



ユーザガイド - 日本語

Fujitsu Server PRIMEQUEST 4000 Series

## **iRMC S6**

コンセプトとインターフェース

Edition 2023 年 8 月版

CA92344-5403-02

## 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 cognitas 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。  
cognitas. Gesellschaft für Technik-Dokumentation mbH  
[www.cognitas.de/en/](http://www.cognitas.de/en/)

## 著作権および商標

Copyright 2023 Fujitsu Limited

All rights reserved.

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

<b>1 はじめに</b> .....	<b>6</b>
1.1 目的と対象ユーザ .....	7
1.2 iRMC のマニュアル .....	7
1.3 本書の表記 .....	8
<b>2 IPMI</b> .....	<b>10</b>
2.1 技術的背景 .....	10
2.2 IPMI over LAN .....	15
2.3 サポートした IPMI OEM コマンド .....	16
2.3.1 SCCI 準拠の自動電源投入／電源切断コマンド .....	17
2.3.2 SCCI 準拠の通信コマンド .....	22
2.3.3 SCCI 準拠のシグナリングコマンド .....	26
2.3.4 BIOS 特有のコマンド .....	27
2.3.5 iRMC 特有のコマンド .....	41
2.4 データセンター管理インターフェース .....	56
2.5 Serial Over LAN (SOL) .....	56
<b>3 iRMC 設定</b> .....	<b>58</b>
3.1 iRMC Web インターフェースを使用した設定 .....	58
3.2 Remote Manager 経由の設定 .....	59
3.3 テキストコンソールリダイレクション経由の設定 .....	59
3.4 スクリプト経由の設定 .....	60
3.5 UEFI セットアップユーティリティを使用した設定 .....	61
3.5.1 LAN インターフェースのテスト .....	62
3.5.2 テキストコンソールリダイレクションの構成 .....	63
3.5.3 シリアルインターフェースの設定 .....	65
<b>4 Telnet/SSH 経由を使用した設定 (Remote Manager)</b> .....	<b>67</b>
4.1 SB の要件 .....	67
4.2 必要なユーザ権限 .....	68
4.3 ログイン .....	71
4.4 「Main」メニュー .....	72

---

4.4.1 「System Information」メニュー	73
4.4.2 「Power Management」メニュー	74
4.4.3 「Enclosure Information」メニュー	76
4.4.3.1 「System Eventlog」メニュー	78
4.4.3.2 「Internal Eventlog」メニュー	78
4.4.4 「Service Processor」のメニュー	80
4.4.5 Console Redirection (EMS/SAC)	81
4.4.6 「Console Logging」メニュー	81
4.4.7 「Console Logging Run State」メニュー	82
<b>5 スクリプト経由の設定</b>	<b>83</b>
5.1 Redfish	84
5.2 REST	87
5.3 プロファイル管理	90
5.3.1 プロファイル	90
5.3.2 自動 BIOS パラメータバックアップ	91
5.4 SCCI	91
5.4.1 iRMC 設定データ	92
5.4.2 SCCI ファイルフォーマット	93
5.4.2.1 SCCI プロバイダ固有のコマンドのパラメータ	94
5.4.2.2 注意事項	97
5.4.2.3 設定データのエクスポートとインポート	97
5.4.3 サポートされる SCCI コマンド	98
5.4.4 スクリプトのサンプル	99
5.4.4.1 cURL のサンプル	99
5.4.4.2 Visual Basic (VB) スクリプト	100
5.4.4.3 Python スクリプト	101
5.4.5 パスワード暗号化ユーティリティ	102
<b>6 LAN over USB</b>	<b>104</b>
6.1 要件	104
6.2 iRMC での LAN over USB の設定	105
6.2.1 MAC アドレスの割り当て	105

---

6.2.2 configSpace 変数による設定 .....	107
6.2.3 Web インターフェースによる設定 .....	110
6.3 Windows サーバでの LAN over USB の設定 .....	111
6.4 Linux サーバでの LAN over USB の設定 .....	112
<b>7 iRMC の監視 .....</b>	<b>113</b>
7.1 SNMP による監視 .....	113
7.2 iRMC システムレポート .....	115
7.2.1 ダウンロード用の cURL スクリプト .....	116
7.2.2 Visual Basic スクリプト .....	117
7.2.3 情報セクション .....	118
7.2.3.1 Summary セクション .....	119
7.2.3.2 BIOS セクション .....	120
7.2.3.3 Processor セクション .....	120
7.2.3.4 Memory セクション .....	121
7.2.3.5 Fans セクション .....	122
7.2.3.6 Temperature セクション .....	122
7.2.3.7 PowerSupplies セクション .....	123
7.2.3.8 Voltages セクション .....	123
7.2.3.9 IDPROM セクション .....	123
7.2.3.10 SensorDataRecords セクション .....	123
7.2.3.11 PCIDevices セクション .....	124
7.2.3.12 SystemEventLog セクション .....	124
7.2.3.13 InternalEventLog セクション .....	125
7.2.3.14 BootStatus セクション .....	125
7.2.3.15 ManagementControllers セクション .....	125
7.2.3.16 Settings セクション .....	126
7.2.3.17 Adapters セクション .....	126
7.2.3.18 Interfaces セクション .....	126
7.2.3.19 Ports セクション .....	127
7.2.3.20 SNMPAgents セクション .....	127
7.2.3.21 ServerViewRaid セクション .....	127

---

# 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ンネルを使用します。



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、システム管理専用で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 SB 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。

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。本取扱説明書は、iRMC のコンセプト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。

- IPMI の章では、IPMI プロトコルの基本原理と、スクリプト内で使用可能なサポートされる OEM コマンドを説明しています。
- 「iRMC 設定」では、iRMC を構成するさまざまな可能性を概説します。
- 次の章では、各種インターフェースを使用する iRMC の設定について詳しく説明します。
  - Remote Manager
  - スクリプトを使用して複数の API
- 「iRMC の監視」では、iRMC の監視方法を詳しく説明します。

## 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』（CA92344-5403）
- 『iRMC S6 Web インターフェース』（CA92344-5405）
- 『iRMC S6 コンフィグレーションとメンテナンス』（CA92344-5407）

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。

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





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 イメージとしてこちらから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の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	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。
monospace semibold (太字の等間隔表示)	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。
<a href="#">青字の文字列</a>	関連するトピックへのリンクを示します。
<a href="#">ピンクの文字列</a>	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。

テーブル 1: 本書の表記



表記	説明
[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 IPMI

### 2.1 技術的背景

iRMC は、IPMI インターフェースを使用して BMC の機能を使用できるようにします。

#### インテリジェントプラットフォーム

「インテリジェントプラットフォーム管理」イニシアチブは、最近のサーバシステムの増しつある複雑さに応えるものです。これらのサーバシステムを監視するための新しいソリューションを開発するために、いくつかのメーカーがこのイニシアチブに参加しています。

「インテリジェントプラットフォーム管理」という用語は、ソリューション（システムの監視およびリカバリのための機能をプラットフォーム管理のためのハードウェアおよびファームウェアに直接実装する）へのアプローチの核心となる面を表しています。

#### 目標

目標は、プラットフォーム管理用に中央システムコントローラ（Baseboard Management Controller - BMC）とインテリジェントプラットフォーム管理ハードウェアの間の。標準化された、抽象的で、メッセージベースのインターフェースを定義することでした。

この標準化委員会は、さまざまなプラットフォーム管理モジュールの中心的特質を標準化された記述にまとめました。

#### 定義

IPMI の仕様は、次のように定義されています。

「IPMI は、管理ソフトウェアで中立的な存在であるハードウェアレベルのインターフェースの仕様であり、DMI、WMI、CIM、SNMP などの標準的な管理ソフトウェアインターフェースを通じて公開できる監視および制御機能を提供する。また、ハードウェアレベルのインターフェースとして、一般的な管理ソフトウェアスタックの下部に存在する」

## 利点

IPMI の仕様では、システムのプロセッサ、BIOS、または OS によるインベントリ、ログ、リカバリおよび監視のための機能の独立性が確保されています。

これは、システムがシャットダウンされ、電源がオフにされたときも、システムをプラットフォーム管理の対象にすることができることを意味します。

## IPMI と他の管理標準

IPMI は、関連する OS の下で動作しているシステム管理ソフトウェアと連携する形で最も効果的に使用されます。IPMI の機能の管理アプリケーションおよび OS によって提供される管理機能への統合により、強力なプラットフォーム管理環境が実現されます。

IPMI と管理ソフトウェアスタックとの関係の概要を以下の図に示します。

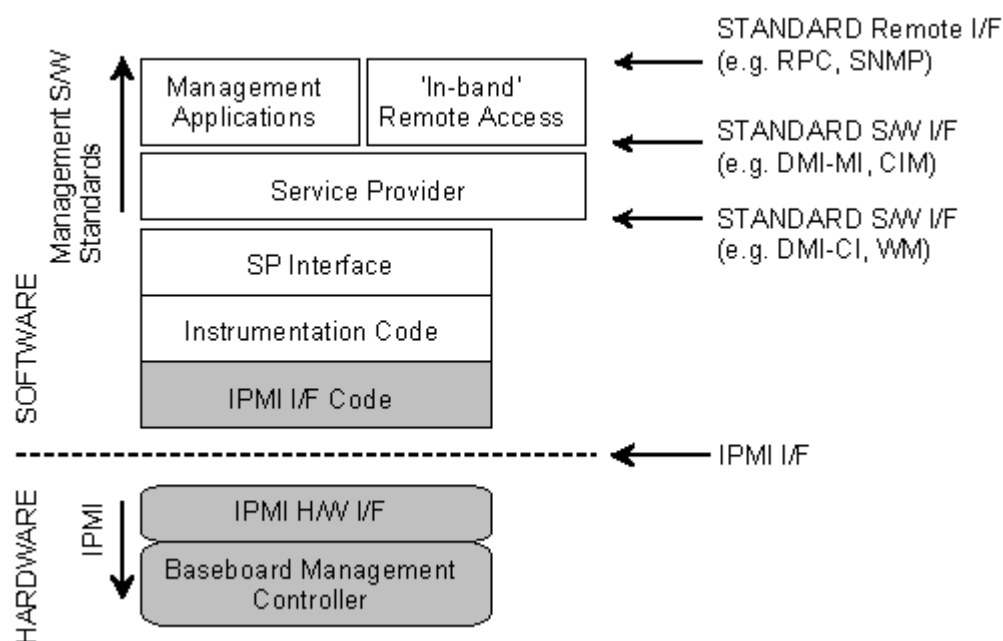


図 2: 管理ソフトウェアスタックでの IPMI (出典: IPMI 仕様)

## IPMI、IPMB および ICMB

IPMI イニシアチブは 3 つの主要な標準を生み出しました。

- IPMI: インテリジェントプラットフォーム管理インターフェース仕様

より高いレベルのアーキテクチャ、IPMI ベースのシステムで使用される現在のコマンド、イベントフォーマット、データパケット、およびプロパティを記述します。

- IPMB: インテリジェントプラットフォーム管理バス  
I2C ベース（書き込み専用）のバスであり、共通ハウジング内のさまざまなモジュール間の標準化された接続を提供します。  
IPMB は、リモート管理モジュールの標準化されたインターフェースとしても使用することができます。
- ICMB: インテリジェントシャーシ管理バス  
(現在、ServerView Remote Management 環境には実装されていません)  
プラットフォーム管理情報のやり取りおよび複数のシステムにわたる制御のための標準化されたインターフェースを提供します。ICMB は、IPMB に接続されるデバイスを使用して実装できるように設計されています。

### IPMI 実装

IPMI の実装のコア要素は Baseboard Management Controller (BMC) です。

BMC は以下のタスクを実行します。

- システム管理ソフトウェアとプラットフォーム管理ハードウェアの間のインターフェースを編成します。
- また、監視、イベントログ、リカバリ制御のための自律的な機能を提供します。
- システム管理ソフトウェアと IPMB の間のゲートウェイとしての役目を果たします。

IPMI では、追加の管理コントローラを、IPMB を使用して接続できるように、プラットフォーム管理を拡張できます。IPMB は I2C ベースのシリアルバスであり、システムのメインモジュール間で動作します。IPMB は、管理コントローラとの通信および管理コントローラ間の通信に使用されます。

複数の管理コントローラがサポートされている場合、IPMI はスケーラブルなアーキテクチャを提供します。つまり、複合サーバシステムでは、異なるサブシステム（たとえば、電源、ホットスワップ RAID ドライブモジュールなど）を監視するために複数のコントローラを使用できます。

IPMI は「ローレベル」の I2C コマンドを提供します。これには、IPMI コマンドでは処理できない「非インテリジェント」な I2C モジュールで IPMB に接続されている管理コントローラを介してアクセスできます。

IPMI 実装の基本的な要素の概要は、以下の図を参照してください。

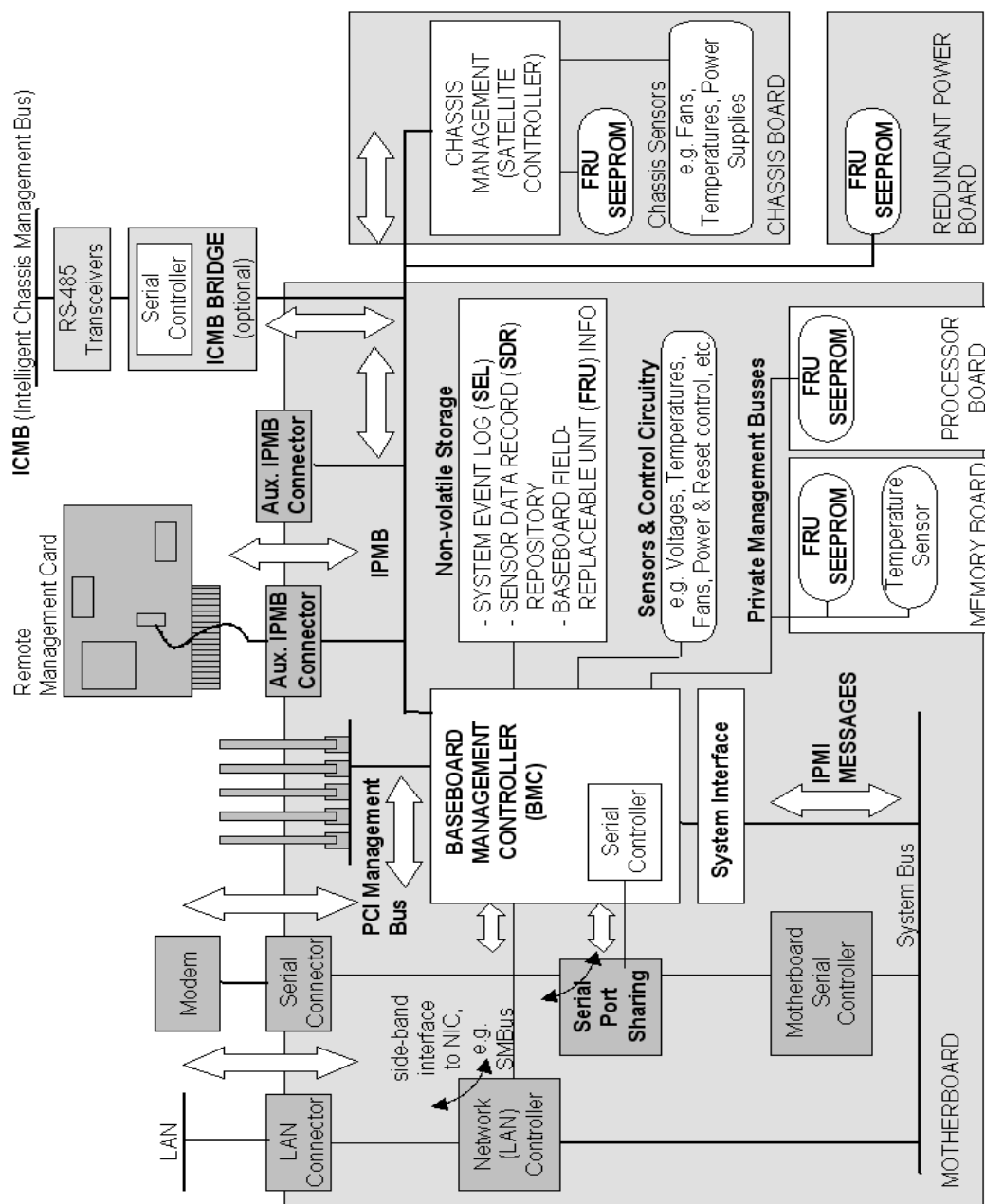


図 3: IPMI ブロック図 (出典: IPMI の仕様)

### IPMI と「in-band」 / 「Out-Of-Band」 管理

システム管理の分野では、「in-band」 管理と「Out-Of-Band」 管理は区別されま

- 「in-band」 管理という用語は、SBで OS が実行されている場合に使用されま
- す。
- 「Out-Of-Band」 管理という用語は、SBで OS が実行されていない場合、たと
- えばハードウェアが故障している場合に使用されます。

IPMI 互換のシステムを持つ環境では、異なるインターフェースが使用できるため、このようなシステムは「in-band」でも「Out-Of-Band」でも管理できます。

### IPMI でのチャンネルのコンセプト

「チャンネル」は、IPMI メッセージがさまざまな接続キャリアを介して BMC にルーティングされるときに使用される仕組みを提供します。最大 9 つのチャンネルをサポートできます。システムインターフェースと IPMB は固定されています。他の 7 つのチャンネルは実装に使用できます。

チャンネルは「セッションベース」か「セッションレス」のどちらかにすることができます。「セッション」というコンセプトには 2 つの意味があります。ユーザ認証を行うコンセプトと、単一のチャンネルを使用した複数の IPMI メッセージストリームをルーティングするコンセプトです。

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

### ユーザ ID

セッションベースのチャンネルにはユーザログインが必要ですが、セッションレスチャンネルにはユーザ認証はありません。

IPMI では、ユーザ設定はチャンネル固有です。したがって、ユーザは BMC に LAN チャンネル経由でアクセスしているか、シリアルチャンネル経由でアクセスしているかに応じて、異なる権限を持つことができます。

### フェンシング

高可用性クラスタでは、障害が発生したと見られるノードが実際にはそうではなかった場合、問題が発生します。理由が何であれ、実際に障害がなく、ストレージソリューションにまだ接続されている場合、VM プロセスで仮想マシンドライブを変更できます。

2 つの VM インスタンスを実行すると、ドライブは破損しやすくなり、仮想マシンの状態が一致しなくなります。この場合、フェンシングが役に立ちます。フェンシングは、クラスタが特定のノードの状態を認識していなくても、そのノードで重要なリソースが実行されないようにすることができます。

つまり、フェンシングは、ダウンしていると考えられるノードを切り離し、共有ストレージへ書き込まないようにする概念を指します。iRMC のフェンシング機能は、IPMI フェンシングが有効になっている場合、リモートデバイスのシャットダウンを要求できます。IPMI フェンシングを有効にする方法については、『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。

### 参照先

IPMI 標準に関する情報は、インターネットの以下のサイトを参照してください。

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

## 2.2 IPMI over LAN

「IPMI over LAN」は、IPMI 標準での LAN インターフェースの仕様を表す現在の名前です。この仕様は、IPMI メッセージを管理対象システムの BMC との間で送受信できる方法を定め、メッセージは、RMCP (Remote Management Control Protocol) データパケットでカプセル化できます。これらの RMCP データパケットは IPv4 (Internet Protocol Version 4) の UDP (User Datagram Protocol) を使用して Ethernet LAN 接続で転送されます。

RMCP プロトコルは、OS が実行されていないときのシステムの状態の管理をサポートするように指定されています。RMCP は簡単な照会/応答プロトコルです。

このような接続のインターフェースは、BMC に割り当てられているオンボード LAN コントローラで提供されます。



このインターフェースは、挿入された LAN カードではなくオンボード LAN コントローラによってのみ提供できます。

RMCP が UDP の下で使用する 2 つのポートのうち、BMC は、ポート 623 (プライマリ RMCP ポート) を使用して LAN コントローラと通信します。

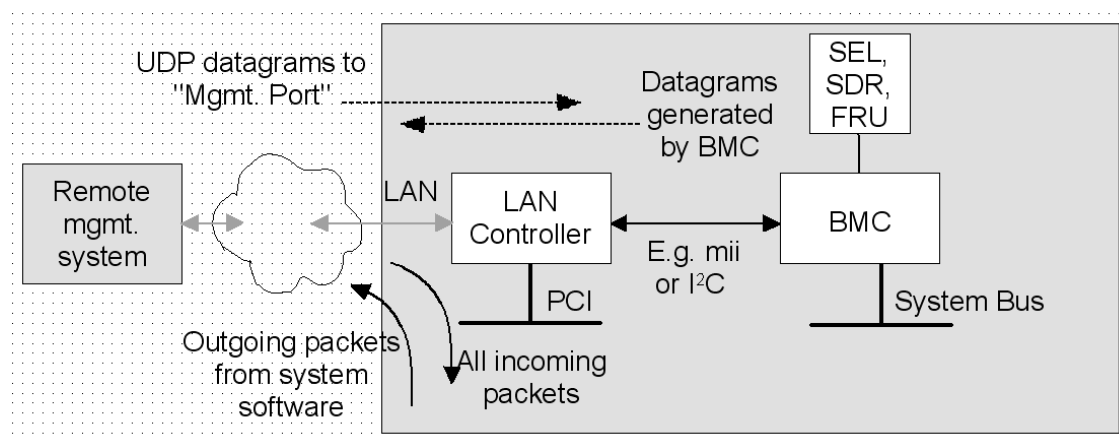


図 4: BMC と LAN コントローラ

## 2.3 サポートした IPMI OEM コマンド

iRMC S6 は以下の OEM 固有の IPMI コマンドをサポートします。

### SCCI 準拠の自動電源投入／電源切断コマンド

(SCCI : ServerView Common Command Interface (ServerView 共通コマンドインターフェース) )

0115 Get Power On Source  
0116 Get Power Off Source  
011C Set Power Off Inhibit  
011D Get Power Off Inhibit  
0120 Set Next Power On Time

### SCCI 準拠の通信コマンド

0205 System OS Shutdown Request  
0206 System OS Shutdown Request and Reset  
0208 Agentless Service Connect Status  
0209 Shutdown Request Canceled

### SCCI 準拠のシグナリングコマンド

1002 Write to System Display

### BIOS 特有のコマンド

F109 Get BIOS POST State  
F115 Get CPU Info  
F163 Get SMBIOS Type Structure  
F1E3 Get/Set NVDIMM Config Info

### iRMC S6 特有のコマンド

F510 Get System Status  
F512 Get EEPROM Version Info  
F542 Get HDD lightpath status (コンポーネント状態信号の読み取り)  
F543 Get SEL entry long text  
F545 Get SEL entry text



F58D Get NVMe Information  
 F5B0 Set Identify LED  
 F5B1 Get Identify LED  
 F5B3 Get Error LED  
 F5E0 Set Configuration Space to Default Values  
 F5F8 Delete User ID

この節では、個別の OEM 特有の IPMI コマンドについて説明します。

### 記述形式

本章で記載する OEM 特有の IPMI コマンドは、IPMI コマンドを記述するための IPMI 標準で使用する形式によって記述されます。

IPMI 標準では、各コマンドに対する入力パラメータと出力パラメータを一覧にしたコマンド表を使用して IPMI コマンドを記述します。

IPMI 標準の情報については以下のサイトを参照してください。

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

## 2.3.1 SCCI 準拠の自動電源投入／電源切断コマンド

### 0115 - Get Power On Source

本コマンドは最後に行われた自動電源投入の理由を返します。理由には以下にあげるものがあります。

要求データ	-	<b>B8</b> NetFnLUN: OEM/Group
	-	<b>01</b> Cmd : コマンドグループコミュニケーション
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>15</b> コマンド指定子

応答データ	-	BC
	-	01
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	3	01 データ長
	4	電源投入原因：最後の自動電源投入の理由

電源投入原因	意味
0x00	ソフトウェアまたはコマンド
0x01	電源スイッチ（フロントパネルまたはキーボード上）
0x02	AC 電源障害後の自動再起動
0x03	クロックまたはタイマー（ハードウェア RTC またはソフトウェアタイマー）
0x04	ファン障害によるシャットダウン後の自動再起動
0x05	臨界温度によるシャットダウン後の自動再起動
0x08	ウォッチドックタイムアウト後の再起動
0x09	リモートオン（モデム RI ライン、SCSI ターミネーションパワー、LAN、IC カードリーダー・・・）
0x0C	CPU エラー後の再起動
0x15	ハードウェアリセットによる再起動
0x16	ウォームスタート後の再起動
0x1A	PCI バス電源管理イベントによる電源投入
0x1D	リモートマネージャ経由のリモート制御による電源投入
0x1E	リモートマネージャ経由のリモート制御による再起動/リセット
0x24	VIOM イベントリブートの自動電源投入/切断
0x25	VIOM init ブートの自動電源投入/切断

## 01 16 - Get Power Off Source

本コマンドは最後に行われた自動電源切断の理由を返します。理由には以下にあげるものがあります。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>01</b> Cmd : コマンドグループコミュニケーション
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>16</b> コマンド指定子
応答データ	-	<b>BC</b>
	-	<b>01</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	3	<b>01</b> データ長
	4	電源切断原因：最後の自動電源切断の理由

電源切断原因	意味
0x00	ソフトウェア (SWOFF、SE: コマンドによる電源切断)
0x01	電源スイッチ (フロントパネルまたはキーボード上)
0x02	AC 電源障害
0x03	クロックまたはタイマー (ハードウェア RTC またはソフトウェアタイマー)
0x04	ファン障害
0x05	臨界温度
0x08	ウォッチドッグタイムアウト繰り返し後の電源切断
0x0C	CPU エラー繰り返し後の電源切断
0x1D	リモートマネージャ経由のリモート制御による電源切断

電源切断原因	意味
0x24	VIOM インベントリブートの自動電源投入/切断
0x25	VIOM init ブートの自動電源投入/切断

### 01 1C - Set Power Off Inhibit

このコマンドは、電源切断防止フラグを設定し、SBの電源を切断しようとする未検出の施行を一時的に抑制します。

電源切断防止フラグが設定されていると、SBの電源切断、パワーサイクルまたは再起動を実行しようとした理由がファームウェアによって保存されますが、動作は実行されません。最後に実行したSBの電源切断、パワーサイクルまたは再起動の理由が常時保存されます。保存された動作は電源切断防止フラグをリセットしたときのみ実行されます。

電源切断防止フラグは、電源障害後、またはリセットボタンの押下時に自動的にリセットされます。

電源切断防止フラグには、メインメモリダンプを作成する際に使用するダンプフラグと同じ効果があります。この場合、ダンプを作成する前にイニシエーターで必ずフラグを設定し、ダンプが完了したときにリセットします。

要求データ	-	B8 NetFn LUN: OEM/グループ
	-	01 Cmd : コマンドグループコミュニケーション
	1:3	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	4	1C コマンド指定子
	5	00 オブジェクトID
	6:7	00 00 値 ID
	8	01 データ長
	9	電源切断防止フラグ : 0 = 防止しない、1 = 防止する
応答データ	-	BC
	-	01
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト

### 01 1D - Get Power Off Inhibit

このコマンドは、電源切断防止フラグの値を取得します。

電源切断防止フラグの詳細については、01 1C - Set Power Off Inhibit の説明を参照してください。

要求データ	-	B8 NetFn LUN: OEM/グループ
	-	01 Cmd : コマンドグループコミュニケーション
	1:3	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	4	1D コマンド指定子
応答データ	-	BC
	-	01
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5	01 応答データ長
	6	電源切断防止フラグ : 0 = 防止しない、1 = 防止する

### 01 20 - Set Next Power On Time

本コマンドは、設定スペースに保存されている電源投入/切断時刻とは別に所定の時間でシステムの電源を投入します。



コマンドが効果を発揮するのは 1 回だけです。

前回 01 20 コマンドで設定した電源投入時刻をキャンセルするには、次の 01 20 コマンドで「0」を電源投入時刻に指定します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>01</b> Cmd : コマンドグループコミュニケーション
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>20</b> コマンド指定子
	5	<b>00</b> オブジェクトID
	6:7	<b>00 00</b> 値 ID
	8	<b>04</b> データ長
	9:12	時刻 (LSB ファースト)
応答データ	-	<b>BC</b>
	-	<b>01</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト

**時刻 (LSB ファースト)**

システムの電源を再度投入した時刻 (UNIX 特有の形式) です。時刻は不揮発メモリに保存されません。設定単位は 1 分毎です。システムの電源を投入した後、内部で時刻が 0 に設定されます。

時刻に「0」を指定した場合、システムの電源は投入されません。

## 2.3.2 SCCI 準拠の通信コマンド



SCCI 準拠の通信コマンドには、Agentless Service が OS で起動していることが必要です。コマンドを実行するには、iRMC S6 と通信する Agentless Service が最終的に動作を行います。

### 02 05 - System OS Shutdown Request

本コマンドは SB の OS のシャットダウンを開始します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>02</b> Cmd : コマンドグループコミュニケーション
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>05</b> コマンド指定子
応答データ	-	<b>BC</b>
	-	<b>02</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト

### 02 06 - System OS Shutdown Request and Reset

本コマンドは SB の OS のシャットダウンを開始した後にシステムを再起動します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>02</b> Cmd : コマンドグループコミュニケーション
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>06</b> コマンド指定子
応答データ	-	<b>BC</b>
	-	<b>02</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト

### 02 08 - Agentless Service Connect Status

本コマンドは Agentless Service がアクティブであるかどうかを確認します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>02</b> Cmd : コマンドグループコミュニケーション
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>08</b> コマンド指定子

応答データ	-	BC
	-	02
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5	01 データ長 (01h または 03h)
	6	<b>接続状態：</b> 00 = 接続が切断され、Agentless Service が接続されていない 01 = 接続が切断され、Agentless Service が接続されている 03 = Agentless Service への接続が確立され、接続がサポートされる機能がバイト 7 と 8 で有効になる 04 = Agentless Service が確立され、Agentless Service によってサポートされる機能がバイト 7 と 8 で有効になる
	7:8	(オプション) Agentless Service がサポートする機能 ビットフィールドの値は、サポートされている場合は 1、サポートされていない場合は 0 [0]: HTI サポート [1]: グレースフルシャットダウン/リブートのサポート [2]: iRMC 再起動のサポート (FW アップデート) [15]: 予約済み



**02 09 - Shutdown Request Cancelled**

本コマンドは発行されたシャットダウン要求をキャンセルします。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>02</b> Cmd : コマンドグループコミュニケーション
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>09</b> コマンド指定子
応答データ	-	<b>BC</b>
	-	<b>02</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト

## 2.3.3 SCCI 準拠のシグナリングコマンド

## 10 02 - Write to System Display

本コマンドは、LocalView ディスプレイ（接続されている場合）に文字を書き込むために使用します。

要求データ	-	B8 NetFnILUN: OEM/Group
	-	10 Cmd: コマンドグループファンテスト
	1:3	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	4	02 コマンド指定子
	5	オブジェクトインデックス: 書き込みを行うディスプレイ 上の行
	6:7	値 ID（未使用）
	8	長さ 書き込む文字数。1 文字単位で増加（文字列がヌル 終端である必要はありません。ディスプレイの長さを超 える文字列は切り捨てられます）
	9	属性: 0 = 文字列を左詰めで書き込みます 1 = 文字列を右詰めで書き込みます
	10:10+n	ディスプレイに書き込む文字（文字列がヌル終端である 必要はありません）
応答データ	-	BC
	-	10
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト

## 2.3.4 BIOS 特有のコマンド

## F1 09 - Get BIOS POST State

本コマンドは BIOS が POST 中であるかどうかの情報を提供します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F1</b> Cmd : コマンドグループ BIOS
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>09</b> コマンド指定子
応答データ	-	<b>BC</b>
	-	<b>F1</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	5	<p>[7:3] - 予備</p> <p>[0] - BIOS POST 状態： 0=BIOS が POST 状態ではありません。 1=BIOS が POST 状態です。</p> <p>[1] - BIOS ビデオ状態:  0 = ビデオ初期化はまだ実行されていない  1 = ビデオ初期化が実行された</p> <p>[2] - 修正不能なエラー表示ランプの状態:  0 = 表示ランプがクリアされていない  1 = 表示ランプがクリアされている</p>

## F1 15 - Get CPU Info

本コマンドは CPU 内部情報を返します。iRMC では、POST フェーズ中に BIOS から本情報を取得します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F1</b> Cmd : コマンドグループ BIOS
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>15</b> CommandsSpecifier
	5	CPU のソケット番号 (0 ベース)
応答データ	-	<b>BC</b>
	-	<b>F1</b>
	1	完了コード: 01 = 未実装の CPU ソケット
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	5:6	CPU ID、LSB ファースト
	7	プラットフォーム ID
	8	ブランド ID
	9:10	CPU の最大コアスピード [MHz]、LSB ファースト
	11:12	Intel QuickPath インターコネクト [MT/s]、LSB ファースト
	13	熱制御オフセット
	14	熱ダイオードオフセット
	15	CPU TJ 最大
	16:17	記録 ID CPU 情報 SDR、LSB ファースト
	18:19	記録 ID CPU ファン制御 SDR、LSB ファースト
	20:21	CPU ID ハイワード、LSB ファースト (N/A = 0000h)

応答データ	22:23	熱設計電力 TDP 値、1/8 W 単位、LSB ファースト (オフション) (N/A = FFFFh)
	24:25	キャッシュサイズ (L1) (ソケットの全 L1 キャッシュの合計)、単位は MSBit = 0 の場合は [KB]、MSBit = 1 の場合は [MB]、LSB ファースト (N/A = FFFFh)
	26:27	キャッシュサイズ (L2) (ソケットの全 L2 キャッシュの合計)、単位は MSBit = 0 の場合は [KB]、MSBit = 1 の場合は [MB]、LSB ファースト (N/A = FFFFh)
	28:29	キャッシュサイズ (L3) (ソケットの全 L3 キャッシュの合計)、単位は MSBit = 0 の場合は [KB]、MSBit = 1 の場合は [MB]、LSB ファースト (N/A = FFFFh)
	30	最大コア数 (N/A = FFh)
	31	現在のコア数 (N/A = FFh)
	32	コアごとの最大スレッド数 (N/A = FFh)
	33	コアごとの現在のスレッド数 (N/A = FFh)
	34:35	SMBIOS の CPU ファミリ (構造 4、オフセット 6)
	36	CPU メーカー: 0 = 不明、1 = INTEL、2 = AMD

### F1E3 Get/Set NVDIMM Config Info

このコマンドは、インストールされた NVDIMM メモリコンポーネントから、現在の構成データを要求します。BIOS はこのコマンドを使用して、NVDIMM メモリコンポーネントの構成を変更できます。



要求された情報を提供するには、BIOS はバージョン R0.81 以上である必要があります。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F1</b> Cmd : コマンドグループ BIOS
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>63</b> コマンド指定子
	5	<b>01</b> バージョン
	6	<b>モード</b> 00 取得する 01 設定する
	7	<b>Volatile Memory Mode</b> (Set コマンドのみ) 00 1LM 01 2LM
	8	<b>AppDirect Cache</b> (Set コマンドのみ) 00 無効 01 有効
	9	<b>1LM Memory Interleave Granularity</b> (Set コマンドのみ) 00 64 B ターゲット, 64 チャンネル 01 256 B ターゲット, 256 チャンネル
	10	<b>NVDIMM Power management</b> (Set コマンドのみ) 00 無効 01 有効

応答データ	-	BC
	-	F1
	1	完了コード:
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5	<b>Volatile Memory Mode</b> (Set コマンドのみ) 00 1LM 01 2LM
	6	<b>AppDirect Cache</b> (Set コマンドのみ) 00 無効 01 有効
	7	<b>1LM Memory Interleave Granularity</b> (Set コマンドのみ) 00 64 B ターゲット, 64 チャンネル 01 256 B ターゲット, 256 チャンネル
	8	<b>NVDIMM Power management</b> (Set コマンドのみ) 00 無効 01 有効

### F1 63- Get SMBIOS Type Structure

このコマンドは、ハンドル値のない BIOS の SMBIOS タイプ 42 を取得します。BIOS がハンドル値を設定します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F1</b> Cmd : コマンドグループ BIOS
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>63</b> コマンド指定子
	5	<b>01</b> バージョン
	6	<b>2A</b> SMBIOS タイプの要求 現在はタイプ 42 のみ (=2Ah をサポート)
	7:8	読み取りオフセット オフセットが 0000h の場合、iRMC は SMBIOS タイプ構造を内部的に作成します。
応答データ	-	<b>BC</b>
	-	<b>F1</b>
	1	完了コード: 01 = 未実装の CPU ソケット
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	5:6	読み取る残りのバイト
	7	このチャンクで返されたデータバイト数
	8:n	データバイト (このチャンクの最大 50 SD バイト)

BIOS がこのコマンドをオフセット 0000h で送信すると、iRMC ファームウェアは SMBIOS タイプ 42 構造から情報を収集し、iRMC 内部キャッシュに書き込みます。BIOS は以降のオフセットを使用して、構造全体を読み取りれます。



以下の表に、SMBIOS タイプ 42 構造と、iRMC が値を取得する方法を示します。

バイト	名前		長さ	値	説明	iRMC からの値の派生方法
00h	タイプ		バイト	42	管理コントローラ ホストインター フェース構造イン ジケータ	
01h	長さ		バイト		構造の長さ。最小 09h	
02h	ハンドル		ワード	0000h	ハンドルは BIOS で設定されます。	
04h	インター フェース タイプ		バイト	40h	管理コントローラ インターフェース タイプ: ネット ワークホストイン ターフェース= 40h	

テーブル 2: SMBIOS タイプ 42 構造

## 2.3 サポートした IPMI OEM コマンド

バイト	名前		長さ	値	説明	iRMC からの値の派生方法
05h	インターフェース固有のデータ長		バイト	n+7	インターフェースタイプで指定された、インターフェース固有のデータ。0 の場合、インターフェース固有のデータはありません。	
06h	インターフェース固有のデータ	デバイスタイプ	バイト	02h	USB ネットワークインターフェース = 02h	
07h		idVendor	2 バイト	046Bh	ベンダー ID (USB Org が割り当て) American Megatrends, Inc.	

テーブル 2: SMBIOS タイプ 42 構造

## 2.3 サポートした IPMI OEM コマンド

バイト	名前		長さ	値	説明	iRMC からの値の派生方法
09h	インターフェース固有のデータ	idProduct	2 バイト	FFB0h	プロダクト ID (メーカーが割り当て)	
0Bh		iSerialnumber	バイト	0Ch	記述子のサイズ (バイト単位)	
0Ch		bDescriptor Type	バイト	03h	文字列記述子 (0x03)	
0Dh	bString	n バイト	1234567890	Unicode でエンコードされた文字列		
0Dh + n	プロトコル数		バイト	01h		
0Dh + n + 1	プロトコルレコード	プロトコル ID	バイト			

テーブル 2: SMBIOS タイプ 42 構造

## 2.3 サポートした IPMI OEM コマンド

バイト	名前	長さ	長さ	値	説明	iRMC からの値の派生方法
00h + n + 2	プロトコルレコード	長さ	バイト			
0	プロトコルレコード	プロトコル固有のレコードデータ	サービス UUID	16 バイト	Redfish サービス ルートリソースの Redfish サービス UUID と同じ	configSpace 変数 0x2032 Con.fBMCRedfishUUID に格納
X+16	プロトコルレコード	プロトコル固有のレコードデータ	ホスト IP 割り当てタイプ	バイト	不明 = 00h、Static = 01h、DHCP = 02h、AutoConfigure = 03h、HostSelected = 04h、その他の値は予約済み	

テーブル 2: SMBIOS タイプ 42 構造

## 2.3 サポートした IPMI OEM コマンド

バイト	名前	プロトコル固有のレコードデータ	長さ	値	説明	iRMC からの値の派生方法
X+17	プロトコルレコード	プロトコル固有のレコードデータ	バイト	01h	不明 = 00h、Ipv4 = 01h、Ipv6 = 02h、その他の値は予約済み	
X+18	プロトコルレコード	ホスト IP アドレス	16 バイト		Static および AutoConfigure に使用。IPv4 では、最初の 4 バイトを使用し、残りのバイトは 0 で埋めます。	configSpace 変数 0x1823 ConfHostUsbLanIPv4AddrHost に格納
X+34	プロトコルレコード	ホスト IP マスク	16 バイト		Static および AutoConfigure に使用。IPv4 では、最初の 4 バイトを使用し、残りのバイトは 0 で埋めます。	configSpace 変数 0x1821 ConfBmcUsbLanIPv4NetMask を使用

テーブル 2: SMBIOS タイプ 42 構造

バイト	名前	プロトコル固有のレコードデータ	長さ	値	説明	iRMC からの値の派生方法
X+50	プロトコルレコード	プロトコル固有のレコードデータ	バイト	01h	Redfish サービス、IP、検索タイプ	不明 = 00h、Static = 01h、DHCP = 02h、AutoConfigure = 03h、HostSelected = 04h、その他の値は予約済み
X+51	プロトコルレコード	プロトコル固有のレコードデータ	バイト	01h	Redfish サービス、IP アドレス形式	不明 = 00h、Ipv4 = 01h、Ipv6 = 02h、その他の値は予約済み

テーブル 2: SMBIOS タイプ 42 構造

## 2.3 サポートした IPMI OEM コマンド

バイト	名前	プロトコル固有のレコードデータ	Redfish サービス IP アドレス	長さ	値	説明	iRMC からの値の派生方法
X+52	プロトコルレコード	プロトコル固有のレコードデータ	Redfish サービス IP アドレス	16 バイト		Static および AutoConfigure に使用。IPv4 では、最初の 4 バイトを使用し、残りのバイトは 0 で埋めます。	configSpace 変数 0x1822 ConfBmcUsbLanIPv4AddrBmc に格納
X+68	プロトコルレコード	プロトコル固有のレコードデータ	Redfish サービス IP マスク	16 バイト		Static および AutoConfigure に使用。IPv4 では、最初の 4 バイトを使用し、残りのバイトは 0 で埋めます。	configSpace 変数 0x1821 ConfBmcUsbLanIPv4NetMask に格納
X+84	プロトコルレコード	プロトコル固有のレコードデータ	Redfish サービス IP ポート	ワード	443 (01BBh)	Static および AutoConfigure に使用。	configSpace 変数 0x1421 ConfBMCHttpsPort に格納

テーブル 2: SMBIOS タイプ 42 構造

## 2.3 サポートした IPMI OEM コマンド

バイト	名前		長さ	値	説明	iRMC からの値の派生方法
X+86	プロトコルレコード	プロトコル固有のレコードデータ	Dword	0000h	Static および AutoConfigure に使用。	configSpace 変数 0x1961 ConfBMCVLANId に格納
X+90	プロトコルレコード	プロトコル固有のレコードデータ	バイト		以下のホスト名文字列の長さ	
X+91	プロトコルレコード	プロトコル固有のレコードデータ	m バイト		Redfish サービスのホスト名	iRMC: /bin/hostname

テーブル 2: SMBIOS タイプ 42 構造



## 2.3.5 iRMC 特有のコマンド

## F5 10 - Get System Status

本コマンドは、電源状態、エラー状態等のシステムの各種内部情報を返します。

要求データ	-	B8 NetFnILUN: OEM/Group
	-	F5 Cmd: コマンドグループメモリ
	1:3	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	4	10 コマンド指定子
	5:8	タイムスタンプ
応答データ	-	BC
	-	F5
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5	状態 LED
	6	シグナリング
	7	通知
	8	POST コード



「タイムスタンプ」は、通知バイトの評価のみに適用されます。

	状態 LED	シグナリング	通知
Bit 7 -	System ON	Localize LED	SEL modified (new SEL entry)
Bit 6 -			SEL modified (SEL Cleared)
Bit 5 -			SDR modified

	状態 LED	シグナリング	通知
Bit 4 -	SEL entries available		Nonvolatile IPMI variable modified
Bit 3 -		CSS ランプ	ConfigSpace modified
Bit 2 -	Watchdog active	CSS ランプ	
Bit 1 -	Agentless Service が接続されている	状態表示ランプ	
Bit 0 -	Post State	状態表示ランプ	New output on LocalView display

### F5 12 - Get EEPROM Version Info

本コマンドは、EEPROM に保存されている現在のバージョン (bootloader、ファームウェアおよび ADR) に関する情報を返します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F5</b> Cmd: コマンドグループメモリ
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>12</b> コマンド指定子
	5	EEPROM# 00=EEPROM 1、01=EEPROM 2

応答データ	-	BC
	-	F5
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5	状態 00=チェックサムエラーランタイム FW、01=OK
	6	メジャー FW リビジョン バイナリコード
	7	マイナー FW リビジョン BCD コード
	8:10	Aux.FW Revision バイナリコード (メジャー/マイナー/Aux)
	11	メジャー FW リビジョン ASCII コード
	12	メジャー SDRR リビジョン BCD コード
	13	マイナー SDRR リビジョン BCD コード
	14	SDRR リビジョン文字 ASCII コード
	15	SDRR-IDLSB バイナリコード
	16	SDRR-IDMSB バイナリコード
	17	メジャー Booter リビジョン バイナリコード
	18	メジャー Booter リビジョン BCD コード
19:20	Aux.Booter Revision バイナリコード (メジャー/マイナー)	

#### F5 42 - Get HDD lightpath status (コンポーネント状態信号の読み取り)

Light Path 診断は、コントロールパネルおよびシステムボード上の LED のシステムです。エラーが発生すると、LED が点灯します。コントロールパネルでエラーが示されると、LED の説明を使用して、問題を診断し、対応策を実施します。

このコマンドは、ハードディスクドライブ (HDD) スロットの状態に関する情報を返します。

要求データ	-	<b>B8</b> NetFn;LUN: OEM/グループ
	-	<b>F5</b> Cmd : コマンドグループ iRMC
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>42</b> コマンド指定子
	5	状態信号が読み取られるコンポーネントの <b>エンティティ ID</b> (IPMI 1.5 仕様の表 37-12)。
	6	状態信号が読み取られるコンポーネントの <b>エン트리インスタンス</b> (0 ベース)。
	7	状態信号が関連付けられているコンポーネントの状態を報告するセンサの <b>センサタイプ</b> (IPMI 仕様の表 36-3)。
[8]	オプション (オプション) Bit 7:2 - 予約 Bit 1 : 完了コード 0x02 が削除される Bit 0 - 1 : コンポーネント状態センサのリターン ID 文字列	

応答データ	-	BC
	-	F5
	1	完了コード: 01 = 状態信号を取得できません 02 = コンポーネントがありません
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5	信号状態: 00 = OK 01 = 確認 02 = 故障前警告 03 = 故障
	6	CSS と 物理 LED を使用可能: Bit 6:0 - 0 = 物理 LED を使用不可 Bit 6:0 > 00 = 物理 LED を使用可能、単一または複数の色、コード Bit 7 = 0: CSS コンポーネントなし Bit 7 = 1: CSS コンポーネント
	[7]	コンポーネント状態センサの ID 文字列の長さ (リクエストバイト 8 の Bit 0 が設定されている場合のみ存在)
	(8:m)	コンポーネント状態センサの ID 文字列 (ASCII 文字) の長さ (リクエストバイト 8 の Bit 0 が設定されている場合のみ存在)

## F5 43 - Get SEL entry long text

本コマンドは任意の SEL エントリをロングテキストに変換します。

要求データ	-	<b>B8</b> NetFn;LUN: OEM/グループ
	-	<b>F5</b> Cmd : コマンドグループ iRMC
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>43</b> コマンド指定子
	5:6	<b>レコード ID</b> SEL レコード、LSB ファースト 0x0000 : 最初のレコードを取得します。0xFFFF : 最後のレコードを取得します。
	7	応答 SEL テキストの <b>オフセット</b>
	8	<b>MaxResponseDataSize</b> 応答の変換済み SEL データサイズ(16:n) サイズ (16:n) (パイロット 1 設計で、最大データサイズは 56 バイト)

応答データ	-	BC
	-	F5
	1	完了コード:
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5:6	次のレコード ID
	7:8	現在のレコード ID
	9	レコードタイプ
	10:13	タイムスタンプ
	14	<b>重大度</b> : Bit 7: 0 = CSS コンポーネントなし 1 = CSS コンポーネントあり Bit 6-4 : 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown Bit 3-0: 予約済み、0000 として読み取り
	15	テキスト全体のデータ長
	16:n	変換済み SEL データ 要求された部分 (n = 16 + MaxResponseDataSize - 1)
n + 1	文字列終了「¥0」という文字をつける	

## F5 45 - Get SEL Entry Short Text

本コマンドは任意のシステムイベントログ (SEL) エントリを ASCII テキストに変換します。

要求データ	-	B8 NetFnILUN: OEM/Group
	-	F5 Cmd : コマンドグループ iRMC
	1:3	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	4	45 コマンド指定子
	5:6	SDR のレコード ID、LSB ファースト
応答データ	-	BC
	-	F5
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5:6	次のレコード ID
	7:8	実際の ID
	9	レコードタイプ
	10:13	タイムスタンプ
	14	<b>重大度</b> : Bit 7:0 = CSS コンポーネントなし 1 = CSS コンポーネントあり Bit 6-4 : 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = 'Unknown' Bit 3-0: 予約済み、0000 として読み取り
	15	ヌル終端文字を含まないデータ長
	16:35	ASCII に変換された SEL データ、最大 20 バイト
n+1	終端ヌル文字	



## F5 8D - Get VNMe Information

このコマンドは、RAID キャッシュの関連する AIC PCIe デバイスの状態情報と指定された温度を取得します。

要求データ	-	<b>B8</b> NetFn/LUN: OEM/グループ
	-	<b>F5</b> Cmd : コマンドグループ iRMC
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>42</b> コマンド指定子
	5	<b>バージョン</b> 00h 初版 02h:FFh 予約済み
	6	<b>コマンド</b> 00h 有効期間の値と資産情報の取得 01h 位置情報の取得 02h:FFh 予約済み
	7	<b>ターゲット指定子</b> 00h 00h でなければならない 01h:FFh 予約済み
	8	<b>センサー番号</b> ターゲット NVMe デバイスのセンサー番号 (Lightpath センサー番号)
	9	<b>センサー LUN</b> ターゲット NVMe デバイスのセンサー LUN (Lightpath センサーの LUN)

応答データ	-	BC
	-	F5
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5:49	<b>コマンド応答データ。デバイス運用固有</b> <b>コマンド 00h</b> 5:8 経過した有効期間の割合 (0% ~ 100%) 9:10 PCI SIG で定義されたターゲット NVMe デバイスのベンダー ID 11:30 ターゲット NVMe デバイスのシリアル番号 (20 文字) 31:46 位置情報文字列 - 16 文字 (例: PCIe SLOT#) 47: 状態 48: Smart 49: 複合温度
	5	<b>コマンド 01h</b> PCIeSSD のタイプ 00h PCIeSSD SFF - シャーシディスクスロットに挿入 01h PCIeSSD AIC - PCI AddInCard
	6	シャーシのロット番号/PCI スロット番号 (バイト 7 による)
7	<b>場所</b> 00h シャーシ前面 01h シャーシ背面 02h PCI スロット	

### F5 B0 - Set Identify LED

本コマンドにより、SB オン/オフの ID ランプ（青色）を切り替えることが可能です。また、ID ランプに直接接続された GPIO の設定および読み込みが可能です。



SB 上の識別切り替えを使用して ID ランプを切り替えることも可能です。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F5</b> Cmd : コマンドグループ BMC
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>B0</b> コマンド指定子
	5	<b>ID LED :</b> 0=ID LEDオフ 1=ID LEDオン 2=ID LED点滅
応答データ	-	<b>BC</b>
	-	<b>F5</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト

### F5 B1 - Get Identify LED

本コマンドは、SB の ID ランプ（青色）の状態に関する情報を返します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F5</b> Cmd : コマンドグループ BMC
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>B1</b> コマンド指定子

応答データ	-	<b>BC</b>
	-	F5
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	5	<b>ID LEDの状態：</b> 0=ID LEDオフ 1=ID LEDオン 2=ID LED点滅

### F5 B3 - Get Error LED

本コマンドは、SB の状態表示ランプ（赤色）および CSSランプ（黄色）の状態に関する情報を返します。状態表示ランプはコンポーネントの最も重大なエラー状態を示します。CSS ランプは、ユーザ自身が障害を修復できるかどうかを示します。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F5</b> Cmd : コマンドグループ BMC
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>B3</b> コマンド指定子

応答データ	-	BC
	-	F5
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	5	<b>エラー LED の状態：</b> 0=CSS off/GEL off 1=CSS off/GEL on 2: CSS off / GEL flashing 3=CSS on/GEL off 4=CSS on/GEL on 5: CSS on / GEL flashing 6: CSS flashing/ GEL off 7: CSS flashing/ GEL on 8: CSS flashing/ GEL flashing

## F5 E0 - Reset ConfigSpace variables to default

本コマンドは、すべての設定スペース変数をデフォルトに強制的に設定します。

要求データ	-	B8 NetFnILUN: OEM/Group
	-	F5 Cmd : コマンドグループ BMC
	1:3	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	4	E0 コマンド指定子
	5:7	43 4C 52=' CLR' セキュリティコード
	8	OxAA: Config Space 変数のデフォルトへの設定を開始 OxBB: ネットワークパラメータがノート 1 で指定されている場合を除き、Config Space 変数のデフォルトへの設定を開始 Ox00: デフォルトの状態にリセット
応答データ	-	BC
	-	F5
	1	完了コード
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト
	5	Ox00: デフォルトへの設定が完了 Ox01: デフォルトへの設定を実行中

## F5 F8 - Delete User ID

システムでは最大 16 人のユーザがサポートされます。本コマンドは、iRMC S6 ユーザを個別に削除することができます。



すべての iRMC ユーザを削除するとシステムを管理することができなくなります。

要求データ	-	<b>B8</b> NetFnILUN: OEM/Group
	-	<b>F5</b> Cmd : コマンドグループ BMC
	1:3	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト
	4	<b>F8</b> コマンド指定子
	5:8	ユーザ ID (1~16)
応答データ	-	<b>BC</b>
	-	<b>F5</b>
	1	完了コード
	2:4	<b>80 28 00</b> IANA-Enterprise-Number FTS、LSB ファースト

## 2.4 データセンター管理インターフェース

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

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

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

DCMI の詳細情報は、DCMI の Web サイトに掲載されています。

<https://www.intel.com/content/www/us/en/homepage.html>

## 2.5 Serial Over LAN (SOL)

「Serial over LAN」は、IPMI V2.0 規格に準拠しているインターフェースであり、LAN 接続上でのシリアルデータ転送を制御します。特に、SOL は、管理対象コンピュータとリモートワークステーションのシリアルコントローラの間でシリアルデータストリームを転送するためのパケットフォーマットおよびプロトコルを指定します。SOL は IPMI-over-LAN 仕様に基づいています。

SOL 接続を確立するためにリモート管理アプリケーションはまず、BMC との IPMI-over-LAN セッションを開始します。これが完了したら、リモートワークステーションから SOL サービスを有効にすることができます。シリアルコントローラとリモートワークステーションの間のデータトラフィックは、IPMI のコマンドと同じ IPMI セッション上で処理されます。

SOL 接続が確立されるとすぐに、シリアルコントローラとリモートワークステーションの間のデータ転送が以下のように実行されます。

- シリアルコントローラからリモートワークステーションへの転送:

シリアルコントローラによって発行されるデータストリームが BMC によってパーティション化され、パッケージ化されて、LAN 上でリモートワークステーションに送信されます。





---

## 3 iRMC 設定

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 (58 ページの [iRMC Web インターフェースを使用した設定](#))
- Remote Manager (59 ページの [Remote Manager 経由の設定](#))
- テキストコンソールリダイレクション (59 ページの [テキストコンソールリダイレクション経由の設定](#))
- スクリプト (60 ページの [スクリプト経由の設定](#))
- UEFI セットアップユーティリティ (61 ページの [UEFI セットアップユーティリティを使用した設定](#))

### 3.1 iRMC Web インターフェースを使用した設定

iRMC Web インターフェースを使用して、iRMC を設定できます。Web インターフェースは、『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。

#### LAN パラメータ

LAN パラメータは、「**管理**」メニューの「**詳細設定**」ページおよび、「**設定**」メニューの「**ネットワーク制御**」ページで設定します。以下のグループを使用して構成できます。

- 「**詳細設定**」ページ：LAN 設定の **管理ネットワーク** グループ
- **管理ネットワーク** ページ：DHCP と DNS 設定を指定する、「**DNS**」および「**DNS 名の登録**」グループ

「**サービス**」ページの「**Web アクセス**」グループで、ポートとネットワークサービスを設定します。

#### 通知情報設定

通知情報のパラメータは、「**設定**」メニューの「**サービス**」ページで設定します。以下のグループを使用して構成できます。

- 「**SNMP**」グループ: SNMP トラップ転送の設定
- 「**E メール警告**」グループ: E メール警告の設定

### テキストコンソールリダイレクション

テキストコンソールリダイレクションは、「サービス」ページの「BIOS コンソールリダイレクション」グループで設定します。

## 3.2 Remote Manager 経由の設定

Remote Manager は、iRMC の Telnet ベースのインターフェースです。リモートマネージャは、Telnet/SSH クライアント経由で呼び出すことができます。

iRMC は、SSH を介した安全な接続をサポートします。リモートマネージャインターフェースはTelnet およびSSH接続と同じものです。

原則として、VT100 シーケンスを解釈する Telnet/SSH クライアントであれば、iRMC へのアクセスに使用できます。ただし、iRMC Web インターフェースまたは ServerView Remote Management フロントエンドの使用を推奨します。

詳細は、[67 ページの Telnet/SSH 経由を使用した設定 \(Remote Manager\)](#) を参照してください。

## 3.3 テキストコンソールリダイレクション経由の設定

テキストコンソールリダイレクションの設定方法および SB の OS に応じて、テキストコンソールリダイレクションは以下の使用方法があります。

- BIOS POST フェーズの間のみ使用できる。
- BIOS POST フェーズ終了後も、OS が稼働している間は使用できる。

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

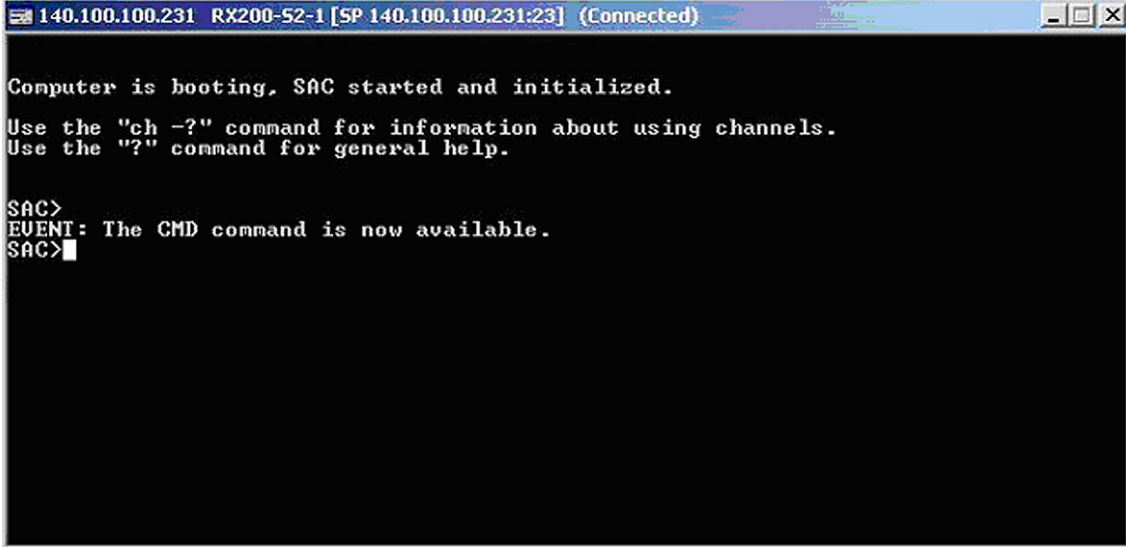
### Windows Server 2019 以降



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

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

Windows Server 2019 以降では、POST フェーズ後、自動的にコンソールリダイレクションを使用できます。さらに設定を行う必要はありません。OS の起動中に、Windows Server SAC コンソールに切り替わります。



```
140.100.100.231 RX200-S2-1 [SP 140.100.100.231:23] (Connected)
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.

SAC>
EVENT: The CMD command is now available.
SAC>
```

図 6: Windows Server SAC コンソール

## Linux

設定は、使用される Linux OS によって異なります。OS のマニュアルを参照してください。

## 3.4 スクリプト経由の設定

iRMC は、iRMC S6 での `/config URL` を使用したリモート設定と制限付きスクリプティングをサポートしています。

iRMC Web インターフェースの「ツール」メニューの「バックアップリストア」ページで、現在の iRMC の設定データを設定ファイル（.pre）に保存（エクスポート）できます。

また、既存の設定ファイル（.pre）の iRMC 設定データをインポート（復元）できます。つまり、iRMC に設定データをロードできます。

あるいは、iRMC 設定をインポートするために、HTTP POST オペレーションを使用して、該当する SCCI コマンドファイルを iRMC の `/config URI` に送信することもできます。

設定ファイルは、以下の言語のコマンドを使用して、SCCI API 経由でインポートできます。

- cURL
- VB スクリプト
- Python
- Redfish
- iRMC プロファイリング

詳細については、[83 ページの スクリプト経由の設定](#)を参照してください。

## 3.5 UEFI セットアップユーティリティを使用した設定

UEFI (Unified Extensible Firmware Interface) とは、Windows 8 以降の PC にプリインストールされた標準ファームウェアインターフェースで、BIOS を置き換えるものです。

### UEFI セットアップユーティリティの開始

1. PC を起動します。
2. ファームウェアの起動が開始されたら、キーを押してブートデバイスメニューを表示します。たとえば、[Esc]、[F2]、[F9]、[F12]、またはその他のキーを押すと、ファームウェアまたはブートメニューが表示されます。
3. ブートデバイスメニューで、ファームウェアモードとデバイスの両方を指定するコマンドを選択します。たとえば、「**UEFI USB Drive**」を選択します。



同じデバイスに別のコマンドがあることがあります。たとえば、「**UEFI USB Drive**」と「**BIOS USB Drive**」が表示されることがあります。各コマンドでは同じデバイスとメディアが使用されますが、PC は別のファームウェアモードで起動します。

---

### 3.5.1 LAN インターフェースのテスト

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

1. SB の UEFI セットアップユーティリティを呼び出します。
2. 「iRMC LAN parameter configuration」メニューを呼び出します。  
「Server Mgmt」 - 「iRMC LAN Parameters Configuration」



図 7: 「Server Mgmt」メニュー

3. 「Management LAN」フィールドで、「Enabled」を指定します。
4. 「Management LAN Port」フィールドで、「Management」を指定します。



詳細は、『iRMC S6 - Web インターフェース』取扱説明書を参照するか、またはお使いの SB の『BIOS (Aptio) Setup Utility』マニュアルを参照してください。

5. 設定を保存します。

6. iRMC コンソールリダイレクションを使用する場合は、テキストコンソールリダイレクションの設定に進みます。詳細は、「59 ページの [テキストコンソールリダイレクション経由の設定](#)」取扱説明書を参照してください
7. iRMC でテキストコンソールリダイレクションを使用しない場合は、UEFI セットアップを終了して、LAN インターフェースのテストを続行します。詳細については、『iRMC S6 - コンフィグレーションとメンテナンス』取扱説明書を参照してください。

## 3.5.2 テキストコンソールリダイレクションの構成

1. SB の UEFI セットアップユーティリティを呼び出します。
2. 「Server Mgmt」メニューを呼び出します。

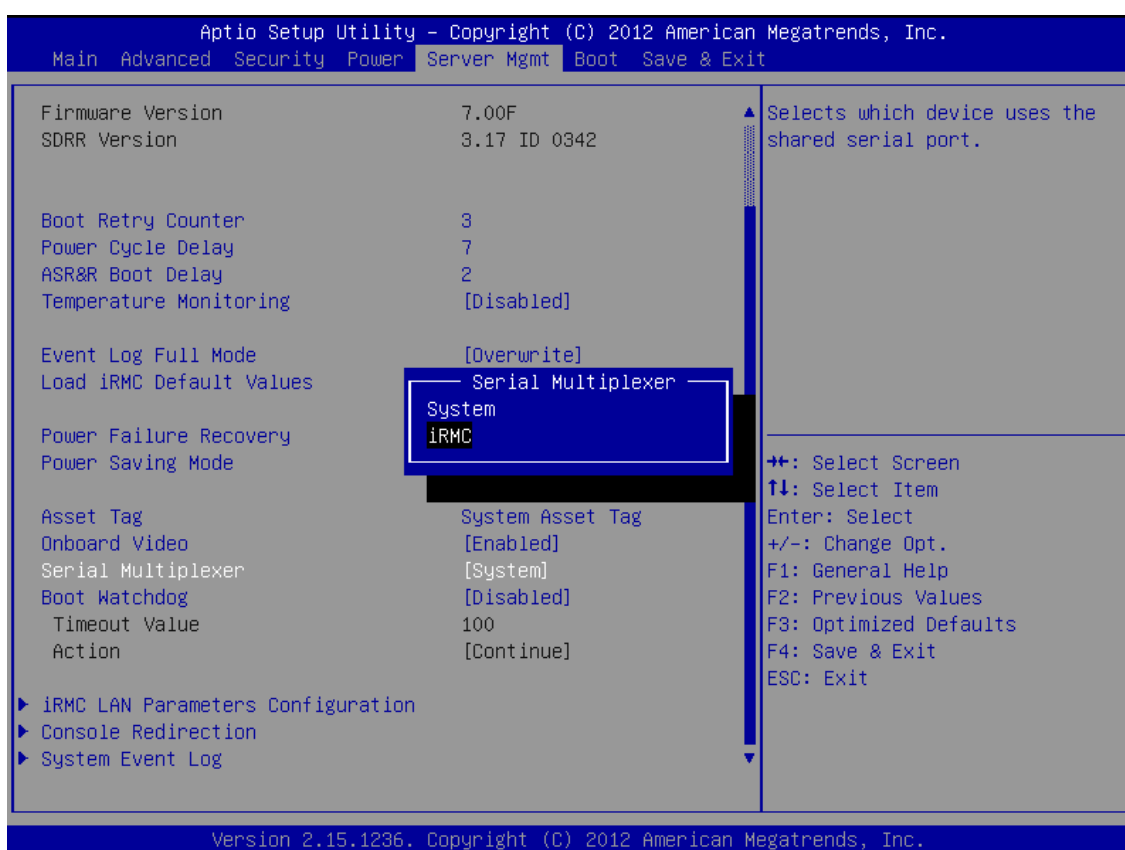


図 8: 「Server Mgmt」メニュー

3. 「Serial Multiplexer」フィールドで、「iRMC」と入力します。

4. 「Console Redirection」メニューを呼び出します。

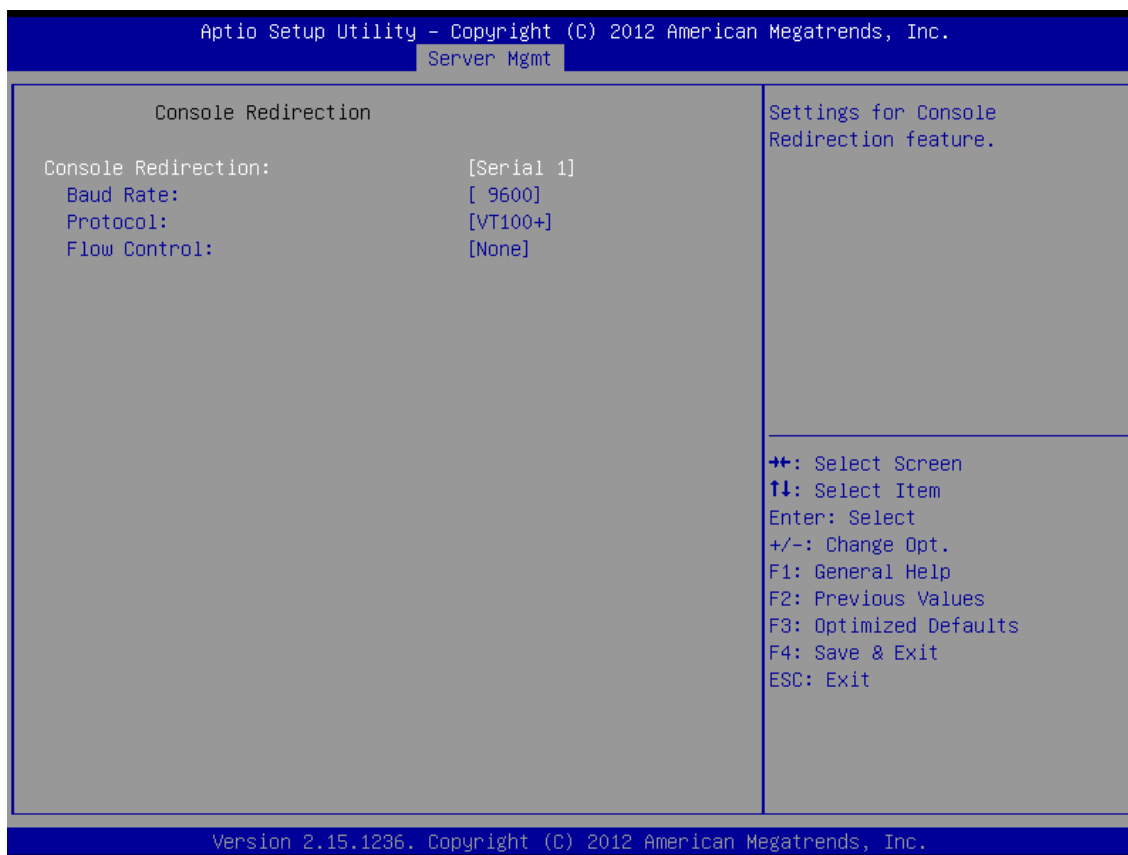


図 9: 「Console Redirection」メニュー

5. 「Console Redirection」フィールドで、「Serial 1」と入力します。この場合、ターミナルは最初のシリアルインターフェースを使用します。
6. 「Baud Rate」フィールドで、ボーレートを指定します。
7. 「Protocol」フィールドの設定は変更しないでください（設定は使用するターミナルのタイプに依存します）。
8. 「Flow Control」フィールドの設定は、使用するターミナルのタイプにも依存します。設定は、ターミナルとSBで同一にする必要があります。
9. 設定を保存して、UEFI セットアップユーティリティを終了します。
10. LAN インターフェースのテストを続行します。詳細については、『iRMC S6 - コンフィグレーションとメンテナンス』取扱説明書を参照してください。



### 3.5.3 シリアルインターフェースの設定

1. SB の UEFI セットアップユーティリティを呼び出します。
2. 「Server Mgmt」メニューを呼び出します。

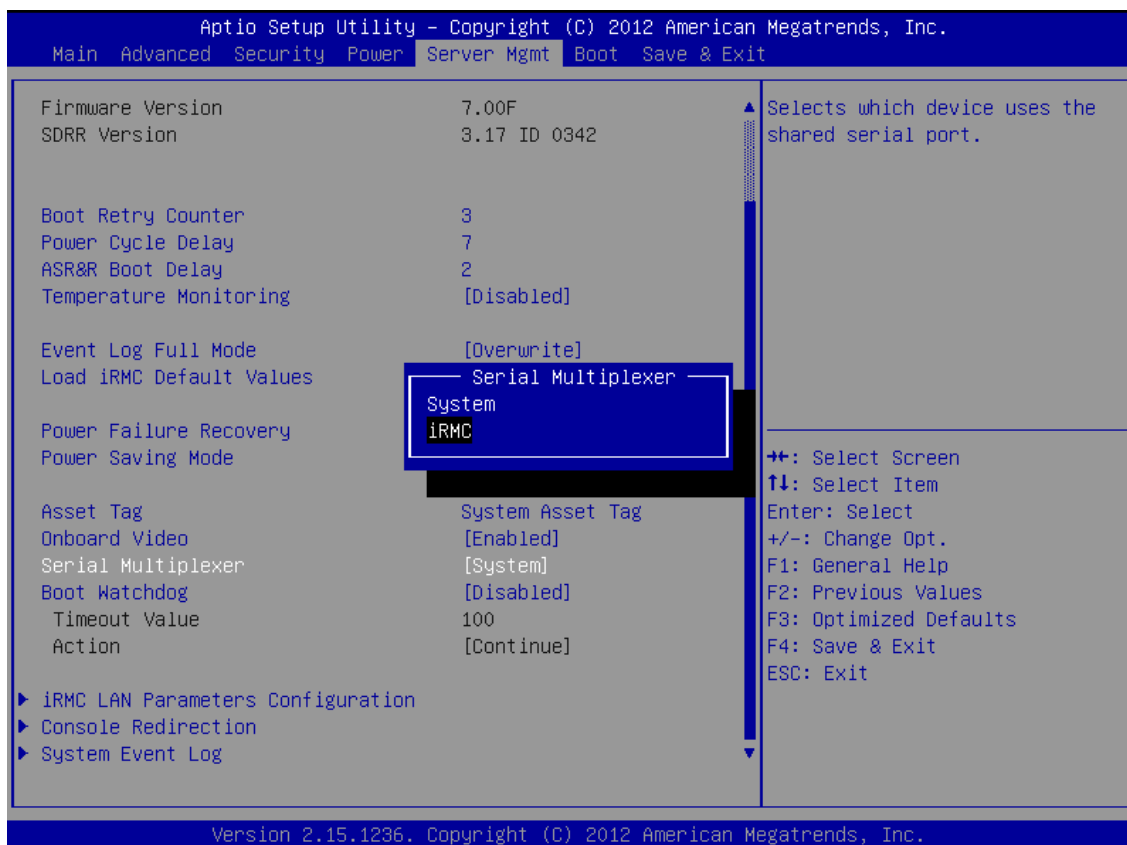


図 10: 「Server Mgmt」メニュー

3. 「Serial Multiplexer」フィールドで、「iRMC」と入力します。
4. 「Advanced」 - 「Super IO Configuration」 - 「Serial Port 1 Configuration」の順に選択して「Serial Port 1 Configuration」タブを開き、シリアルポートを設定します。

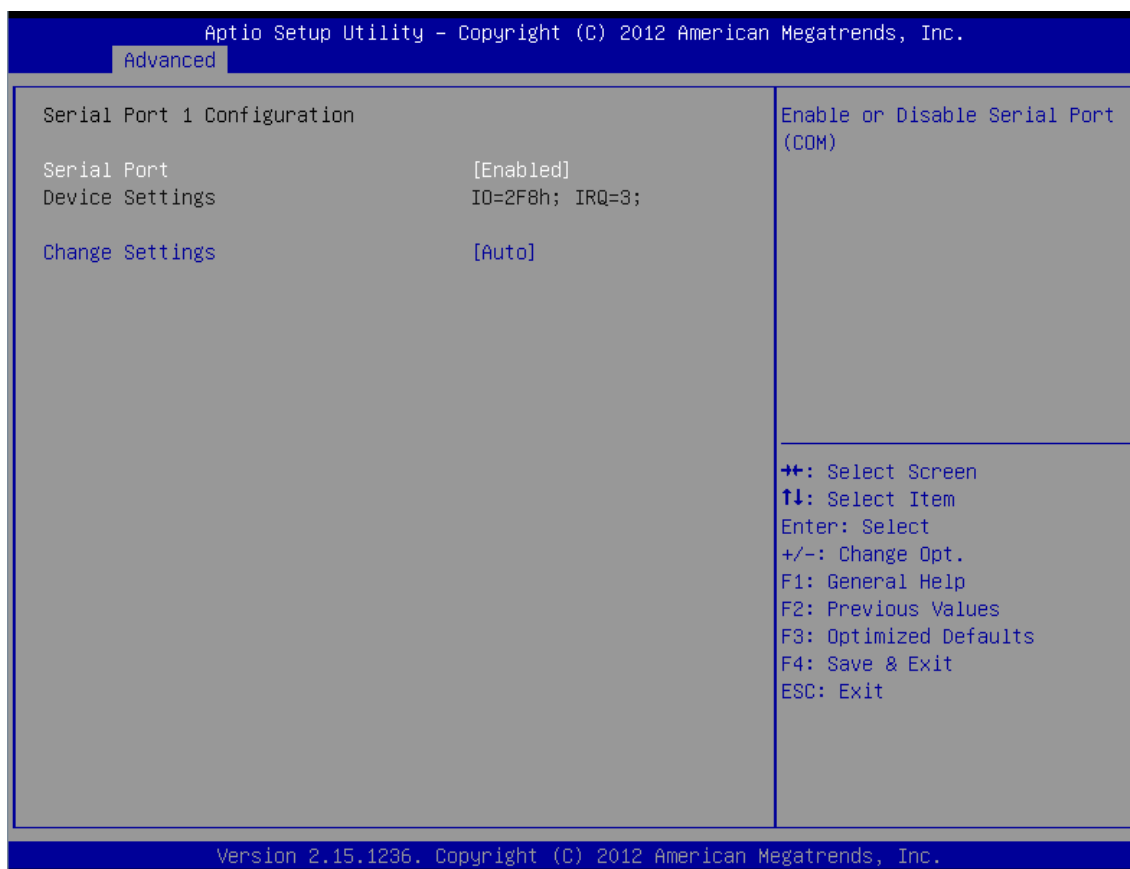


図 11: 「Serial Port 1 Configuration」 タブ

5. 「Serial Port」 フィールドに「Enabled」と入力します。
6. 設定を保存して、UEFI セットアップユーティリティを終了します。
7. LAN インターフェースのテストを続行します。詳細については、『iRMC S6 - コンフィグレーションとメンテナンス』取扱説明書を参照してください。

---

## 4 Telnet/SSH 経由を使用した設定 (Remote Manager)

iRMC では Telnet ベースのインターフェースを使用できます。このインターフェースは Remote Manager と呼ばれています。リモートマネージャは、Telnet/SSH クライアント経由で呼び出すことができます。

iRMC は、SSH (Secure Schell) を介した安全な接続をサポートします。リモートマネージャインターフェースは Telnet および SSH 接続と同じものです。原則として、VT100 シーケンスを解釈する Telnet/SSH クライアントであれば、iRMC へのアクセスに使用できますが、iRMC Web インターフェースを推奨します。

この章では、Remote Manager からの iRMC の操作および各種機能の詳細を説明します。

### 4.1 SB の要件

iRMC への Telnet 経由のアクセスを有効にしておくこと (詳細は、『iRMC S6 - Web インターフェース』取扱説明書の「ポート番号とネットワークサービス - ポート番号とネットワークサービスの設定」の項を参照)。



パスワードはプレーンテキストで送信されるので、Telnet プロトコルを使用したアクセスはデフォルトでは無効です。

ServerView Operations Manager にはマネジメントポートの値が認識されないため、Remote Management フロントエンドはデフォルト値で動作します。Remote Management Front-end が起動したときに自動的に接続は確立されないため、Remote Management Front-end が起動した後にマネジメントポートの標準以外の値を変更できます。

## 4.2 必要なユーザ権限

以下の表に、リモートマネージャの各機能を使用するために必要な権限の概要を示します。

メニューとコマンド	必要な IPMI 権限レベル				必要な許可			
	OEM	管理者	オペレーター	ユーザ	ユーザアカウント変更	iRMC 設定変更	AVR使用権限	リモートストレージ有効
システム情報	0	0	0	0				
View Chassis / Mainboard / OS Information						0		
Set Asset Tag						0		
Set System Name.1)						0		
Set System Operating System Information.1)						0		
Set System Description						0		
Set System Location Information (SNMP).1)						0		

テーブル 3: リモートマネージャに必要なユーザ権限

4.2 必要なユーザ権限

メニューとコマンド	必要な IPMI 権限レベル					必要な許可			
	OEM	管理者	オペレーター	ユーザ	ユーザアカウント変更	iRMC 設定変更	AVR使用権限	リモートストレージ有効	
Set System Contact Information (SNMP).1)						0			
<b>電源制御</b>	0	0	0						
<b>View Enclosure Information</b>	0	0	0	0					
System Eventlog - View/Dump System Eventlog	0	0	0	0					
System Eventlog - Clear System Eventlog	0	0	0						
Internal Eventlog - View/Dump Internal Eventlog	0	0	0	0		0			
Internal Eventlog - Clear Internal Eventlog	0	0	0	0		0			
Sensor overviews (温度, ファン ...)	0	0	0	0					
<b>View Service Processor...</b>	0	0	0	0					
Service Processor... - List IP Parameters						0			
Service Processor... - Configure IP Parameters						0			

テーブル 3: リモートマネージャの必要なユーザ権限

## 4.2 必要なユーザ権限

メニューとコマンド	必要な IPMI 権限レベル			必要な許可				
	OEM	管理者	オペレーター	ユーザ	ユーザアカウント変更	iRMC 設定変更	AVR使用権限	リモートストレージ有効
Service Processor... - Toggle Identify LED	0	0	0	0				
Service Processor: - Reset iRMC S6 (warm/cold reset)	0	0				0		
Change password <sup>2)</sup>					0			0
Console Redirection (EMS/SAC) <sup>2)</sup>	0	0						0
Console Logging <sup>2)</sup>	0	0						0

1) 実行中の ServerView Agentless Service がいない場合のみの動作可能

2) システムによっては使用できない機能

テーブル 3: リモートマネージャに必要なユーザ権限

## 4.3 ログイン

iRMC に接続する際、ログイン資格情報（ユーザ名とパスワード）の入力が必要です。iRMC S6 への接続が確立されるとすぐに、リモートマネージャのログインウィンドウ（Telnet/SSH ウィンドウ）がリモートワークステーションのターミナルクライアントに表示されます。

ServerView Agentless Service がある時点ですでにシステム上で起動しているかいないかで、ログインウィンドウの表示は、システム情報付きとシステム情報なしになります。



SSH 接続でログインした場合: SBのホストキーがリモートワークステーションにまだ登録されていない場合、SSH クライアントはセキュリティ警告を発行し、推奨する続行方法を示します。

```
iRMC S5 Remote Manager
login as: admin
admin@10.172.201.216's password:
*****
*   Welcome to PRIMERGY Remote Manager   *
*   Firmware Revision 1.07P (1.00)       *
*   SDR 3.18 ID 0516 RX2540M4           *
*   Firmware built Jul 6 2017 04:35:03 CEST *
*****

System Type   : PRIMERGY RX2540 M4
System ID    : YM6D000056
System Name   : localhost.localdomain
System OS    : Unknown
System Status: (Identify LED is OFF)
Power Status : Off
Asset Tag    : Unknown

Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...

(c) Change password
(*) Console Redirection (EMS/SAC)

(1) Console Logging

Enter selection or (0) to quit: █
```

図 12: リモートマネージャ: メインメニュー (システム情報なし)

リモートマネージャウィンドウには、影響を受けるシステムに関する情報が表示されます。その情報は SB を識別し、その稼動状態 (電源状態) を表示します。いくつかの詳細情報 (システム名など) だけが、その SB が適切に設定されている場合に限示されます。

リモートマネージャが使用できるためには、ユーザ名とパスワードでログインしなければなりません。

次に、該当するイベントがイベントログに書き込まれ、リモートマネージャの関連のあるメインメニューが表示されます (詳細は、72 ページの「Main」メニューを参照)。

ログインプロセスは、[Ctrl] + [D] を使用していつでも終了できます。

## 4.4 「Main」メニュー

Remote Manager のメインメニューには、次の機能があります。

```
Main Menu
(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...

(c) Change password
(*) Console Redirection (EMS/SAC)
(1) Console Logging

Enter selection or (0) to quit:
```

図 13: Remote Manager: Main Menu

### (1) System Information

SB の情報を表示し、資産タグを設定します詳細は、73 ページの「System Information」メニューを参照してください。

### (2) Power Management

SB の電源をオン/オフします詳細については、74 ページの「Power Management」メニューを参照してください。



**(3) Enclosure Information**

現在のシステム状態に関する情報を要求。たとえば、エラーログとイベントログからのエラーやイベントのメッセージ（温度、ファンなど）をチェックします。詳細については、76 ページの「Enclosure Information」メニューを参照してください。

**(4) Service Processor**

iRMC を設定します（ファームウェアの更新または IP アドレスの変更など）。詳細については、80 ページの「Service Processor」のメニューを参照してください。

**(c) Change password**

パスワードを変更します。

**(r) Console Redirection (EMS/SAC)**

テキストコンソールリダイレクション。詳細については、81 ページの Console Redirection (EMS/SAC) を参照してください。

**(l) Console Logging**

メッセージ出力をテキストコンソールにリダイレクトします。詳細は、81 ページの「Console Logging」メニューを参照してください。

## 4.4.1 「System Information」メニュー

メインメニューから「System Information」を選択すると、「(1) System Information」メニューが開きます。

```
System Information Menu
(1) View Chassis Information
(2) View Mainboard Information
(3) View OS and SNMP Information

(4) Set ASSET Tag
(5) Set System Name
(6) Set System Operating System Information
(7) Set System Description
(8) Set System Location Information (SNMP)
(9) Set System Contact Information (SNMP)
(i) Set System Primary IPv4 or IPv6 Address

Enter selection or (0) to quit:
```

図 14: Remote Manager: 「System Information」メニュー

**(1) View Chassis Information**

SB が搭載されているキャビネットの情報およびその製品データ。

- (2) **View Mainboard Information**  
Sb の情報およびその製品データ。
- (3) **View OS and SNMP Information**  
SBの OS と ServerView バージョンの情報と、SNMP 設定の情報。
- (4) **Set ASSET Tag**  
SBのユーザ固有の資産タグを設定します。
- (5) **Set System Name**  
SBの名前を設定します。
- (6) **Set System Operating System Information**  
OS の情報を設定します。
- (7) **Set System Description**  
SBの説明を設定します。
- (8) **Set System Location Information (SNMP)**  
ServerView Agentless Service では設定できない、SBの位置情報を設定します。
- (9) **Set System Contact Information (SNMP)**  
ServerView Agentless Service では設定できない、SBの連絡先情報を設定します。
- (i) **Set System Primary IPv4 or IPv6 Address**  
SBのプライマリ IP アドレス (IPv4 または IPv6) を設定します。

#### 4.4.2 「Power Management」メニュー

メインメニューから「Power Management」を選択すると、「(2) Power Management」メニューが開きます。

```
Power Management Menu

(*) Immediate Power Off
(*) Immediate Reset
(*) Power Cycle
(4) Power On

(*) Graceful Power Off (Shutdown)
(*) Graceful Reset (Reboot)
(*) Raise NMI (via iRMC S6)

Enter selection or (0) to quit:
```

図 15: Remote Manager: 「Power Management」メニュー

**(\*) Immediate Power Off**

OSの状態にかかわらず、SBの電源を切断します。

**(\*) Immediate Reset**

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）。

**(\*) Power Cycle**

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。

**(4) Power On**

SBの電源を投入します。

**(\*) Graceful Power Off (Shutdown)**

グレースフルシャットダウン後に電源を切断します。

このメニュー項目は、ServerView Agentless Service が iRMC S6 にインストールされ、「Connected」として署名されている場合にのみ使用できます。



このコマンドは、ESXi OS を実行する SB では実行できません。

**(\*) Graceful Reset (Reboot)**

グレースフルシャットダウン後にリセットします。

このメニュー項目は、ServerView Agentless Service が iRMC S6 にインストールされ、「Connected」として署名されている場合にのみ使用できます。



このコマンドは、ESXi OS を実行する SB では実行できません。

- (\*) Raise NMI (via iRMC S6)  
NMI パルス (マスク不可割り込み)

### 4.4.3 「Enclosure Information」メニュー

メインメニューから「Enclosure Information」を選択すると、「(3) Enclosure Information」メニューが開きます。

```
Enclosure Information Menu
(e) System Eventlog
(i) Internal Eventlog
(t) Temperature
(v) Voltages/Current
(f) Fans
(p) Power Supplies
(d) Door Lock
(m) Memory Sensors
(c) CPU Sensors
(s) Component Status
(l) List All Sensors
Enter selection or (0) to quit: █
```

図 16: Remote Manager: 「Enclosure Information」メニュー

- (e) System Eventlog  
「System Eventlog」メニューを呼び出します (詳細は、[78 ページの「System Eventlog」メニュー](#)の項を参照)。
- (i) Internal Eventlog  
「Internal Eventlog」メニューを呼び出します (詳細は、[78 ページの「Internal Eventlog」メニュー](#)の項を参照)。
- (t) Temperature  
温度センサとその状態に関する情報を表示します。
- (v) Voltages/Current  
電圧と電流、およびその状態の情報を表示します。
- (f) Fans  
ファンとセンサとその状態に関する情報を表示します。
- (p) Power Supplies  
電源と冗長の状態の情報を表示します。
- (d) Door Lock  
フロントパネルまたはハウジングが開いているかどうかを表示します。

**(m) Memory Sensors**

メモリの状態に関する情報を表示します。

**(c) CPU Sensors**

SB のプロセッサの位置を特定します。

**(s) Component Status**

PRIMEQUEST 診断ランプを備えたすべてのセンサに関する詳細な情報を表示します。

**(l) List All Sensors**

すべてのセンサの詳細な情報を表示します。

#### 4.4.3.1 「System Eventlog」メニュー

「Enclosure Information」サブメニューから「(e) System Eventlog」を選択すると、「System Eventlog」メニューが開きます。

```
System Eventlog Menu

(1) View System Eventlog (text, newest first)
(2) View System Eventlog (text, oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)

(5) View System Eventlog Information
(6) Clear System Eventlog

Enter selection or (0) to quit: █
```

図 17: Remote Manager: 「System Eventlog」メニュー

##### (1) View System Eventlog (text, newest first)

システムイベントログの内容が、可読形式で、入力時期の新しいものから順に画面に出力されます。

##### (2) View System Eventlog (text, oldest first)

イベントログの内容が、可読形式で、入力時期の古いものから順に画面に出力されます。

##### (3) Dump System Eventlog (raw, newest first)

イベントログの内容が入力時期の新しいものから順にダンプされます。

##### (4) Dump System Eventlog (raw, oldest first)

イベントログの内容が入力時期の古いものから順にダンプされます。

##### (5) View System Eventlog Information

システムイベントログの情報を表示します。

##### (6) Clear System Eventlog

システムイベントログの内容を消去します。

##### (7) Change System Eventlog mode

システムイベントログのバッファモードをリングバッファからリニアバッファに、またはこの逆に変更します。

#### 4.4.3.2 「Internal Eventlog」メニュー

「Enclosure Information」サブメニューから「(i) Internal Eventlog」を選択すると、「Internal Eventlog」メニューが開きます。

```
Internal Eventlog Menu
(1) View Internal Eventlog (text, newest last)
(2) Dump Internal Eventlog (raw, newest last)
(3) View Internal Eventlog Information
(4) Clear Internal Eventlog
(5) Change Internal Eventlog mode
Enter selection or (0) to quit: █
```

図 18: Remote Manager: 「Internal Eventlog」メニュー

**(1) View Internal Eventlog (text, newest last)**

内部イベントログの内容が、可読形式で、入力時期の古いものから順に画面に出力されます。

**(2) Dump Internal Eventlog (raw, newest last)**

内部イベントログの内容が入力時期の古いものから順にダンプされます。

**(3) View Internal Eventlog Information**

内部イベントログの情報を表示します。

**(4) Clear Internal Eventlog**

内部イベントログの内容を消去します。

**(5) Change Internal Eventlog mode**

内部イベントログのバッファモードをリングバッファからリニアバッファに、またはこの逆に変更します。

#### 4.4.4 「Service Processor」のメニュー

メインメニューから「Service Processor」を選択すると、「(4) Service Processor」メニューが開きます。

```
Service Processor Menu

(1) Configure IP Parameters
(2) List IP Parameters

(3) Toggle Identify LED

(4) Reset iRMC S6 (Warm reset)
(5) Reset iRMC S6 (Cold reset)

Enter selection or (0) to quit:
```

図 19: Remote Manager: 「Service Processor」メニュー

##### (1) Configure IP Parameters

iRMC の IPv4/IPv6 アドレス設定をガイド付きダイアログで設定します。個々の設定の詳細については、『iRMC S6 Web インターフェース』取扱説明書の「ネットワークインターフェース設定」の項を参照してください。

##### (2) List IP Parameters

IP パラメータを表示します。

##### (3) Toggle Identify LED

PRIMEQUEST の ID ランプのオン/オフを切り替えます。

##### (4) Reset iRMC S6 (Warm reset)

iRMC をリセットします。接続が閉じられます。  
インターフェースだけが再起動されます。

##### (5) Reset iRMC S6 (Cold reset)

iRMC をリセットします。接続が閉じられます。  
iRMC 全体が再起動されます。




「Reset iRMC S6 (Cold Reset)」または「Reset iRMC S6 (Warm Reset)」の後に SB を再起動することを推奨します。



## 4.4.5 Console Redirection (EMS/SAC)

メインメニューの「(r) Console Redirection (EMS/SAC)」コマンドからコンソールリダイレクションを開始できます。

 テキストベースのコンソールリダイレクションは、シリアル 1 の LAN 上でのみ動作します。

コンソールリダイレクションを OS の実行中にも使用する場合は、「Serial 1 Multiplexer」を「System」に設定する必要があります。

キーボードのショートカット「[ESC] + [I]」または「[~] + [.]」（チルダドット）を使用して、テキストコンソールを終了します。

使用する PRIMEQUEST サーバのタイプによっては、このオプションのうちの 1 つだけが機能します。

## 4.4.6 「Console Logging」メニュー

メインメニューの「(l) Console Logging」コマンドでは、メッセージ出力（ログ）をテキストコンソールにリダイレクトできます（シリアルインターフェース）。

メインメニューから「(1) Console Logging」を選択すると、「Console Logging」メニューが表示されます。

```
Console Logging Menu

(1) Change Logging Run state
(2) Clear Console Logging buffer
(3) Replay Console (Fast mode)
(4) Replay Console (Continuous mode)

Enter selection or (0) to quit: █
```

図 20: Remote Manager: 「Console Logging」メニュー

### (1) Change Logging Run state

ログ実行状態を表示し、変更します。詳細については、[82 ページの「Console Logging Run State」メニュー](#)を参照してください。

### (2) Clear Console Logging buffer

コンソールログバッファをクリアします。

- (3) **Replay Console (Fast mode)**  
コンソールログを表示します（高速モード）。
- (4) **Replay Console (Continuous mode)**  
コンソールログを表示します（連続モード）。

#### 4.4.7 「Console Logging Run State」メニュー

「Console Logging」メニューから「(1) Change Logging Run State」を選択すると、「Console Logging Run State」メニューが開きます。

```

Console Logging Run State Menu
State: STOPPED (Normal Mode)

(r) Start Console Logging
(*) Stop Console Logging

(t) Toggle to Text Mode
(*) Toggle to Normal Mode

Enter selection or (0) to quit: █

```

図 21: Remote Manager: 「Console Logging Run State」メニュー

- (r) **Start Console Logging**  
メッセージのテキストコンソールへの出力を開始します。
- (\*) **Stop Console Logging**  
メッセージのテキストコンソールへの出力を停止します。
- (t) **Toggle to Text Mode**  
テキストモードに切り替えます。  
メッセージがコンソールに出力される前に、すべてのエスケープシーケンスは除外されます。
- (\*) **Toggle to Normal Mode**  
ノーマルモードに切り替えます。  
ノーマルモードでは、メッセージがコンソールに出力される前に、次のエスケープシーケンスのみが除外されます。  
<ESC>(
<ESC>stop
<ESC>Q
<ESC>R<ESC>r<ESC>R
<ESC>^
これは、色、擬似グラフィックスなどを一定の限度まで表現できることを示します。

---

## 5 スクリプト経由の設定

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、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。

iRMC のシステムレポートには、現在の設定および取り付けられたハードウェアに関する情報が記載されます。

---

## 5.1 Redfish

Redfish は Out-Of-Band 管理の規格で、2015 年に初めて Distributed Management Task Force (DMTF) が発行しました。ハイパーメディア RESTful インターフェース内部のデータモデル表現を使用しています。データモデルは、標準のマシン読み取り可能なスキーマの観点で定義され、JSON で表現されたメッセージのペイロードと、オープンデータプロトコル (OData) バージョン 4 を使用するプロトコルが使用されます。ハイパーメディア API である Redfish は、一貫したインターフェースを使用して多様な実装を表現できます。データセンターリソースの検出と管理、イベントの処理、長期タスクの管理を実行するメカニズムが備わっています。

Redfish はモノリシックサーバからコンバインドインフラストラクチャおよびハイパースケールアーキテクチャまで、あらゆる範囲のサーバアーキテクチャをサポートします。Redfish は、コンバインドインフラストラクチャおよびラックレベル管理に対して特に有効で、そのモデリングは、複数のノード、ネストしたシャーシ、大型でアクティブに管理されているエンクロージャ内のサーバブレードの管理に対応して拡張できます。

Redfish データモデルは、サーバ状態、インベントリ、使用できる処理機能を表現するデータの構造とフォーマットを定義するもので、ベンダーに依存しません。そのため、管理者は自動管理スクリプトを作成して、任意の Redfish 準拠サーバを管理し、異種混在サーバファームの効率的な運用を強化できます。

### 主要な機能

Redfish アーキテクチャスタイルの主要機能は、以下のとおりです。

- シンプルさと使いやすさの向上
- 暗号化接続と全体的に強化されたセキュリティ
- スクリプトで簡単に制御できる、プログラムによるインターフェース
- Web API およびデータフォーマットに対する、一般的な規格に準拠

HTTPS は HTTP のセキュアバージョンで、HTTP を TLS または SSL で暗号化されたネットワーク接続内で動作させて、安全な通信を可能にします。Redfish では HTTPS 暗号化を利用して、安全で信頼できる通信を実現しています。すべての Redfish ネットワークトラフィックは、イベント通知を含め、ネットワーク上を暗号化して送信できます。

Redfish で採用されている Web インターフェースは多くのプログラミング言語でサポートされており、ツリー状の構造によって情報を見つけやすくしています。Redfish クエリから返されたデータを、キーと値のペアで構成される、検索可能な辞書に変換できます。辞書の値を検索することで、Redfish 管理ノードの設定と現在の

状態を簡単に見つけられます。これらの設定を更新し、1 つまたは複数のノードにアクションを発行できます。

## JSON データ

Redfish は JSON を使用してデータを表現しています。JSON は、人間が読み書きしやすく、マシンも解析しやすい、軽量のデータ相互交換フォーマットです。JSON は JavaScript プログラミング言語のサブセットに基づき、言語にまったく依存しないテキスト形式を使用しています。しかし JSON は、C、C++、C#、Java、JavaScript、Perl、Python など、C 言語ファミリのプログラマーにとって馴染みのある表記規則を使用しています。

## OData

OData は、RESTful API を使用する情報の定義と交換に対するオープンプロトコル規格です。OData は元々は 2007 年に Microsoft が作成し、その後 OASIS 規格団体によって標準化されました。OData は Redfish に必要なネットワークを提供し、データ構造がサーバベンダー間で相互交換可能な状態を維持します。

## Redfish アーキテクチャ

Redfish が採用している RESTful API は Web ベースで、URI を使用してアクセスできます。URI は Web ブラウザから入力できます。Redfish API はシンプルなフォルダ構造を使用し、Redfish ルート `/redfish/` から開始します。

トップレベルのルートから、Redfish インターフェースは分岐してさまざまな「コレクション」をカバーします。各コレクションには複数のサブ項目が含まれ、ツリー状の構造が作成されます。

URI は、リソースの主な一意の識別子です。Redfish URI は RFC3986 で規定されているように 3 つの部分で構成されています。パート 1 は URI のスキーマと権限を定義し、パート 2 はルートサービスとバージョンを指定し、パート 3 は一意のリソース識別子を定義します。

## Redfish の処理

Redfish では、HTTP メソッドで RESTful API の処理を実装します。これによって、ユーザは実行しているリクエストのタイプを指定できます。

Redfish の処理	HTTP メソッド	説明
Read	GET	指定されたリソースをサーバから要求します。GET には副作用はありません。サーバの状態は変更されません。このため、GET は安全とみなされています。
生成	POST	新しい (サブ) リソースを指定したリソースの下に挿入します。POST には副作用が伴います。たとえば、データベースフィールドが変更されたり、プロセスがサーバ上で開始されたりします。
アップデート	PATCH	指定されたリソースの一部が変更されます。ここでは副作用が許可されています。各 PATCH 要求には、以前の GET 要求の応答からの Etag が必要です。
削除	DELETE	指定されたリソースを削除します。

### 認証

所定のリソースの機密性に応じて、Redfish クライアントでアクセスを認証する必要があります。必要な認証情報とサポートされる認証形式は、管理対象のプラットフォームによって決定します。iRMC の場合、認証はローカル iRMC ユーザ認証情報またはその他のサポートされる認証情報 (LDAP や Active Directory など) を使用してサポートされます。

iRMC データは、以下に示す場合を除き、認証および承認されたユーザのみがアクセスできます。認証は、Redfish サービスによってサポートされる共通 HTTP ヘッダーのサブセットを使用して実現します。中でも特徴的なのが、X-Auth-Token ヘッダーです。認証の詳細は、Redfish 使用のセッション管理のセクションに記載されています。

Redfish API では、次の 2 つの方法を使用して Redfish URI にアクセスできます。

- 基本認証: この方法では、各 Redfish API リクエストに対してユーザ名とパスワードが指定されます。
- セッションベースの認証: この方法は、複数の Redfish 処理リクエストを発行するときに使用されます。

### 自動ノード検出

サービス自体はよく知られた URI ですが、サービスホストを検出する必要があります。Redfish は UPnP と同様に、SSDP を検出に使用します。SSDP は、プリンタなどのさまざまなデバイスでサポートされています。シンプルかつ軽量で、IPv6 に対応し、組み込み環境への実装に適しています。

ファームウェアバージョン 1.6 の iRMC では、最初の検出段階で SSDP プロトコルを提供します。Redfish 仕様では、Redfish サービスルートから転送される追加システム情報を提供する、UPnP 応答への SSDP 拡張を定義しています。iRMC 自動検出はこの Redfish ベースのアプローチに対応し、次の情報を提供します。

- マシンの詳細情報
- アライブ通知
- シャットダウン通知

サーバを SSDP で検出されたくない場合は、スクリプトまたは iRMC Web インターフェースの「**Services**」ページから、自動検出機能を常に無効にします。SSDP プロトコルが通信に使用するポート 50000 を閉じることでもあります。

iRMC に関する Redfish の詳細情報は、[Redfish のホワイトペーパー](#)および Fujitsu マニュアルサーバの『[Specification iRMC Redfish API](#)』を参照してください。

## 5.2 REST

REST (Representational State Transfer) は、リソース指向アーキテクチャ (ROA) スタイルで、Web 規格を Web 対応の方法で使用する方法を規定します。これにより、再利用性、拡張性、明確さ、および Web サービスの既存のネットワーク構造への外部システムのシンプルな統合が実現します。Web ブラウザを使用してリソース間を移動するため、REST ではシンプルで明確な、統一されたインターフェースを必要とします。そこで、特定の仕様に準拠し、特定のアクセスメソッド (HTTP メソッドなど) で制約される必要があります。

REST は、サービス指向アーキテクチャ (SOA) に基づく Web サービスの代替手法です。Web サービスは、REST アーキテクチャを使用すると RESTful API (Application Programming Interface) または REST API と呼ばれます。SOAP ベースの Web サービスとは異なり、RESTful API には「公式」な規格はありません。その理由は、REST はアーキテクチャスタイルで、SOAP はプロトコルだからです。REST 自体は規格ではありませんが、RESTful 実装には HTTP、URI、JSON、XML などの規格が使用されます。

各 REST リソースには、HTTP メソッドの GET、POST、PUT、DELETE を介した汎用インターフェースがあります。クライアントとサーバが相互に通信できるようにするためには、ログ規約は不要です。ほとんどのアプリケーションシナリオは、このアクセスメソッドで対応できます。

リソース指向の Web サービス (RESTful Web サービスも含む) の場合、メッセージは固定されたサービス エンドポイントには送信されません。その代り、推奨されるアクセスメソッド (GET、PUT、POST、DELETE) で、アドレス可能なリソースを直接処理します。

クライアントの状態は、情報またはリソースが要求されて変更されるたびに、変化します。**Representational State Transfer** (REST) は、アプリケーションの現在の状態から次の状態への遷移を視覚化します。状態の遷移は、アプリケーションの次の状態を表すデータを転送して実行されます。

リソースは RESTful API の基本コンポーネントです。リソースはアドレス可能で、少なくとも 1 つの表示形式（表現）を持っている必要があります。要求のヘッダーには、使用されるクライアントのタイプと、このクライアントに必要な表現に関する情報が含まれます。サーバに送信された各要求には、要求の解釈に必要なすべての情報が格納されている必要があります。URI (Uniform Resource Identifier: リソースの名前とアドレス) はリソースを識別しますが、HTTP ヘッダーにはアクセスタイプ (GET など)、戻り値の形式、認証などの情報が格納されています。REST では、URI がコンテンツの 1 ページのみを表現し、この同じ URI の複数の要求に応答する際に REST サーバが同じ Web ページのコンテンツを配信することが要求されます。

リンクまたは URI はクライアントに一連の状態遷移を提供します。これにより、クライアントはアプリケーションによって直感的に管理されます。このコンテキストでは、各処理が状態コードと追加のリンクを提供することが重要です。追加のリンクをそれぞれの表現で提供することで、その他のサービスを統合できます。

アプリケーションの要求に応じて、言語や形式が異なる、さまざまな表現でリソースを配信できます (HTML、JSON、XML など)。HTTP 状態コードは、インターフェースレベルでアクセス制御を埋め込みます。ユーザデータを考慮する必要はありません。これはサービスパフォーマンスをサポートし、データ保護に準拠します。

リソースの表現も直接選択できます。この目的のためには、**Content-Type** 属性を HTTP ヘッダーで明示的に設定する必要があります。表現において、リソースでどの処理が許可され、どの処理が許可されていないかを指定することが重要です。

### 主要な機能

REST アーキテクチャスタイルの主要機能は、以下のとおりです。

- 一意に識別可能なリソース
- 一意に参照できる URI またはリンク
- 異なる言語や形式など、リソースのさまざまな表現 (HTML、JSON、または XML)



リソースの**表現**は、他のリソースを参照することができます。クライアントが表現のリンクをたどると、ある状態から別の状態に変化します。

- アドレス可能性
- ステートレス

REST メッセージには、メッセージを理解するためにサーバまたはクライアントが必要とするすべての情報が格納されています。サーバもアプリケーションも、2



つのメッセージ間の状態情報を保存しません。これはステートレスプロトコルと呼ばれ、各処理が単独で、以前の処理から完全に切り離されています。

- 標準 HTML 関数による統一インターフェース (HTTP メソッドの GET、PUT、POST、DELETE)
- 通信はオンデマンドで実行されます。クライアントがアクティブで、パッシブサーバから表現を要求するか、リソースを変更します。
- 状態コード

要求がサーバに送信されるたびに、クライアントは可能なすべてのアプリケーションシナリオについて通知する必要があります。このために、特定の状態コードが使用されます。たとえば要求が HTML 状態コード「**201 - Created**」で確認される場合、新しいリソースが作成されたことを意味します。以下の表に、一部の HTML 状態コードを示します。

HTML 状態コード	意味	HTML 状態コード	意味
200	OK	400	不正な要求
201	作成日時	401	未認証
202	許可	403	禁止
204	<No Content>	404	見つかりません

## HTML メソッド

以下の表に、RESTful API の実装に一般に使用される HTTP メソッドを示します。これらのメソッドは、リソースの要求または変更に使えます。

HTTP メソッド	説明
GET <sup>1)</sup>	指定されたリソースをサーバから要求します。GET には副作用はありません。サーバの状態は変更されません。このため、GET は安全とみなされています。
POST	新しい (サブ) リソースを指定したリソースの下に挿入します。POST には副作用が伴います。たとえば、データベースフィールドが変更されたり、プロセスがサーバ上で開始されたりします。
PUT <sup>1)</sup>	指定されたリソースが作成されます。リソースがすでに存在する場合、リソースは変更されます。
PATCH	指定されたリソースの一部が変更されます。ここでは副作用が許可されています。
DELETE <sup>1)</sup>	指定されたリソースを削除します。

1) GET、PUT、DELETE メソッドは幂等です。すなわち、同じ要求が複数回送信された場合の副作用は、要求が 1 回だけ送信されたときと同じです。

iRMC に関する REST の詳細情報は、関連する[ホワイトペーパー](#)および Fujitsu マニュアルサーバの『[Specification iRMC Redfish API](#)』を参照してください。

## 5.3 プロファイル管理

プロファイル管理を使用すると、RESTful API を使用してフル SB 設定を送信および取得することができます。

プロファイル管理は以下の機能をサポートします。

- iRMC のプロファイルストアでのプロファイル（またはサブプロファイル）の作成。
- iRMC のプロファイルストアからのプロファイル（またはサブプロファイル）の取得。
- 実行する iRMC へのプロファイル（またはサブプロファイル）の適用。
- プロファイルの作成および適用を行うために、状態およびログ情報を提供するセッションを取得。
- プロファイルのバージョンコントロール。

### 5.3.1 プロファイル

プロファイルは SB の構成パラメータのセットで、XML または JSON 形式で使用できます。

SB プロファイルには、サブプロファイルとも呼ばれる次のセクションが含まれています。

`SystemConfig`  
`SystemConfig` セクションは、次の 2 つのサブプロファイルに分かれています。

サブプロファイル	意味
<code>IrmcConfig</code>	iRMC 構成のパラメータで構成されます。
<code>BiosConfig</code>	BIOS 構成のパラメータで構成されます。

`AdapterIrmcConfig`  
 仮想化構成のパラメータで構成されます（Virtual IO Management に基づきます）。

`HWConfigurationIrmc`  
 Out-Of-Band RAID 構成のパラメータで構成されます。

サービスプラットフォームがサポートする eLCM を使用すると、以下の追加のサブプロファイルを使用して自動デプロイメントプロセスを許可できます。

HWConfiguration

RAID および LAN アダプタ構成のパラメータで構成されます。

OSInstallation

OS インストールおよびデプロイメント構成のパラメータで構成されます。

iRMC は、現在サポートされているプロファイルのバージョンをアドバタイズし、クライアントによるプロファイル管理を有効にします。さらに各サブプロファイルにはメジャーな情報とマイナーな情報を含む固有のバージョンがあります。

iRMC は、同じメジャー番号と、同じまたはそれより低いマイナー番号を持つすべてのプロファイルを受け入れます。これらの場合、下位互換性が保証されます。

iRMC の RESTful API を使用するプロファイル管理の使用については、Fujitsu マニュアルサーバで『[Specification iRMC Restful API](#)』を参照してください。

サービスプラットフォームのサポートに関する詳細は、『eLCM の概要』取扱説明書を参照してください。

## 5.3.2 自動 BIOS パラメータバックアップ

iRMC のプロファイルストアに BiosConfig サブプロファイルを作成するには、BIOS パラメータをバックアップする必要があります。BIOS パラメータのバックアップを要求すると、管理対象ノードが起動し、現在の BIOS 構成のパラメータを読み取ります。

「設定」メニューにある「システム」ページの「自動 BIOS パラメータバックアップ」機能で、BiosConfig サブプロファイルの作成を自動化します。

「自動 BIOS パラメータバックアップ」を有効にすると、BIOS 構成パラメータが各ブートプロセス中に自動的に送信されます。このため、この機能により

「BiosConfig」サブプロファイルの作成の速度は速くなりますが、各ホストシステムのブート速度は遅くなります。

構成は、Config Space 変数を 1CC0

ConfPermanentBiosConfigStorageEnabled にして変更できます。

## 5.4 SCCI

SCCI は、Fujitsu が定義した汎用アプリケーションプログラミングインターフェース (API) で、さまざまな Server Management Controller ハードウェアおよび Server Management ソフトウェア (ServerView Agentless Service など) に対応します。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。

iRMC Web インターフェースの「**Backup and Restore**」ページで、現在の iRMC の設定データを設定ファイル (.pre) に保存 (エクスポート) できます。既存の設定ファイルからデータを復元 (インポート) することもできます。つまり、iRMC に設定データをロードできます。

あるいは、iRMC の設定データをインポートするために、HTTP POST オペレーションを使用して、該当する SCCI コマンドファイルを iRMC の /config URI に送信することもできます。

設定ファイルは、以下の言語のコマンドを使用して、SCCI API 経由でインポートできます。

- cURL
- VB スクリプト
- Python
- Powershell

この節では以下について説明します。

- SCCI (ServerView Common Command Interface) 準拠のインターフェースを iRMC の設定に使用する方法
- iRMC でサポートされる SCCI コマンド
- さまざまなスクリプト言語を使用した、iRMC のスクリプト設定
- iRMC\_PWD.exe プログラムを使用した、暗号化パスワードの生成手順



以下で説明するインターフェースは主にリモート設定を行うためのもので、SCCI 実装ではありません。SCCI コマンドと設定の定義、および SCCI ファイルフォーマットのみ使用します。

## 5.4.1 iRMC 設定データ

iRMC は、NVRAM (不揮発性 RAM) の次の個別のセクションにある内部設定データを保存します。

- Fujitsu 固有の ConfigSpace 変数 (CSV)。ファームウェアが固定の内部記述テーブルまたはマッピングテーブルを使用してアドレス指定します。
- オリジナルのメーカー固有の OMD NVCFG データ。オフセット定義でアクセスされます。

オリジナルの OMD NVCFG データからの一部の構成データは、内部的にファームウェアによってマッピングされ、ConfigSpace アクセスメソッドでアクセス可能になります。たとえば、iRMC の DNS サーバと DNS 設定に、IPMI OEM LAN 設定パラメータおよび ConfigSpace を使用してアクセスできます。両方のメソッドは、オリジナルの NVCFG 領域にある同じ低レベルのデータ構造にアクセスします。

iRMC 固有でない ServerView ソフトウェアコンポーネント (ServerView Agentless Service など) は、標準の IPMI 関連のコマンド、および標準の IPMI ユーザ設定や IPv4 ネットワーク設定などの設定項目などをマッピングすることもあります。これにより、IPMI BMC 層と上位のソフトウェアレベル間に抽象化レベルを実装します。

### リモート iRMC 設定の利点

Web ベースのアクセスによるリモート iRMC 設定には、次の利点があります。

- HTTP POST オペレーションを使用して、ファイルを iRMC にアップロードできます。特別なツールは必要ありません。認証された HTTP POST オペレーションをサポートする任意のジェネリックツールやスクリプティング環境を使用できます。サンプルスクリプトが ServerView Suite DVD 2 に収録されています。
- iRMC Web サーバのビルトイン認証と認証手法を使用できます。
- ローカル iRMC ユーザアカウントを使用する、RFC 2617 ベースの HTTP 1.1 Basic および Digest 認証をサポートします。
- 標準の HTTPS ベースのアクセスによるオプションの強力なビルトイン暗号化機能を装備しています。
- グローバルユーザアカウント (LDAP ディレクトリサーバによって管理されます) および HTTP 1.1 Basic 認証で使用できます。



HTTP 1.1 Basic 認証を使用する場合、暗号化と機密保持上の理由から、HTTPS プロトコルを使用してユーザ名とパスワードの組み合わせを保護するようにしてください。

- XML ベースの設定ファイルフォーマットを使用できます。手作業でファイルを編集するか、リファレンスインストーラまたは Server Configuration Manager からファイルをエクスポートするかをできます。
- SCCI ベースのインストール手法 (Server Configuration Manager など) で設定ファイルを再利用できます。
- 新しい設定項目と新しくサポートされる SCCI コマンドを容易に拡張できます。

## 5.4.2 SCCI ファイルフォーマット



使用する XML 設定ファイル (.pre) のフォーマットは、Windows プラットフォームの ServerView Agentless Service と共にインストールされる、セットアップ設定ヘルプファイルから取得されます。この説明と iRMC S6 固有の注意事項のコピーを以下に示します。

設定ファイルは XML 構文に基づいています。

- 各構成設定は、「<CMD>」で始まるシンプルな XML フラグメントで構成されます。
- 構成設定の完全なシーケンスは、「<CMDSEQ> および </CMDSEQ>」というタグのペアで囲まれます。

以下は、2 つの構成設定を持つ代表的なコマンドシーケンスの例です。

```
<CMDSEQ>
<CMD Context="SCCI" OC="ConfigSpace" OE="3800" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">04</DATA>
<CMD Context="SCCI" OC="ConfigSpace" OE="3801" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">00</DATA> </CMD>
</CMDSEQ>
```

Context を内部で使用して、オペレーションプロバイダを選択します。現在、サポートされるプロバイダは SCCI のみです。

### 5.4.2.1 SCCI プロバイダ固有のコマンドのパラメータ

以下の SCCI プロバイダ固有のコマンドを使用できます。

#### Operation Code (OC)

コマンド/オペレーションコードを指定する 16 進値または文字列。



iRMC は、制限された SCCI コマンドセットのみサポートします。サポートされるコマンドの一覧については、[98 ページのサポートされる SCCI コマンドの表](#)を参照してください。

#### Operation Code Extension (OE)

拡張されたオペレーションコードの 16 進値。デフォルト: OE=0  
ConfigSpace 読み書きオペレーションには、この値で ConfigSpace ID を定義します。

#### Object Index (OI)

オブジェクトのインスタンスを選択する 16 進値。Default:OI=0"

#### Operation Code Type (Type)

構成設定の場合、値 GET (読み取りオペレーション) および SET (書き込みオペレーション) がサポートされます。デフォルト: Type=GET



SET にはデータが必要です。適切なデータタイプを指定するには、下記の Data (DATA) パラメータを使用します。

## Cabinet Identifier (CA)

拡張キャビネットを選択して、そのキャビネット ID 番号を使用できます。



このパラメータをシステムキャビネットのリクエスト発行に使用しないでください。

## Data (DATA)

SET パラメータ（書き込みオペレーション）を指定する場合、データタイプ（Type パラメータ）と、場合によってはデータ長（Len パラメータ）が必要です。

現在、以下のデータタイプがサポートされます。

- `xsd::integer`

整数値

例

```
<DATA Type="xsd::integer">1234</DATA>
```

- `xsd::hexBinary`

バイトストリーム。各バイトは 2 つの ASCII 文字でコード化されます。下記の例で示すように Len パラメータを使用して、ストリームの長さ（バイト数）を指定します。

データタイプ `xsd::hexBinary` は、制約なく使用できます。使用するバイト数は、Len パラメータで指定されます。

例

4 バイト `0x00 0x01 0x02 0x04` のストリームは、以下の ASCII ストリームとしてコード化されます。

```
<DATA Type="xsd::hexBinary" Len="4">0001020304</DATA>
```

- `xsd::string`

通常、文字列の転送に使用されます。string タイプは、IPv4 アドレスおよび MD5 ベースのユーザパスワードにも使用できます。この場合、文字列データは、受け付けられるターゲットフォーマットに内部で変換されます。

暗号化データの転送

Fujitsu 専用のデータ暗号化は、ユーザまたはサービス (LDAP/SMTP) アクセスパスワードや、iRMC の AVR ライセンスキーなどの機密データでサポートされます。iRMC\_PWD.exe プログラムを使用して、パスワードデータを暗号化することができます（[102 ページのパスワード暗号化ユーティリティ](#)を参照）。

Encrypted="1" を <DATA> タグで設定して、書き込むデータを暗号化することを示す必要があります。

例

「Hello World」という文字列を転送する場合：

```
<DATA Type="xsd::string">Hello World</DATA>
```

クリア（読み取り可能）テキストとしてパスワードを転送する場合：

```
<DATA Type="xsd::string">My Readable Password</DATA>
```

暗号化されたパスワードを転送する場合：

```
<DATA Type="xsd:string"
Encrypted="1">TpV1TJwCyHEIsC8tk24ci83JuR91</DATA>
```

IPv4 アドレス「192.23.2.4」を転送する場合：

```
<DATA Type="xsd:string">192.23.2.4</DATA>
```



xsd:string データタイプの使用は、読み込み可能な文字列、IP アドレス、MD5 ベースのユーザパスワードに限定されます。

その他のすべてのデータには、xsd:hexbinary データタイプを使用してください。



ä, à, å, æ などの言語固有の文字は、使用しているアプリケーションで実際に必要でない限り、文字列に直接指定しないでください。

SCCI および ConfigSpace インターフェースは、どちらも文字の暗号化情報を保存しません。つまり、US-ASCII 以外の文字は使用しているアプリケーションによって内部で解釈されるので、使用しないようにしてください。特殊文字を実際に指定する必要がある場合、適切な BOM を含む UTF-8 フォーマットでファイルの編集と保存を行ってください。

### Command Status (Status)

構成設定を転送すると、Status にオペレーションの結果が含まれます。オペレーションが正常終了した場合、値 0 が返されます。



すべての公開された構成設定の仕様については (ConfigSpace) 、Scripting Toolkit に付属の SCCI\_CS.pdf ファイルを参照してください。



### 5.4.2.2 注意事項

.pre ファイルに指定されるすべてのコマンドは、通常順次に実行されます。この規則の例外を以下に示します。

- ネットワーク接続の切断を防ぐため、IPv4 および VLAN ネットワーク構成のコマンドをコマンドシーケンスの最後で実行します。
- 現在、IPv6 構成は不揮発性 IPv6 構成パラメータの構成に限定されています。

回避策として、以下の手順を実行することもできます。

1. スクリプトを以下のように調整します。
  - a. スクリプトの先頭で、IPv6 を無効にします。
  - b. IP パラメータを設定します。
  - c. スクリプトの末尾で、IPv6 を有効にします。

2. スクリプトを IPv4 アドレスから送信します。

- SSL 証明書と関連する適合先の秘密鍵は、コマンドシーケンスの最後に実行されます。両方のコンポーネントは、同じ .pre ファイルに保存されている必要があり、互いに一致することが確認されます。
- SB のパワーマネジメントオペレーション、または iRMC の再起動が必要な場合は、以下のようにします。

これらのコマンドを別のコマンドファイルで実行することを推奨します（必須ではありません）。構成と電源管理処理を別のタスクに切り分けることで、これを実現できます。

- スクリプトの外部で、連続するコマンド実行にオプションの遅延を実装する必要があります。

例えば、以下のようにして実装できます。

1. スクリプトを適切な別のスクリプトに分割します。
2. クライアントの機能範囲を使用して、個々のファイルの送信に遅延を挿入します。

### 5.4.2.3 設定データのエクスポートとインポート

iRMC Web インターフェースの「バックアップとリストア」ページで、現在の iRMC の設定データを設定ファイル (.pre) に保存（エクスポート）できます。また、既存の設定ファイル (.pre) から iRMC 設定データをインポートできます。つまり、iRMC に設定データをロードできます（詳細は、『iRMC S6 - Web インターフェース』取扱説明書を参照）。

あるいは、iRMC 設定をインポートするために、HTTP POST オペレーションを使用して、該当する SCCI コマンドファイルを iRMC の /config URI に送信することもできます。

### 5.4.3 サポートされる SCCI コマンド

iRMC S6 は下記の SCCI コマンドをサポートします。

SCCI OpCode	SCCI コマンド文字列	意味
0xE002	ConfigSpace	ConfigSpace 書き込み
0x0111	PowerOnCabinet	SB の電源を入れます。
0x0112	PowerOffCabinet	SB の電源をオフにします。
0x0113	PowerOffOnCabinet	SB のパワーサイクルを実行します。
0x0204	ResetServer	SB をハードリセットします。
0x020C	RaiseNMI	NMI パルス (マスク不可割り込み)
0x0205	RequestShutdownAndOff	グレースフルシャットダウン、実行中のエージェントが必要
0x0206	RequestShutdownAndReset	グレースフルリブート、実行中のエージェントが必要
0x0209	ShutdownRequestCancelled	シャットダウンリクエストのキャンセル
0x0203	ResetFirmware	BMC リセットを実行します。
0x0250	ConnectRemoteFdlImage	Remote Image Mount (NFS または CIFS 共有) でフロッピーディスクイメージを接続/接続解除します。
0x0251	ConnectRemoteCdlImage	Remote Image Mount (NFS または CIFS 共有) で CD/DVD .iso イメージを接続/接続解除します。

SCCI OpCode	SCCI コマンド文字列	意味
0x0252	ConnectRemoteHdlImage	Remote Image Mount (NFS または CIFS 共有) でハードディスクイメージを接続/接続解除します。

Server Control Command Interface および対応する設定スペース値のマニュアルは、[Fujitsu マニュアルサーバ](#)にあります。

## 5.4.4 スクリプトのサンプル

### 5.4.4.1 cURL のサンプル

オープンソースコマンドラインツール cURL で、URL 構文で指定したデータを転送できます。ソースコードの最新バージョンと、OS のプリコンパイルバージョンは、<http://curl.haxx.se/> からダウンロードできます。

以下に、cURL を使用して設定ファイルを iRMC に送信する方法についていくつかの例を示します。



cURL コマンドラインオプションの詳細は、cURL のマニュアルを参照してください。

- Basic 認証 (デフォルト) とデフォルトの iRMC S6 admin アカウントでの HTTP アクセス
 

```
curl --basic -u admin:admin --data @Config.pre
http://<iRMC IP address>/config
```
- Digest 認証とデフォルトの iRMC admin アカウントでの HTTP Access :
 

```
curl --digest -u admin:admin --data @Config.pre
http://<iRMC IP address>/config
```
- 認証チェックなし (-k) で、Digest 認証とデフォルトの iRMC admin アカウントでの HTTPS Access
 

```
curl --digest -k -u admin:admin --data @Config.pre
https://<iRMC IP address>/config
```
- LDAP ユーザアカウントでの HTTPS アクセス。
 

LDAP ユーザには、基本認証を指定する必要があります。

```
curl --basic -k -u LDAPuser:LDAPpassword --data @Config.pre
https://<iRMC IP address>/config
```

#### 5.4.4.2 Visual Basic (VB) スクリプト

次のVB スクリプトでは、設定ファイルを iRMC に送信します。

```
IP_ADDRESS = "<iRMC IP address>"
USER_NAME = "admin"
PASSWORD = "admin"
FILE_NAME = ".\ConfigFile.pre"
Const ForReading = 1
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile(FILE_NAME, ForReading)
' -----
On Error Resume Next
Set xmlHttp = CreateObject("Microsoft.XMLHTTP")
xmlHttp.Open "POST", "http://" & IP_ADDRESS & "/config", False,
USER_NAME, PASSWORD
xmlHttp.setRequestHeader "Content-Type", "application/x-www-
form-urlencoded"
xmlHttp.Send objFile.ReadAll
Wscript.Echo xmlHttp.responsexml.xml
```

### 5.4.4.3 Python スクリプト

```
#!/usr/bin/python3
import sys
import httpplib2
from urllib.parse import urlencode
# =====
# iRMC
USER = 'admin'
PWD = 'admin'
IP_ADDR = '192.168.1.100'
# =====
h = httpplib2.Http()
# Basic/Digest authentication
h.add_credentials(USER, PWD)
def doit(data,ausgabe=sys.stdout):
    try:
        resp, content = h.request("http://%s/config" % IP_ADDR,
            "POST", data)
        if resp['status'] == '200':
            data = content.decode('utf-8')
            print(data,file=ausgabe)
        else:
            print('STATUS:',resp['status'],file=ausgabe)
            print(str(resp),file=ausgabe)
        except Exception as err:
            print('ERROR:',str(err),file=ausgabe)
            print()
# Example 1 - send a configuration file to the iRMC
try:
    data = open('ConfigFile.pre').read()
    doit(data)
except Exception as err:
    print('ERROR:',str(err),file=ausgabe)
# Example 2 - Set Config Space Values
# 0x200 (ConfCabinetLocation) and
# 0x204 (ConfSystemContact) direct from the script
#
LocationContact = '''<?xml version="1.0" encoding="UTF-8"
```

```

<CMDSEQ>
<!-- ConfCabinetLocation -->
<CMD Context="SCCI" OC="ConfigSpace" OE="200" OI="0" >
<DATA Type="xsd:string">%s</DATA>
</CMD>
<!-- ConfSystemContact -->
<CMD Context="SCCI" OC="ConfigSpace" OE="204" OI="0" >
<DATA Type="xsd:string">%s</DATA>
</CMD>
</CMDSEQ>
...
doit(LocationContact % ("Ostsee","Kiel"))

```

### 5.4.5 パスワード暗号化ユーティリティ

Fujitsu iRMC パスワード暗号化および検証ユーティリティの iRMC\_PWD.exe は Win32 プログラムで、SCCI スクリプトに使用する暗号化パスワードを生成できます。iRMC\_PWD.exe は、1 つのパスワードの暗号化にも、スクリプト設定用の SCCI バッチファイルの生成にも使用できます。

#### iRMC\_PWD 標準コマンドラインオプション

```

[-h] [-?]
    この説明。

[-v]
    暗号化されたパスワード文字列を確認します。

[-o] <oid>
    暗号化するデータのオブジェクト ID。

[-u] <username>
    指定したオブジェクト ID のユーザ名 (オプション) 。

[-x] <opCodeExt>
    暗号化する ConfigSpace データの OpCode 拡張。

[-p] <パスワード>
    指定したオブジェクト ID のパスワード。
    デフォルト: 1452 (ConfBMCAcctUserPassword)
    指定可能な値は次のとおりです。
    1452 - ConfBMCAcctUserPassword
    1273 - ConfAlarmEmailSMTPAuthPassword
    197A - ConfLdapiRMCgroupsUserPasswd
    502 - ConfBmcRadiusSharedSecret

```

1A52 - ConfBmcRemoteFdImageUserPassword  
 1A62 - ConfBmcRemoteCdImageUserPassword  
 1A72 - ConfBmcRemoteHdImageUserPassword  
 1980 - ConfBMCLicenseKey

### iRMC\_PWD コマンドライン出力オプション

[-b]  
 出力ファイルを WinSCU BATCH ファイルとして作成します。

[-f] <Output File>  
 出力ファイルの名前を指定します。  
 デフォルト: iRMC\_pwd.txt  
 バッチモードのデフォルト: iRMC\_pwd.pre

### 例

oid 2を使用して、ユーザ名を admin に、パスワードを SecretPassword に設定／変更する .pre ファイルを生成するとします。

これを実現するには、以下のコマンドを入力します。

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b
iRMC_PWD が以下の内容の .pre ファイルを生成します。
```

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CMDSEQ>
<!-- "ConfBMCacctUserName" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1451" OI="2" Type="SET">
  <DATA Type="xsd:string">admin</DATA>
  <STATUS>0</STATUS>
</CMD>
<!-- "ConfBMCacctUserPassword" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1452" OI="2" Type="SET">
  <DATA Type="xsd:string"
  Encrypted="1">N2BZd3oLHAgc11pnHCAV9P/ItwRue4qBB3IU7Xsh</DATA>
  <STATUS>0</STATUS>
</CMD>
</CMDSEQ>
```

図 22: 生成される .pre ファイルの内容

---

## 6 LAN over USB

iRMC とSB間で既存のインバンドインターフェースのほかに、iRMC には LAN over USB と呼ばれる新しい高速インバンドインターフェースがあります。システムボード上の iRMC ハードウェアには、内蔵 USB イーサネットデバイスが搭載されています。

内蔵 USB イーサネットデバイスには 2 つのネットワーク接続ポイントがあり、iRMC 接続ポイントとホスト OS 接続ポイントと呼ばれています。ホスト OS から iRMC へのローカル接続を確立するには、各接続ポイント (iRMC とホスト OS) に、同じサブネット内の MAC アドレスとルーティング不可能な一意の IPv4 アドレスを割り当てる必要があります。MAC アドレスは自動的に割り当てられますが、IPv4 アドレスは手動で設定する必要があります。

デフォルトで、LAN over USB インターフェースの iRMC IP アドレスが、静的 IPv4 アドレス 169.254.0.2、サブネットマスク 255.255.0.0 に設定されます。IP アドレスがネットワーク内で競合する場合、iRMC の LAN over USB インターフェースに別の IP アドレスを設定できます。



ルーティング不可能な IPv4 アドレスは安全なプライベートアドレスをみなされ、外部インターネットユーザによるシステム内の移動を防止します。

iRMC の LAN over USB 機能は、以下のタスクをホスト OS からローカルに実行する場合に特に便利です。

- iRMC のサーバ管理機能。通常は iRMC Web インターフェースから、またはサーバの Management LAN 接続を介して Redfish API から実行されます。
- 将来的な拡張による、SB と iRMC 間のデータおよびコマンドの双方向転送。

LAN over USB 機能を使用するには、iRMC とSBを設定する必要があります。

### 6.1 要件

LAN over USB 機能には、以下のSBが必要です。

- Linux または Windows OS を実行していること
- RNDIS ドライバ: Linux の場合、ネイティブで十分です。Windows の場合、新しいカタログファイルが必要です。



---

## 6.2 iRMC での LAN over USB の設定

LAN over USB インターフェースを有効にするには、まず iRMC 側の設定を実行する必要があります。

LAN over USB を iRMC に設定する一般的な手順を以下に示します。

1. 両方の接続ポイント（MAC アドレスと IPv4 アドレス）の iRMC で LAN over USB 設定がネットワーク環境に適しているか、確認します。
2. iRMC で LAN over USB を有効にします。

### 6.2.1 MAC アドレスの割り当て

顧客が設置したシステムにファームウェアアップデートを介して導入できる外部からルーティング可能な LAN over USB インターフェースをサポートするため、iRMC はシステム固有の一意の MAC アドレスを生成します。このアドレスは、LAN over USB MAC アドレスの不揮発性プレフィックス設定が iRMC 側で変更されない限り、マザーボードの有効期間内は変更されません。

両方の接続ポイントの MAC アドレスは、iRMC LAN ネットワークポートの MAC アドレスから派生します。それぞれ 6 バイトの MAC アドレスには、3 バイトの OUI（organizationally unique identifier）フィールドと 3 バイトの NIC 固有のフィールドがあります。OUI は IEEE によって割り当てられます。たとえば、90-1B-0E（FTS GmbH）や 00-22-4D（MITAC）などです。

OUI には、オクテット 0 のビット（ビット 1）があり、これは OUI が普遍的に管理されているか（ビット 1 = 0）ローカルに管理されているか（ビット 1 = 1）を示します。iRMC は、割り当てられていないローカルに管理された OUI と既存の iRMC MAC アドレスからのデータを組み合わせて使用して、一意のシステム固有のアドレスを生成します。

たとえば、10-20-xx と 14-20-xx という OUI は、IEEE によってグローバルで割り当てられていません。ローカルに管理されているものは、12-20-xx と 16-20-xx です。このアプローチで、新しい LAN over USB MAC アドレスを以下のように割り当てます。

既存の iRMC LAN MAC アドレスは xx-xx-xx-zz-zz-zz と表現できます。ここで、xx-xx-xx は OUI、zz-zz-zz は NIC 固有です。LAN over USB に対して、iRMC アルゴリズムは 2 つの MAC アドレスを生成します。

- 1 つはホスト接続ポイント用: LAN over USB ホスト側 MAC = aa-aa-yy-zz-zz-zz
- もう 1 つは iRMC 接続ポイント用: LAN over USB iRMC 側 MAC = cc-cc-yy-zz-zz-zz

AA AA  
 ホスト側 MAC アドレス用 OUI

CC CC  
 iRMC 側 MAC アドレス用 OUI

YY  
 iRMC MAC アドレスの OUI バイト (XX-XX-XX) の合計

ZZ-ZZ-ZZ  
 iRMC MAC アドレスの NIC 固有のバイト。

iRMC は、プレフィックスとして使用される OUI の値の範囲を指定します。MAC アドレスの最後の 3 つのバイトは、iRMC ファームウェアから自動的に設定されます。

ホスト側 OUI	iRMC 側 OUI
12-20-XX	16-20-XX
12-50-XX	16-50-XX
12-70-XX	16-70-XX
12-80-XX	16-80-XX
12-B0-XX	16-B0-XX
12-E0-XX	16-E0-XX
22-30-XX	26-30-XX
22-50-XX	26-50-XX
22-70-XX	26-70-XX
22-D0-XX	26-D0-XX

テーブル 4: MAC アドレスプレフィックスに可能な値

## 6.2.2 configSpace 変数による設定

SCCI API の configSpace データには、LAN over USB 機能を手動で設定する以下のパブリック変数が含まれています。

変数名	値 ID	タイプ	値の範囲	デフォルト	意味
ConfBmcUsbLan Enable	Ox1820	ビット	0: 無効 1: 有効	0	iRMC で LAN over USB を有効/無効にします。LAN over USB が有効になると、デフォルト値が作業環境で定義されます。
ConfBmcUsbLan IPv4NetMask	Ox1821	文字列		255.255.0.0	LAN over USB インターフェースの iRMC 側のサブネットマスク。
ConfBmcUsbLan IPv4AddrBmc	Ox1822	文字列		169.254.0.2	LAN over USB インターフェースの iRMC 接続ポイントの IP V4 アドレス。

テーブル 5: インバンド通信の変数

変数名	値 ID	タイプ	値の範囲	デフォルト	意味
ConfBmcUsbLan IPv4AddrHost	0x1823	文字列		169.254.0.1	LAN over USB イン ターフェ ースのホス ト接続ポ イントの IP V4 アドレス。
ConfBmcUsbLan MacAddrBmcOUI	0x1824	配列	{0x16, 0x20} {0x16, 0x50} {0x16, 0x70} {0x16, 0x80} {0x16, 0x80} {0x16, 0xE0} {0x26, 0x30 } {0x26, 0x20} {0x26, 0x50} {0x26, 0x70} {0x26, 0xD0}	{0x16, 0x20}	LAN over USB イン ターフェ ースの iRMC 接続ポ イントの MAC アドレス。

テーブル 5: インバンド通信の変数

変数名	値 ID	タイプ	値の範囲	デフォルト	意味
ConfBmcUsbLan macAddrHostOUI	0x1825	配列	{0x12, 0x20} {0x12, 0x50} {0x12, 0x70} {0x12, 0x80} {0x12, 0x80} {0x12, 0xE0} {0x22, 0x30 } {0x22, 0x20} {0x22, 0x50} {0x22, 0x70} {0x22, 0xD0}	{0x12, 0x20}	LAN over USB イン ターフェ ースのホス ト接 続ポイン トの MAC アドレス。

テーブル 5: インバンド通信の変数

設定変数は、以下の言語のコマンドを使用して、SCCI API 経由でインポートできます。

- cURL
- VB スクリプト
- Python
- Redfish
- iRMC プロファイリング

対応する `configSpace` 変数の値を変更するときに iRMC USB LAN インターフェースを再構成すると、変更を適用するために iRMC ファームウェアがインターフェースを自動的に再起動します。ConfBmcUsbLanEnable 変数を書き込んでインターフェースを有効または無効にすると、変更が即座に適用されます。

他の USB LAN 変数が更新されると、およそ 3 秒後に USB LAN インターフェースが再起動されます。そこで複数の変数を連続して変更でき、LAN over USB インターフェースは最後の変数を変更した後に再起動されます。

SB が Windows OS で実行されている場合、ConfBmcUsbLanEnable 変数はプラグアンドプレイデバイスとほぼ同様に機能します。LAN over USB インターフェイス用の RNDIS ドライバがインストールされ、iRMC の IPv4 設定に従って静的 IPv4 アドレスが SB に設定されると、ConfBmcUsbLanEnable 変数を使用して LAN over USB インターフェイスのオン/オフを切り替えられるようになります。変数が 0 に設定されると、デバイスマネージャから追加のネットワークデバイスがすぐに消えます。1 に設定されると、以前と同じ IPv4 アドレスでインターフェイスが再度表示されます。



ConfBmcUsbLanEnable 変数が初めて 1 に設定されると、デバイスマネージャから追加のネットワークデバイスがすぐに消え、ドライバがインストールされた後に Windows からローカルネットワークアドレスが自動的に割り当てられます。Windows は iRMC 設定空間での設定されたアドレスを無視します。USB over LAN インターフェイスは iRMC の指示で SB 上で機能しますが、この逆は成立しません。

### 6.2.3 Web インターフェイスによる設定

LAN over USB 機能は「設定」メニューの「サービス」ページからも設定できます。

USBホストLAN有効化	<input type="checkbox"/>
iRMC IPアドレス	169.254.0.2
ホストIPアドレス	169.254.0.1
サブネットマスク	255.255.0.0
ホストMACアドレス(OUI)	1220
iRMC MACアドレス(OUI)	1620

適用 キャンセル

図 23: 「USBホストLAN構成」グループ

このグループでは、以下のパラメータを指定できます。

#### USB ホスト LAN

iRMC で LAN over USB を有効/無効にします。LAN over USB が有効になると、他のパラメータが有効になり、編集できるようになります。

#### iRMC IP アドレス

LAN over USB インターフェイスの iRMC 接続ポイントのサブネットマスク。

#### ホスト IP アドレス

LAN over USB インターフェイスのホスト接続ポイントの IP V4 アドレス。



メインボードを変更したためなどの理由でホストの IP アドレスが変更された場合、このフィールドの値も変更する必要があります。iRMC は SB のシステム設定とは同期されず、変更を手動で設定する必要があります。

#### サブネットマスク

LAN over USB インターフェースの iRMC 側のサブネットマスク。

#### ホスト MAC アドレス(OUI)

LAN over USB インターフェースのホスト接続ポイントの MAC アドレスの OUI 部分。

#### iRMC MAC アドレス(OUI)

LAN over USB インターフェースの iRMC 接続ポイントの MAC アドレスの OUI 部分。

## 6.3 Windows サーバでの LAN over USB の設定

Windows ホストで LAN over USB を設定するには、次の手順に従います。

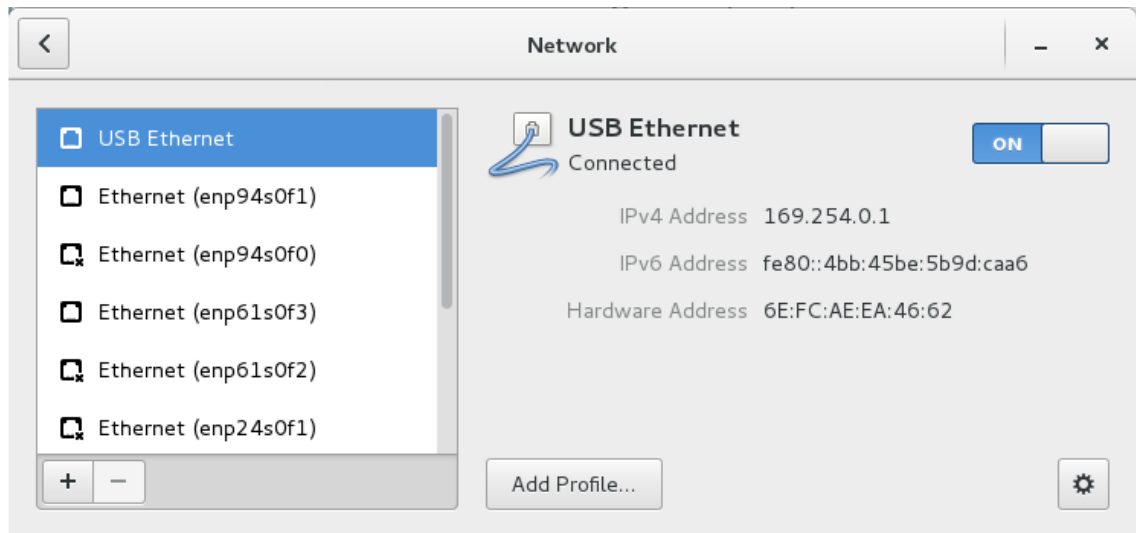
1. Fujitsu サポートページから、個々のホスト OS に固有のドライバを取得します。
2. ドライバパッケージの内容を SB にコピーします。
3. `ami.inf` ファイルを右クリックします。
4. コンテキストメニューから「インストール」を選択します。
5. ドライバがインストールされたら、デバイスマネージャを開きます。
6. 「ネットワークアダプタ」ページに、「AMI Remote NDIS6 based Device」または「Virtual Networking Device」というデバイスがあり、インストール可能な状態になっています。
7. 「AMI Remote NDIS6 based Device」を右クリックして、コンテキストメニューから「プロパティ」を選択します。
8. 「詳細」ページを開きます。
9. 「ネットワークアドレス」フィールドに、iRMC 接続ポイントの IPv4 アドレスを入力します。
10. 「OK」をクリックします。

設定された IP アドレスからの接続が可能になります。

## 6.4 Linux サーバでの LAN over USB の設定

Linux サーバでは、すでに存在するイーサネットデバイスドライバで十分ですが、iRMC 接続ポイントの IP アドレスで設定する必要があります。

1. 「System Tools/Settings」から「Network」ダイアログを開きます。



2. リストで「USB Ethernet」を選択します。
3. 「Add Profile」をクリックします。
4. 「Profile」ダイアログで、iRMC 接続ポイントのサブネットマスクと IPv4 アドレスを入力します。



---

## 7 iRMC の監視



iRMC が内部エラーを検出し、操作の続行が困難な場合、iRMC はセルフリセットによって自動的に復旧します。このとき、iRMC への通信は数分間利用できなくなります。iRMC はシステムイベントログ (SEL) にエントリを書き込み、設定されている場合は SNMP トラップを送信してセルフリセットを通知します。

### 7.1 SNMP による監視

SNMP (Simple Network Management Protocol) はアプリケーション層プロトコルで、SNMP マネージャとエージェント間の通信に使用するメッセージフォーマットを提供します。SNMP は、ネットワーク内のデバイスの監視と管理に使用される、標準化されたフレームワークと共通言語を提供します。

SNMP フレームワークは 3 つの部分で構成されています。

- SNMP マネージャ
- SNMP エージェント
- MIB

SNMP マネージャは、SNMP を使用してネットワークホストのアクティビティを制御および監視するために使用されるシステムです。最も一般的な管理システムは、ネットワーク管理システム (NMS) です。NMS という用語は、ネットワーク管理専用のデバイスにも、このようなデバイスで使用されるアプリケーションにも使用されます。さまざまなネットワーク管理アプリケーションを SNMP で使用できます。これらはシンプルなコマンドラインアプリケーションから多機能のグラフィカルユーザインターフェースまで、多岐にわたります。

SNMP エージェントは管理対象デバイス内のソフトウェアコンポーネントで、デバイスのデータを管理し、これらのデータを必要に応じて管理側システムに報告します。エージェントと MIB はルーティングデバイス (ルータ、アクセスサーバ、またはスイッチ) にあります。SNMP エージェントを有効にするには、マネージャとエージェントの関係を定義する必要があります。

管理情報ベース (MIB) はネットワーク管理情報のバーチャル情報ストレージエリアで、管理対象オブジェクトのコレクションで構成されています。MIB 内には、関連するオブジェクトのコレクションが MIB モジュール内で定義されています。MIB モジュールは、STD 58、RFC 2578、RFC 2579、RFC 2580 での規定に従い、SNMP MIB モジュール言語で記述されています。

SNMP エージェントには MIB 変数が含まれ、SNMP マネージャは Get または Set 処理でその値を要求または変更できます。マネージャはエージェントから値を取得したり、値をそのエージェントに格納したりできます。エージェントは、デバイスパラメータとネットワークデータに関する情報のリポジトリである MIB からデータを収集します。エージェントは、マネージャからのデータの Get または Set 要求に応答することもできます。

SNMP の主な機能は、SNMP エージェントから通知を生成する機能です。これらの通知には、SNMP マネージャから要求を送信する必要はありません。非同期通知をトラップまたはインフォーム要求として生成できます。トラップは、SNMP マネージャにネットワークの状態を通知するメッセージです。インフォーム要求（インフォーム）は、SNMP マネージャからの受領確認の要求を含むトラップです。通知によって、不適切なユーザ認証、再起動、接続の終了、近接ルータへの接続の損失、またはその他の重大なイベントを示すことができます。

トラップは、トラップを受け取ったときに受信側が確認を送信せず、トラップが受信されたかどうかを送信側が確認できないので、インフォームほど信頼性がありません。インフォーム要求を受信した SNMP マネージャは、SNMP 応答プロトコルデータユニット（PDU）を使用してメッセージを確認します。マネージャがインフォーム要求を受信しない場合、応答は送信されません。送信側が応答を送信しない場合、インフォーム要求をもう一度送信できます。このようにすることで、インフォームは目的の宛先に届く可能性が高くなります。

ただし、インフォームはルータやネットワークで多くのリソースを使用するので、トラップが推奨されることがよくあります。送信されるとすぐに破棄されるトラップとは異なり、インフォーム要求は、応答が受信されるか、要求がタイムアウトするまで、メモリ内に保持される必要があります。また、トラップが送信されるのは 1 度だけですが、インフォームは複数回再送信できます。再試行によってトラフィックが増加し、ネットワークでのオーバーヘッドが高くなります。このように、トラップとインフォーム要求には、信頼性とリソースとのトレードオフがあります。SNMP マネージャがどの通知も受信することが重要な場合は、インフォーム要求を使用します。ただし、ネットワーク上のトラフィックおよびルータのメモリに配慮が必要で、すべての通知を受信しなくてもよい場合は、トラップを使用します。

iRMC では以下のバージョンの SNMP をサポートします。

- SNMPv1 は RFC 1157 で定義された、インターネットのフル規格です（RFC 1157 は、RFC 1067 および RFC 1098 として公開された以前のバージョンを置き換えます）。セキュリティはコミュニティ文字列を基盤としています。
- SNMPv2c は実験的なインターネットプロトコルで、RFC 1901、RFC 1905、RFC 1906 で定義されています。SNMPv2c は SNMPv2p（SNMPv2 Classic）のプロトコル処理およびデータタイプを更新したもので、SNMPv1 のコミュニティベースのセキュリティモデルを使用します。
- SNMPv3 は相互運用可能な規格ベースのプロトコルで、RFC 2273 ~ 2275 で定義されています。SNMPv3 は、ネットワーク上でパケットの認証と暗号化を

組み合わせて、デバイスへのセキュアなアクセスを実現します。

SNMPv3 で提供されるセキュリティ機能は、以下のとおりです。

- メッセージの整合性: パケットが転送中に改変されていないことを確認する
- 認証: メッセージが有効な送信元から発信されたことを確認する
- 暗号化: パケットの内容を暗号化することで、不正なソースによって読み取られないようにする

デフォルトで、SNMP サービスは iRMC S6 では無効になっています。

iRMC S6 の SNMP サービスは、以下の SNMP MIB での GET 要求をサポートします。

- STATUS.MIB
- OS.MIB
- SC2.MIB
- MIB-2.MIB 別名 RFC1213.MIB

これらの MIB は FUJITSU Software ServerView Suite DVD に収録されています。また、[ServerView サポートページ](#)からダウンロードすることもできます。

SNMP サービスが有効な場合、これらの MIB によって提供される情報を SNMP マネージャを実行中のシステムで使用できます。

## 7.2 iRMC システムレポート

通常、情報はホスト OS で実行される ServerView Agentless Service によって収集され、さまざまな種類のハードウェアおよびソフトウェアの情報が含まれます。収集された情報には、iRMC 情報（センサ、IDPROM/FRU、イベントログ）のほか、ホストにインストールされているソフトウェアとドライバ、実行されているプロセスなどが含まれます。

ServerView Agentless Service が実行されていない場合でも、この情報のサブセットとして、主にサービスインシデントが iRMC から直接 Out-Of-Band で使用可能です。

この項では、iRMC のスクリプトによるダウンロードと自動評価の例を示し、iRMC から提供されるシステムレポートの項目を説明します。

## 7.2.1 ダウンロード用の cURL スクリプト

cURL はオープンソースのコマンドラインツールで、URL 構文で指定されたデータを転送します。ソースコードの最新バージョンと、各 OS のプリコンパイルバージョンは、<http://curl.haxx.se/> からダウンロードできます。

以下は、cURL で iRMC からシステムレポートファイルを取得する方法の例です。cURL コマンドラインオプションの詳細は、cURL のマニュアルを参照してください。デフォルトの cURL は取得したデータを標準出力に送信するので、これをリダイレクトまたはパイプ処理して、さらに処理するか、取得したデータを `-o <出力ファイル名>` で保存できます。

- Digest 認証とデフォルトの iRMC admin アカウントでの HTTP アクセスで、`report.xml` に保存する (`-o`)

```
curl --digest -o report.xml -u admin:admin  
http://192.168.1.100/report.xml
```

- 認証チェックなし (`-k`) で、Digest 認証とデフォルトの iRMC admin アカウントでの HTTPS Access

```
curl --digest -k -u admin:admin  
https://192.168.1.100/report.xml
```

- LDAP ユーザアカウントでの HTTPS アクセス

LDAP ユーザに対しては、認証パラメータを LDAP サーバに渡して検証する必要があるため、基本認証を指定する必要があります。

```
curl --basic -k -u LDAPuser:LDAPpassword  
https://192.168.1.100/report.xml
```

## 7.2.2 Visual Basic スクリプト

スクリプトは Visual Basic でも作成できます。以下の VB スクリプトは、report.xml を iRMC から取得して、これも report.xml という名前のローカルファイルに保存します。

```
IP_ADRESSE = "192.168.1.100"
USER_NAME = "admin"
PASSWORD = "admin"
FILE_NAME = ".\report.xml"
ADDONS = "/report.xml"
' -----
-----
On Error Resume Next
Function SaveBinaryData(FileName, ByteArray)
    Const adTypeBinary = 1
    Const adSaveCreateOverWrite = 2
    Dim BinaryStream
    Set BinaryStream = CreateObject("ADODB.Stream")
    BinaryStream.Type = adTypeBinary
    BinaryStream.Open
    BinaryStream.Write ByteArray
    BinaryStream.SaveToFile FileName, adSaveCreateOverWrite
    WScript.Echo "Antwort:" & BinaryStream.Read
End Function
Set xmlHttp = CreateObject("Msxml2.XMLHTTP")
xmlHttp.Open "GET", "http://" & IP_ADRESSE & ADDONS, False,
USER_NAME, PASSWORD
xmlHttp.Send
If InStr(xmlHttp.GetResponseHeader("Content-Type"), "xml") > 0
    Then
        SaveBinaryData FILE_NAME,xmlHttp.ResponseBody
    Else
        Wscript.Echo ADDONS &" not found on " &IP_ADRESSE
    End If
```

### 7.2.3 情報セクション

以下のシステムレポートセクションをサポートします。

セクション	サブセクション	備考/制限
システム	BIOS	ConfigSpace からの BIOS バージョンのみ
	Processor	
	メモリ	
	ファン	
	Temperatures	
	PowerSupplies	
	電圧	
	IDPROMS	
	SensorDataRecords	
	PCIDevices	スロット内の PCI バージョンおよびデバイス ID のみ、オンボードデバイスの情報なし
	SystemEventLog	
	InternalEventLog	
	BootStatus	
ManagementControllers	iRMC S6 のみ	
ネットワーク	設定	
	Adapters	
	Interfaces	
	ポート	
Software/ServerView	SNMPAgents	
	ServerViewRaid	

### 7.2.3.1 Summary セクション

生成された XML の最初のセクションとして Summary セクションがあり、レコード作成の日付と時刻、現在の iRMC の IP アドレス、SystemEventLog セクションの Critical/Major および Warning (Minor) エントリの数などの情報が含まれ、使用できるセクションのインベントリリストがあります。

サンプル出力:

```
<?xml version="1.0" encoding="UTF-8"?>
<Root Schema="2" Version="97.30F" OS="iRMC"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Summary>
<Created>
<IsAdmin>true</IsAdmin>
<Date>2014/02/05 17:27:15</Date>
<BuildDuration>3</BuildDuration>
<Company>FUJITSU</Company>
<Computer>iRMCFDAF9F</Computer>
<OS>iRMC S5 8.64F SDR: 3.35 ID 0413 RX2520M1</OS>
<Domain></Domain>
<HostIPv4Address>10.172.103.13</HostIPv4Address>
<HostIPv6Address>fe80::219:99ff:fe80:af9f</HostIPv6Address>
</Created>
<Errors Count="1">
<Eventlog>
<Message>59 important error(s) in event log!</Message>
</Eventlog>
</Errors>
<Warnings Count="1">
<Eventlog>
<Message>23 important warning(s) in event log!</Message>
</Eventlog>
</Warnings>
<Content>
<Item Name="System/Bios"></Item>
<Item Name="System/Processor"></Item>
<Item Name="System/Memory"></Item>
<Item Name="System/Fans"></Item>
<Item Name="System/Temperatures"></Item>
<Item Name="System/PowerSupplies"></Item>
```

```

<Item Name="System/Voltages"></Item>
<Item Name="System/IDPROMS"></Item>
<Item Name="System/SensorDataRecords"></Item>
<Item Name="System/PCIDevices"></Item>
<Item Name="System/SystemEventlog"></Item>
<Item Name="System/InternalEventlog"></Item>
<Item Name="System/BootStatus"></Item>
<Item Name="System/ManagementControllers"></Item>
<Item Name="Network/Settings"></Item>
  <Item Name="Network/Adapters"></Item>
  <Item Name="Network/Interfaces"></Item>
  <Item Name="Network/Ports"></Item>
  <Item Name="Software/ServerView/SNMPAgents"></Item>
  <Item Name="Software/ServerView/ServerViewRaid"></Item>
</Content>
</Summary>
<System>

```

### 7.2.3.2 BIOS セクション

iRMC は SB の SMBIOS 構造にアクセスできないため、提供される情報は非常に限定的なサブセットのみです。

例:

```

<Bios Schema="1">
<SMBIOS Version="Unknown">
<Type0 Name="BIOS Information" Type="0">
<BiosVersion>V4.6.5.4 R1.0.0 for D3239-A1x</BiosVersion>
</Type0>
</SMBIOS>
</Bios>

```

### 7.2.3.3 Processor セクション

生成された情報は、F113 および F115 OEM IPMI コマンドに基づき、CDiagReport.h に準拠しています。

```

<Processor Schema="1">
<CPU Boot="true">
<SocketDesignation>CPU</SocketDesignation>
<Manufacturer>Intel</Manufacturer>
<Model>
<Version>Intel(R) Xeon(R) CPU E3-1270 v3 @ 3.50GHz</Version>

```



```

<BrandName>Intel (R) Xeon (R) CPU E3-1270 v3 @ 3.50GHz</BrandName>
</Model>
<Speed>3500</Speed>
<Status Description="ok">1</Status>
<CoreNumber>4</CoreNumber>
<LogicalCpuNumber>8</LogicalCpuNumber>
<Level1CacheSize Unit="KByte">256</Level1CacheSize>
<Level2CacheSize Unit="KByte">1024</Level2CacheSize>
<Level3CacheSize Unit="KByte">8192</Level3CacheSize>
</CPU>
</Processor>

```

### 7.2.3.4 Memory セクション

生成された情報は、メモリ SPD データをデコードし、メモリ状態とコンフィグレーションセンサを評価して取得されます。CDiagReport.h 実装に準拠しています。

```

<Memory Schema="2">
<Modules Count="4">
<Module Name="DIMM-2A" CSS="true">
<Status Description="empty">0</Status>
</Module>
<Module Name="DIMM-1A" CSS="true">
<Status Description="ok">1</Status>
<Approved>>false</Approved>
<Size Unit="GByte">2</Size>
<Type>DDR3</Type>
<BusFrequency Unit="MHz">1600</BusFrequency>
<SPD Size="256" Revision="1.2" Checksum="true">
<Checksum>
<Data>33879</Data>
<Calculated>33879</Calculated>
</Checksum>
<ModuleManufacturer>SK Hynix</ModuleManufacturer>
<ModuleManufacturingDate>2013,4</ModuleManufacturing Date>
<ModulePartNumber>HMT325U7EFR8A-PB </ModulePartNumber>
<ModuleRevisionCode>12372</ModuleRevisionCode>
<ModuleSerialNumber
AsString="4C633E39">1281572409</ModuleSerialNumber>
<ModuleType>UDIMM</ModuleType>
<DeviceType>DDR3_SDRAM</DeviceType>
<DeviceTechnology>256Mx8/15x10x3</DeviceTechnology>

```

```
<BufferedRegistered>None</BufferedRegistered>
<BusFrequency Unit="MHz">DDR1600</BusFrequency>
<VoltageInterface>1.35V/1.5V</VoltageInterface>
<BurstLengths>8;(4);</BurstLengths>
<CASLatencies>6;7;8;9;10;11;</CASLatencies>
<DataWith>72</DataWith>
</SPD>
<ConfigStatus Description="Normal">0</ConfigStatus>
</Module>
```

### 7.2.3.5 Fans セクション

ファンのデータはファンセンサから取得および生成され、CDiagReport.h 実装に準拠しています。

```
<Fans Schema="1" Count="2">
<Fan Name="FAN1 SYS" CSS="true">
<Status Description="not manageable">5</Status>
</Fan>
<Fan Name="FAN PSU" CSS="false">
<Status Description="not manageable">5</Status>
</Fan>
</Fans>
```

### 7.2.3.6 Temperature セクション

生成された情報は CDiagReport.h 実装に準拠しています。

```
<Temperatures Schema="1" Count="7">
<Temperature Name="Ambient" CSS="false">
<Status Description="ok">6</Status>
<CurrValue>27</CurrValue>
<WarningThreshold>37</WarningThreshold>
<CriticalThreshold>42</CriticalThreshold>
</Temperature>
<Temperature Name="Systemboard" CSS="false">
<Status Description="ok">6</Status>
<CurrValue>37</CurrValue>
<WarningThreshold>60</WarningThreshold>
<CriticalThreshold>65</CriticalThreshold>
</Temperature>
```

### 7.2.3.7 PowerSupplies セクション

生成された情報は CDiagReport.h 実装に準拠しています。

```
<PowerSupplies Schema="1" Count="1">  
<PowerSupply Name="PSU" CSS="false">  
<Status Description="ok">1</Status>  
</PowerSupply>  
</PowerSupplies>
```

### 7.2.3.8 Voltages セクション

生成された情報は CDiagReport.h 実装に準拠しています。

```
<Voltages Schema="1" Count="11">  
<Voltage Name="BATT 3.0V" CSS="false">  
<Status Description="ok">1</Status>  
<CurrValue>3.24</CurrValue>  
<NomValue>3.00</NomValue>  
<Thresholds>  
<MinValue>2.02</MinValue>  
<MaxValue>3.50</MaxValue>  
</Thresholds>  
</Voltage>
```

### 7.2.3.9 IDPROM セクション

生成された情報は CDiagReport.h 実装に準拠しています。さらに、FRU SDR レコードから取得される実際の名前は、インスタスタグの「Name」属性として提供されます。

エントリは非常に長いので、例として生成されたファイルを確認してください。

### 7.2.3.10 SensorDataRecords セクション

生成された情報は CDiagReport.h 実装に準拠しています。

エントリは非常に長いので、例として生成されたファイルを確認してください。

### 7.2.3.11 PCIDevices セクション

iRMC は PCI データに直接アクセスできないため、限定的な情報のサブセットしか報告できません。この情報は、SB の BIOS が F119 OEM IPMI コマンドで送信した内容と、F11A OEM IPMI コマンドで取得できる内容に基づきます。

```
<PCIDevices Schema="1">
<Device>
<ConfigSpace>
<VendorId>1000</VendorId>
<DeviceId>005B</DeviceId>
<SubVendorId>11D3</SubVendorId>
<SubDeviceId>1734</SubDeviceId>
<BaseClass>Mass storage controller</BaseClass>
<SubClass>RAID controller</SubClass>
</ConfigSpace>
<Slot>4</Slot>
</Device>
</PCIDevices>
```

### 7.2.3.12 SystemEventLog セクション

生成された情報は CDiagReport.h 実装に準拠しています。

```
<SystemEventlog Schema="1">
<Entry>
<Date>2014/02/05 16:48:13</Date>
<Severity>MINOR</Severity>
<ErrorCode>19000B</ErrorCode>
<Message>'DIMM-1B': Non Fujitsu Memory Module detected -
Warranty restricted!</Message>
<Data Size="14">
<HexDump Lines="1" BytesPerLine="14">
<Line Offset="0">
<Hex>02 4D 6B F2 52 20 00 04 E1 FE 6F A0 00 03</Hex>
</Line>
</HexDump>
</Data>
</Entry>
```

### 7.2.3.13 InternalEventLog セクション

生成された情報は CDiagReport.h 実装に準拠しています。

```
<InternalEventlog Schema="1">
<Entry>
<Date>2014/02/05 15:53:00</Date>
<Severity>INFO</Severity>
<ErrorCode>2300B1</ErrorCode>
<Message>iRMC Browser http connection user 'admin' login from
10.172.103.28</Message>
</Entry>
```

### 7.2.3.14 BootStatus セクション

生成された情報は CDiagReport.h 実装に準拠しています。

```
<BootStatus Schema="1">
<PowerOnReason AsString="Power Switch">1</PowerOnReason>
<PowerOffReason AsString="Software">0</PowerOffReason>
<PowerFailBehavior AsString="remain off">1</PowerFailBehavior>
</BootStatus>
```

### 7.2.3.15 ManagementControllers セクション

ホストする iRMC についての情報のみが提供されます。

```
<ManagementControllers Schema="1">
<iRMC Name="iRMC">
<Firmware>97.30F</Firmware>
<IPAddress>10.172.103.13</IPAddress>
<IPSubnetMask>255.255.255.0</IPSubnetMask>
<IPGateway>10.172.103.1</IPGateway>
<MACAddress>00-19-99-FD-AF-9F</MACAddress>
<ManagementLANPort>0</ManagementLANPort>
<IPNominalSpeed>0</IPNominalSpeed>
</iRMC>
</ManagementControllers>
```

### 7.2.3.16 Settings セクション

使用されるネットワーク設定の情報を提供します。

```
<Settings Schema="1"></Settings>
```

### 7.2.3.17 Adapters セクション

使用されるネットワークアダプタの情報を提供します。

```
<Adapters Schema="1">
  <Adapter Index="0">
    <Name>{14C6F7A0-A9F9-4655-821A-2EF42F98581A}</Name>
    <Description>Intel(R) I210 Gigabit Network
Connection</Description>
    <Type>N/A</Type>
    <DHCP>true</DHCP>
    <MACAddress>00-19-99-FF-E0-5A</MACAddress>
    <ConnectionName>Local Area Connection</ConnectionName>
  </Adapter>
  ...
</Adapters>
```

### 7.2.3.18 Interfaces セクション

使用されるネットワークインターフェースの情報を提供します。

```
<Interfaces Schema="1">
  <Interface Index="0" IfIndexV4="1" IfIndexV6="1">
    <Type>24</Type>
    <Description>Software Loopback Interface 1</Description>
    <IPConfig>
      <Entry Index="0">
        <IPAddress>127.0.0.1</IPAddress>
        <IPAddressType>N/A</IPAddressType>
        <IPSubnetMask>255.0.0.0</IPSubnetMask>
        <IPGateway>172.17.118.1</IPGateway>
      </Entry>
    <Gateways>
      <Entry Index="0">
        <IPGateway>172.17.118.1</IPGateway>
      </Entry>
    </Gateways>
  </IPConfig>
```

```

    <IPV6Config>
    <Addresses>
    <Address Index="0">
    <Unicast>::1</Unicast>
    <Type>N/A</Type>
    </Address>
    </Addresses>
  </IPV6Config>
</Interface>
...
</Interfaces>

```

### 7.2.3.19 Ports セクション

使用されるネットワークポートの情報を提供します。

```
<Ports Schema="1"></Ports>
```

### 7.2.3.20 SNMPAgents セクション

実行中の SNMP エージェントの情報を提供します。

```

<SNMPAgents Schema="1">
  <ProductVersion>N/A</ProductVersion>
</SNMPAgents>

```

### 7.2.3.21 ServerViewRaid セクション

RAID がネットワークで使用されている場合に情報を提供します。

```

<ServerViewRaid Schema="1" Installed="true">
<Version></Version>
<amEMSV Version="2" ReadSocket="permanent">
<System Name="SW1-RX2520M1-1">
<Name>SW1-RX2520M1-1</Name>
<Vendor></Vendor>
<OSProduct>Windows Server 2008 R2 Enterprise (x64)</OSProduct>
<OSEdition></OSEdition>
<Version></Version>
<OSServicePack></OSServicePack>
<Build></Build>
<OSFeatures></OSFeatures>
<ProcArchitecture></ProcArchitecture>
<CAS></CAS>

```

```
<LDAP></LDAP>
<Adapter Nr="0" Type="SAS" Name="LSI MegaRAID SAS 9286CV-8e (0)"
NumberOfPorts="8" RealPortCount="2">
<AdapterNumber>0</AdapterNumber>
<Name>LSI MegaRAID SAS 9286CV-8e (0)</Name>
<Vendor>LSI Logic</Vendor>
<Product>LSI MegaRAID SAS 9286CV-8e</Product>
<SerialNumber>SV225P2245</SerialNumber>
<SASAddress>0x500605B00502AC00</SASAddress>
<PortCount>8</PortCount>
<PCIBus></PCIBus>
<PCIDevice></PCIDevice>
<PCIFunction></PCIFunction>
<DriverName>megasas2.sys</DriverName>
<DriverVersion>6.706.06.00</DriverVersion>
<UEFIDriverVersion></UEFIDriverVersion>
<Protocol>SAS600</Protocol>
<FWPackageVersion>23.34.0-0007</FWPackageVersion>
<FirmwareVersion></FirmwareVersion>
<FirmwareBuildTime></FirmwareBuildTime>
<BIOSVersion></BIOSVersion>
<BIOSBuildTime></BIOSBuildTime>
<MemorySize>1024</MemorySize>
<FlashROMSize>16</FlashROMSize>
<AlarmPresent>>true</AlarmPresent>
<NVRAMPresent>>true</NVRAMPresent>
<NVRAMSize>32</NVRAMSize>
<CorrErrorCount>0</CorrErrorCount>
<UncorrErrorCount>0</UncorrErrorCount>
<Activity>Idle</Activity>
<InconsistPolicy>Make Data Consistent</InconsistPolicy>
<SMARTSupport>Enabled</SMARTSupport>
<PollingInterval minValue="1" maxValue="65535"
stepping="1">300</PollingInterval>
<PatrolReadMode>Automatic</PatrolReadMode>
<PatrolReadMaxPD minValue="0" maxValue="255"
stepping="1">255</PatrolReadMaxPD>
<ContinuousPatrolling>No</ContinuousPatrolling>
<PatrolReadDelay minValue="4" maxValue="1016"
stepping="4">168</PatrolReadDelay>
<PatrolRdIterations>5</PatrolRdIterations>
```



```
<PatrolReadRate minValue="0" maxValue="100"
stepping="1">20</PatrolReadRate>
<AlarmControl>Disabled</AlarmControl>
<RebuildRate minValue="0" maxValue="100"
stepping="1">30</RebuildRate>
<BGIRate minValue="0" maxValue="100" stepping="1">30</BGIRate>
<MDCRate minValue="0" maxValue="100" stepping="1">30</MDCRate>
<MigrationRate minValue="0" maxValue="100"
stepping="1">30</MigrationRate>
<AutoFlushFreq minValue="0" maxValue="100"
stepping="1">4</AutoFlushFreq>
<DelayBetweenSpins minValue="0" maxValue="6"
stepping="1">6</DelayBetweenSpins>
<DevicesPerSpins minValue="1" maxValue="8"
stepping="1">2</DevicesPerSpins>
<AutoRebuild>Enabled</AutoRebuild>
<CoercionMode>None</CoercionMode>
<AbortMDCOnError>Disabled</AbortMDCOnError>
<InitMode>Normal Initialization</InitMode>
<BootLogDriveNumber minValue="-1" maxValue="63"
stepping="1">0</BootLogDriveNumber>
<CopyBack>Enabled</CopyBack>
<CopybackOnSMARTError>Enabled</CopybackOnSMARTError>
<CorrectMediaErrorsPR>Enabled</CorrectMediaErrorsPR>
<CopybackSSDPnSMARTErr>Enabled</CopybackSSDPnSMARTErr>
<PRonSSD>Disabled</PRonSSD>
<SpindownUnconfDisks>Enabled</SpindownUnconfDisks>
<SpindownHotSpare>Enabled</SpindownHotSpare>
<SpndownDelayTime minValue="30" maxValue="1440"
stepping="1">30</SpndownDelayTime>
<MDCScheduleMode>Disabled</MDCScheduleMode>
<NCQ>Enabled</NCQ>
<Status>Degraded</Status>
<DeviceID>005B</DeviceID>
<SubDeviceID>9291</SubDeviceID>
<VendorID>1000</VendorID>
<SubVendorID>1000</SubVendorID>
<BusType>PCIe</BusType>
<MaxLogDrives>64</MaxLogDrives>
<MaxPhysDevices>256</MaxPhysDevices>
<BBUPresent>>false</BBUPresent>
```

```
<UARTPresent>true</UARTPresent>
<LogicalDrive LogDriveNumber="0" Name="LogicalDrive_0">
  <LogDriveNumber>0</LogDriveNumber>
  <LogicalSize>2092320</LogicalSize>
  <PhysicalSize>2371296</PhysicalSize>
  <RAIDLevel>RAID-6</RAIDLevel>
  <Stripesize>64K</Stripesize>
  <Name>LogicalDrive_0</Name>
  <InitState>Initialized</InitState>
  <WriteMode>Write-through</WriteMode>
  <ReadMode>No read-ahead</ReadMode>
  <CacheMode>Direct</CacheMode>
  <AccessMode>Read write</AccessMode>
  <DefaultWriteMode>Write-through</DefaultWriteMode>
  <DefaultReadMode>No read-ahead</DefaultReadMode>
  <DefaultCacheMode>Direct</DefaultCacheMode>
  <DiskCacheMode>Disabled</DiskCacheMode>
  <Status>Partially degraded</Status>
  <Activity>Idle</Activity>
  <OSDevice></OSDevice>
</LogicalDrive>
<Ports Number="2">
  <Port Nr="0" Type="SAS" Name="Port B">
    <Name>Port B</Name>
    <Enclosure Name="FUJITSU ETERNUS JX40 (1)">
      <EnclosureNumber>1</EnclosureNumber>
      <Vendor>FUJITSU</Vendor>
      <Product>ETERNUS JX40</Product>
      <HardwareVersion>0206</HardwareVersion>
      <Name>FUJITSU ETERNUS JX40 (1)</Name>
      <Status>OK</Status>
      <SASAddress>0x500000E0D38027FE</SASAddress>
      <Processor Name="FUJITSU JX40 (1:1)">
        <PortNumber>0</PortNumber>
        <DeviceNumber>60</DeviceNumber>
        <EnclosureNumber>1</EnclosureNumber>
        <Name>FUJITSU JX40 (1:1)</Name>
        <Type>SES</Type>
        <Vendor>FUJITSU</Vendor>
        <Product>JX40</Product>
```

```
<SerialNumber>WK12090174</SerialNumber>
<PartNumber>CA07217-C871</PartNumber>
<HardwareVersion>AA </HardwareVersion>
<FirmwareVersion>V02L06</FirmwareVersion>
<Status>OK</Status>
<Fan Name="FAN0 PSU0 (0) ">
<Name>FAN0 PSU0 (0)</Name>
<Location>PSU0</Location>
<FanSpeed>Low</FanSpeed>
<Status>OK</Status>
</Fan>
...
<PowerSupply Name="PSU0 (0) ">
<PartNumber>CA05954-1100</PartNumber>
<SerialNumber>FA09350317</SerialNumber>
<HardwareVersion>08C 0</HardwareVersion>
<Status>OK</Status>
<Name>PSU0 (0)</Name>
</PowerSupply>
...
<TemperatureSensor Name="Sensor (0) ">
<Name>Sensor (0)</Name>
<Location>LED panel</Location>
<WarningTemperatureH>45</WarningTemperatureH>
<Status>OK</Status>
<Temperature>24</Temperature>
</TemperatureSensor>
...
</Processor>
<PhysicalDrive DeviceNumber="67" Name="SEAGATE ST9146803SS
(1:1)" DeviceStatus="0" ComponentStatus="1">
<PortNumber>0</PortNumber>
<Name>SEAGATE ST9146803SS (1:1)</Name>
<Vendor>SEAGATE</Vendor>
<Product>ST9146803SS</Product>
<Type>SAS</Type>
<FirmwareVersion>3104</FirmwareVersion>
<SerialNumber>3SD1JDVN</SerialNumber>
<SASAddress>0x5000C50017284209</SASAddress>
<TransferSpeed>600</TransferSpeed>
<TransferWidth>1</TransferWidth>
```

```
<RPM>10.0</RPM>
<DeviceNumber>67</DeviceNumber>
<Slot>1</Slot>
<EnclosureNumber>1</EnclosureNumber>
<PhysicalSize>140014</PhysicalSize>
<ConfigurableSize>139488</ConfigurableSize>
<Status>Operational</Status>
<Activity>Idle</Activity>
<ForeignConfig>>false</ForeignConfig>
<MediaErrorCount>0</MediaErrorCount>
<MiscErrors>0</MiscErrors>
<PFACount>0</PFACount>
<MediaType>HDD</MediaType>
<PowerStatus>Active</PowerStatus>
<Temperature>27</Temperature>
</PhysicalDrive>

</Enclosure>
</Port>
...
</Ports>
</Adapter>
<Multiplexer>
<Status>Operational</Status>
<StatusOverall>Warning</StatusOverall>
<StatusAdapters>Warning</StatusAdapters>
<StatusLogicalDrives>Warning</StatusLogicalDrives>
<StatusDisks>OK</StatusDisks>
</Multiplexer>
</System>
</amEMSV>
</ServerViewRaid>
```