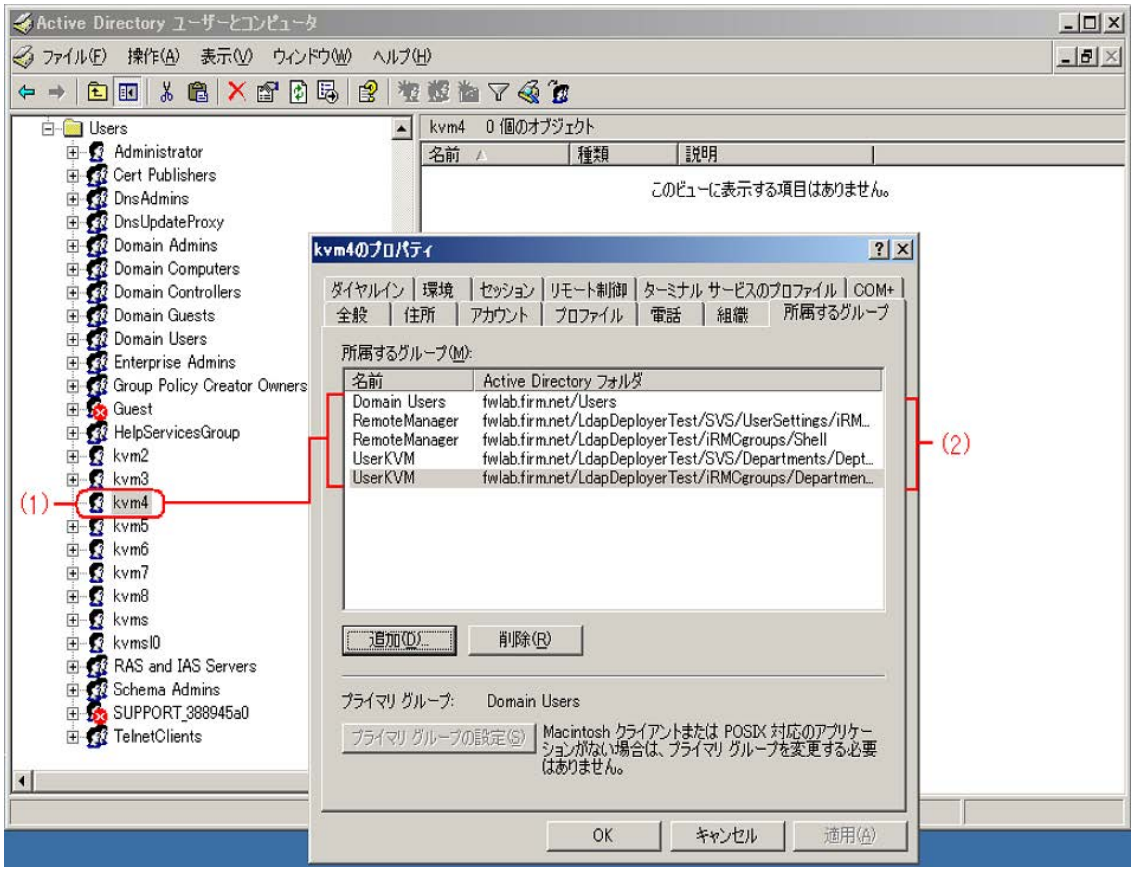


図 33: ユーザ kvms4 の「**プロパティ**」ダイアログボックス

5.4.2 コラボレーションの構成ステップ

iRMC は各種 LDAP ディレクトリサービスで使用できるので、実行中のディレクトリサービスとのコラボレーションを構成してグローバルユーザ認証を確実に行うには、いくつかのステップが必要です。

1. SVS_LdapDeployer ユーティリティを使用して、必要な SVS OU を作成します。
2. オプション: CA 証明書を使用して、iRMC と LDAP サーバ間の安全な接続を準備します。
3. iRMC ユーザ管理をディレクトリサービスに統合します。
4. ディレクトリサービスで、ユーザロールを iRMC ユーザに割り当てます。
5. オプション: ディレクトリサービスで Eメール警告送信を設定します。
6. LDAP 認証について iRMC を設定します。

5.4.3 SVS_LdapDeployer ユーティリティ

ディレクトリサービスで グローバル iRMC ユーザ管理を行うには、LDAP ディレクトリサービスに（OU）SVS ストラクチャを提供する必要があります。SVS_LdapDeployer ユーティリティでは、必要な SVS ストラクチャの生成や変更ができます。

SVS_LdapDeployer は XML 設定ファイルに基づいて LDAP ストラクチャを生成します。この入力ファイルには、SVS ストラクチャの XML 構文によるストラクチャ情報が含まれています。

ディレクトリサーバ接続に有効なデータは、設定ファイルの <Settings> 領域に入力する必要があります。SVS_LdapDeloyer の設定ファイルまたはコマンドラインで、サーバにアクセスするための認証データを入力できます。

SVS_LdapDeployer を呼び出すときに認証データを指定しないと、実行時に SVS_LdapDeployer から認証データを入力するように求められます。

SVS_LdapDeployer は Java アーカイブ（SVS_LdapDeployer.jar）で、Fujitsu サポートページのダウンロードエリアで提供されています。VS_LdapDeployer には各種用途向けの一連のサンプル設定ファイルとディレクトリサービスが付属し、sampleFiles フォルダ内で分類されています。

5.4.3.1 SVS_LdapDeployer の構文

以降では、「LDAPv1 ストラクチャ」および「LDAPv2 ストラクチャ」という用語を使用して、認証データの ServerView 固有の設定レイアウトを示します。LDAP プロトコルのバージョン 1 および 2 を指すものではありません。

iRMC S6 のユーザ管理では、LDAPv2 ストラクチャが必要です。

構文

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

<command>

実行する処理を指定します。

以下のコマンドを使用可能です。

-deploy
: グローバル iRMC ユーザ管理の LDAP ストラクチャをディレクトリサーバの中に作成します。

`-delete`
グローバル iRMC ユーザ管理に用いた LDAP ストラクチャをディレクトリサーバから削除します。

次のコマンドは、互換性の理由でのみ説明します。iRMC S6 では使用されません。

`-import`
既存の LDAP v1 ストラクチャから同等の LDAP v2 ストラクチャを作成します。両方のストラクチャは、<Settings>\<root> で指定される同じサブツリーに配置されます。

`-synchronize`
LDAP v2 ストラクチャに何らかの変更を行うと、その変更を反映して既存の LDAP v1 ストラクチャを同じように変更します。

<file>
SVS_LdapDeploy が入力ファイルとして用いる設定ファイル（`.xml`）。この設定ファイルには、SVS ストラクチャの XML 構文によるストラクチャ情報が含まれています。


設定ファイルの構文は、`jar` アーカイブと共に提供されるサンプル設定ファイルで説明されています。

<options>
指定されたコマンドの実行をコントロールするためのオプションです。すべてのオプションは任意です。

`-structure v1 | -structure v2 | -structure both`
iRMC S3 のみ: LDAP v1 ストラクチャまたは、LDAP v2 ストラクチャ、あるいは、LDAP v1 と LDAP v2 両方のストラクチャを作成します。

`-username <user>`
ディレクトリサーバにログインするためのユーザ名です。

`-password <password>`
<user> のパスワード

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

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

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

`-kpwd [<password>]`
ランダムに生成された鍵を保護するためのパスワードを指定します。
<password> が指定されない場合は、現行のランタイムのスナップショットを基にしてパスワードが自動的に生成されます。デプロイメントファイルに保存されたユーザパスワードの暗号化を解読するには、暗号化に使用したものと同じコンテキストでアプリケーションを実行する必要があります。

5.4.3.2 SVS_LdapDeployer の起動

前提条件:

- LDAP ディレクトリサービスが対応するサーバにインストールされて実行中であること。
- 次の手順で使用するユーザアカウントに Administrator ロールが割り当てられていること。

次の手順に従って SVS_LdapDeployer を起動します。

1. Fujitsu ダウンロードエリアを開いて SVS_LdapDeployer ユーティリティをダウンロードします。
2. ダウンロードした zip ファイルを解凍します。
3. 関連するすべてのデータを含む適切な設定ファイルを編集するか、作成します。
4. LDAP ディレクトリサーバにログインします。
5. Java アーカイブ（`jar` アーカイブ）の `SVS_LdapDeployer.jar` と設定ファイルをディレクトリサーバ上のフォルダに保存します。
6. ディレクトリサーバのコマンドインターフェースを開きます。
7. `jar` アーカイブの `SVS_LdapDeployer.jar` が常駐するフォルダに移動します。
8. SVS_LdapDeployer ユーティリティを呼び出します（次の例を参照）。

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

SVS_LdapDeployer の実行中に行われるさまざまな手順が通知されます。詳細な情報は `log.txt` ファイルで見ることができます。このファイルは SVS_LdapDeployer 実行時に毎回実行フォルダの中に作られます。

ディレクトリサービスにOU **SVS** の生成後に、使用するディレクトリサービスで対応するツールを使用して、ユーザエントリをグループに作成して割り当てる必要があります。

5.4.3.3 例

次の例は、SVS_LdapDeployer を使用するための、3 つの典型的なシナリオで構成されます。

LDAP v2 ストラクチャの初期設定の実行

iRMC のグローバルユーザ管理を初めて設定する場合は、LDAP v2 ストラクチャが必要です。

推奨する方法:

LDAP v2 ストラクチャ（(SVS）の **Department** 定義を生成します:

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

LDAP v2 ストラクチャの再生成と展開

LDAP v2 ストラクチャを再生成するか、既存の LDAP v2 ストラクチャを展開する場合。

推奨する方法:

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

または

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

LDAP v2 ストラクチャの再生成と、認証データの要求と保存

LDAP v2 ストラクチャを再生成する場合。認証データはコマンドラインを用いて作成し、保存します。

推奨する方法:

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

ログインデータを保存した後には、ユーザ名およびとパスワードを指定せずに SVS_LdapDeployer を使用してディレクトリサーバに接続してください。SVS_

LdapDeployer では、XML 設定ファイルに保存されている値を使用します（使用可能な場合）。

SVS_LdapDeployer で保存されたパスワードを使用できるのは、暗号化されたパスワードを解読できる場合のみです。そのため、SVS_LdapDeployer は、`-store_pwd` を用いた前の呼び出しで適用したのと同じランタイム環境で実行する必要があります。このコンテキストで言う「同じランタイム環境」とは、「同じコンピュータを使用する同じユーザ」または「鍵が保存されているフォルダにアクセスする許可を持つユーザ（`-kloc` オプション）を意味します。

今後は、SVS_LdapDeployer を呼び出すときに、すでに保存してあるユーザアカウントを使用することもできます。また、データをコマンドラインに明確に指定するか、SVS_LdapDeployer そのように要求する場合には、他の認証データを一時的に使用することもできます。

5.4.4 Microsoft Active Directory による iRMC ユーザ管理

この項では、iRMC ユーザ管理を Microsoft Active Directory に統合する方法を説明します。

前提条件: LDAP v2 ストラクチャが既に Active Directory で作成されている（「89 ページの SVS_LdapDeployer ユーティリティ」の項を参照）。

iRMC ユーザ管理を Microsoft Active Directory に統合するには、次の手順を実行します。

1. Active Directory サーバで iRMC LDAP/SSL アクセスを設定します。
2. iRMC ユーザを Active Directory の iRMC ユーザグループに割り当てます。

5.4.4.1 Active Directory サーバ上の iRMC LDAP/SSL アクセスの設定

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

iRMC が SSL 経由で LDAP を使用できるようにするには、RSA 証明書が必要です。

LDAP アクセスを設定する手順は以下の通りです。

1. 企業 CA をインストールします。
2. ドメインコントローラ用の RSA 証明書を作成します。
3. サーバに RSA 証明書をサーバにインストールします。

企業 CA のインストール

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

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

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

企業 CA をインストールして正しく設定するには、Active Directory 環境とインストール済みの IIS（Internet Information Services）が必要です。

企業 CA のインストールは以下の手順で行います。

1. コントロールパネルを開いて次を選択します。

   「ソフトウェア」-「Windows コンポーネントの追加と削除」

2. Windows コンポーネントのウィザードで、「Components」から「Certificate Services」を選択します。
3. 「Certificate Services」をダブルクリックし、「Certificate Services Web Enrollment Support」と「Certificate Services CA」のオプションが選択されていることを確認します。
4. 「Enterprise root CA」を選択します。
5. 「Use custom settings to generate the key pair and CA certificate」オプションを選択します。
6. 「Microsoft Base DSS Cryptographic Provider」を選択して 長さ 1024 バイトの DSA 証明書を作成します。
7. 公開認証局証明書（CA 証明書）をエクスポートします。

   これは次の手順で行います。

   a. Windows のプロンプトウィンドウで「mmc」と入力して、Management Console を起動させます。
   b. ローカルコンピュータ証明書のスナップインを追加します。
   c. 「Certificates（Local Computer）」-「Trusted Root Certification Authorities」-「Certificates」へと進み、ダブルクリックします。
   d. 新規に作成された認証局からの証明書をダブルクリックします。
   e. 証明書ウィンドウの「Details」タブを開きます。
   f. 「Copy to File」をクリックします。
   g. 認証局証明書のファイル名を選び、「Finish」をクリックします。

8. 公開認証局証明書をドメインコントローラ上の証明書ディレクトリ Trusted Root Certification Authorities にロードします。

これは次の手順で行います。

a. CA 証明書を収めたファイルをドメインコントローラに転送します。
b. Windows エクスプローラーで、新規に作成された CA からの証明書を開きます。
c. 「Install Certificate」をクリックします。
d. 「Place all certificates in the following store」の下の「Browse」をクリックし、「Trusted Root Certification Authorities」を選択します。
e. Windows のプロンプトウィンドウで「mmc」と入力して、Management Console を起動させます。
f. ローカルコンピュータ証明書のスナップインを追加します。
g. 現在のユーザの証明書のスナップインを追加します。
h. CA 証明書を、現在のユーザの Trusted Root Certification Authorities ディレクトリからローカルコンピュータの Trusted Root Certification Authorities にコピーします。

ドメインコントローラ証明書の作成

ドメインコントローラの RSA 証明書の作成は、以下の手順で行います。

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

```
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic
Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
[EnhancedKeyUsageExtension]OID=1.3.6.1.5.5.7.3.1; this is for
Server Authentication
```

2. ファイル `request.inf` で、`Subject=` の下の指定を、用いているドメインコントローラの名前に合わせます（例:

Subject = "CN=domino.fwlab.firm.net"）。

3. Windows のプロンプトウィンドウに次を入力します:

   ```
   certreq -new request.inf request.req
   ```

4. 認証局ブラウザに次の URL を入力します: http://localhost/certsrv
5. 「Request a Certificate」をクリックします。
6. 「advanced certificate request」をクリックします。
7. 「Submit a certificate request」をクリックします。
8. ファイル request.req の内容を「Saved Request」ウィンドウにコピーします。
9. 「Web Server」証明書のテンプレートを選択します。
10. 証明書をダウンロードして、ファイル request.cer などに保存します。
11. Windows のプロンプトウィンドウに次を入力します:

    ```
    certreq -accept request.cer
    ```

12. 証明書を秘密鍵付きでエクスポートします。

    これは次の手順で行います。

    a. Windows のプロンプトウィンドウで「mmc」と入力して、Management Console を起動させます。
    b. ローカルコンピュータ証明書のスナップインを追加します。
    c. 次のように移動します。
       「Certificates（Local Computer）」-「Personal Certificates」-「Certificates」
    d. 新規サーバ認証局証明書をクリックします。
    e. 証明書ウィンドウの「Details」タブを開きます。
    f. 「Copy to File」をクリックします。
    g. 「Yes, export the private key」を選択します。
    h. パスワードを割り当てます。
    i. 証明書のファイル名を選び、「Finish」をクリックします。

ドメインコントローラ証明書のサーバへのインストール

ドメインコントローラ証明書のサーバへのインストールは、次の手順で行います。

1. 作成されたばかりのドメインコントローラ証明書のファイルをドメインコントローラにコピーします。
2. ドメインコントローラ証明書をダブルクリックします。
3. 「Install Certificate」をクリックします。
4. 証明書をエクスポートするときに割り当てたパスワードを使用します。
5. 「Place all certificates in the following store」の下の「Browse」をクリックし、「Personal Certificates」を選択します。

6. Windows のプロンプトウィンドウで「mmc」と入力して、Management Console を起動させます。
7. ローカルコンピュータ証明書のスナップインを追加します。
8. 現在のユーザの証明書のスナップインを追加します。
9. ドメインコントローラ証明書を現在のユーザの「Personal Certificates」ディレクトリからローカルコンピュータの「Personal Certificates」ディレクトリにコピーします。

5.4.4.2 iRMC ユーザへのユーザロールの割り当て

ユーザロール（認証役割）を iRMC ユーザに以下のエントリのいずれかにより割り当てることができます。

- ユーザ
- ロール/グループ

Active Directory でユーザをグループに個別に割り当てます。

次の手順に従って、OU SVS のロールエントリに基づいてユーザロールを割り当てます。

1. スナップイン「Active Directory ユーザとコンピュータ」を開きます。

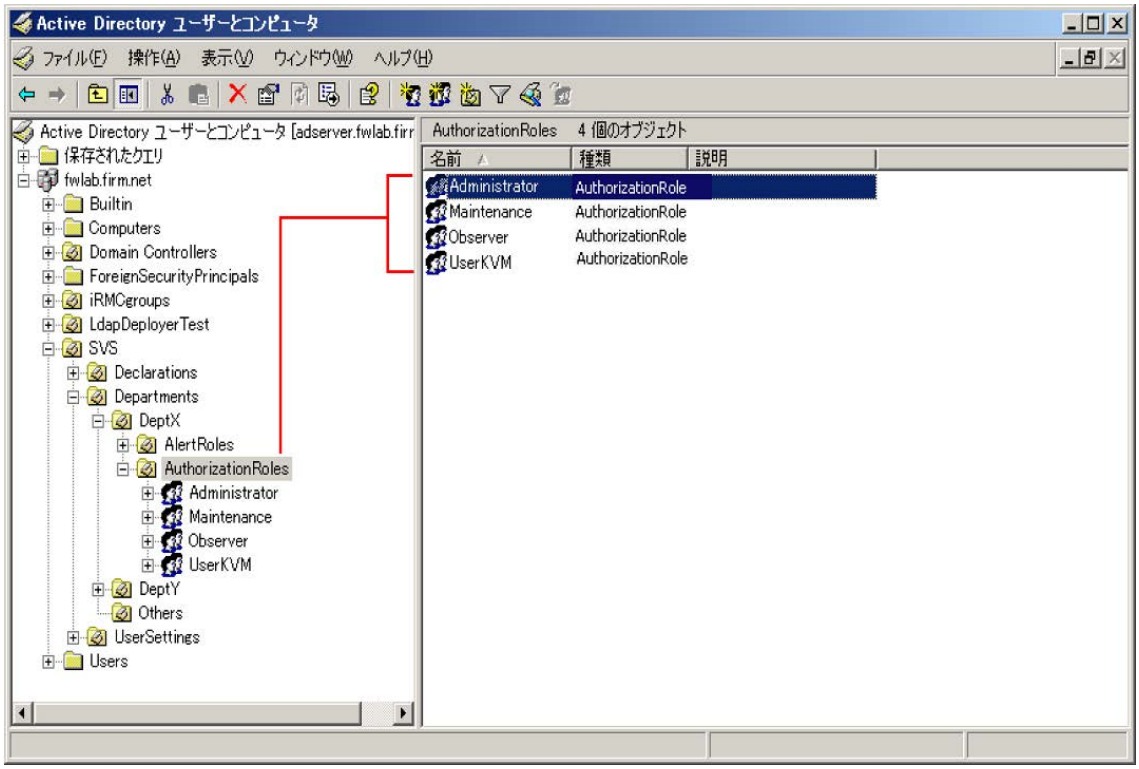


図 34: 「Active Directory ユーザとコンピュータ」スナップイン

2. 認証役割をダブルクリックします（ここでは **Administrator**）。

   「**Administrator のプロパティ**」ダイアログボックスが開きます。

3. 「**メンバー**」タブを開きます。

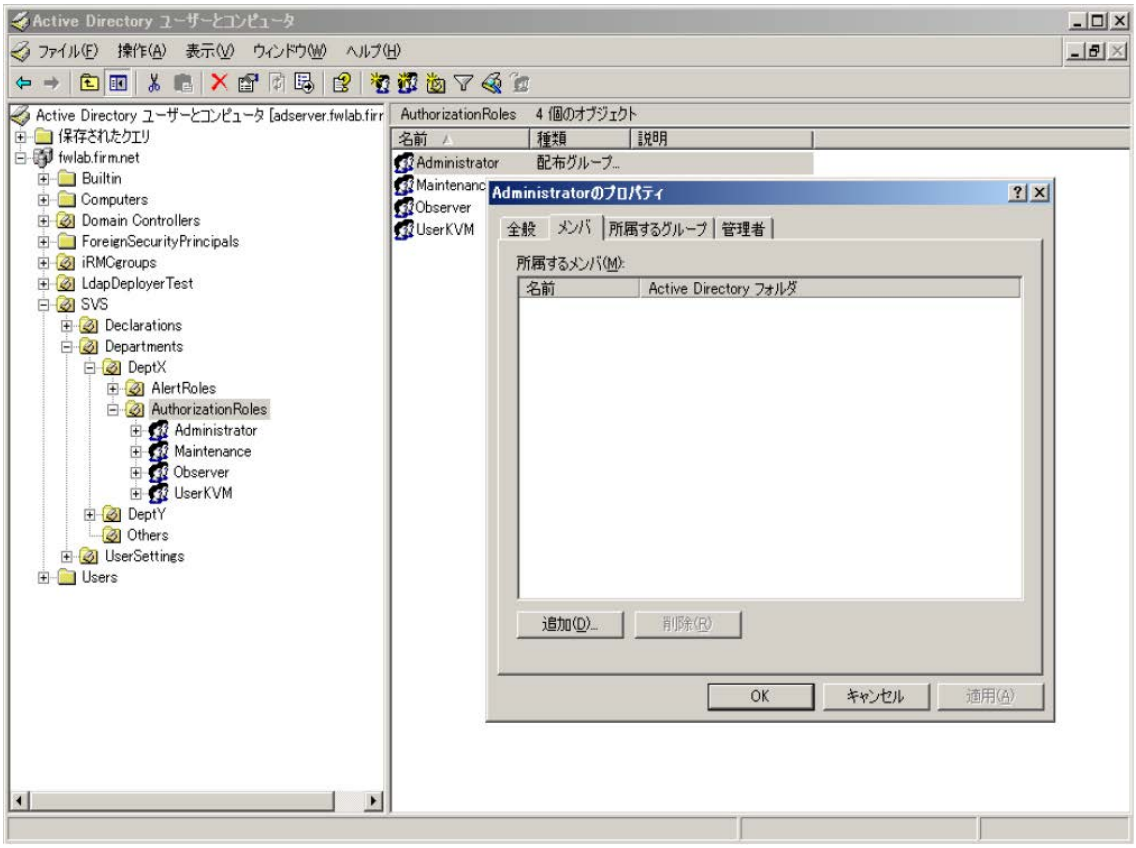


図 35:「**Administrator のプロパティ**」ダイアログボックス

4. 「**追加**」をクリックします。

   「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログボックスが開きます。

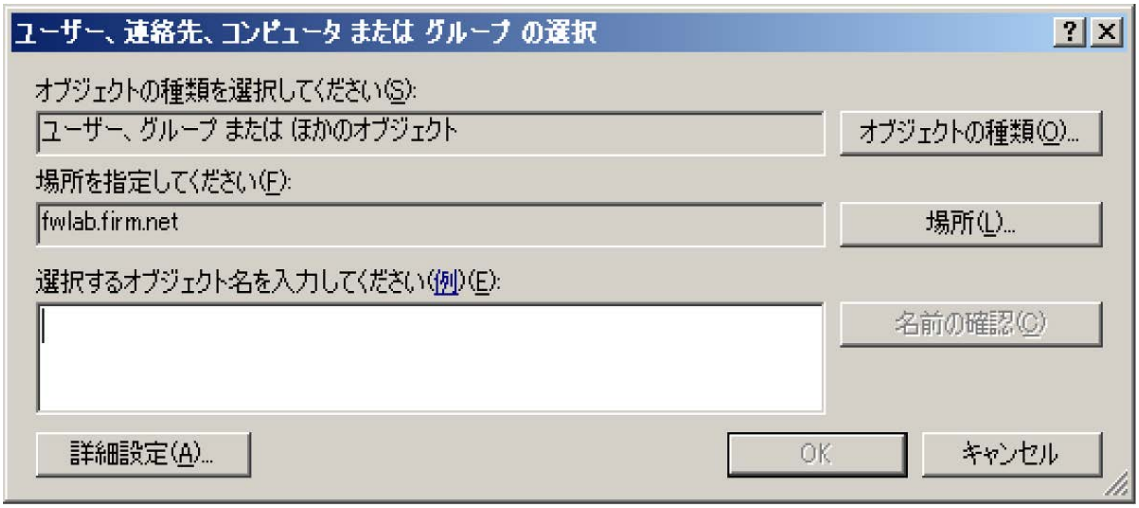


図 36: 「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログボックス

5. 「**場所**」をクリックします。

   「**場所**」ダイアログボックスが開きます。

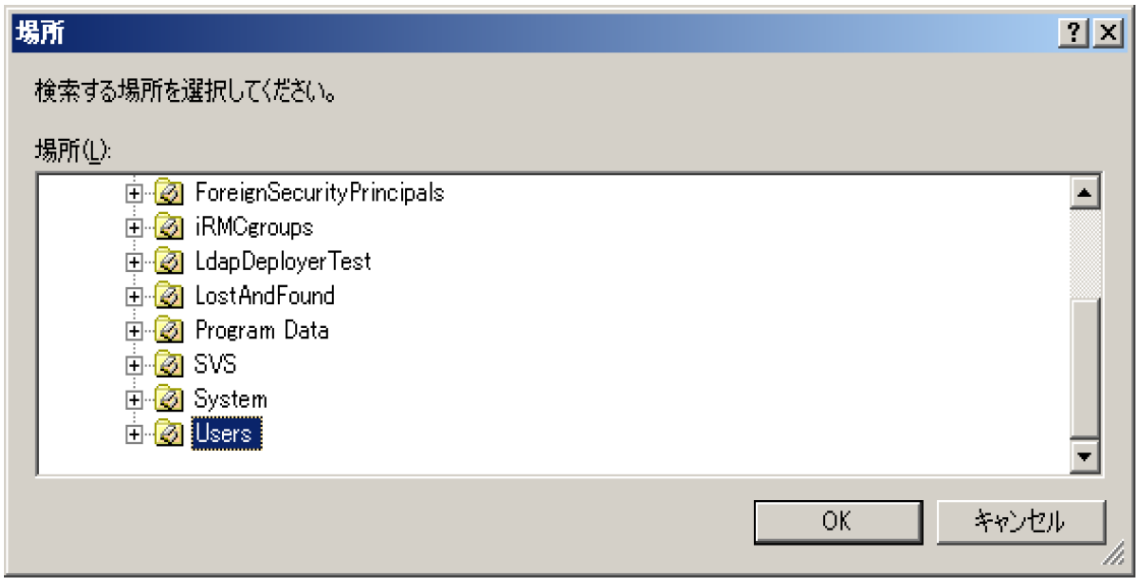


図 37: 「**場所**」ダイアログボックス

6. 該当するユーザを含むコンテナ（OU）を選択します。（デフォルト値は OU Users です。）ディレクトリ内の他の位置にユーザを入力することもできます。
7. 「**OK**」をクリックして確定します。

   「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログボックスが開きます。

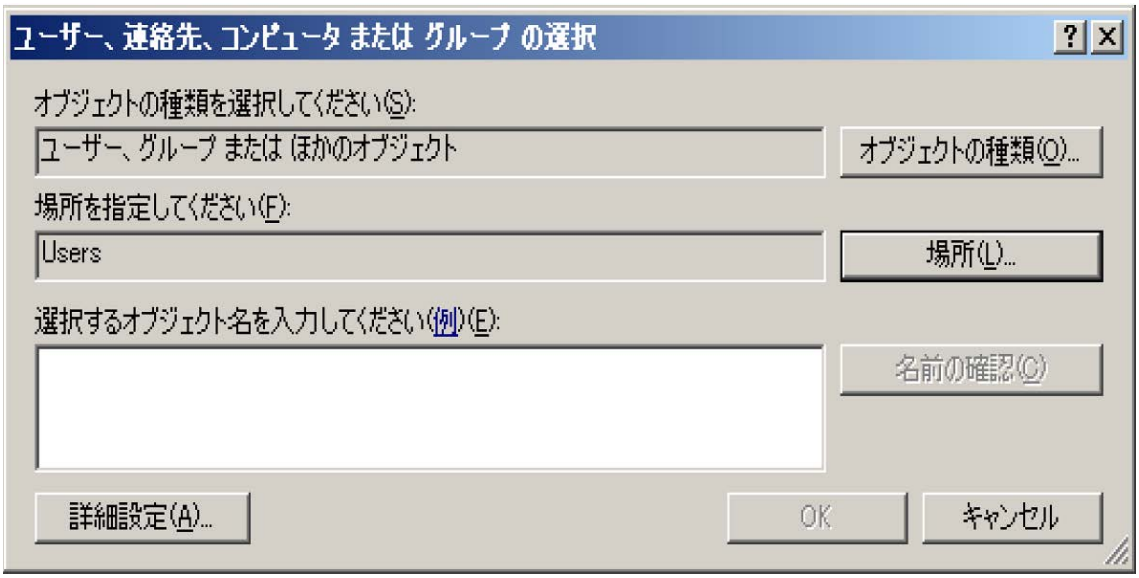


図 38:「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログボックス

8. 「**詳細設定**」をクリックします。

   「**ユーザ、連絡先、コンピュータまたはグループの選択**」拡張ダイアログボックスが開きます。

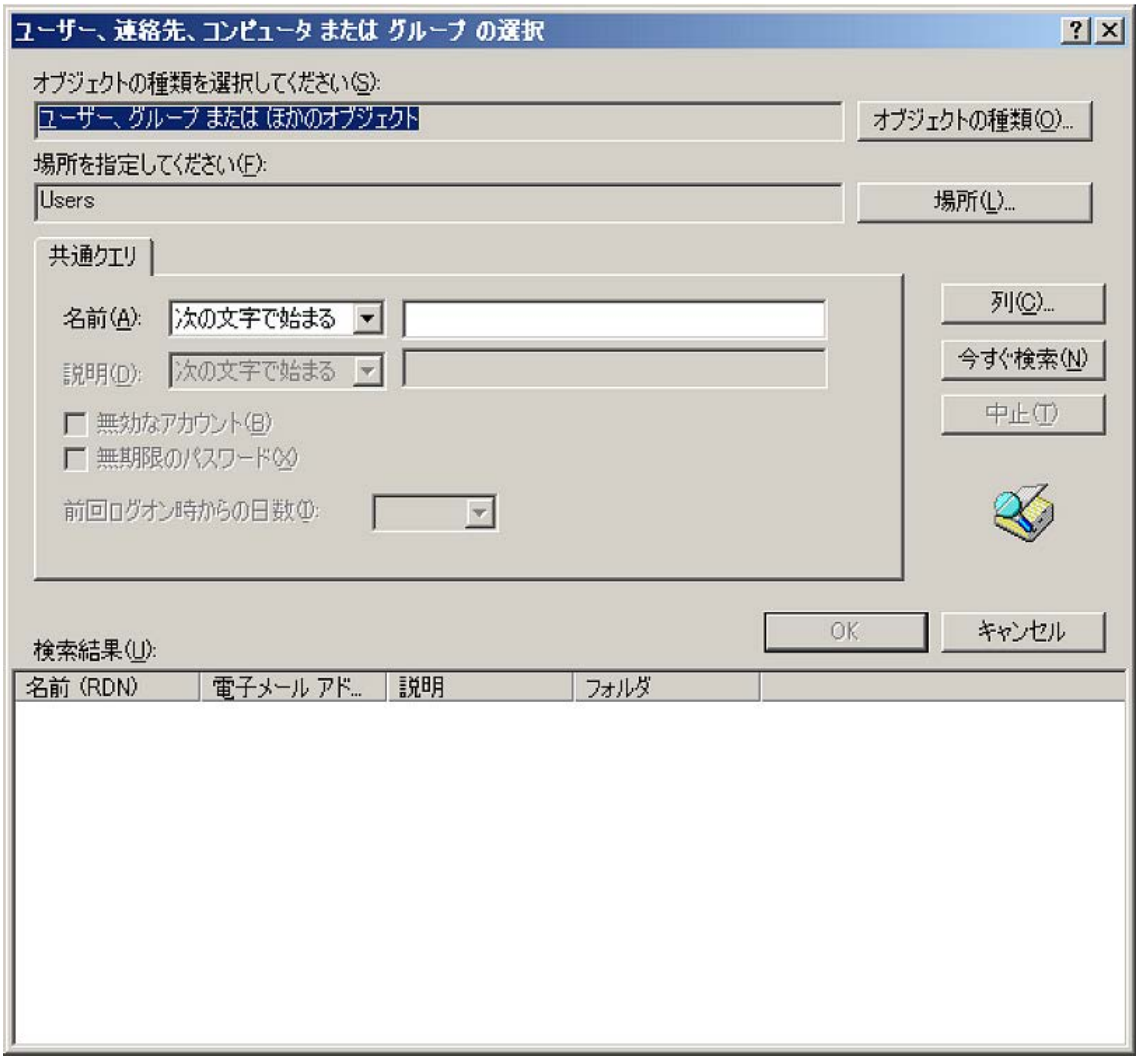


図 39:「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログボックス - 検索画面

9. 「**今すぐ検索**」をクリックしてドメイン内のすべてのユーザを表示します。
「**検索結果**」領域に検索されたすべてのユーザが表示されます。

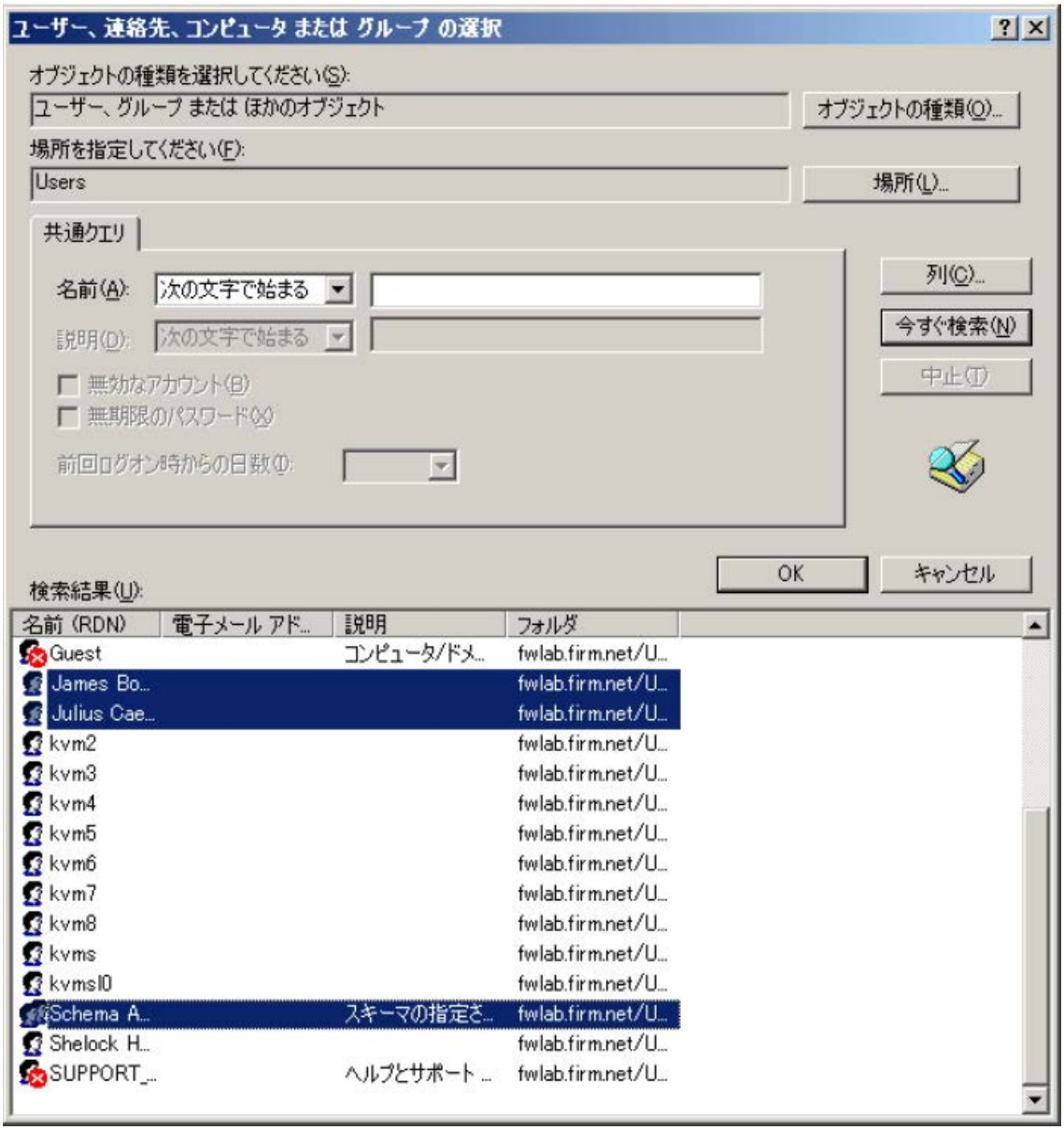


図 40:「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログボックス - 検索結果表示

10. グループに追加するユーザを選択し、「**OK**」をクリックして確定します。
    選択したユーザが表示されます。

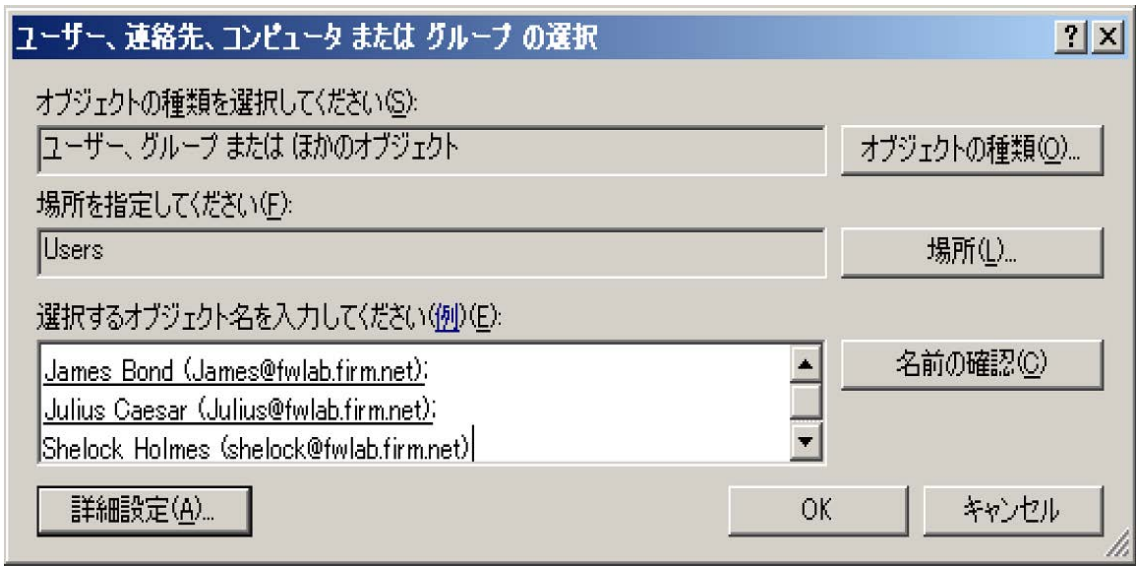


図 41:「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログ - 検索結果確認

11. 「**OK**」で確定します。

5.4.5 Novell eDirectory によるグローバル iRMC ユーザ管理

この項では、iRMC ユーザ管理を Novell eDirectory に統合する方法を説明します。

前提条件: LDAP v2 ストラクチャが既に Novell eDirectory で作成されている（「89 ページの SVS_LdapDeployer ユーティリティ」の項を参照）。

iRMC ユーザ管理を Novell eDirectory に統合するには、次の手順を実行します。

1. iRMC ユーザ管理の Novell eDirectory への統合
2. iRMC ユーザの許可グループへの割り当て

5.4.5.1 iRMC ユーザ管理の Novell eDirectory への統合

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

- iRMC プリンシパルユーザを作成します。
- eDirectory の iRMC グループとユーザ許可を宣言します。
- ユーザを許可グループに割り当てます。

eDirectory での iRMC ユーザの LDAP 認証プロセス

グローバル RMC ユーザが iRMC にログインする際の認証は、定義済みのプロセスに従って処理されます（57 ページの 「ユーザ管理」概念を参照）。次の図で、この認証プロセスを、Novell eDirector でのグローバル iRMC ユーザ管理ついて説明します。

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

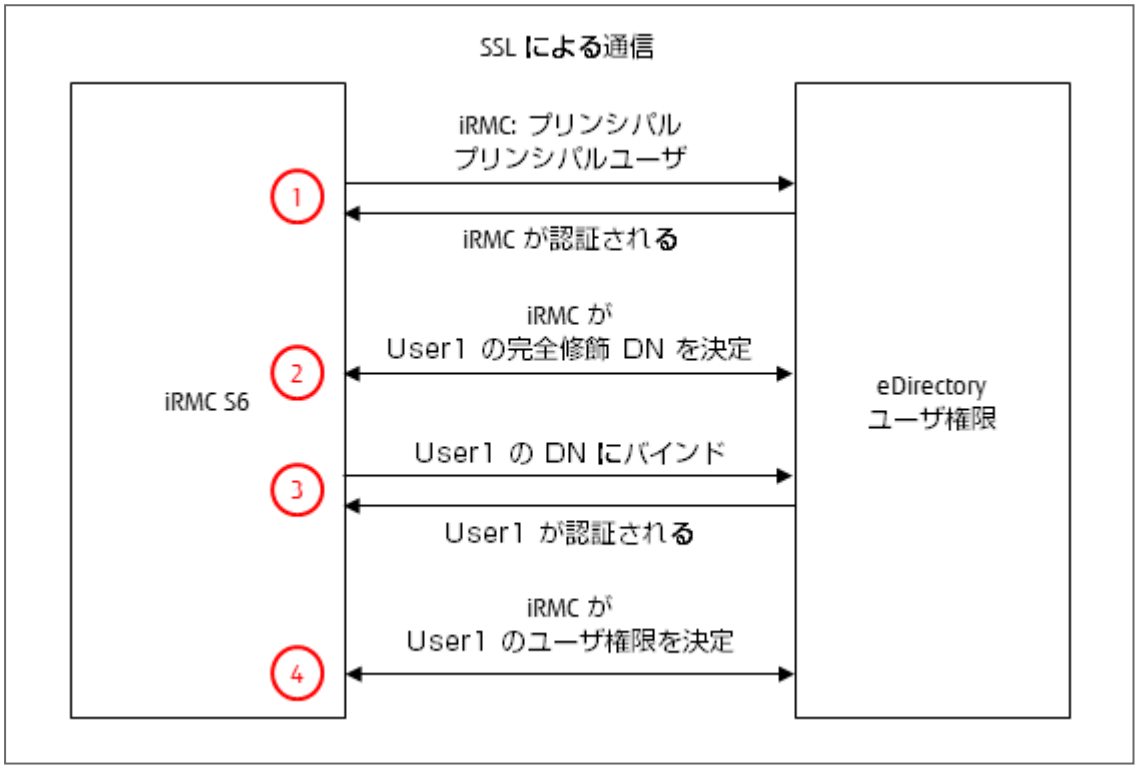


図 42: グローバル iRMC 許可の認証ダイアグラム

1. iRMC は、定義済みで既知の許可データ（RMC 設定）を使用して、「プリンシパルユーザ」として eDirectory サーバにログインし、正常にバインドされるのを待機します。
2. iRMC は eDirectory サーバに、「cn=User1」のユーザの完全修飾識別名（FQDN）を提供するように要求します。eDirectory は定義済みのサブツリー（iRMC 設定）から DN を決定します。
3. iRMC は、User1 の FQDN を使用して eDirectory サーバにログインし、正常にバインドされるのを待機します。
4. iRMC は eDirectory サーバに、User1 のユーザ許可を提供するように要求します。

プリンシパルユーザの許可データと DN を含むサブツリーは、iRMC の Web インターフェースの「**ユーザ管理**」ページで設定します。ユーザの CN は、検索されるサブツリーの中で一意でなければなりません。

iRMC 用のプリンシプルユーザの作成

iRMC 用のプリンシプルユーザを以下の通り作成します。

1. 有効な認証データを使用して iManager にログインします。
2. 「Roles and Tasks」を選択します。
3. 「Users - Create User」を選択します。
4. 表示されるテンプレートに必要な項目を入力します。
   - プリンシパルユーザの識別名（DN）とパスワードは 対応する iRMC の設定の項目に一致しなければなりません。
   - ユーザの「Context:」はツリーのどの位置にあっても構いません。
5. 以下のサブツリーにプリンシパルユーザの検索許可を割り当てます。
   - サブツリー（OU）SVS.
   - ユーザを含むサブツリー（OU）（たとえば「people」）

iRMC グループとユーザへのユーザ許可の割り当て

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

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

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

- プリンシパルユーザ
- iRMC ユーザが含まれるサブツリー

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

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

「Rights to Other Objects」ページが表示されます。

5. 「Trustee Name」に、許可を付与するオブジェクトの名前を指定します（下の図の SVS.sbdr4）。
6. 「Context to Search From」に eDirectory のサブツリー（SVS）を指定します。iManager はこのサブツリーから、トラスティ「Users」が現在読み取り許可を持っているオブジェクトを検索します。
7. 「OK」をクリックします。

   進捗ディスプレイに検索の状況が表示されます。検索作業か終了すると、「Rights to Other Objects」ページに検索結果が表示されます。

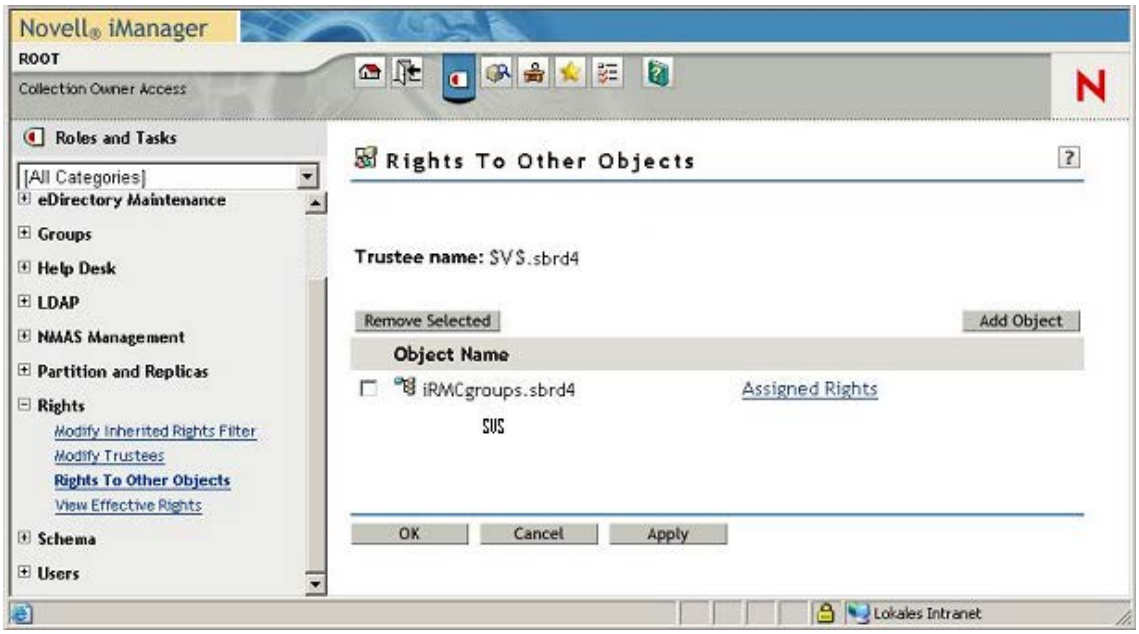


図 43:「iManager」 -「Roles and Tasks」 -「Rights To Other Objects」

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

8. 必要に応じてトラスティに追加の許可を割り当ててください。
   a. 「Add Object」をクリックします。
   b. オブジェクトセレクタボタン  をクリックして、トラスティに許可を割り当てたいオブジェクトを選択します。
   c. 「Assigned Rights」をクリックします。

      プロパティ「All Attributes Rights」が表示されない場合は:

      i. 「Add Property」をクリックします。

         「Add Property」ダイアログボックスが開きます。

図 44:「iManager」 -「Roles and Tasks」 -「Rights To Other Objects」 -「Add Property」ダイアログボックス

ii. プロパティ「All Attributes Rights」をハイライトさせ、「OK」をクリックして追加します。

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

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

e. 「適用」をクリックして設定を有効にします。

5.4.5.2 iRMC ユーザの許可グループへの割り当て

以下のエントリのいずれかにから開始し、iRMC ユーザを（たとえば OU「people」から）iRMC 許可グループに割り当てることができます。

- ユーザエントリ（ユーザエントリの数がごく少い場合はこの方が適当）
- ロールエントリ／グループエントリ（ユーザエントリの数が多い場合はこの方が適当）

次の例は iRMC ユーザをOU「people」から許可グループに割り当てる方法を示します。割り当てをロールエントリ／グループエントリから開始する方法を説明しています。ユーザエントリに基づく割り当て方法もほぼ同じです。

eDirectory でユーザをグループに個別に割り当てます。

次の手順に従います。

1. ウェブブラウザから iManager を起動します。
2. 有効な認証データを使用して iManager にログインします。

3. 「Roles and Tasks」を選択します。
4. 「Groups - Modify Group」を選択します。

   「Modify Group」ページが開きます。
5. iRMC ユーザを割り当てたいすべての許可グループについて次の作業を実行します。

   a. オブジェクトセレクタボタン を使用して、iRMC ユーザを追加するグループを選択します。LDAP v2 ストラクチャの例（下の図を参照）ではこれは、Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4 です。

   b. 「メンバー」タブを開きます。

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

図 45: 「iManager」-「Roles and Tasks」-「Modify Group」-「Members」タブ（LDAP v2）

   c. iRMC グループに割り当てたい OU「people」のすべてのユーザについて、次の作業を実行します。

      i. オブジェクトセレクタボタン をクリックします。

         「Object Selector（Browser）」ダイアログボックスが開きます。

図 46: iRMC グループへのユーザの割り当て - ユーザの選択

ii. 「Object Selector（Browser）」ダイアログボックスで、OU「people」の中の必要なユーザを選択し、「OK」をクリックして確定します。

選択されたユーザが「Modify Group」ページの「Members」タブの表示領域にリストされます。

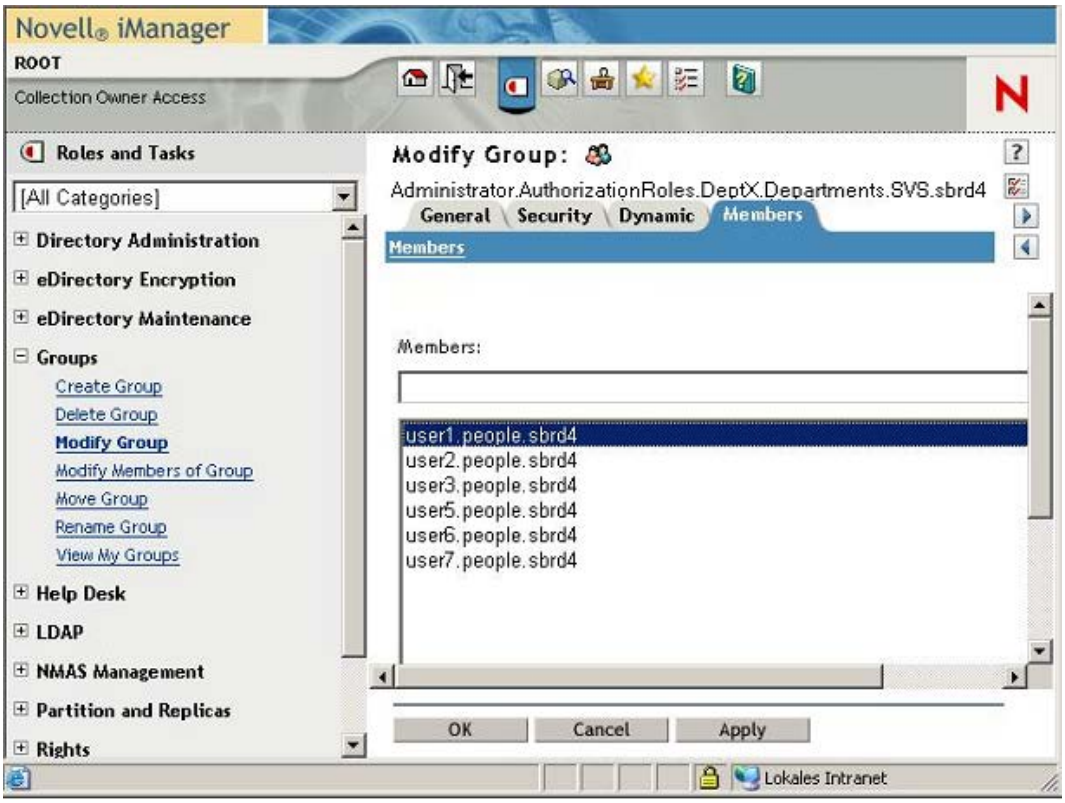


図 47: 「Members LDAP v2」タブで選択された iRMC ユーザの表示

iii. 選択されたユーザが iRMC グループに追加されるように、「Apply」または「OK」で確定してください（ここでは、 ... .SVS.sbdr4）。

5.4.5.3 Novell eDirectory 管理のためのヒント

NDS デーモンの再起動

次の手順で NDS デーモンを再起動します。

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

```
rcndsd restart
```

`nldap` デーモンの再起動に失敗し、理由が分からない場合

1. `nldap` デーモンを「手作業」で起動します。

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

iManager から応答がない場合

1. iManager を再起動してください。

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

NLDAP サーバ設定の再ロード

次の手順に従います。

1. ConsoleOne を起動して eDirectory にログインします。

ConsoleOne を初めて起動する場合は、ツリーが設定されていません。

以下の手順でツリーを設定してください。

a. 「My World」の下のノード「NDS」を選択します。

b. メニューバーから「ファイル」-「認証」の順に選択します。

c. 次のログイン用認証データを入力します。

- ログイン名: root
- パスワード: <password>
- ツリー: MY_TREE
- コンテキスト: mycompany

2. ウィンドウの左側部分で、「ベース DN」オブジェクト（Mycompany）をクリックします。

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

3. 「LDAP サーバ」オブジェクトを右クリックし、コンテキストメニューで「プロパティ」を選択します。
4. 「一般」タブで、「Refresh NLDAP Server Now」をクリックします。

NDS メッセージトレースの設定

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

以下の手順を推奨します。

1. コマンドボックス（たとえば bash）を開きます。

ndtrace の設定

1. eDirectory のディレクトリ /home/eDirectory に移動します。

   ```
   cd /home/eDirectory
   ```

2. `screen` コマンドを使用して screen を起動します。
3. `ndstrace` コマンドを使用して ndstrace を起動します。
4. 有効化したいモジュールを選択します。

たとえば、イベントが発生した時間を表示したい場合は、「dstrace TIME」と入力します。

LDAP および TIME モジュールを有効化するには、以下を入力して行うことを強く推奨いたします。

```
dstrace LDAP TIME
```

5. quit と入力して ndstrace を終了します。

   これで ndstrace の設定は終了しました。

別のターミナルでのメッセージの出力

1. ndstrace を起動して、メッセージ出力をリダイレクトします。

   ```
   ndstrace -l >ndstrace.log
   ```
2. 以下の連結キーを使用して別のターミナルを開きます:
   [Ctrl] + [a]、[Ctrl] + [c]
3. ログの記録を開始します。

   ```
   tail -f ./ndstrace.log
   ```
4. 仮想ターミナル間の切り替えには、次の連結キーを使用します: [Ctrl] + [a] 、 [Ctrl] + [0]
   （ターミナルには 0 から 9 までの番号が付きます）

5.4.6 OpenLDAP によるグローバル iRMC ユーザの管理

この項では、iRMC ユーザ管理を Open LDAP に統合する方法を説明します。

前提条件: LDAP v2 ストラクチャが既に Open LDAP で作成されている（「89 ページの SVS_LdapDeployer ユーティリティ」の項を参照）。

iRMC ユーザ管理を Open LDAP に統合するには、次の手順を実行します。

- iRMC プリンシパル iRMC ユーザの作成。
- 新規 iRMC ユーザの作成とそのユーザに対する許可グループの割り当て。

5.4.6.1 新しい iRMC ユーザの作成

次の手順に従います。

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

   これは次の手順で行います。

   a. 新規ユーザを作成するサブツリー（サブグループ）を選択します。新規ユーザはサブツリー内のどこにでも作成できます
   b. 「**編集**」メニューを開きます。
   c. 「**エントリを追加**」を選択します。
   d. 「**Person**」を選択します。
   e. 識別名 **DN** を編集します。
   f. 「**設定**」をクリックしてパスワードを入力します。
   g. 苗字 **SN** を入力します。
   h. 「**適用**」をクリックします。
4. 新しいユーザを許可グループに割り当てます。

   これは次の手順で行います。

   a. ユーザを所属させる **SVS** サブツリー（サブグループ）を次のように選択します。

      cn=UserKVM、ou=YourDepartment、ou=Departments,ou=SVS, dc=myorganisation、dc=mycompany
   b. 「**編集**」メニューを開きます。
   c. 「**Add Attribute**」を選択します。
   d. 属性名として「Member」を指定します。値にはここで作成したユーザの完全修飾 DN を次のように指定してください。

      cn=UserKVM、ou=YourDepartment、ou=Departments,ou=SVS, dc=myorganisation、dc=mycompany

5.4.6.2 プリンシパルユーザの作成

プリンシパルユーザを作成するには、Jarek Gawor 氏著作の LDAP browser/editor などの LDAP ブラウザが必要です。この LDAP browser/editor はグラフィカルユーザインターフェースにより使いやすくなっています。このブラウザはインターネットでダウンロードできます。

以下の手順で LDAP browser/editor をインストールしてください。

1. 圧縮アーカイブ `Browser282.zip` を任意のインストール用ディレクトリで解凍します。
2. JAVA ランタイム環境用の環境変数 `JAVA_HOME` をインストール用ディレクトリに設定してください。例:

   ```
   JAVA_HOME=C:\Program Files\Java\jre7
   ```

プリンシパルユーザ（ObjectClass: **Person**）を作成するには、次の手順に従います。

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

プリンシパルユーザの識別名（DN）とパスワードは 対応する iRMC の設定の項目に一致しなければなりません。

8. 「**設定**」をクリックしてパスワードを入力します。
9. 苗字 **SN** を入力します。
10. 「**適用**」をクリックします。

5.4.6.3 OpenLDAP 管理のヒント

LDAP サービスの再起動

次の手順で LDAP サービスを再起動します。

1. コマンドボックスを開きます。
2. ルート許可でログインします。
3. 次のコマンドを入力します。

```
rcldap restart
```

メッセージログの記録

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

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

各種レベルについては、http://www.zytrax.com/books/ldap/ch6/#loglevel を参照してください。

次の表に、ログレベルとその意味の概要を示します。

ログレベル	意味
-1	全面的なデバッグ実行
0	デバッグ実行なし
1	ログファンクションコール
2	試験パケットの取扱い
4	ヘビートレースデバッグ実行
8	接続管理
16	送信/受信パケット表示
32	フィルタ処理の検索
64	設定ファイル処理
128	アクセス制御リスト処理
256	接続/操作/イベントのステータスログの記録
512	送信済みエントリのステータスログの記録

ログレベル	意味
1024	シェルバックエンドによる出力通信
2048	エントリパースの出力結果

テーブル 7: OpenLDAP - ログレベル

5.4.7 グローバル iRMC ユーザへの Eメール警告の設定

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

前提条件 Eメール警告送信には、以下の要件を満たす必要があります。

- プリンシパルユーザが iRMC Web インターフェースで設定され、LDAP ツリーを検索する許可が付与されている必要があります。
- 「**ユーザ管理**」ページで LDAP 設定を構成する場合は、Eメール警告を「**LDAP**」グループで有効にしておく必要があります。

5.4.7.1 グローバル Eメール警告送信

ディレクトリサーバ経由のグローバル Eメール警告送信には警告ロールが必要です。この警告ロールは管理ロールに加えて SVS_LdapDeployer ユーティリティの設定ファイル（89 ページの）で定義されます。

警告グループ（警告ロール）の表示

警告ロールは警告タイプ（たとえば、温度のしきい値を超えた、など）をまとめてグループ化しますが、それぞれに重要度（たとえば「致命的」）が割り当てられています。ユーザを特定の警告グループに割り当てると、ユーザが Eメールで受け取る警告のタイプと重大度が指定されます。

警告ロールの構文は、`jar` アーカイブ `SVS_LdapDeployer.jar` と共に提供されるサンプル設定ファイルで説明されています（Fujitsu サポートページからダウンロードしてください）。

警告タイプの表示

以下の警告タイプがサポートされます。

警告タイプ	原因
FanSens	ファンセンサ
Temperat	温度センサ
HWError	異常ハードウェアエラー
セキュリティ	セキュリティ
SysHang	システムのハング
POSTErr	POST エラー
SysStat	システム状態
DDCtrl	ディスクドライブとコントローラ
NetInterf	ネットワークインターフェース
RemMgmt	リモートマネージメント
SysPwr	電源制御
メモリ	メモリ
Others	その他

テーブル 8: 警告タイプ

各々の警告タイプには以下の重大度のいずれかが割り当てられます: **警告**、**異常**、**全て**、（**なし**）

優先メールサーバ

グローバル Eメール警告送信には、優先メールサーバの「Automatic」設定が適用されます。Eメールを即時に送ることができない場合、たとえば 1 番目のメールサーバが使用不可能な場合には、Eメールは 2 番目のメールサーバに送られます。

サポートされるメールフォーマット

以下の Eメールフォーマットがサポートされています。

- 標準
- 固定件名
- ITS フォーマット
- Fujitsu REMCS フォーマット

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

LDAP Email テーブル

Eメール警告送信が設定されていて（118 ページの）、「**LDAP Eメール警告を有効にする**」オプションが選択されている場合、警告が発信されると以下のユーザに Eメールが送信されます。

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

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

グローバル Eメール警告には Eメール配布リストの使用を推奨します。

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

- Eメール警告が設定されたグローバル iRMC ユーザのリスト。
- 各グローバル iRMC ユーザに対して:
  - 警告タイプ毎に設定された警告のリスト（タイプと重大度）。
  - 要求されたメールフォーマット。

LDAP Eメールテーブルは以下の状況で更新されます。

- iRMC が初めて起動、または再起動されたとき。
- LDAP の設定が変更されたとき。
- 定期的（任意）iRMC Web インターフェースでの LDAP 設定の一環として、アップデート間隔を指定します（「**LDAP 警告テーブルの更新**」オプションを使用）。

ディレクトリサーバ上のグローバル Eメール警告送信の設定

この項ではディレクトリサーバ上の Eメール警告送信を設定する方法を説明します。設定は、iRMC ダイアログでも行う必要があります。これらは、iRMC Web インターフェースで設定します。

次の手順に従います。

1. ディレクトリサービスに Eメール警告を送信するユーザの Eメールアドレスを入力します。

Eメールアドレス設定に使用する方法は、運用するディレクトリサービス（Active Directory、eDirectory または OpenLDAP）によって異なります。

2. 警告ロールを定義する設定ファイルを作成します。
3. この設定ファイルを使用して SVS_LdapDeployer を起動し、対応する LDAP v2 ストラクチャ（SVS）をディレクトリサーバ上に生成させます（91 ページの SVS_LdapDeployer の起動 の項を参照）。

5.4.7.2 警告ロールの表示

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

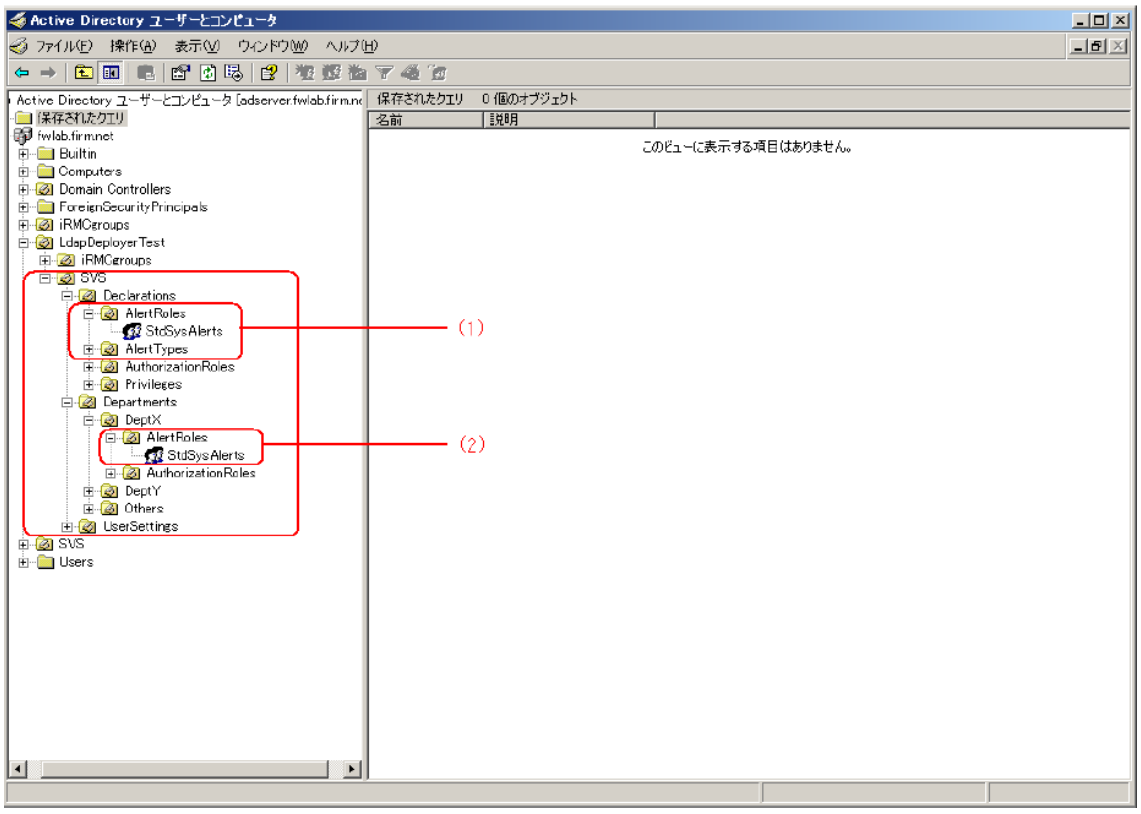


図 48: OU SVS と警告ロール

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

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

個々の警告ロールのユーザに Eメールが確実に送信されるようにするため、 関連部門を iRMC に設定する必要があります（上の図の「DeptX」）。

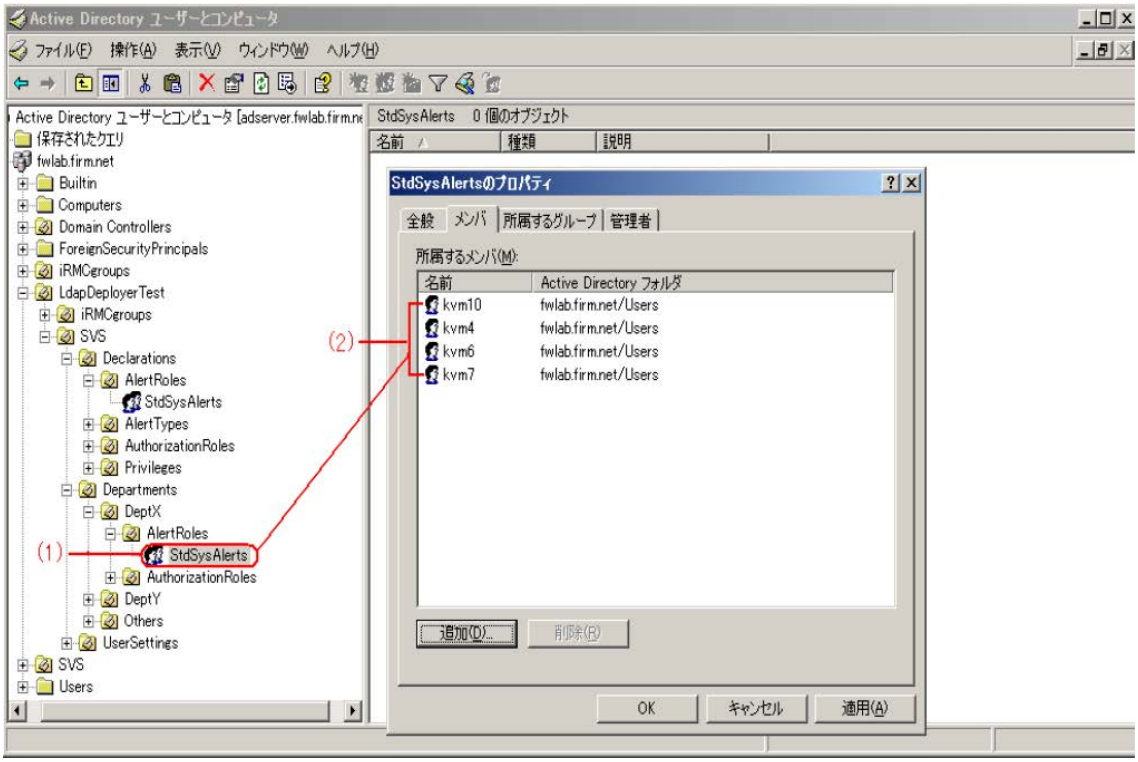


図 49: 警告ロール「StdSysAlert」に割り当てられたユーザ

「Active Directory ユーザとコンピュータ」の構造ツリーの「SVS」-「Departments」-「DeptX」-「Alert Roles」の下にある警告ユーザ（例: StdSysAlerts）を選択し（1）、コンテキストメニューから「プロパティ- - メンバ」を選択してこのユーザの「プロパティ」ダイアログボックスを開くと、警告ロールに所属する全てのユーザ（ここでは「StdSysAlerts」）が「メンバ」タブのに表示されます（2）。

5.4.7.3 iRMC ユーザへの警告ロール割り当て

ユーザエントリまたはロールエントリに基づいて、警告ロールをiRMC ユーザに割り当てることができます。

各種ディレクトリサービス（Microsoft Active Directory、Novell eDirectory および OpenLDAP）において、iRMC ユーザへの iRMC 警告ロールの割り当ては、iRMC ユーザへの iRMC 権限ロールの割り当てと同じ方法で、同じツールを使用して行います。

たとえば、Active Directory の場合は、「**Active Directory ユーザとコンピュータ**」スナップインの「**プロパティ**」ダイアログボックスの中の「**追加**」をクリックして割り当てを行います。（120 ページの）。

5.4.8 LDAP 認証の iRMC の設定

最後の手順として、LDAP サーバのディレクトリサービスの SVS ストラクチャを作成して構成した後、iRMC 自体をユーザ認証のために LDAP サーバに接続するように設定する必要があります。

設定手順は接続の種類によって異なります。

- SSL/TLS を使用せず安全でない: この場合、DNS 機能を有効にする必要があります。「**ネットワーク制御**」ページにある「**DNS**」グループの「**DNS サーバ 1**」フィールドに、ターゲットのディレクトリサービスサーバの IP アドレスを入力します。
- SSL/TLS を使用して安全: この場合、DNS 情報は関係ありません。

DNS の設定（安全でない接続の場合のみ）

1. iRMC の Web インターフェースを開きます。
2. 「**設定**」メニューで「**ネットワーク制御**」ページを開きます。
3. 「**DNS**」グループで、「**DNS を有効にする**」オプションをオンにします。
4. 「**DNS サーバ 1**」フィールドで、使用する LDAP サーバの IP アドレスまたはホスト名を入力します。

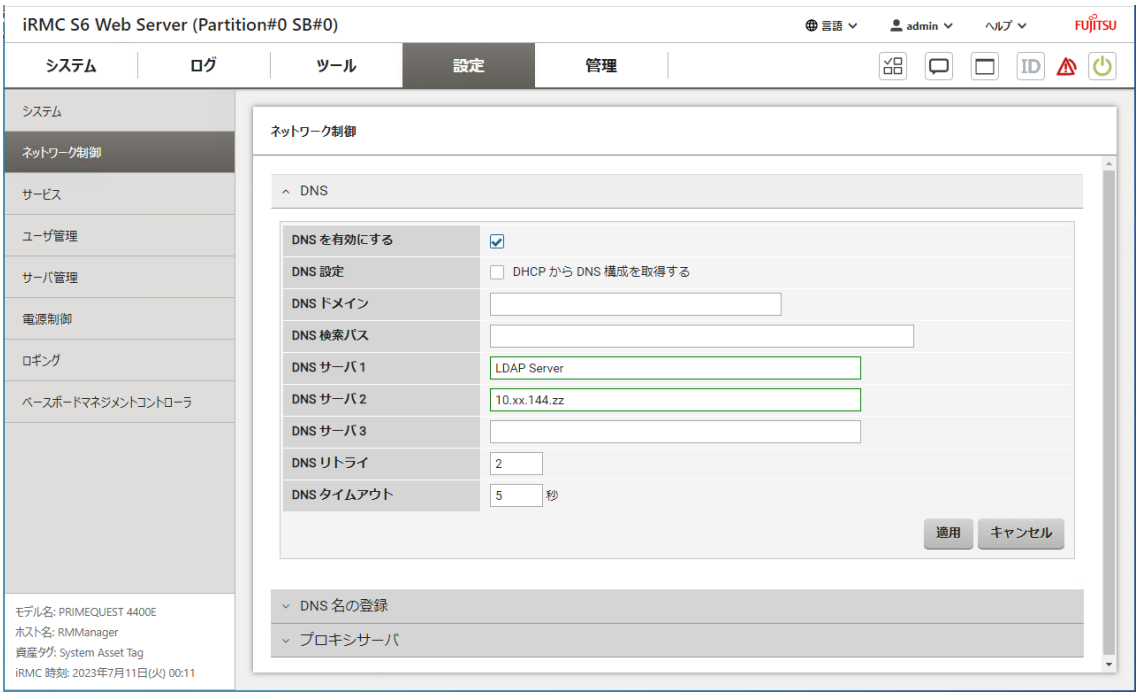


図 50: DNS 設定の構成

5. 「**適用**」をクリックして設定を確定します。

   設定がチェックされて適用されます。

変更内容を反映するには、「**ツール**」メニューの「**アップデート**」ページにある「**リブート**」ボタンで、iRMC をリブートする必要があります。

LDAP の設定

1. 「**設定**」メニューで「**ユーザ管理**」ページを開きます。
2. 「**LDAP**」グループで「**LDAP を有効にする**」オプションをオンにします。
3. 安全な接続の場合は「**LDAP SSL/TLS を有効にする**」オプションをオンに、安全でない接続の場合はオフにします。
4. リストから LDAP サーバで実行中の「**ディレクトリサーバタイプ**」を選択します。
5. 「**プライマリ LDAP サーバ**」グループの「**サーバ**」フィールドに IP アドレスまたはホスト名を入力します。
6. 対応する**ネットワークポート**を選択します。
7. 「**ディレクトリ設定**」グループで「**権限タイプ**」を選択します。
8. ディレクトリサービスの設定に従って、「**組織名**」と「**ドメイン名**」フィールドに値を入力します。値は両方のシステムで同じである必要があります。

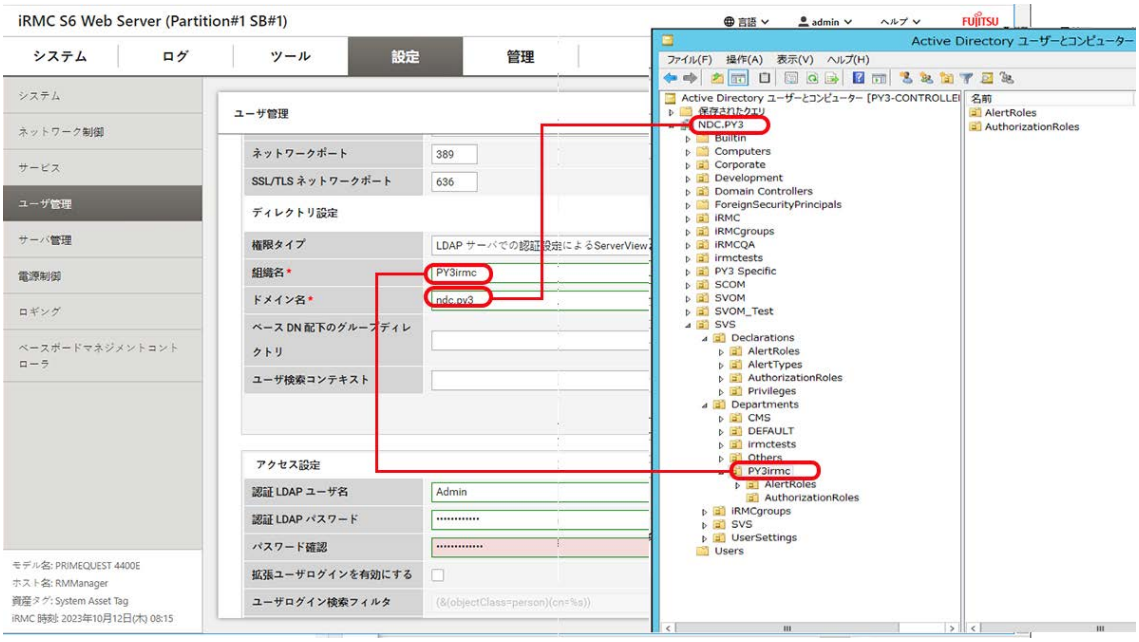


図 51: LDAP 接続の設定

9. 「**適用**」をクリックして設定を確定します。

LDAP サーバへの接続の確立

1. 「**LDAP**」グループ内の「**アクセス設定**」グループで、「**認証 LDAP ユーザ名**」フィールドに LDAP ユーザ名を入力します。
2. 「**認証 LDAP パスワード**」フィールドに入力したパスワードを入力します。
3. 「**パスワード確認**」フィールドにパスワードをもう一度入力します。

4. 「**LDAPアクセスのテスト**」をクリックして接続データが正しいかどうかをテストします。

   設定がチェックされ、接続を確立できる場合は、「**LDAPアクセスのテスト**」アイコンの近くに成功のフィードバックが表示されます。

Eメール警告の設定

1. 「**LDAP**」グループ内の「**Eメール警告設定**」で、「**LDAP Eメール警告を有効にする**」オプションをオンにします。
2. 「**LDAP 警告テーブルの更新**」に、警告テーブルを内部に保存する時間間隔を整数で入力します。
3. 「**適用**」をクリックして設定を確定します。

   LDAP サーバへの常時接続が確立され、すべての設定が適用されます。

5.4.9 ユーザ許可の設定

「**ユーザ管理**」ページの「**ディレクトリ設定**」グループで、iRMC 管理者は次の 2 つの方法でユーザ許可を設定できます。

LDAP サーバで許可を管理

「**権限タイプ**」リストから「**LDAP サーバでの認証設定による標準 LDAP グループ**」を選択した場合、ユーザとグループは LDAP 側で作成されます。

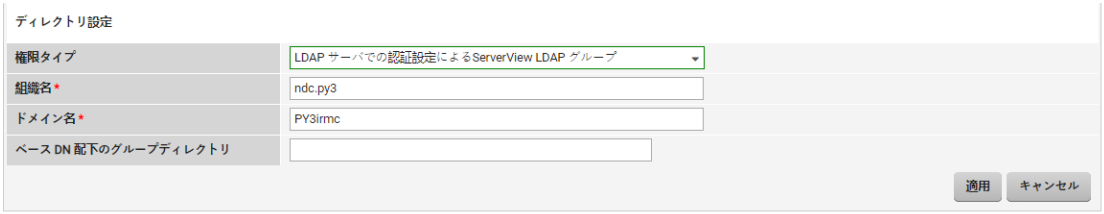


図 52: LDAP サーバでの認証設定による標準 LDAP グループ

iRMC 許可を付与するには、ユーザを適切な LDAP グループに割り当てます。

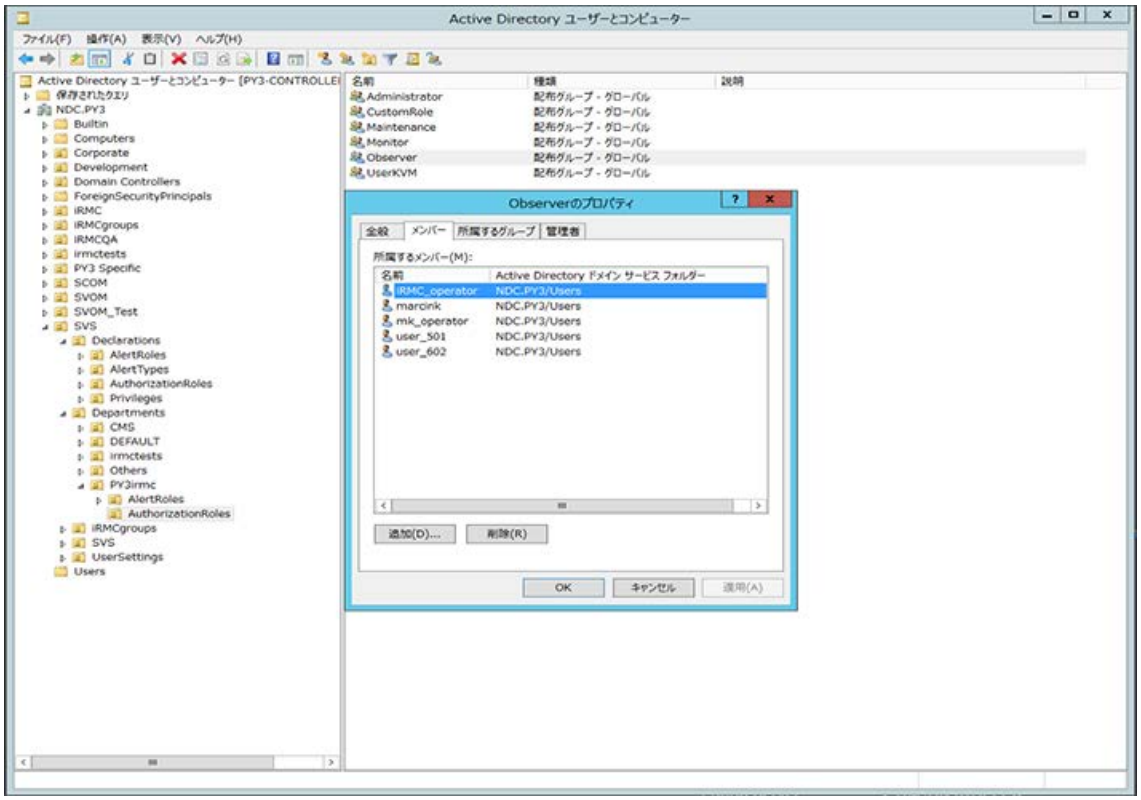


図 53: Observer グループのメンバ

iRMC で許可を管理

「**権限タイプ**」リストから「**iRMC での認証設定による標準 LDAP グループ**」を選択した場合、ユーザとグループは LDAP 側で作成され、さらにユーザはグループに割り当てられます。

図 54: iRMC での認証設定による ServerView LDAP グループ

ただし、対応する LDAP グループを iRMC で作成することで、このグループに適切な許可を設定することができます。

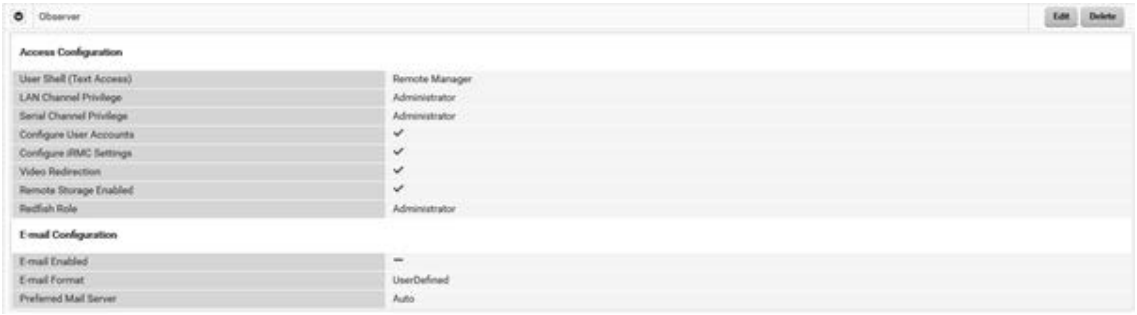


図 55: iRMC の対応する LDAP グループ

そのため、Observer グループに管理者許可を提供できるので、LDAP サーバで定義されるグループが最初から提供することはありません。

6 OS のリモートインストール

ServerView Installation Manager （以下 Installation Manager）および iRMC の「ビデオリダイレクション（AVR）」および「バーチャルメディア」機能を使用して、リモートワークステーションから管理対象サーバ上にオペレーティングシステムをインストールできます。

この章では、以下の特定のトピックについて説明します。

- 「バーチャルメディア」機能によって提供される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一般的な手順。これ以降、このようなストレージメディアは、略して仮想ストレージメディアと呼びます。
- ServerView Suite 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します。
- 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 をインストールします。
- 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 をインストールします。
- 仮想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。読者が Installation Manager の機能に精通していることを前提としています（詳細は、『ServerView Installation Manager』取扱説明書を参照）。

iRMC S6 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要件 : iRMC の LAN インターフェースを設定する必要があります。

6.1 OS のインストールの一般的な手順

Installation Manager では、iRMC を経由する OS のリモートインストールを、管理対象サーバにローカルのインストールおよび構成とみなします。インストールは、バーチャルメディアを使用して、AVR ウィンドウを経由してリモートワークステーションから実行します。

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. 起動元にする仮想ストレージメディア（DVD または Installation Manager ブートイメージ）を仮想ストレージメディアとして接続します。
2. DVD 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 OS をインストールします。

下記の場合、CD/DVD を使用すると、Installation Manager を使用しなくても OS をインストールおよび構成することができます。

Windows

バーチャルメディアによる 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。仮想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 を使用したインストールの所要時間は、OS 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。

Linux

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、外部デバイス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、次のメディアとのバーチャルメディア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

6.2 バーチャルメディアとしてのストレージメディアの接続

バーチャルメディア機能を使用すると、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。
- リモートイメージマウントによってネットワークの中心に置かれるイメージファイル。

「バーチャルメディア」機能の詳細は、『iRMC S6 - Web インターフェース』取扱説明書を参照してください。

バーチャルメディア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。

Java アプレット

1. 「リモート ストレージ有効」を許可してiRMC Web インターフェースにログインします。
2. 「**設定**」メニューで、「**サービス**」ページを開きます。
3. 「**AVR（Advanced Video Redirection）**」で、「**KVM リダイレクションタイプ**」リストから「**JViewer（Java）**」オプションを選択します。
4. 「**適用**」をクリックして変更を送信します。
5. メニューバーで、  をクリックしてコンテキストメニューを開きます。
6. 「**ビデオリダイレクションの開始**」を選択して、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。別のリダイレクションセッションが実行されている場合、両方のセッションが「**AVR 実行中セッション表**」に表示されます。
7. 「**メディア**」-「**バーチャルメディアウィザード...**」をクリックします。

   または
8. または、ツールバーの 3 つのバーチャルメディアアイコンのいずれかをクリックします。

   「**バーチャルメディア**」ダイアログボックスが開きます。
9. 「**バーチャルメディア**」ダイアログボックスの適切なパネルで「**選択**」をクリックします。

   「**開く**」ファイルブラウザダイアログボックスが開きます。

10. 「**開く**」ダイアログボックスで、リモートステーションからバーチャルメディアとして使用できるようにするストレージメディアのディレクトリに移動します。
    - Installation Manager を使用するインストール

      ServerView Suite DVD 1 または Installation Manager ブートイメージ。
    - 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、そこから仮想ストレージメディアとして接続するか、Remote Image Mount を使用して接続することをお勧めします。
11. 「**タイプのファイル**」フィールドで、必要なデバイスタイプを選択します。
12. 「**ファイル名**」フィールドでバーチャルメディアとして接続するストレージメディアを指定します。
    1. ISO イメージ（ISO/NRG イメージ）の場合はファイル名を入力します。または、エクスプローラでファイル名をクリックします。
    2. ドライブの場合はドライブ名を入力します。次に例を示します。

       `D` ドライブの場合は「D」（Windows）

       `/dev/..`（Linux）
13. 「**開く**」をクリックして選択を確定します。

    選択したストレージメディアがバーチャルメディアとして使用可能になり、「**バーチャルメディア**」ダイアログボックスの対応するパネルに表示されます。
14. 「**接続**」をクリックして、DVD-ROM ドライブ（DVD）または Installation Manager ブートイメージをバーチャルストレージメディアとして接続します。

HTML5

1. 「リモート ストレージ有効」を許可してiRMC Web インターフェースにログインします。
2. 「**設定**」メニューで、「**サービス**」ページを開きます。
3. 「**AVR（Advanced Video Redirection）**」で、「**KVM リダイレクションタイプ**」リストから「**HTML5 Viewer**」オプションを選択します。
4. 「**適用**」をクリックして変更を送信します。
5. メニューバーで、  をクリックしてビデオリダイレクションセッションを開始します。

   その結果、AVR ウィンドウが開かれます。

6. ステータスバーで、「Select」をクリックします。「Upload file」ダイアログボックスが開きます。ここで ISO イメージを選択すると、「CD image」フィールドに表示されます。
7. 「Start Media」をクリックします。
   CD イメージがマウントされます。

6.3 管理対象サーバのブート

管理対象サーバを ServerView Suite DVD 1 から起動して、Installation Manager で設定するには、以下の手順に従います。

1. iRMC Web インターフェースのメニューバーで、  をクリックして電源をオフにし、  をクリックして管理対象サーバを起動またはリブートします。AVR ウィンドウのブートプロセスの進行状況に従います。

   管理対象サーバの BIOS POST フェーズでは、仮想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。仮想ストレージメディアは、BIOS ブートシーケンスに共有エントリ「CD-ROM DRIVE」と表示されます。

   バーチャルメディアとして接続されている ローカル CD-ROM/DVD-ROM ドライブと CD-ROM/DVD-ROM ドライブの両方が管理対象サーバに存在する場合は、管理対象サーバは、仮想イメージによって提供される CD-ROM/DVD-ROM ドライブから起動します。
2. サーバの起動中に [F2] を押します。
3. 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。
4. バーチャルストレージメディア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。
5. 設定を保存して、UEFI セットアップを終了します。

   管理対象サーバが、バーチャル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。

システムが仮想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。

1. 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バーチャルメディアとして接続します。
2. 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 を仮想ストレージメディアから起動するには、5 分程度かかります。処理中は、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。

3. 「**Installation Manager**」で「**標準モデル**」を選択します。
4. 設定データをネットワーク上のメディアに格納します。これに必要な共有をあらかじめ設定する必要があります。

> 準備した設定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。環境に応じて、一時的な 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。

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ます。

5. 「**次へ**」をクリックして、Installation Manager を起動します。

Installation Manager の「**ようこそ**」ページが開きます。

図 56: Installation Manager - ようこそページ

6. 「**デプロイメント**」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。

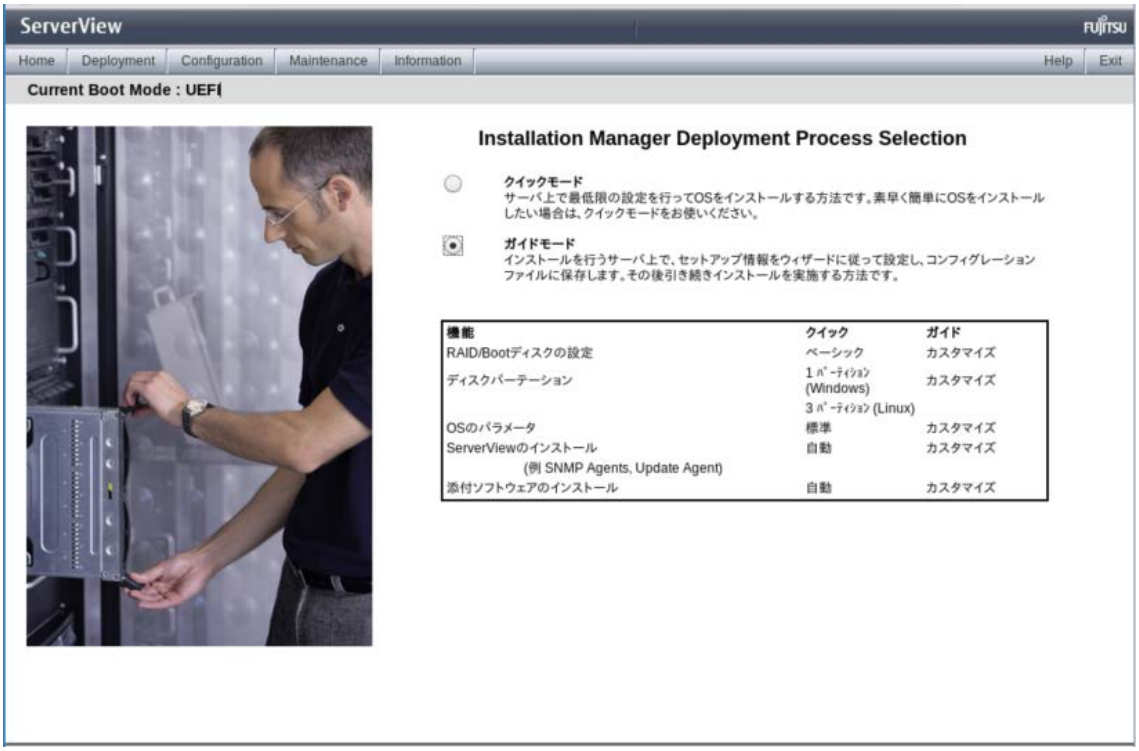


図 57: Installation Manager: 標準またはガイドモードのインストールの選択

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。

7. 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 ドライブを仮想ストレージメディア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（134 ページの 管理対象サーバへの Windows のインストール）。

Installation Manager の設定が完了したら、Windows インストール用（134 ページの 管理対象サーバへの Windows のインストール）、Linux インストール用（135 ページの 管理対象サーバへの Linux のインストール）または ESXi インストール用（137 ページの 管理対象サーバへの ESXi のインストール）の「**設定内容の確認**」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。

6.4 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、Installation Manager の「**設定内容の確認**」ページが表示されます。

図 58: 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。

1. AVR ウィンドウのメニューバーで、「**メディア**」 - 「**バーチャルメディアウィザード**」を選択して、「**バーチャルメディア**」ダイアログボックスを開きます。
2. 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。
3. バーチャルメディア接続をクリアするには、対応する「**切断**」ボタンをクリックします。
4. すべてのバーチャルメディア接続をクリアします。

5. 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。
6. このドライブに、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。

7. Windows インストール CD/DVD が入っている CD-ROM/DVD-ROM ドライブをバーチャルストレージとして接続します。
8. 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、Installation Manager で確認ダイアログボックスが開き、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。
9. もう一度、現在のすべてのバーチャルメディア接続をクリアします。
10. 確認ダイアログボックスで、「**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。

6.5 管理対象サーバへの Linux のインストール

管理対象サーバに Linux をインストールする前に、インストール中にマウスの使用はできますが、同期はできないことをに注意してください。

仮想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仮想ストレージメディア接続を取り外して、新しいメディアを仮想ストレージメディアとして接続する必要があります。

設定が完了すると、Installation Manager の「**設定内容の確認**」ページが表示されます。

図 59: 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。

1. AVR ウィンドウのメニューバーで、「**メディア**」 - 「**バーチャルメディアウィザード**」を選択して、「**バーチャルメディア**」ダイアログボックスを開きます。
2. 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。
3. バーチャルメディア接続をクリアするには、対応する「**切断**」ボタンをクリックします。
4. すべてのバーチャルメディア接続をクリアします。
5. 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。
6. このドライブに、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。

7. Windows インストール CD/DVD が入っている CD-ROM/DVD-ROM ドライブをバーチャルストレージとして接続します。
8. 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、Installation Manager で確認ダイアログボックスが開き、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。
9. もう一度、現在のすべてのバーチャルメディア接続をクリアします。
10. 確認ダイアログボックスで、「**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。

6.6 管理対象サーバへの ESXi のインストール

管理対象サーバに ESXi をインストールする前に、インストール中にマウスの使用はできますが、同期はできないことをに注意してください。

仮想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仮想ストレージメディア接続を取り外して、新しいメディアを仮想ストレージメディアとして接続する必要があります。

設定が完了すると、Installation Manager の「**設定内容の確認**」ページが表示されます。

図 60: 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。

1. AVR ウィンドウのメニューバーで、「**メディア**」 - 「**バーチャルメディアウィザード**」を選択して、「**バーチャルメディア**」ダイアログボックスを開きます。
2. 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。
3. バーチャルメディア接続をクリアするには、対応する「**切断**」ボタンをクリックします。
4. すべてのバーチャルメディア接続をクリアします。
5. 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。
6. このドライブに、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。

7. Windows インストール CD/DVD が入っている CD-ROM/DVD-ROM ドライブをバーチャルストレージとして接続します。
8. 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、Installation Manager で確認ダイアログボックスが開き、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。
9. もう一度、現在のすべてのバーチャルメディア接続をクリアします。
10. 確認ダイアログボックスで、「**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。

7 ファームウェアのアップデート

iRMC S6 はフラッシュメモリで 2 つのバンクを使用します。各バンクの容量は 46 MB で、ファームウェアイメージが格納されます。バンクのファームウェアイメージは異なる場合があります。iRMC SPI ROM には、低、高い、リカバリの 3 つのリージョンがあります。

これらのリージョンに保存されるイメージはそれぞれ、低イメージ、高イメージ、ゴールデンイメージと呼ばれています。

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、いわゆるファームウェアセレクタで決定します（ファームウェアセレクタ）を参照。141 ページの ファームウェアセレクタ

iRMCのファームウェアは EEPROM では実行されず、その代わりに起動時に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 OS 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。

iRMC が起動すると、iRMC がイメージを読み取るリージョンはアクティブリージョンとなり、iRMC F/W がイメージを読み取らないリージョンは非アクティブリージョンとなります。

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。

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。

現行バージョンのファームウェアは ServerView Suite DVD 2 に格納されています。または Fujitsu 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 2 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。

7.1 ファームウェアセレクタ

ファームウェア変更で、実行する iRMC S6 ファームウェアを指定します。iRMC がリセットされて再起動されるたびに、ファームウェア変更が評価され、対応するファームウェアへのブランチを処理します。

ファームウェア変更には、次の値があります:

0 ファームウェアバージョン最も新しいファームウェアイメージ

1 ファームウェア1（フラッシュメモリの最初のバンクのファームウェアイメージ）

2 ファームウェア2（フラッシュメモリの2番目のバンクのファームウェアイメージ）

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 Web インターフェースの「**システム概要**」ページの「**動作中の iRMC ファームウェア**」グループ（詳細は、『iRMC S6 - Web インターフェース』取扱説明書を参照）を通じた照会。
- 「**管理**」メニューの「**保守**」ページにある「**ファームウェアアップデート**」グループを通じた設定。

7.2 ゴールデンイメージ

ファームウェアアップデートの前に、使用するイメージファイルがチェックされます。

- 認証されていないイメージが使用されるのを防止するために、イメージファイルが検証されます。
- イメージファイルが変更されているかチェックされます。

チェックの結果、イメージファイルがオリジナルのファイルでなく、フラッシュ時に破損していることが示された場合、ゴールデンイメージを使用して自動的に修復されます。このゴールデンイメージは、変更された、または破損したファームウェアイメージを上書きします。

iRMC ファームウェアイメージの修復プロセス中は、iRMC の電源を切ったり入れたりしないでください。ファームウェアの修復中は、電源投入 LED が白色に点滅します。変更されたファームウェアイメージの検出とその修復は、システムイベントログ（SEL）に記録されます。ファームウェアの iRMC 設定は変更されません。

ゴールデンイメージの構成とアップデートは、Web インターフェースまたは iRMC の Redfish API を使用して行うことができます。

図 61: Web インターフェース内のファームウェアイメージの修復用のゴールデンイメージ

ゴールデンイメージはアクティブイメージと同じファームウェアバージョンに調整されます。

iRMC の脆弱性に対する iRMC フィックスなどのセキュリティフィックスが存在する場合は、アクティブなイメージと共にゴールデンイメージをアップデートします。

7.3 Web インターフェースを使用したファームウェアアップデート

このアップデートは、サーバオペレーティングシステム（OS）のオンラインまたはオフラインモードで実行できます。

「**管理**」メニューの「**保守**」ページを使用して、iRMC のファームウェアをアップデートできます。詳細は、『iRMC S6 - Web インターフェース』取扱説明書を参照してください。

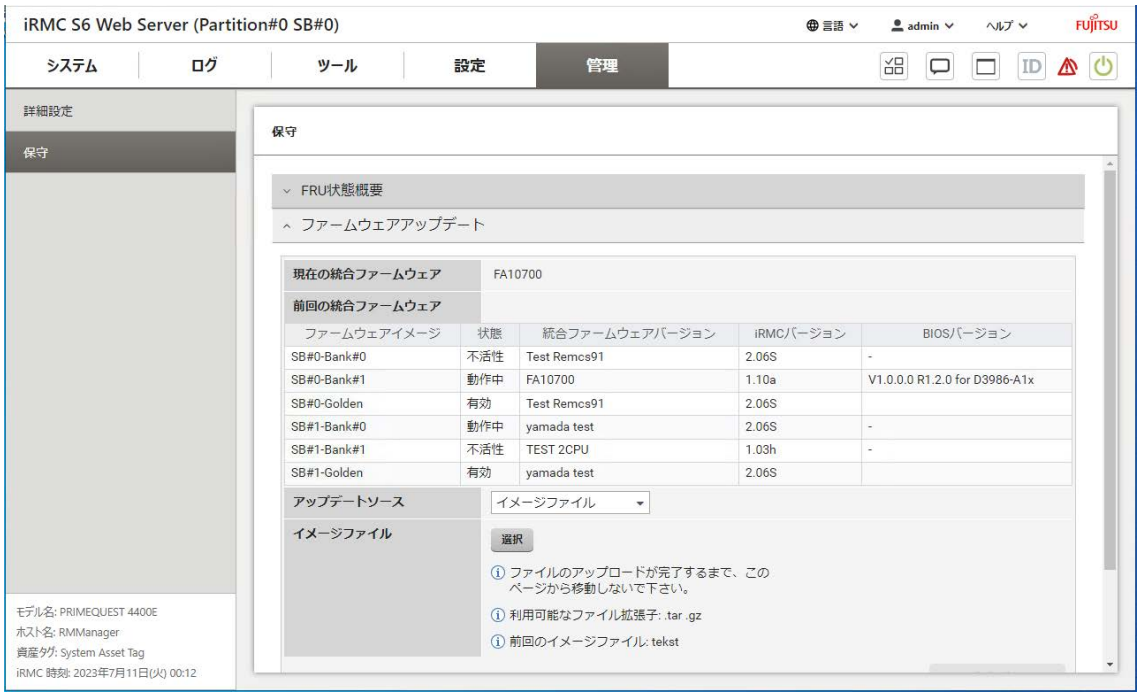


図 62: 「**メンテナンス**」ページ

7.4 ファームウェアダウングレード

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のEEPROMEEPROM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イメージの以前のバージョンに設定し（141 ページの ファームウェアセレクタ）、その後 iRMC 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。

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、「**ダウングレード**」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　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　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。

7.5 ファームウェアの整合

SB を交換する際、ファームウェアバージョンを整合させることが必要です。交換前にSBに装着されていたSDカードは、交換するSBに装着されます。SBのファームウェアバージョン番号が異なる場合にSBを交換すると、ファームウェアSDカードに保存されているものが復元されます。

整合により、交換前に iRMC のファームウェアまたは BIOS が動作バージョンに自動的に復元されます。自動整合には、SD カードを SB に取り付けておく必要があります。

実行中の BIOS および iRMC のイメージは、SB に取り付けられた SD カードに保存（バックアップ）されます。SB の交換後、イメージが SD カードから読み出され、BIOS/iRMC の SPI ROM に書き込まれます（復元）。

以下の場所に保存されているシリアル番号を比較して、iRMC が SB の交換を検出します。

- FRUSB のROM
- 電源投入時の Operator Panel（OPL）の ROM

シリアル番号が異なる場合、SB が交換されたことになります。この場合、OPL に保存されたシリアル番号は新しい SB の番号にアップデートされ、ファームウェアバージョンの整合が自動的に開始されます。

SB の交換後、ファームウェアバージョンの自動整合の前に電源がオフになると、ファームウェアバージョンの整合は失敗します。ファームウェアバージョン整合は、電源を再度投入しても、自動的には再実行されません。再度電源をオンにすると、シリアル番号は同一になり、SB が交換されていないと判断されます。

手動整合

iRMC Web インターフェースまたは Redfish API を使用してファームウェアバージョン整合を手動で開始して、SD カードに保存された情報を SPI ROM に復元できます。

iRMC Web インターフェースに管理者としてログインして、次の手順に従います。

1. 「**管理**」メニューの「**保守**」ページを開きます。
2. 「**ファームウェアアップデート**」グループを開きます。
3. 「**アップデートソース**」リストから「**メモリカード**」を選択します。
4. 「**アップデートの開始**」をクリックします。

   SD カードからファームウェアアップデート（iRMC および BIOS）が開始されます。

   iRMC の高低の両側が、SB 交換前の状態にアップデートされます。

復元中、以下の機能は抑制されます。

- iRMC Web インターフェースおよび Redfish API の両方における、手動での自動バージョン整合
- システムの電源オン

手動でのバージョン整合は、システムの電源がオンになっていても実行できます。

7.6 ファームウェアのバックアップ

SD カードが交換またはフォーマットされた場合、SD カードへのファームウェアのバックアップが必要になりました。このとき、SD カードに保存されたファームウェアイメージが失われます。

そこで、これらの操作を実行する場合、ファームウェアイメージを SD カードに自動的にバックアップします。

SD カードの交換/フォーマット、ファームウェアアップデート、SB 交換を組み合わせた場合の影響について、以下の表にまとめています。

ファームウェアアップデートの後、新しいファームウェアイメージが iRMC に保存される前に SD カードが交換またはフォーマットされた場合、ファームウェアイメージのバックアップデータは完全に失われます。

SD カードを交換/フォーマットして、ファームウェアイメージが SD カードにアップデートされる前に SB を交換すると、BIOS ファームウェアバージョンのカウントが失敗します。

操作の組み合わせ			結果	問題	対策
最初の操作	2 番目の操作のタイミング	2 番目の操作			
ファームウェアアップデート	iRMC への転送が完了する前	SD カードの交換またはフォーマット	SD カードを交換した後にサーバが電源オンになったとき、「Both the SD card and OS storage lost the update image（SD カードと OS ストレージの両方でアップデートイメージが失われた）」という SEL メッセージが出力されない。	SB の交換後にファームウェアのリストアが失敗する	BIOS バックアップ

操作の組み合わせ			結果	問題	対策
最初の操作	2 番目の操作のタイミング	2 番目の操作			
SD カードの交換	SD カードへの転送が完了する前	BIOS アップデート	ファームウェアアップデート後に、新しいファームウェアバージョンが SD カードに記録される。電源投入時に新しい BIOS が iRMC に保存される。	いいえ	
ファームウェアアップデート	iRMC への転送中	シャットダウン	次回ブート時にアップデートイメージが iRMC に転送される。	いいえ	
SD カードの交換	SD カードへの転送中	シャットダウン	次回ブート時にファームウェアイメージが SD カードに転送される。	いいえ	
ファームウェアアップデート	SD カードへの転送が完了する前	SB 交換	SB の交換後、BIOS が交換前のバージョンにアップデートされる。次回の電源投入時に、アップデートされたイメージが iRMC に保存される。	いいえ	
SD カードの交換	iRMC への転送が完了する前	SB 交換	SEL に、SB の交換後に SD カード上にイメージがないというエラーメッセージが出力される。	はい	ファームウェアアップデート

8 RAID 構成

RAID（Redundant Array of Independent Disks）は、複数の物理ディスクを組み合わせて 1 つの論理ドライブとして運用し、データの冗長性やパフォーマンスを向上させるデータストレージ仮想化技術です。データは、必要な冗長性とパフォーマンスのレベルに応じて、RAID レベルと呼ばれる複数の方法のいずれかでドライブ全体に分散されます。

iRMC は HW と SW RAID をサポートします。

- ハードウェア RAID は、RAID カードまたはデバイスの RAID コントローラチップによって提供されます。RAID コントローラチップにはファームウェアがあり、アレイ自体を制御できます（故障した HDD/SSD の取り外し、HDD/SSD の取り付け、LED の制御）。
- ソフトウェア RAID は、OS の機能または OS にインストールされているアプリケーションによって提供されます。

8.1 ハードウェア RAID

さまざまなメンバーディスクにデータを分散したり複製するために、さまざまな RAID スキームがあります。各構成で、容量、パフォーマンス、復元力の一意のバランスを提供します。通常、3 つの主要なコンセプトは、ストライピング、ミラーリング、パリティです。これらのコンセプトにはそれぞれメリットと制約がありますが、組み合わせることで、パフォーマンスを向上させることができます。

ストライピングで複数の物理ディスクにデータを均等に分散し、ミラーリングで 2 つ以上のディスクにデータを複製する一方で、パリティで生データを使用してエラー修正のためのパリティ情報を計算して保存します。ストライピングで情報の書き込みとアクセスを同時に行うことにより、RAID のパフォーマンスを向上しながら、ディスク障害時には、残りの正常なドライブからミラーリングでデータにアクセスすることができます。

iRMC は、管理対象サーバにインストールされているコントローラにバインドされた各種 RAID アレイの作成と管理をサポートします。このコンテキストにおける管理とは、次の意味です。

- RAID コントローラの完全性チェックを構成する
- この RAID コントローラに関連する物理ディスクを管理する
- これらの物理ディスクで実行する論理ドライブの作成と管理を行う

8.1.1 サポートされる RAID レベル

RAID レベルで、論理ドライブの様々なディスクにデータを分散させる方法について説明します。分かりやすくするために、各種 RAID タイプですべて、同じサイズのディスクドライブ一式を使用します。実際は、異なる容量のデバイスを使用した場合、各ドライブで使用可能な容量は、容量が最も少ないディスクドライブによって制限されます。

RAID レベル	技術	最小ディスク数	データセキュリティ	ディスク障害後のリビルド	2 台のディスク障害後のリビルド
RAID 0	ストライピング	2	なし	いいえ	いいえ
RAID 1	ミラーリング	2	ディスク障害	ミラーディスクのコピー	いいえ
RAID 1E	ストライピングとミラーリング	3	ディスク障害	XOR を使用したオリジナルコンテンツの計算	いいえ
RAID 5	分散パリティでのブロックレベルストライピング	3	ディスク障害	XOR を使用したオリジナルコンテンツの計算	なし
RAID 6	二重分散パリティでのブロックレベルストライピング	4	2 台のディスク障害	ディスクのオリジナルコンテンツの計算	ディスクのオリジナルコンテンツの計算
RAID 10	ミラーのストライプ	4	サブアレイ単位のディスク障害	ミラーディスクのコピー	異なるミラーの 2 台のディスクが影響を受ける場合のみ: ミラーディスクのコピー

RAID レベル	技術	最小ディスク数	データセキュリティ	ディスク障害後のリビルド	2 台のディスク障害後のリビルド
RAID 50	検出されたパリティのストライプ	6	ディスク障害	XOR を使用したオリジナルコンテンツの計算	異なるミラーの 2 台のディスクが影響を受ける場合のみ: ミラーディスクのコピー
RAID 60	二重分散パリティのストライプ	8	ディスク障害	ディスクのオリジナルコンテンツの計算	異なるミラーの 2 台のディスクが影響を受ける場合のみ: ミラーディスクのコピー

8.1.2 完全性チェック

RAID コントローラ、その関連の物理ディスク、論理ドライブで、完全性チェックおよびアクションを行うことができます。

バックグラウンド初期化（BGI）

バックグラウンド初期化は、論理ドライブの作成時に強制的に行われる整合性チェックです。この処理は、論理ドライブを作成してから、指定して時間後に自動的に開始されます。

バックグラウンド初期化では、ディスクのメディアエラーをチェックします。初期化によって、ストライピングされたデータセグメントがドライブグループ内のすべてのディスクで同じになります。バックグラウンド初期化率のデフォルト値は 30% で、これが推奨値です。リビルド率を変更する前にバックグラウンド初期化を停止する必要があります。そうしないと、リビルド率の変更がバックグラウンド初期化率に反映されません。

整合性チェック（MDC）

整合性チェック動作では、RAID レベル 1、5、6、10、50、60 を使用する論理ドライブのデータの整合性をチェックします（RAID-0 にはデータの冗長性はありません）。例えば、パリティが存在するシステムでは、整合性チェックとは、1つのディスク上のデータを計算して、その結果をパリティディスクの内容と比較することです。

MDC（整合性確保）では、データの正確性をチェックするだけではなく、不整合データの自動修復を試行します。

コピーバック

コピーバックによって、データを論理ドライブのコピー元ディスクから、論理ドライブの一部ではないコピー先ディスクにコピーできます。コピーバックは、アレイの特定の物理構成の作成や復元（デバイスの I/O バスのアレイメンバの特定の配置など）によく使用されます。コピーバックは、自動でも手動でも実行できます。

通常、ディスクに障害が発生した場合や、発生することが予想されている場合は、データはホットスペアにリビルドされます。障害が発生したディスクは、新しいディスクに交換されます。次に、データがホットスペアから新しいディスクにコピーされ、ホットスペアは再構築用のディスクから元のホットスペア状態に戻ります。コピーバック動作はバックグラウンドの処理として実行され、論理ドライブはホストに対してオンラインで利用可能です。

コピーバックは、論理ドライブの一部であるディスクで Self-Monitoring Analysis and Reporting Technolog（SMART）の最初のエラーが発生した場合にも開始されます。コピー先のディスクは、リビルド用のディスクとして利用可能なホットスペアです。SMART エラーが発生したディスクには、コピーバッ

クが正常に終了した後にのみ、失敗のマークが付けられます。これによって、アレイが劣化した状態になることが防止されます。
。

パトロールリード
パトロールリードには、システムのディスク障害の原因になるディスクエラーの可能性のチェックと、エラーの修正アクションが含まれます。目的は、障害によってデータ損失が発生する前にディスク障害を検出することにより、データの完全性を保護することです。修正アクションは、アレイ構成やエラーの種類によって異なります。
パトロールリードが開始されるのは、コントローラが一定時間アイドル状態で、他に実行中のバックグラウンドタスクがない場合だけです。そのため、負荷の高い I/O プロセス中に実行を継続することができます。

一部のチェックの実行にはより多くの時間がかかるため、忙しくない時間帯にスケジュールすることができます。

8.1.3 RAID コントローラ

管理対象サーバのインストール済みの RAID コントローラ（ストレージコントローラ）は、Web インターフェースの「**外部記憶装置**」ページに表示されます。

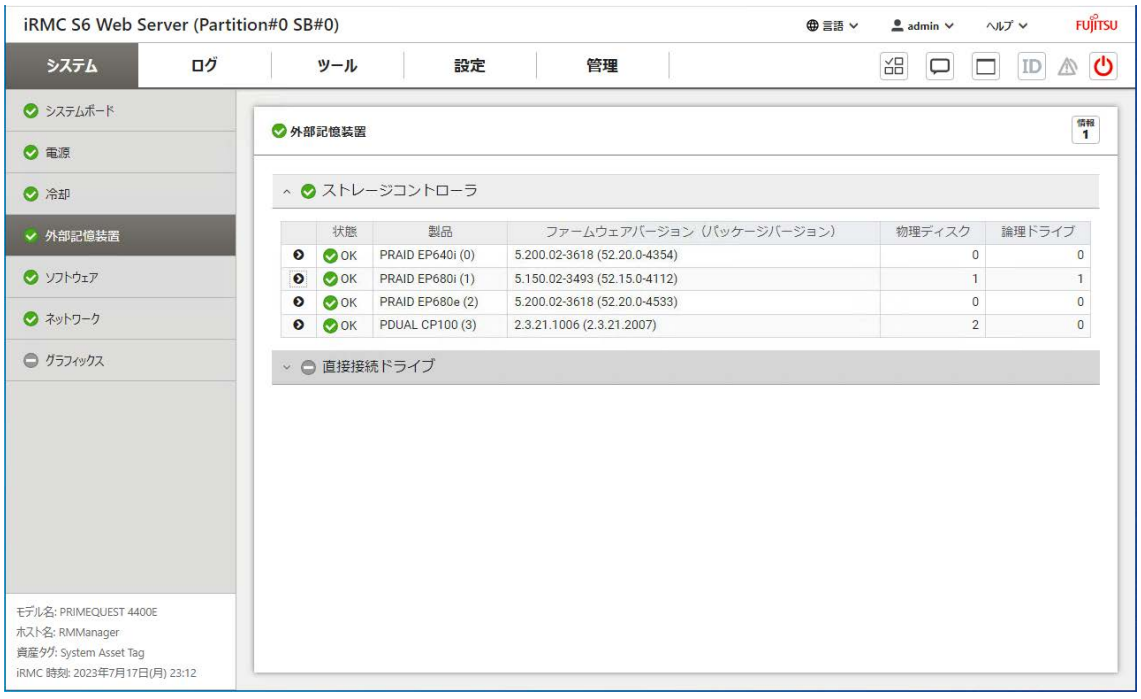


図 63: 「**外部記憶装置**」ページ

RAID コントローラは、SB に統合するか、アドオン PCI または PCIe 拡張カードとして使用可能な物理デバイスです。コントローラは全てを実行し、固有の CPU とメ

モリが内蔵されています。コントローラは、固有のハードディスクインターフェースと RAID レベルをサポートするように設計されています。

「**ストレージコントローラ**」グループでコントローラのエントリの近くにある をクリックすると、このコントローラに関連するすべてのアイテムがドロップダウンに表示されます。

- プロパティ
- 関連タスク
- 物理ディスク
- エンクロージャ
- 論理ドライブ

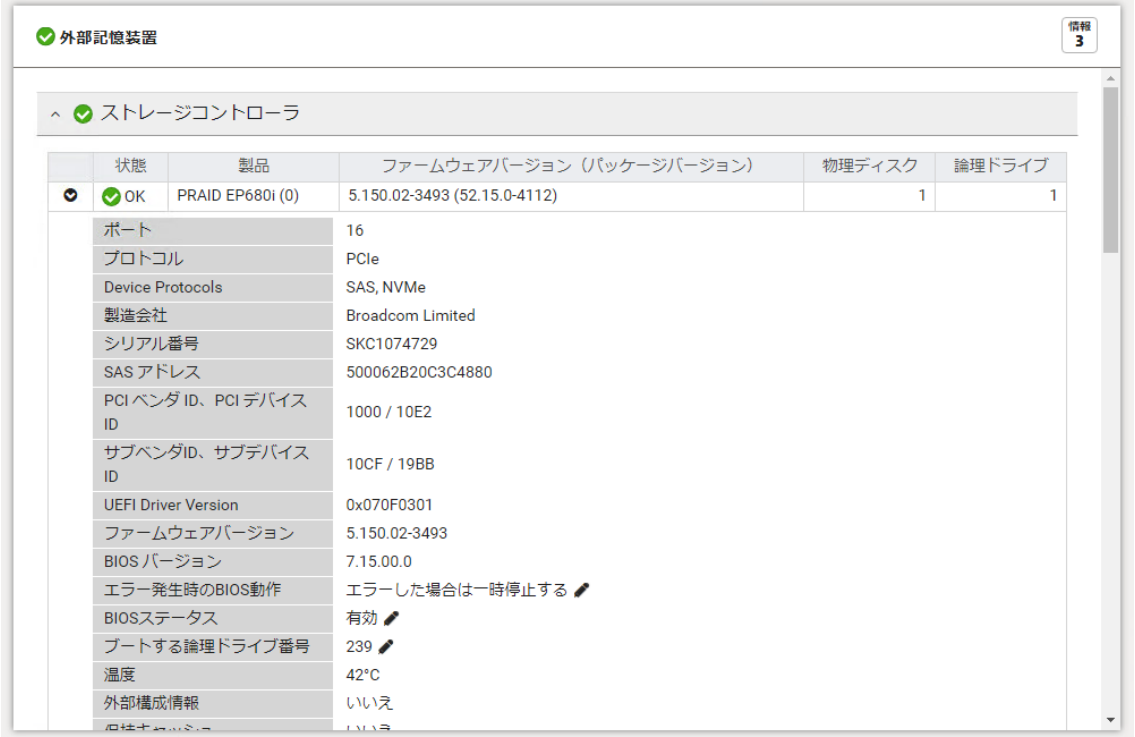


図 64:「ストレージコントローラ」ドロップダウン

マークの付いた全てのプロパティを編集できます。 をクリックすると小さいダイアログボックスが開き、関連するパラメータとその値が表示されます。

図 65:「編集」ダイアログボックス

一部のハードウェアコントローラには、停電時のデータ損失を回避したり、読み取りおよび書き込み動作を向上するために、追加のキャッシュがあります。

8.1.3.1 物理ディスク

RAID コントローラで管理される物理ディスクは、ストレージコントローラのプロパティで「**物理ディスク**」グループの表に表示されます。

図 66:「**物理ディスク**」グループ

表の列には、物理ディスクの主なプロパティが表示されます。「**状態**」列には、ディスクの現在の状態が表示されます。

状態	意味
可能	ディスクは論理ドライブに含まれませんが、レディ状態です。
動作中	ディスクは論理ドライブに含まれ、動作しています。
グローバルホットスペア	ディスクは、一般的なデータ損失を回避するために、グローバルホットスペアとして構成されています。
専用ホットスペア	ディスクは、個々の論理ドライブのデータ損失を回避するために、専用ホットスペアとして構成されています。
失敗	ディスクが損傷しています。

「**物理ディスク**」グループでディスクのエントリの近くにある をクリックすると、このディスクに関連するすべてのプロパティとタスクがドロップダウンに表示されます。

図 67: 「**物理ディスク**」ドロップダウン

物理ディスクに関連するタスクが復元（コピーバックとリビルド）とデータ損失の回避を中心に行われます。

コントローラで RAID 構成の整合性や残りのアレイとの同期に問題があることが検出された場合、Foreign（外部）とマークされます。これは、ドライブが別のマシンに移動されたときに発生することがありますが、ドライブがオフラインになったときに発生することもあります。ドライブは、故障した場合、故障が今発生している場合、ファームウェアで予期しない状況が発生した場合に、オフラインになる可能性があります。

Self-Monitoring and Reporting Technology（SMART）機能は、すべてのモーター、ヘッド、物理ディスクエレクトロニクスの特定の物理的な局面を監視し、物理ディスクの故障の予兆を検知することができます。SMART 対応物理ディスクのデータを監視して、値の変化を特定し、値がしきい値の制限内にあるかどうかを判断します。

ホットスペアは、故障したディスクの代替として冗長論理ドライブで使用可能な物理ディスクです。ドライブが故障すると、ホットスペアがそれに取って代わり、論理ドライブが再作成されます。動作の進行中に、新しいディスクでデータがリビルドされます。リビルドが完了するまで、データへのアクセスには少し時間がかかりますが、いつでもアクセスできます。

全ての論理ドライブで使用可能なグローバルホットスペア、または 1 つの論理ドライブにのみ割り当てられる専用ホットスペアを構成できます。

8.1.3.2 論理ドライブ

ストレージコントローラおよびその関連の物理ディスクのプロパティで、「**論理ドライブ**」グループに論理ドライブが表示されます。

図 68: 「**論理ドライブ**」グループ

表の列には、論理ドライブの主なプロパティが表示されます。「**ステータス**」列には、ドライブの現在の状態が表示されます。

ステータス	意味
動作中	論理ドライブは動作中です。
デグレード	物理ディスクは故障しています。
失敗	論理ドライブは破損しているため、アクセスできません。

「**論理ドライブ**」グループでディスクのエントリの近くにある をクリックすると、このディスクに関連するすべてのプロパティとタスクがドロップダウンに表示されます。

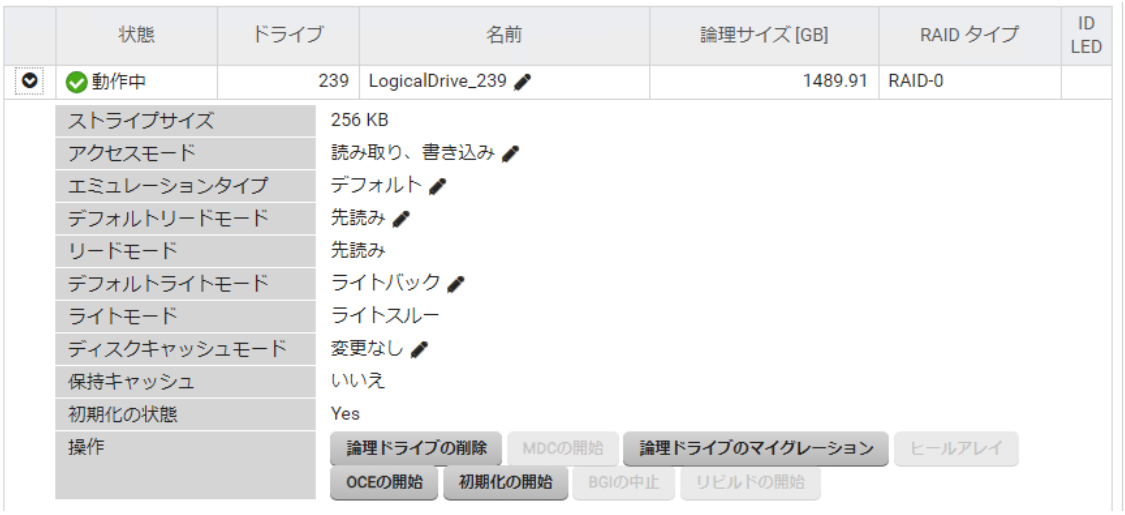


図 69: 「**論理ドライブ**」ドロップダウン

論理ドライブに関連するタスクは、整合性チェック（BGI および MDC）と復元を中心に行われます。RAID-1、RAID-5、RAID-10 のいずれかのタイプのクリティカル

な論理ドライブの場合は、論理ドライブのリビルドを開始できます。一般に、障害が発生したディスクは自動的にホットスペアに置き換わり、その後、コントローラに設定されている場合はリビルドが自動的に開始します。アクションはバックグラウンドで実行し、その他に障害があるディスクがなければ、論理ドライブで引き続き操作できます。

iRMC Web インターフェースを使用すると、論理ドライブを作成でき、さらに必要なディスクをディスクグループをバンドルすることもできます。必要に応じて、論理ドライブを別の RAID レベルに移行して、その目的で物理ディスクのボリュームを編集することができます。

アレイのすべてのディスクに空き記憶領域がある場合、既存の論理ドライブや実行中の論理ドライブを別の RAID レベルに移行して、容量をオンラインで拡張することができます。その後、オペレーティングシステムのツールを使用して、既存のファイルシステムを新しい容量に適合させることができます。

8.1.4 論理ドライブの作成

論理ドライブを作成する前に、使用する RAID レベル、選択した RAID レベルに必要なパラメータ、この論理ドライブを構成するドライブの種類（物理ドライブや論理ドライブ）を決定する必要があります。ここでは、ユーザは RAID の概念および各種 RAID レベルに精通していることを前提としています。

1. iRMC の Web インターフェースで「**システム**」メニューの「**外部記憶装置**」ページを開きます。
2. 「**ストレージコントローラ**」グループで、論理ドライブを管理する動作コントローラの詳細ドロップダウンリストを展開します。

   コントローラの全ての情報が表示されます。
3. 「**物理ディスク**」テーブルの下で「**論理ドライブの生成**」をクリックします。

   「**論理ドライブの生成**」ダイアログボックスが開きます。
4. 「**設定**」タブで関連パラメータに入力します。

   このタブで、RAID レベルとアクセスモードを設定します。
5. 「**レイアウト**」タブを開きます。

   このタブで、論理ドライブとして使用する物理ドライブを選択します。ディスクグループが存在しない場合は作成します。
6. 必要な全てのオプションを設定したら、「**OK**」をクリックして設定を確定します。

   オプションがチェックされ、どれも妥当である場合は、論理ドライブが作成されます。
7. 全ての設定はいつでも編集できます。

8.1.5 論理ドライブの削除

1. iRMC の Web インターフェースで「**システム**」メニューの「**外部記憶装置**」ページを開きます。
2. 「**ストレージコントローラ**」グループで、論理ドライブを管理する動作コントローラの詳細ドロップダウンリストを展開します。

   コントローラの全ての情報が表示されます。
3. 「**論理ドライブ**」で削除する論理ドライブを展開します。
4. テーブルで「**論理ドライブの削除**」をクリックします。

   論理ドライブが削除されます。

8.2 ソフトウェア RAID

PRIMEQUEST 4000 は、SB に割り当てられた HDD/SSD 用のソフトウェア RAID です。

ソフトウェア RAID は、Linux OS 標準および GDS に搭載される MD（Multiple Device）サブシステムにより、ハードウェア RAID の RAID 1 と同じ機能を実現します。

ソフトウェア RAID は、各コンポーネントに取り付けられたブートデバイスからブートします。ソフトウェア RAID は、システムのブート後に、ブートデバイスおよびソフトウェアと同期します。ソフトウェア RAID では、RAID カード側の構成は RAID 0 に設定する必要があります。

9 トラブルシューティング

問題が発生した場合は、次の方法で記録されます。

- デバイスのアラーム LED 経由
- iRMC の Web インターフェース（「**システム**」メニュー、「**保守**」メニュー）

また、E メールでアラーム通知を定義したアドレスに送信するように iRMC を設定することもできます。E メール通知には、事前に設定が必要です。

アラーム LED

PRIMEQUEST 4000 サーバに組み込まれた各コンポーネントには、独自の LED セットが搭載されています。

LED	色	意味
電源状態	緑色	関連するコンポーネントの電源状態を表示します。
アラームステータス	オレンジ色	関連するコンポーネントにエラーが発生しているかどうかを表示します。
場所情報	青色	関連するコンポーンネントが、iRMC Web-GUI でチェックされたかどうかを識別します。

デバイスが正常に動作している場合、アラーム LED は消灯しています。

デバイス内部で問題が発生すると、アラーム LED がオレンジ色に点灯します。問題がデバイスで解消されない限り、アラーム LED は点灯します。複数の問題が発生した場合でも、このランプは変わりません。

電子メールによるアラーム通知

アラーム電子メール通知により、システムの問題が報告されます。

問題が発生した場合のアラーム電子メール通知は、iRMC Web-GUI の「**設定**」メニューで、「**サービス**」ページの「**電子メールアラーム**」グループで設定できます。

エラー状態タイプ、パーティション、ターゲットコンポーネントなどで、通知をフィルタリングすることもできます。

担当営業員

それでも解決できない異常については、修理相談窓口または担当営業員に連絡してください。

連絡する前に、ユニット、ソース、部品番号、イベント ID、エラーの説明と、メインユニットに貼付されているラベルに記載されているモデル名とシリアル番号を確認してください。

担当営業員に提供する詳細については、「**保守**」ページですべてのパーティションのシステムレポートを生成できます。

9.1 正常性情報の詳細確認

「**システム**」メニューには、SB のコンポーネントの状態と稼働状態に関する情報が表示されます。

図 70:「**システム**」メニューの「**概要**」ページ

コンポーネントの稼働状態は以下のアイコンで示されます。

OK：コンポーネントの状態は良好です。

機能はサポートされていますが、無効になっています。

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。

「**保守**」ページで、関連するパーティションで使用される FRU（Field Replaceable Units）の稼働状態を確認できます。

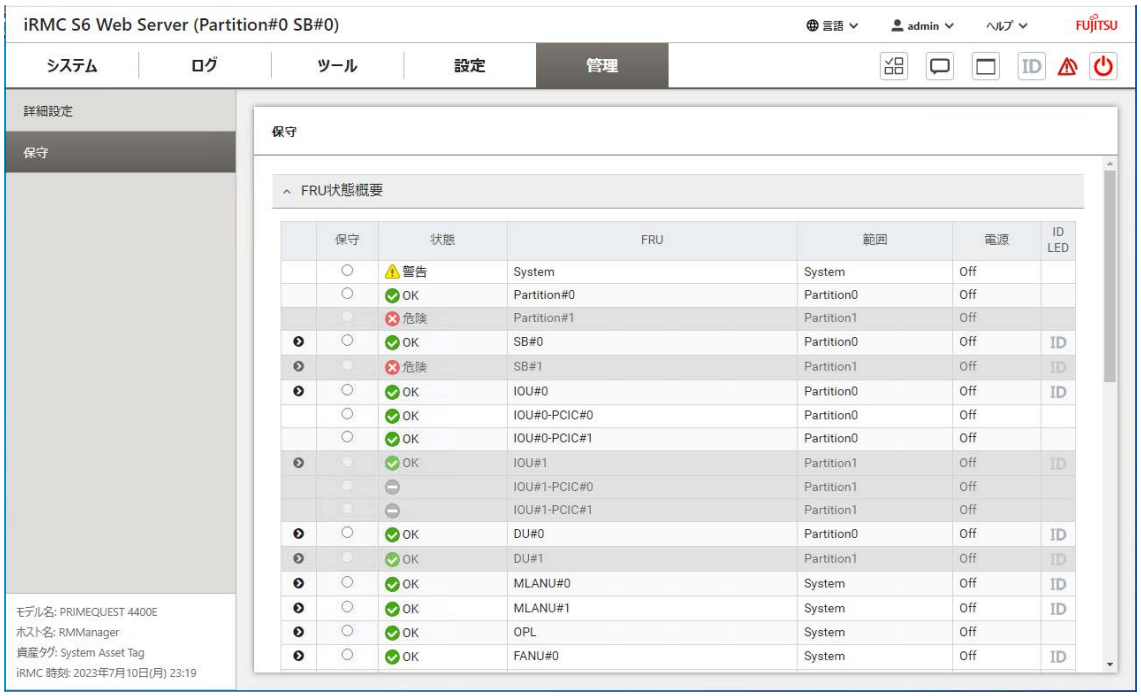


図 71:「**保守**」ページ

各 FRU のステータスと詳細情報を確認するには、 をクリックして関連するドロップダウンを開きます。**部品番号またはシリアル番号**の読み取りエラーが表示された場合は、フィールドエンジニアまたは営業担当者に連絡してください。

9.2 ログ情報

管理対象パーティションで実行中の iRMC と OS は、次のログを提供します。

ログタイプ	ログの内容	場所	ストレージフォーマット	ダウンロード形式	ビューア
SEL	以下のプログラムによって検出されたイベントまたはエラー : • BIOS • iRMC • Syslog • レポートなどのアクションを実行する SVAS のイベントログ • OSIV/XSP動作機構からバイナリのみ	iRMC	バイナリ	バイナリ、テキスト	テキストエディタ、専用のビューア
IEL	iRMC の操作とアクセス。詳細なログは SEL バイナリに記録されます。	iRMC	バイナリ	テキスト	テキストエディタ
PrimeCollect	SEL、ハードウェア情報、OS 情報	iRMC	XML	XML	XML ビューア、ブラウザ
富士通技術サポート	iRMC の内部ログ	iRMC	バイナリ	テキスト、GZIP 圧縮	テキストエディタ

テーブル 9: ログ情報の一覧

ログタイプ	ログの内容	場所	ストレージフォーマット	ダウンロード形式	ビューア
Redfish	以下のプログラムによって検出されたイベントまたはエラー : • BIOS • iRMC • SYSLOG • レポートなどのアクションを実行する SVAS のイベントログ • OSIV/XSP動作機構からバイナリのみ	iRMC	テキスト	XML	テキストエディタ
Syslog（Linux、LVM）	カーネル、アプリ、ドライバなどのイベント	パーティション	テキスト	テキスト	テキストエディタ
イベント ログ（Windows）	カーネル、アプリ、ドライバなどのイベント	パーティション	バイナリ	バイナリ、テキスト	テキストエディタ、イベントビューア
Mcelog（Linux） EDAC（Linux） FTrace rasdaemon（Linux）	メモリエラー、マシンチェックの例外（64 ビット Linux）	パーティション	テキスト	テキスト	OS ユーティリティ
WHEA（Windows）	ハードウェアエラー、マシンチェックの例外を解析する機能	パーティション	イベントログ		

テーブル 9: ログ情報の一覧

SEL 情報は調査のために重要ですので、最初に「**イベントログの保存**」ボタンをクリックして情報を保存します。この情報は、フィールドエンジニアまたは担当営業担当者に連絡する際に必要になります。