ユーザーガイド – 日本語

FUJITSU Server PRIMERGY CX1430 M1 BMC ユーザーガイド

2018 年 4 月

著作権および商標

お届けまでの日数は在庫状況によって異なります。技術的修正の権利を有します。

使用されているハードウェア名およびソフトウェア名は、各社の商標です。

– 本書の内容は、改善のため事前連絡なしに変更することがあります。

– 本書に記載されたデータの使用に起因する、第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。

– 無断転載を禁じます。

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

Intel、インテルおよび Xeon は、米国およびその他の国における Intel Corporation またはその子会社の商標または登録商標です。

本書をお読みになる前に

安全にお使いいただくために

本書には、本製品を安全に正しくお使いいただくための重要な情報が記載されています。

本製品をお使いになる前に、本書を熟読してください。特に、添付の『安全上のご注意』をよくお読みになり、理解されたうえで本製品をお使いください。また、『安全上のご注意』および当マニュアルは、本製品の使用中にいつでもご覧になれるよう大切に保管してください。

電波障害対策について

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

アルミ電解コンデンサについて

本製品のプリント板ユニットやマウス、キーボードに使用しているアルミ電解コンデンサは寿命部品であり、寿命が尽きた状態で使用し続けると、電解液の漏れや枯渇が生じ、異臭の発生や発煙の原因になる場合があります。

目安として、通常のオフィス環境（25 ℃）で使用された場合には、保守サポート期間内（5 年）には寿命に至らないものと想定していますが、高温環境下での稼働等、お客様のご使用環境によっては、より短期間で寿命に至る場合があります。寿命を超えた部品について、交換が可能な場合は、有償にて対応させていただきます。なお、上記はあくまで目安であり、保守サポート期間内に故障しないことをお約束するものではありません。

ハイセイフティ用途での使用について

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用等の一般的用途を想定して設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療器具、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう設計・製造されたものではございません。お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本製品を使用しないでください。ハイセイフティ用途に使用される場合は、弊社の担当営業までご相談ください。

瞬時電圧低下対策について

本製品は、落雷などによる電源の瞬時電圧低下に対し不都合が生じることがあります。電源の瞬時電圧低下対策としては、交流無停電電源装置などを使用されることをお勧めします。

（社団法人電子情報技術産業協会 (JEITA) のパーソナルコンピュータの瞬時電圧低下対策ガイドラインに基づく表示）

外国為替及び外国貿易法に基づく特定技術について

当社のドキュメントには「外国為替及び外国貿易法」に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

高調波電流規格について

本製品は、高調波電流規格 JIS C 61000-3-2 適合品です。

日本市場の場合のみ：
SATA ハードディスクドライブについて

このサーバの SATA バージョンは、SATA/BC-SATA ストレージインタフェースを搭載したハードディスクドライブをサポートしています。ご使用のハードディスクドライブのタイプによって使用方法と動作条件が異なりますので、ご注意ください。

使用できるタイプのハードディスクドライブの使用方法と動作条件の詳細は、以下の Web サイトを参照してください。

http://jp.fujitsu.com/platform/server/primergy/harddisk/

目次

目次

1 はじめに

本装置は、サーバをシステムのステータスに関係なく包括的に制御する機能を提供する中央システムコントローラ（Baseboard Management Controller - BMC) を搭載しています。

BMC にはサーバへのリモートアクセスを実現するソフトウェア Megarac SP-X が搭載されており、IPMI (Intelligence Platform Management Interface) に基づいたサーバ管理を行うことができます。

Megarac SP-X は Web ベースの GUI も提供しており、システム管理者はシステムの状態監視やコンピュータイベントの管理をリモートから容易に行うことができます。

表記規定

このマニュアルで使用されているフォントや記号の意味は、以下のとおりです。

斜体のテキスト	コマンドまたはメニューアイテムを示します。
かぎ括弧（「 」）	章の名前や強調されている用語を示します。
二重かぎ括弧（『 』）	他のマニュアル名などを示しています。
 **注意！**	この記号が付いている文章には、特に注意してください。この表示を無視して、誤った取り扱いをすると、生命が危険にさらされたり、システムが破壊されたり、データが失われる可能性があります。
	追加情報、注記、ヒントを示しています。

2 Megarac SP-X Web GUI (Graphic User Interface)

BMC ファームウェアには組み込み Web サーバ機能があり、ユーザーは Web ブラウザ（Microsoft Internet Explorer など）を使用して BMC に接続できます。

Web GUI には、管理中のサーバのシステム情報、システムイベント、システムステータス、およびその他のシステム関連の情報が表示されます。Web ベースの GUI は以下のブラウザでサポートされます。

サポートブラウザ:

– Google Chrome (latest version)

– Internet Explorer 11 以降

– Firefox (latest version) [制限有]

Firefoxはメモリ制限があるため、Remote ControlのKVM機能をご使用の際には、Google ChromeまたはInternet Explorerのご使用を推奨します。

クライアントのシステム用件:

– メモリ 8GB

メモリがシステム用件を満たさない場合、Remote ControlのKVM機能でラグが発生したり、Image Redirection機能が正しく動作しない場合があります。

2.1 ログイン

IP アドレスまたは URL（デフォルト DHCP 静的 \IP アドレス）を Web ブラウザのアドレスバーに入力します。

BMC に接続すると、ログイン画面が表示され、ユーザー名とパスワードの入力が求められます。SSL で保護されたこの認証は、認証されていない侵入者が BMC Web サーバにアクセスするのを防ぎます。

ユーザー認証されると、役割の権限に従って、サーバを管理できます。

Administrator、Operator 権限レベルには、Web インターフェースにログインする権限があります。User および No Access 権限レベルでは、BMC Web GUI を通じてアクセスできません。

権限レベル

- Administrator ：全てのコマンドを実行することができます。Web GUIでは全ての機能をご使用いただけます。
- Operator ：アウトオブバンドインターフェースの挙動に影響のあるコマンド以外のコマンドが実行できます。Web GUIではSensorや Logs&Reportsなどの閲覧機能のみ使用できます。
- User ：限られたBMCコマンドのみ実行できます。
- No Access ：BMCへのアクセス権限はありません。

ログイン Web ページ

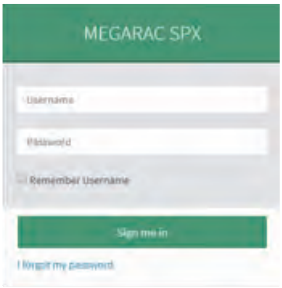

図 1: ログイン画面

フィールド	デフォルト
Username	admin
Password	admin

表 1: デフォルトユーザー名とパスワード

ログイン後1800秒間アクセスが無い場合、自動でWeb GUIからログアウトされます。
ログアウト後サイドログインできない場合には、ご使用のブラウザのキャッシュと履歴を削除の上、再度ログインをお試しください。

2.2 ユーザーインターフェースの構造

BMC Web インターフェースの構造を以下に示します。

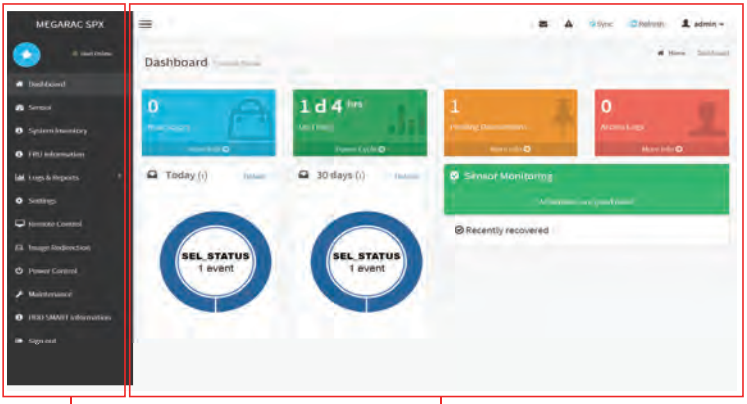

図 2: BMC Web インターフェースの構造

メニューバー

メニューバーには、BMC の個々のファンクションがあります。

ログイン時には "Dashboard" が選択されています。

ワークエリア

メニューバーからファンクションをクリックすると、そのリンクが有効になり、そのファンクションのワークエリアが表示され、任意の出力、ダイアログボックス、オプション、リンクおよびボタンが表示されます。

ログイン時は Dashboard のワークエリアが表示されています。

前画面に戻る場合には、ブラウザの戻るボタンは使わないようご注意ください。
WebGUIからログアウトしてしまう場合がございます。

2.3 Dashboard

このページには、デバイスのステータスに関する情報全般が表示されます。

New Scripts: Automation Engine のページを表示します。（この機能はサポートしていません）

Up Time: Power Control ページを表示します。

Pending Deassertions: Event Log ページに移動します。

Access Logs: さまざまなセンサおよび占有 / 使用可能スペースによって発生したすべてのイベントが、ログにグラフィカルに表示されます。また Audit Log ページを表示できます。

Today and 30 days (Event Logs)：このデバイスのさまざまなセンサによって発生した Event Log の一覧を表示します。

Sensor Monitoring：デバイス上のすべての重要なセンサを一覧表示します。

図 3: Dashboard ページ

2.3.1 Up Time

ワークエリアの「Up Time」メニューから「Power Cycle」をクリックすると、「Power Control」ページが表示されます。

（詳細は 66 ページ の「Power Control」の項を参照。）

2.3.2 Pending Deassertion

このデバイスの各種センサで発生したイベントログのリストがこのページに表示されます。

ワークエリアの「Pending Deassertions」メニューから「More info」をクリックすると、「Event Log」ページが表示されます。（詳細は 19 ページ の「Logs&Reports」の項を参照）。

2.3.3 Access Log

ワークエリアの「Access Logs」メニューから「More info」をクリックすると、「Audit Log」ページが表示されます。

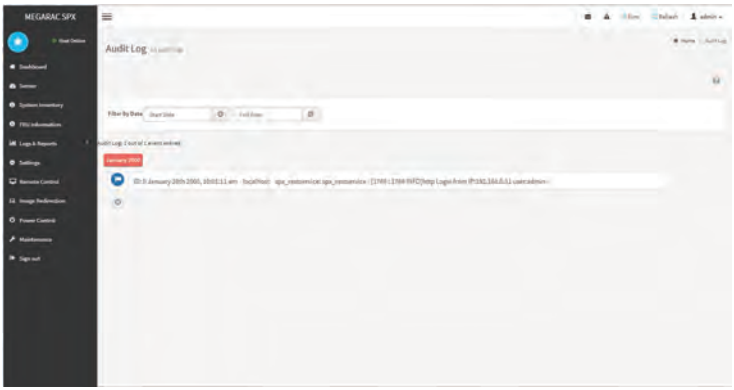

図 4: Audit Log ページ

「Audit Log」ページのフィールドについて説明します。

アイテム		説明
Filter by Date	Start Date	監査ログの開始日を選択します。
	End Date	監査ログの終了日を選択します。

表 2: Audit Log

手順：

1. 「Filter by Date」のドロップダウンリストから監査ログの開始日および終了日を選択します。

2.4 Sensor

2.4.1 Sensor Reading

「Sensor Readings」ページにセンサ関連のすべての情報が表示されます。

注意！

動作項目の説明

センサの読み取りが変化している間は、それに応じてドットが生成されます。青色のグラフは、このセンサの読み取り値が頻繁に変化することを意味します。代わりにドット / グラフが無いことはセンサの読み取りが安定していることを意味します。すべてのセンサの動作は整合性が取れています。

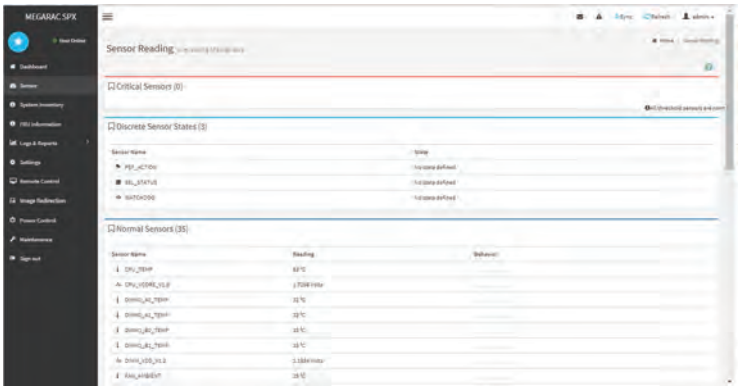

図 5: Sensor Reading ページ

2.4.2 Sensor detail

Critical Sensor または Normal Sensor のリストから特定のセンサを選択すると、「Sensor detail」ページが表示されます。

選択したセンサのセンサ情報（ライブウィジェット）としきい値が以下のように表示されます。

図 6: Sensor detail ページ

画面の右側にセンサのしきい値が表示されます。

以下の合計 6 つのしきい値があります。

– Upper Non-Recoverable（回復不可能な状態になる上限）
– Upper Critical（重大な状態の上限）
– Upper Non-Critical（重大でない状態の上限）
– Lower Non-Critical（重大でない状態の下限）
– Lower Critical（重大な状態の下限）
– Lower Non-Recoverable（回復不可能な状態になる下限）

一部のセンサーはグラフが表示されません。

2.5 System Inventory

このページには、サーバで使用されているコンポーネントが表示され、カーソルを合わせることで、各コンポーネントのベンダー名、モデル、およびソフトウェアバージョンなどの詳細情報を確認できます。

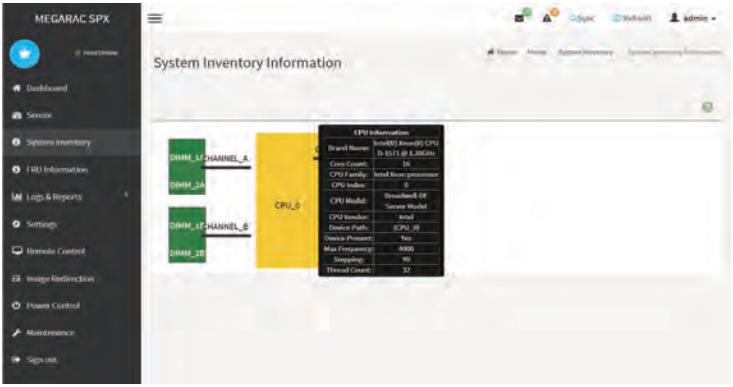

図 7: System Inventory ページ

2.6 FRU Information

このページには、BMC の FRU デバイスの情報が表示されます。

FRU ページには、「Available FRU Device」、「Chassis Information」、「Board Information」、「Product Information」などの情報が表示されます。

「Available FRU Device」セクションの「FRU Device ID」を選択すると、選択したデバイスの詳細が表示されます。

「FRU Information」ページのスクリーンショットを次に示します。

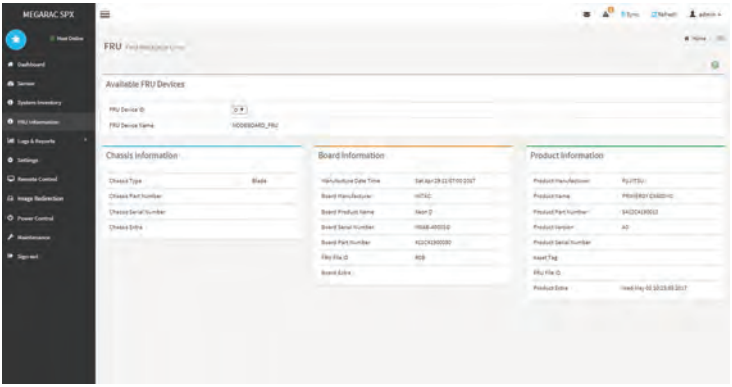

図 8: FRU Information ページ

次の項で各フィールドについて簡単に説明します。

2.6.1 Available FRU Device

アイテム	説明
FRU device ID	デバイスの ID。
FRU Device Name	選択した FRU デバイスのデバイス名。
Chassis Information	選択した FRU デバイスのChassis Information。
Board Information	選択した FRU デバイスのBoard Information。
Product Information	選択した FRU デバイスのProduct Information。

表 3: Available FRU Device

2.6.2 Chassis Information

- Chassis Type : シャーシのタイプ
- Chassis Part Number : シャーシの部品図番
- Chassis Serial Number : シャーシのシリアル番号
- Chassis Extra : シャーシの追加情報

2.6.3 Board Information

- Manufacture Date Time : ボードの製造日時
- Board Manufacturer : ボードの製造ベンダー
- Board Product Name : ボードの製品名
- Board Serial Number : ボードのシリアル番号
- Board Part Number : ボードの部品図番
- FRU File ID : ボードのFRUフィールドID
- Board Extra : ボードの追加情報

2.6.4 Product Information

- Product Manufacturer Name : 製品の製造ベンダー
- Product Name : 製品名
- Product Part Number : 製品の部品図番
- Product Version : 製品の版数
- Product Serial Number : 製品のシリアル番号
- Asset Tag : 資産タグ
- FRU File ID : 製品のFRUフィールドID
- Product Extra : 製品の製造日時

2.7 Logs&Reports

2.7.1 IPMI Event Log

このデバイスの各種センサで発生したイベントログのリストがこのページに表示されます。

メニューバーの「Logs&Reports」から「IPMI Event Log」を選択すると、「Event Log」ページが表示されます。

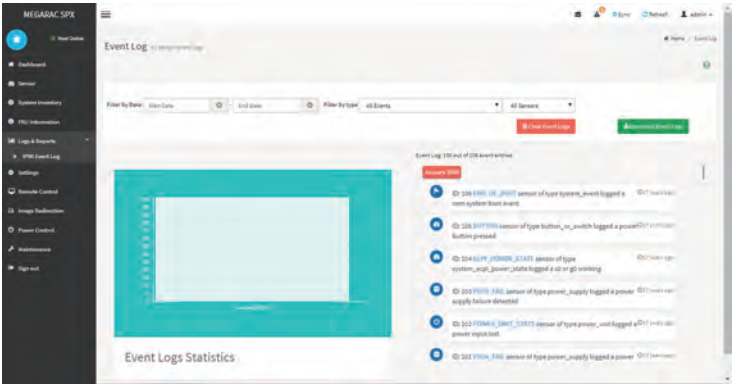

図 9: Event Log ページ

「Event Log」ページのフィールドについて説明します。

アイテム		説明
Filter by Date	Start Date	イベントログの開始日を選択します。
	End Date	イベントログの終了日を選択します。
Filter by Type	All Events	フィルタのタイプを選択します。
	All Sensors	センサのタイプを選択します。
Clear Event Logs		イベントログを削除します。
Download Event Logs		イベントログをダウンロードします。

表 4: Event Log Category

手順

1. 「Filter by Date」のドロップダウンリストからイベントログの開始日および終了日を選択します。
2. 「Filter by Type」のドロップダウンリストからフィルタとセンサのタイプを選択します。
3. リストからイベントを削除するには、「Clear Event Logs」ボタンをクリックします。
4. リストからイベントをダウンロードするには、「Download Event Logs」ボタンをクリックします。

2.8 Settings

このページのグループ毎に、さまざまなコンフィグレーション設定が可能です。

設定ページには「Media Redirection Settings」、「Network Settings」、「Platform Event Filter」、「SMTP Settings」 、 「SSL Settings」 「User Management」があります。

図 10: Settings ページ

2.8.1 Media Redirection Settings

このページを使用して、リダイレクト用に BMC にメディアを設定します。

Media Redirection ページには「General Settings」、「VMedia Instance Settings」、「Remote Session」設定があります。

図 11: Media Redirection ページ

2.8.1.1 General Settings

このページを使用して、ネットワーク上の共有フォルダに置かれた仮想メディアファイルを読み込ませる設定を行います。

CD / DVD メディアの場合、ISO / NRG ファイル形式がサポートされています。

フロッピー / ハードディスクの場合、img / ima ファイル形式がサポートされています。

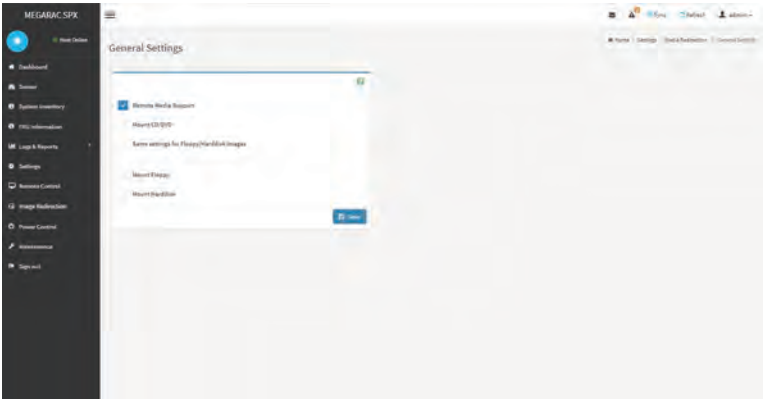

図 12: General Settings ページ

「General Settings」ページのフィールドについて説明します。

アイテム	説明
Remote Media Support	このオプションにチェックを入れると仮想メディアファイルの項目が表れます。
Mount CD/DVD	CD/DVD をマウントします。
Same settings for Floppy/Harddisk Images	チェックすると Floppy, Harddisk に同様の設定が反映されます（個別設定が不要です）。
Mount Floppy	Floppy をマウントします。
Mount Harddisk	Harddisk をマウントします。
Save	設定を保存します。

表 5: General Settings

手順 （CD/DVD の場合）

1. 「Remote Media Support」オプションにチェックを入れると、仮想メディアデバイスの項目が表示されます。
2. 「Mount CD/DVD」オプションにチェックを入れると、ネットワークファイル共有設定項目が表示されます。（Floppy, Harddisk を選択した場合も同じ項目が表示されます。）

図 13: ネットワークファイル共有設定項目

3. 「Server Address for CD/DVD Images」フィールドにリモートメディアの仮想メディアファイルが置かれたサーバの Address を指定します。
4. 「Path in server」フィールドに上記サーバで仮想メディアファイルが置かれたパスを指定します。
5. 「Share Type for CD/DVD」項目でネットワークファイルシステム (nfs/cifs) の選択をします。
6. 「Username, Password and Domain Name」の各フィールドに上記サーバの共有フォルダに接続するための認証情報 (Domain はオプション) を入力します。
7. 「Same settings for Floppy/Harddisk Images」オプションにチェックを入れると、Floppy, Harddisk に同様の設定が反映されます。（個別設定が不要です。）
8. 設定完了後、「Save」をクリックして設定を保存します。

2.8.1.2 VMedia Instance Settings

このページを使用して、仮想メディアデバイス設定を行います。

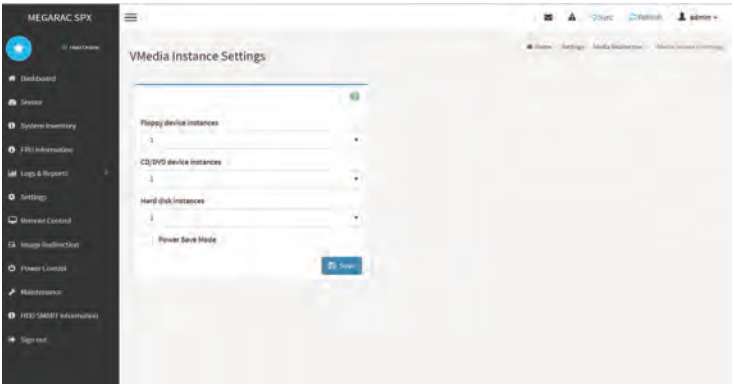

図 14: VMedia Instance Settings ページ

「Vmedia Instance Settings」ページのフィールドについて説明します。

アイテム	説明
Floppy device instances	仮想メディアリダイレクションをサポートするフロッピーデバイスの数。
CD/DVD device instances	仮想メディアリダイレクションをサポートする CD/DVD デバイスの数。
Hard disk instances	仮想メディアリダイレクションをサポートするハードディスクデバイスの数。
Power Save Mode	Power Save Mode の有効 / 無効を選択します。
Save	構成した設定を保存します。

表 6: VMedia Instance Setting

手順

1. フロッピーデバイス、CD/DVD デバイス、ハードディスクデバイスの数をドロップダウンリストから選択します。
2. 必要に応じて「Power Save Mode」を有効にします。
3. 「Save」をクリックして行った変更を保存します。

2.8.1.3 Remote Session

このページを使用して、次のリダイレクトセッションの仮想メディア構成を設定します。

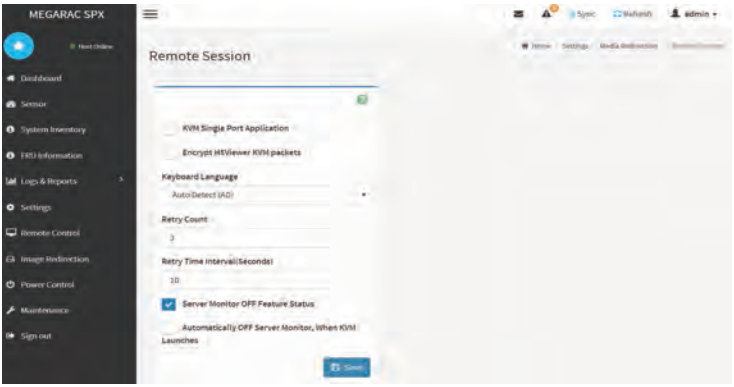

図 15: Remote Session ページ

「Remote Session」ページのフィールドについて説明します。

アイテム	説明
KVM Single Port Application	KVM シングルポートアプリケーションを有効 / 無効にします。
Encrypt H5Viewer KVM packets	H5Viewer (HTML5 クライアント) での KVM パケットを暗号化します。（KVM シングルポートアプリケーションが無効時のみ表示）
Keyboard Language	キーボードの言語を選択します。
Retry Count	リトライ回数を表示します。
Retry Time Interval (Seconds)	リトライ間隔（秒）を表示します。
Save Monitor OFF Feature Status	サーバのモニター OFF 機能ステータスを有効 / 無効にします。
Automatically OFF Server Monitor, When KVM Launches	「KVM が起動すると、サーバモニタを自動的に OFF にする」を有効 / 無効にします。
Save	現在の変更を保存します。

表 7: Remote Session

手順

1. 「KVM Single Port Application」項目にチェックを入れて有効にします。
2. 「Keyboard Language」で、キーボードの言語を選択します。
3. 「Save Monitor OFF Feature Status」項目にチェックを入れて有効にします。
4. 「Automatically OFF Server Monitor, When KVM Launches」項目にチェックを入れず無効にします
5. 「Save」をクリックするとエントリが保存されます。

2.8.2 Network Settings

このページを使用して、使用可能な LAN チャネルのネットワーク設定を行います。

「Network Settings」ページには「Network IP Settings」、「Network Link Configuration」、「DNS Configuration」設定があります。

図 16: Network Settings ページ

2.8.2.1 Network IP Settings

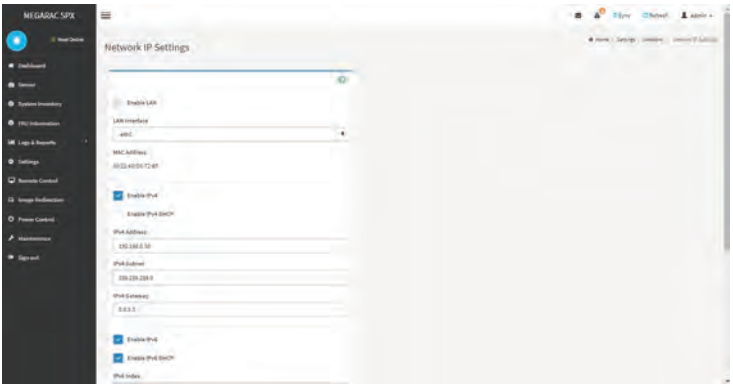

図 17: Network IP Settings ページ

「Network IP Settings」ページのフィールドについて説明します。

アイテム	説明
Enable LAN	LAN を有効 / 無効にします。
LAN Interface	LAN インターフェースを選択します。
MAC Address	MAC Address を表示します。
Enable IPv4	IPv4 を有効 / 無効にします。
Enable IPv4 DHCP	IPv4 DHCP を有効 / 無効にします。
IPv4 Address	IPv4 Address を設定します。
IPv4 Subnet	IPv4 Subnet を設定します。
IPv4 Gateway	IPv4 Gateway を設定します。
Enable IPv6	IPv6 を有効 / 無効にします。
Enable IPv6 DHCP	IPv6 DHCP を有効 / 無効にします。
IPv6 Index	IPv6 Index を表示します。読み取り専用のフィールドです。
IPv6 Address	IPv6 Address を表示します。読み取り専用のフィールドです。
Subnet Prefix Length	Subnet Prefix Length を表示します。読み取り専用のフィールドです。
Enable VLAN	VLAN を有効 / 無効にします。
VLAN ID	VLAN ID を表示します。読み取り専用のフィールドです。
VLAN Priority	VLAN Priority を表示します。読み取り専用のフィールドです。
Save	エントリを保存します。

表 8: Network IP Settings

手順

1. 「Enable LAN」をオンにすると、LAN の設定が有効になります。
2. 「LAN Interface」、「MAC Address」の数値が表示されます。
3. 「Enable IPv4」オプションを有効にします。
4. 「Enable IPv4 DHCP」を有効にすると、DHCP を使用して IPv4 アドレスを動的に設定します。
5. このフィールドが無効な場合、「IPv4 Address」、「IPv4 Subnet」、「IPv4 Gateway」の各フィールドに入力します。
6. 「Enable IPv6」オプションを有効にします。

7. IPv6 の設定が有効な場合、「Enable IPv6 DHCP」オプションを有効または無効にします。
8. このフィールドが無効な場合、「IPv6 Index」、「IPv6 Address」、「Subnet Prefix length」、「Default Gateway」の各フィールドに入力します。
9. 「Enable VLAN」をオンにすると、VLAN の設定が有効になります。
10. 「VLAN ID」フィールドに入力します。
11. 「VLAN Priority」フィールドに入力します。
12. 「Save」をクリックするとエントリが保存されます。

2.8.2.2 Network Link Configuration

このページを使用して、使用可能なネットワークインターフェースのネットワークリンク構成を設定します。

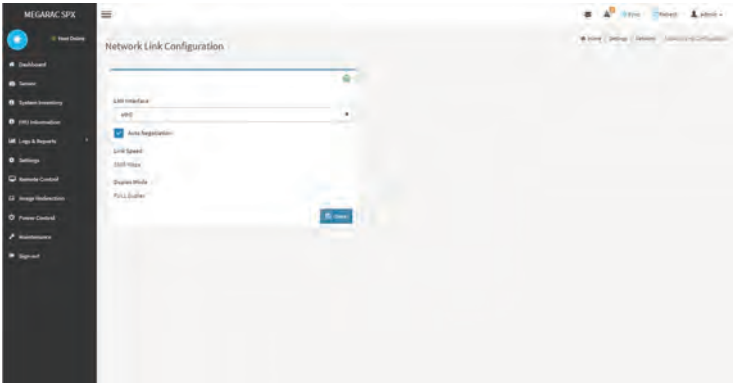

図 18: Network Link Configuration ページ

「Network Link Configuration」ページのフィールドについて説明します。

アイテム	説明
LAN Interface	LAN インターフェースを選択します。
Auto Negotiation	Auto Negotiation を有効 / 無効にします。
Link Speed	Link Speed を表示します。
Duplex Mode	半二重 (HALF) または全二重 (FULL) を表示します。

表 9: Network Link Configuration

手順

1. 「LAN Interface」を選択します。
2. 「Auto Negotiation」オプションを有効にします。
3. 「Link Speed」の数値が表示されます。
4. 「Duplex Mode」が表示されます。
5. 「Save」をクリックするとエントリが保存されます。

2.8.2.3 DNS Configuration

BMC GUI では、「DNS Configuration」ページを使用して、デバイスの DNS 設定を管理します。

「DNS Configuration」ページを開くには、メニューの「Settings」、「Network Settings」、「DNS Configuration」を順にクリックします。次のスクリーンショットに「DNS Configuration」ページのサンプルスクリーンショットを示します。

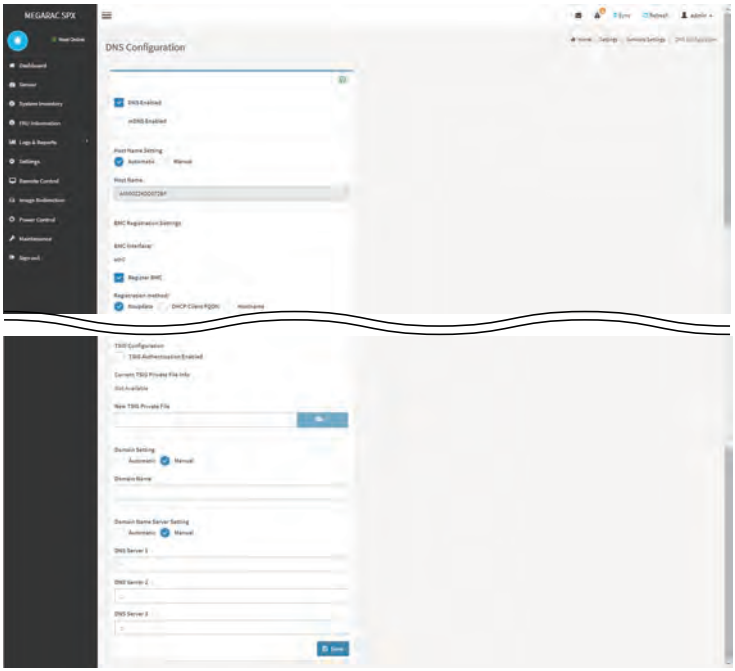

図 19: DNS Configuration ページ

「DNS Configuration」ページのフィールドについて説明します。

アイテム	説明
DNS Enabled	DNS を有効 / 無効にします。
mDNS Enabled	mDNS を有効 / 無効にします。
Host Name Setting	「Automatic」または「Manual」での設定を選択します。
Host Name	デバイスのホスト名が表示されます。「Host Name Setting」で「Manual」を選択した場合は、デバイスのホスト名を指定します。
BMC Registration Settings	
BMC Interface	使用可能な BMC インターフェースがリストされます。
Register BMC	オプションをチェックして BMC 設定を登録します。
Registration method:	「Nsupdate」、「DHCP Client FQDN」または「Hostname」での登録を選択します。
TSIG Configuration	
TSIG Authentication Enabled	TSIG 認証の有効 / 無効を選択します。
Current TSIG Private File Info	現在の TSIG プライベートファイル情報を表示します。
New TSIG Private File	新しい TSIG プライベートファイルを選択します。
Domain Setting	「Automatic」または「Manual」での設定を選択します。
Domain Name	デバイスのドメイン名が表示されます。「Domain Setting」で「Manual」を選択した場合は、デバイスのドメイン名を指定します。「Automatic」を選択すると、Domain Name が自動的に設定されるように設定できません。このフィールドは無効になります。
Domain Name Server Setting	「Automatic」または「Manual」での設定を選択します。
DNS Server 1	デバイスに設定される DNS サーバの IP アドレスを設定します。
DNS Server 2	デバイスに設定される DNS サーバの IP アドレスを設定します。
DNS Server 3	デバイスに設定される DNS サーバの IP アドレスを設定します。
Save	入力した変更を保存します。

表 10: DNS Configuration

手順

1.「DNS Enabled」オプションにチェックして、DNS を有効にします。
2.「mDNS Enabled」オプションのチェックを外して、mDNS を無効にします。
3.「Host Name Setting」で「Automatic」または「Manual」を選択します。

「Automatic」の場合、ホスト名は必要ありませんが「Manual」の場合は必要です。

4.「Manual」を選択した場合は、「Host Name」フィールドに入力します。
5.「BMC Registration Settings」で、
   (1)「BMC Interface」のドロップダウンリストから設定を選択します。
   (2)「Register BMC」オプションをチェックして、この DNS 設定で登録します。
   (3)「Registration method:」の「Nsupdate」、「DHCP Client FQDN」または「Hostname」から「Nsupdate」にチェックします。
6.「TSIG Configuration」で、
   (1)「TSIG Authentication Enabled」オプションで、TSIG 認証の有効 / 無効を選択します。
   (2) 有効にした場合は、「Current TSIG Private File Info」に現在の TSIG プライベートファイル情報が表示されます。
   (3) 有効にして新しい TSIG プライベートファイルを読み込む場合は、「New TSIG Private File」フィールドから選択します。
7.「Domain Setting」で、
   (1)「Automatic」または「Manual」を選択します。
   (2)「Manual」を選択した場合はデバイスのドメイン名を指定します。
   (3)「DNS Server 1」、「DNS Server 2」、「DNS Server 3」フィールドに IP アドレスを入力します。
8.「Save」をクリックするとエントリが保存されます。

2.8.3 Platform Event Filters

PEF（Platform Event Filter）は、受信された、または内部で生成されたイベントメッセージに選択したアクションを行うために、BMC を設定するメカニズムを提供します。これらのアクションには、システムの電源オフ、システムのリセット、アラート生成のトリガーなどの動作があります。BMC GUI では Platform Event Filters ページを使用して以下の機能を設定します。

– Event Filters

– Alert Policies

– LAN Destinations

「Platform Event Filters」ページを開くには、メニューの「Settings」、「Platform Event Filter」を順にクリックします。次のスクリーンショットに「Platform Event Filter」ページのサンプルスクリーンショットを示し、各タブについて説明します。

図 20: Platform Event Filters ページ

2.8.3.1 Event Filters

PEF を実装して少なくとも 40 のエントリを「Event Filters」タブに入力することをお勧めします。これらのエントリのサブセットを、温度過上昇、電源システムの故障、ファンの故障イベントなどの、共通のシステム故障イベントに対してあらかじめ設定しておいてください。残りのエントリは、'OEM' または System Management Software によって設定されたイベントのために使用可能にできます。システム用に予約していることを個々のエントリにタグ付けできるので、あらかじめ設定されたエントリの、実行時に設定可能なエントリに対する割合は、必要に応じて割り当て直すことができます。

図 21: Platform Event Filters - Event Filters ページ

イベントのどれかを選択すると、「Event Filter Configuration」ページが開きます。

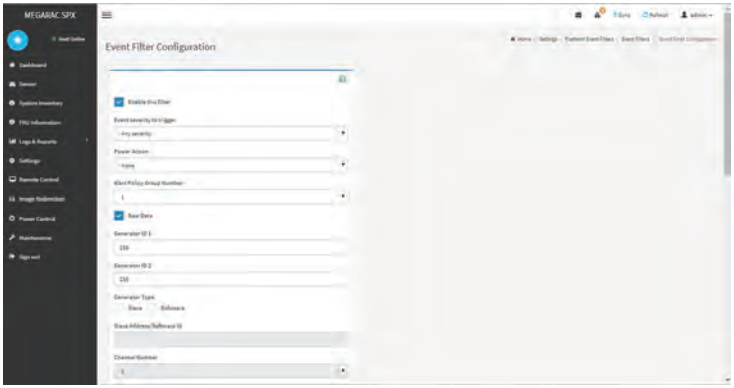

図 22: Event Filter Configuration ページ

次に「Event Filter Configuration」ページのフィールドについて説明します。

アイテム	説明
Enable this filter	このチェックボックスで PEF の設定を有効にします。
Event severity to trigger	イベントの重要度をリストから 1 つ選択します。
Power Action	電源アクションのいずれかを選択します。
Alert Policy Group Number	アラートポリシーのグループ番号を選択します。
Raw Data	このチェックボックスで Raw データの設定を有効にします。
Generator ID 1	Generator ID 1 を設定します。
Generator ID 2	Generator ID 2 を設定します。
Generator Type	Generator Type を「Slave」か「Software」を選択します。
Slave Address/Software ID	Slave Address/Software ID を表示します（読み取り専用）。
Channel Number	チャネル番号を表示します（読み取り専用）。
IPMB Device LUM	IPMB Device LUM を表示します（読み取り専用）。
Sensor type	センサリストから特定のセンサタイプを選択します。
Sensor name	センサリストから特定のセンサ名を選択します。
Event Options	イベントオプションを選択します。
Event trigger	Event / Reading 型の値を与えるために使用します。
Event Data 1 AND Mask	ワイルドカードまたは比較ビットを表示します。
Event Data 1 Compare 1	各ビット位置の比較結果が、正しいかどうかを表示します。
Event Data 1 Compare 2	各ビット位置の比較結果が、正しいかどうかを表示します。
Event Data 2 AND Mask	ワイルドカードまたは比較ビットを表示します。
Event Data 2 Compare 1	各ビット位置の比較結果が、正しいかどうかを表示します。
Event Data 2 Compare 2	各ビット位置の比較結果が、正しいかどうかを表示します。
Event Data 3 AND Mask	ワイルドカードまたは比較ビットを表示します。
Event Data 3 Compare 1	各ビット位置の比較結果が、正しいかどうかを表示します。
Event Data 3 Compare 2	各ビット位置の比較結果が、正しいかどうかを表示します。
Delete	設定を削除します。
Save	入力した変更を保存します。

表 11: Event Filter Configuration

手順

1. 「Enable this filter」オプションをチェックして、PEF の設定を有効にします。
2. 「Event severity to trigger」のドロップダウンリストからイベントの重要度をリストから 1 つ選択します。
3. 「Power Action」のドロップダウンリストから、「None」、「Power Down」、「Power Cycle」、「Reset」の電源アクションのいずれかを選択します。
4. 「Alert Policy Group Number」のドロップダウンリストから、設定したアラートポリシーのグループ番号を選択します。
5. 「Raw Data」オプションをチェックして、Raw データの設定を有効にします。
6. 「Generator ID 1」,「Generator ID 2」を設定します。
7. 「Generator Type」から「Slave」か「Software」を選択します。
8. 「Sensor type」のドロップダウンリストから、特定のセンサタイプを選択します。
9. 「Sensor name」のドロップダウンリストから、特定のセンサ名を選択します。
10. 「Event Options」のドロップダウンリストから、イベントオプションを選択します。
11. 「Event trigger」のドロップダウンリストから 1 ～ 255 の値を選択する。
12. 「Event Data 1 (/2/3) AND Mask」のドロップダウンリストから 0 ～ 255 の値を選択する。
13. 「Event Data 1 (/2/3) Compare 1(/2)」のドロップダウンリストから 0 ～ 255 の値を選択する。
14. 「Delete」をクリックすると、リストを削除します。
15. 「Save」をクリックすると、入力した変更を保存します。

2.8.3.2 Alert Policies

このページを使用して、アラートポリシーを設定します。このページの入力は、追加、削除、変更ができます。

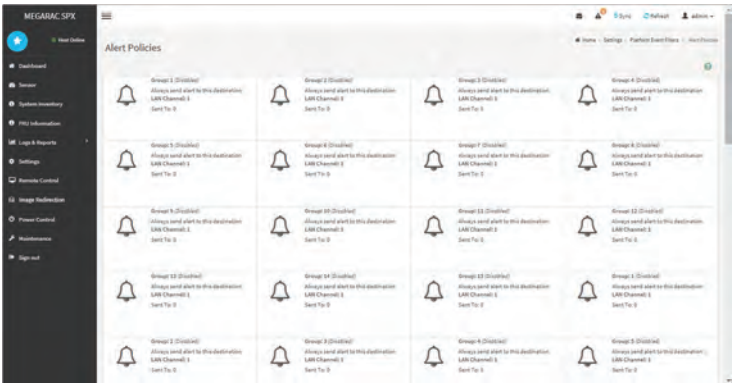

図 23: Platform Event Filters - Alert Policies ページ

アラートポリシーのどれかを選択すると、「Alert Policies」ページが開きます。

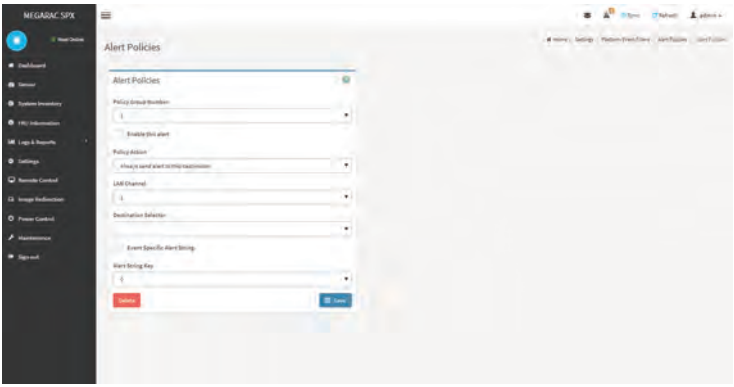

図 24: Alert Policies ページ

次に「Alert Policies」ページのフィールドについて説明します。

アイテム	説明
Policy Group Number	設定のポリシーグループ数を表示します。
Enable this alert	アラートポリシーの設定を有効 / 無効にします。
Policy Action	ポリシーのアクションを選択します。
LAN Channel	使用可能な LAN チャネルを選択します。
Destination Selector	設定された宛先リストから特定の宛先を選択します。
Event Specific Alert String	アラートポリシーのエントリがイベント固有である場合は、チェックボックスをオンにします。
Alert String Key	このアラートポリシーのエントリに送信するアラート文字列を検索するために使用する値を 1 つ選択します。
Delete	アラートポリシーリストを削除します。
Save	アラートポリシーリストを保存します。

表 12: Alert Policies

手順

1. 「Policy Group Number」のドロップダウンリストから、アラートポリシーを設定するスロットを選択します。
2. 「Enable this alert」オプションをチェックして、ポリシー設定を有効にします。
3. 「Policy Action」のドロップダウンリストから、ポリシーのアクションを選択します。
4. 「LAN Channel」のドロップダウンリストから、使用可能な LAN チャネルを選択します。
5. 「Destination Selector」のドロップダウンリストから、設定された宛先リストから特定の宛先を選択します。
6. アラートポリシーのエントリがイベント固有である場合は、「Enable Specific Alert String」オプションをチェックします。
7. 「Alert String Key」フィールドで、このアラートポリシーのエントリに送信するアラート文字列を検索するために使用する値を 1 つ選択します。
8. 「Delete」をクリックして、アラートポリシーページの設定を削除します。
9. 「Save」をクリックして、アラートポリシーページの設定を保存します。

2.8.3.3 LAN Destinations

このページを使用して、LAN 宛先を設定します。

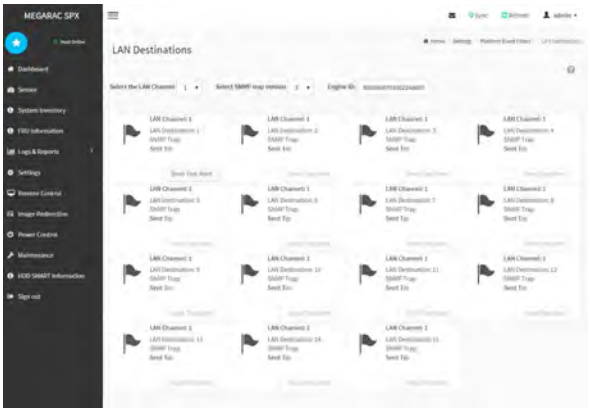

図 25: Platform Event Filters - LAN Destinations ページ

「LAN Destinations」ページのフィールドについて説明します。

アイテム	説明
select SNMP trap version	SNMP trapのバージョン(V1/V3)を選択します。
Engine ID	SNMP v3で使用するEngine IDが表示されます。

表 13: LAN Destinations

LAN Destinations のどれかを選択すると、「LAN Destination Configuration」ページが開きます。

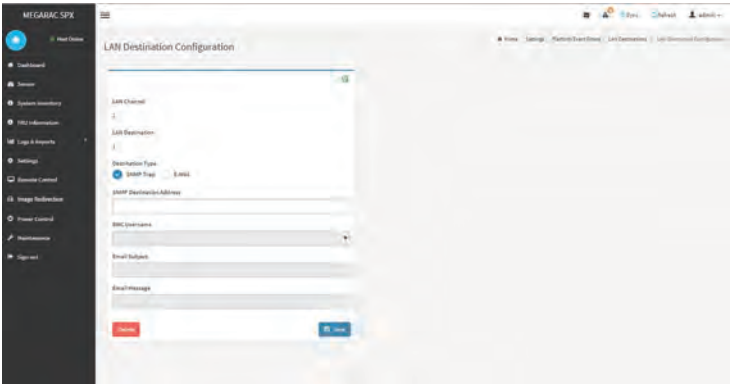

図 26: LAN Destination Configuration ページ

次に「LAN Destination Configuration」ページのフィールドについて説明します。

アイテム	説明
LAN Channel	LAN チャネルを表示します。
LAN Destination	新しく設定したエントリの宛先番号を表示します（読み取り専用）。
Destination Type	宛先タイプは、SNMP トラップまたは E-mail アラートのいずれかです。
SNMP Destination Address	SNMP 宛先アドレスを入力します。（SNMP トラップの場合のみ）
BMC Username	BMC ユーザー名を入力します。（SNMP v3またはE-mail アラートの場合）User management であらかじめSNMPv3関連の設定、またはEmail アドレスを設定しておく必要があります。
Email Subject	E-mail のメッセージの件名を入力します。（E-mail アラートの場合のみ）また、User management で Email Format が AMI format になっている場合は入力できません。
Email Message	E-mail の本文を入力します。（E-mail アラートの場合のみ）また、User management で Email Format が AMI format になっている場合は入力できません。
Delete	LAN 宛先リストを削除します。
Save	LAN 宛先の設定を保存します。

表 14: LAN Destination Configuration

手順

1. 「LAN Channel」フィールドに、設定したエントリの宛先が表示されます（読み取り専用のフィールド）。
2. 「LAN Destination」フィールドに、新しく設定したエントリの宛先が表示されます（読み取り専用のフィールド）。
3. 「Destination Type」フィールドで、宛先タイプ (SNMP Type、E-mail) を選択します。
4. 「SNMP Destination Address」フィールドに、SNMP 宛先アドレスを入力します。
5. 「BMC Username」フィールドに、BMC ユーザー名を入力します。
6. 「Email Subject」フィールドに、E-mail のメッセージの件名を入力します。
7. 「Email Message」フィールドに、E-mail の本文を入力します。
8. 「Delete」をクリックして、LAN 宛先リストを削除します。
9. 「Save」をクリックして、LAN 宛先の設定を保存します。

2.8.4 SMTP Settings

SMTP（Simple Mail Transfer Protocol）は、IP（Internet Protocol）ネットワーク経由で E-mail（電子メール）を送信するためのインターネット標準規格です。

このページを使用して、デバイスの SMTP 設定を行うことができます。

「SMTP Settings」ページを開くには、メニューの「Settings」、「SMTP Settings」を順にクリックします。次のスクリーンショットに「SMTP Settings」ページのサンプルスクリーンショットを示し、各タブについて説明します。

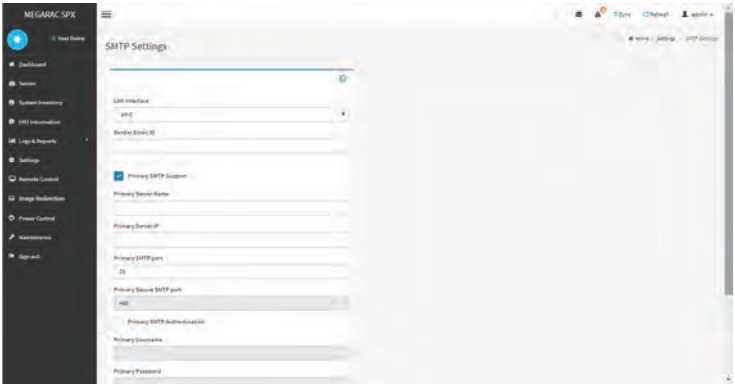

図 27: SMTP Settings ページ

次に「SMTP Settings」ページのフィールドについて説明します。

アイテム	説明
LAN Interface	LAN インターフェースを選択します。
Sender Email ID	送信元 E-mail ID を入力します。
Primary SMTP Support	プライマリ SMTP サポートを有効／無効にします。
Primary Server Name	プライマリサーバ名を入力します。
Primary Server IP	プライマリサーバ IP を入力します。
Primary SMTP port	プライマリ SMTP ポートを入力します。
Primary Secure SMTP port	プライマリ Secure SMTP ポートを表示します。
Primary SMTP Authentication	プライマリ SMTP 認証を有効／無効にします。
Primary Username	プライマリユーザー名を表示します。

表 15: SMTP Settings

アイテム	説明
Primary Password	プライマリパスワードを表示します。
Primary SMTP SSLTLS Enable	プライマリ SMTP SSLTLS を有効／無効にします。
Primary SMTP STARTTLS Enable	プライマリ SMTP STARTTLS を有効／無効にします。
Secondary SMTP Support	セカンダリ SMTP サポートを有効／無効にします。
Save	新しい SMTP サーバ構成を保存します。

表 16: SMTP Settings

手順

1. 「LAN Interface」のドロップダウンリストから LAN インターフェースを選択します。
2. 「Sender Email ID」フィールドに入力します。
3. プライマリ SMTP サポートの設定を有効にする場合は、「Primary SMTP Support」オプションをチェックします。
4. 「Primary Server Name」フィールドに入力します。
5. 「Primary Server IP」フィールドに入力します。
6. 「Primary SMTP port」フィールドに入力します。
7. 「Primary Secure SMTP port」フィールドに入力します。
8. プライマリ SMTP 認証の設定を有効にする場合は、「Primary SMTP Authentication」オプションをチェックします。
9. 「Primary Username」フィールドに入力します。
10. 「Primary Password」フィールドに入力します。
11. プライマリ SMTP SSLTLS の設定を有効にする場合は、「Primary SMTP SSLTLS Enable」オプションをチェックします。
12. プライマリ SMTP STARTTLS の設定を有効にする場合は、「Primary SMTP STARTTLS Enable」オプションをチェックします。
13. セカンダリ SMTP サポートの設定を有効にする場合は、「Secondary SMTP Support」オプションをチェックします。
14. 「Save」をクリックすると、入力した詳細を保存します。

2.8.5 SSL Settings

セキュアソケットレイヤープロトコルは、Web サーバとブラウザ間のセキュアなトランザクションを保証するために、Netscape によって作成されました。

このプロトコルは、サードパーティである認証局（CA：Certificate Authority）を使用して、トランザクションの片端または両端を識別します。

MegaRAC GUI を使用して、SSL 証明書を BMC に設定します。これを使用して、デバイスにセキュアモードでアクセスできます。

「SSL Settings」ページを開くには、メインメニューの「Settings」をクリックします。このページにはタブが 3 つあります。

– 「View SSL Certificate」オプションを使用して、アップロードされた SSL 証明書を読み取り可能な形式で表示します。

– 「Generate SSL Certificate」オプションを使用して、設定の詳細に基づき SSL 証明書を生成します。

– 「Upload SSL Certificate」オプションを使用して、証明書と秘密鍵ファイルを BMC にアップロードします。

次のスクリーンショットに「SSL Settings」ページのサンプルスクリーンショットを示します。

図 28: SSL Settings

View SSL Certificate

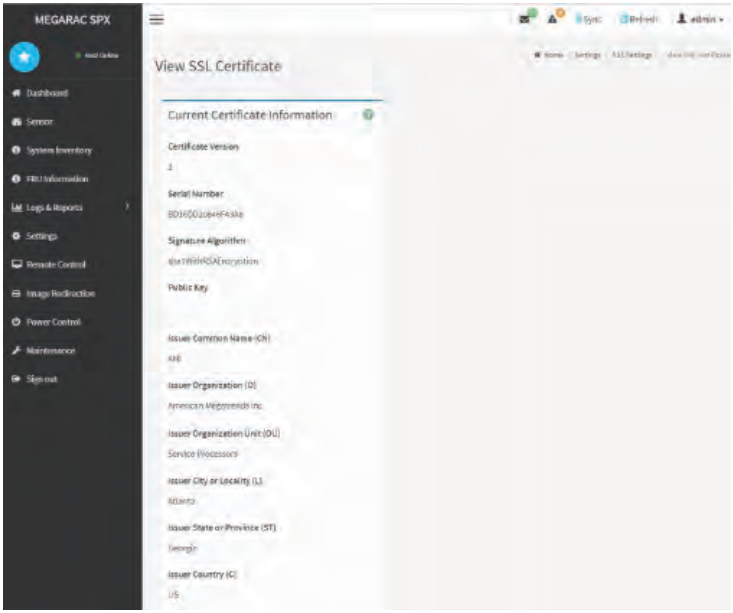

図 29: View SSL Certificate

次に「View SSL Certificate」ページのフィールドについて説明します。

アイテム	説明
基本情報	このセクションには、アップロードされた SSL 証明書の基本情報が表示されます。以下のフィールドが表示されます。 – バージョン – Serial Number – Signature Algorithm – Public Key
Issued From	このセクションには、以下の証明書発行者情報が表示されます。 – Common Name（CN） – Organization（O） – Organization Unit（OU） – City or Locality（L） – State or Province（ST） – Country（C） – Email Address
Validity Information	このセクションには、アップロードされた証明書の有効期限が表示されます。 – Valid From – Valid Till
Issued To	このセクションには、証明書の発行者に関する情報が表示されます。 – Common Name（CN） – Organization（O） – Organization Unit（OU） – City or Locality（L） – State or Province（ST） – Country（C） – Email Address

表 17: View SSL Certificate

手順

1. 「Upload SSL」タブをクリックして新しい証明書と新しい秘密鍵を表示します。
2. 「Upload」をクリックして新しい証明書と新しい秘密鍵をアップロードします。

3.「Generate SSL」タブで、各フィールドに下記の詳細を入力します。

(1) 証明書が生成されるコモンネーム。

(2) 証明書が生成される N 組織名。

(3) 証明書が生成される O 組織全体における部門名。

(4) 組織の市町村名。

(5) 組織の都道府県名。

(6) 組織の国名。

(7) 組織の E-mail アドレス。

(8) 証明書の日数は、「Valid For」フィールドの期間有効です。

4. 証明書のキーの長さ（ビット）を選択します。

5.「Save」をクリックすると証明書が生成されます。

6.「View SSL」タブをクリックすると、アップロードされた SSL 証明書がユーザーが読み取り可能な形式で表示されます。

証明書をアップロード / 生成するとすぐに、HTTPs サービスが再起動します。

– これで、インターネットブラウザの IP アドレスフィールドで次の形式を使用して、Generic MegaRAC® SP にセキュアにアクセスすることができます：https://<your MegaRAC® SP's IP address here>

– たとえば、MegaRAC® SP の IP アドレスが 192.168.0.30 の場合、次のように入力します：
https://192.168.0.30

– <http> の後の <s> に注意してください。Generic MegaRAC® SP にアクセスする前に、証明書を承認する必要があります。

Generate SSL Certificate

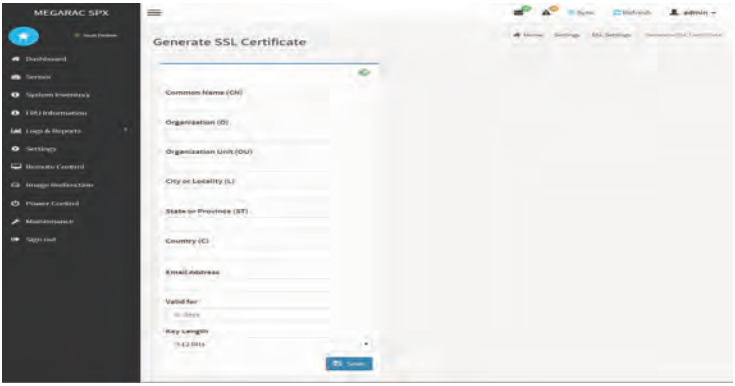

図 30: Generate SSL Certificate

次に「Generate SSL Certificate」ページのフィールドについて説明します。

アイテム	説明
Common Name（CN）	証明書が生成されるコモンネーム。 – 最大 64 文字です。 – 特殊文字の '#' と '$' は使用できません。
Organization（O）	証明書が生成される組織名。 – 最大 64 文字です。 – 特殊文字の '#' と '$' は使用できません。
Organization Unit（OU）	証明書が生成される組織全体における部門名。 – 最大 64 文字です。 – 特殊文字の '#' と '$' は使用できません。
City or Locality（L）	組織の市町村名（必須）。 – 最大 64 文字です。 – 特殊文字の '#' と '$' は使用できません。
State or Province（ST）	組織の都道府県名（必須）。 – 最大 64 文字です。 – 特殊文字の '#' と '$' は使用できません。
Country（C）	組織の国名（必須）。 – 2 文字のみ使用できます。 – 特殊文字は使用できません。
Email Address	組織の E-mail アドレス（必須）。
Valid for	証明書の有効期限。 – 値の範囲は 1 ～ 3650 日です。
Key Length	証明書の鍵の長さ（ビット）。
Save	新しい SSL 証明書を生成します。

表 18: Generate SSL Certificate

HTTPs サービスが再起動して、新しく生成された SSL 証明書を適用します。

Upload SSL Certificate

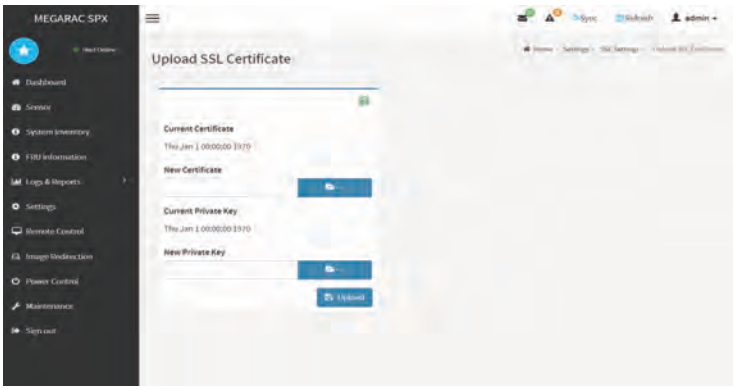

図 31: Upload SSL Certificate

次に「Upload SSL Certificate」ページのフィールドについて説明します。

アイテム	説明
Current Certificate	現在の証明書の情報が表示されます（読み取り専用）。
New Certificate	証明書ファイルは PEM 形式である必要があります。
Current Privacy Key	現在の秘密鍵の情報が表示されます（読み取り専用）。
New Privacy Key	秘密鍵ファイルは PEM 形式である必要があります。
Upload	SSL 証明書と秘密鍵を BMC にアップロードします。

表 19: Upload SSL Certificate

アップロードが成功すると、HTTPs サービスが再起動して、新しくアップロードされた SSL 証明書を適用します。

2.8.6 User Management

このページを使用して、サーバの現在のユーザースロットのリストを表示することができます。新しいユーザーの追加、および既存のユーザーの変更または削除ができます。

「User Management」ページを開くには、メニューの「Settings」、「User Management」を順にクリックします。次のスクリーンショットに「User Management」ページのサンプルスクリーンショットを示し、各タブについて説明します。

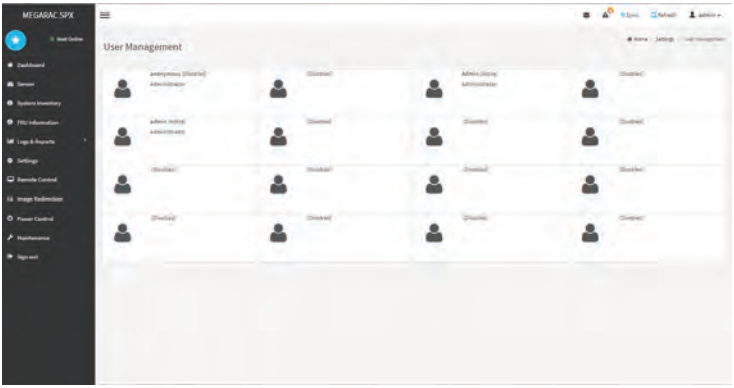

図 32: User Management ページ

ユーザーのどれかを選択すると、「User Management Configuration」ページが開きます。

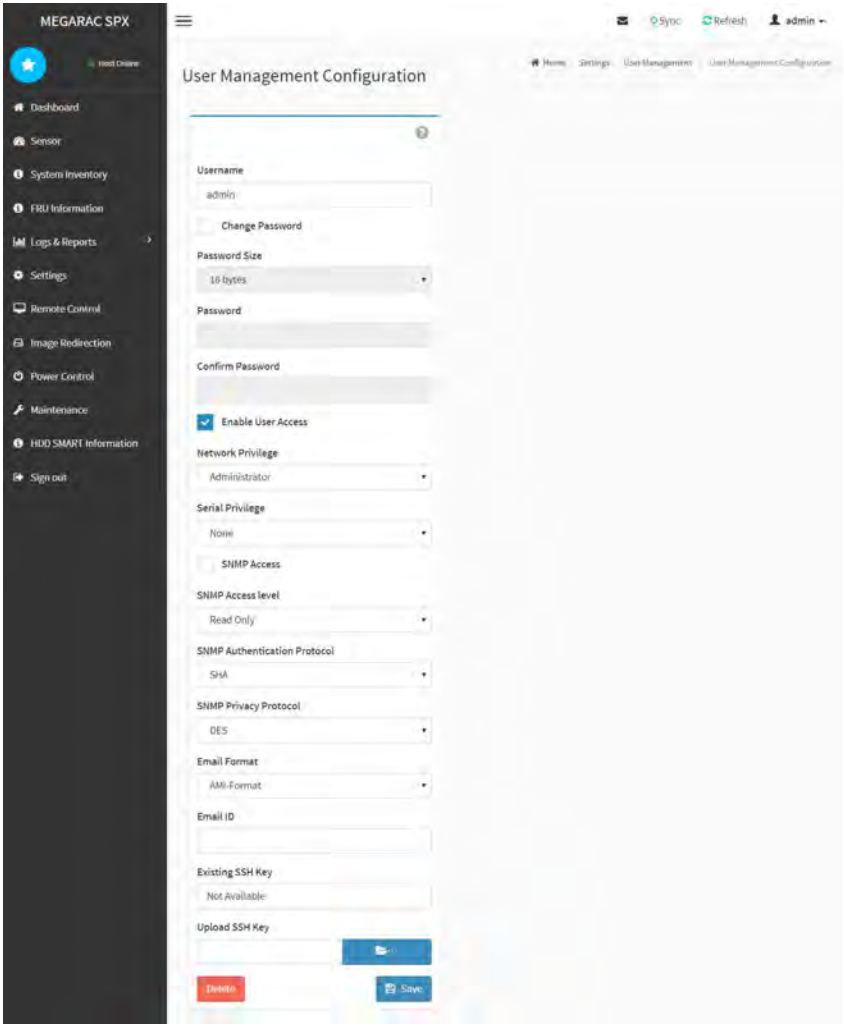

図 33: User Management Configuration ページ

次に「User Management Configuration」ページのフィールドについて説明します。

アイテム	説明
Username	ユーザーの名前を表示します。
Change Password	パスワードの変更を有効／無効にします。
Password Size	パスワードのサイズを選択します。
Password	パスワードを入力します。
Confirm Password	パスワードを再入力します。
Enable User Access	ユーザーのアクセス権限を有効 / 無効にします。
Network Privilege	ユーザーのネットワークアクセス権限を選択します。
Serial Privilege	ユーザーのシリアル権限を選択します。
SNMP Access	ユーザーのSNMPアクセス権限を有効 / 無効にします。
SNMP Access level	ユーザーのSNMPアクセス権限を選択します。
SNMP Authentication Protocol	SNMP v3の認証プロトコルを選択します。
SNMP Privacy Protocol	SNMP v3のプライバシープロトコルを選択します。
Email Format	E-mail 形式を選択します。
Email ID	E-mail ID を入力します。
Existing SSH Key	現在の SSH キーを表示します。
Upload SSH Key	SSH キーをアップロードします。
Delete	既存のユーザーを削除します。

表 20: User Management Configuration

手順

新しいユーザーの追加：

新しいユーザーを追加するには、「User Management」ページから空きスロット (Disabled) を選択してクリックします。「User Management Configuration」ページが開きます。

1. 「User Name」フィールドにユーザー名を入力します。

   ユーザー名は、4 ～ 16 文字の英数字の文字列です。

   – 先頭はアルファベットでなければなりません。

   – 大文字小文字を区別します。

   – 特殊文字の、カンマ（,）、ピリオド（.）、コロン（:）、セミコロン（;）、スペース（ ）、スラッシュ（/）、バックスラッシュ（\）、左括弧（(）、右括弧（)）は使用できません。

2. パスワードの変更を有効にする場合は、「Change Password」オプションをチェックします。

3. 「Password Size」のドロップダウンリストから、パスワードのサイズを選択します。

4. 「Password」、「Confirm Password」フィールドに、新しいパスワードを入力して確定します。

   – 空白は使用できません。

   – このフィールドは 20 文字以下しか設定できません。

5. 「Enable User Access」オプションで、ユーザーアクセス権限を有効または無効にします。

6. 「Network Privilege」のドロップダウンリストから、ユーザーに割り当てられているネットワーク権限（Administrator、Operator、User、None のいずれか）を選択します。

7. 「Serial Privilege」のドロップダウンリストから、ユーザーに割り当てられているシリアル権限（Administrator、Operator、User、None のいずれか）を選択します。

8. Email Format：次の 2 種類の形式を使用できます。
   - AMI-Format：このメール形式の件名は「Alert from（ユーザーのホスト名）」です。
     メールの本文には、センサ情報（センサタイプや説明など）が表示されます。
   - Fixed-Subject Format：この形式では、ユーザーの設定に従ってメッセージを表示します。
     E-mail アラート用の件名とメッセージを設定する必要があります。
9. 「Email ID」フィールドに、ユーザーの E-mail アドレスを入力します。
   ユーザーがパスワードを忘れた場合、設定した E-mail アドレスに新しいパスワードが送信されます。

   E-mail アドレスを送信するように SMTP サーバを設定します。
10. 「Existing SSH Key」フィールドで、現在の SSH キーを表示します。
11. 「Upload SSH Key」フィールドで「Browse」をクリックして、SSH キーファイルを選択します。

    SSH キーファイルは、PUB 形式である必要があります。
12. 「Delete」をクリックすると、既存のユーザーを削除します。
13. 「Save」をクリックすると、ユーザー情報を保存します。

既存のユーザーの変更：

リストから既存のユーザーを選択してクリックすると、「User Management Configuration」ページが開きます。

1. 必要なフィールドを編集します。
2. パスワードを変更するには、「Change Password」オプションを有効にします。
3. 編集や変更の後、「Save」をクリックしてユーザーリストページに戻ります。

既存のユーザーの削除：

1. 既存のユーザーを削除するには、リストからユーザーを選択して「Delete」をクリックします。

2.9 Remote Control

このページは KVM 機能と Java SOL 機能で構成されています。

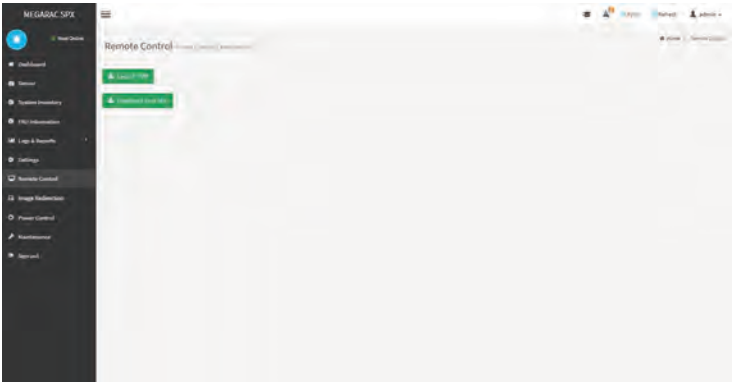

図 34: Remote Control ページ

2.9.1 KVM function

「Remote Control」ページの [Launch KVM] をクリックすると、「KVM function」画面が開きます。

「KVM function」メニューは、次のメニュー項目で構成されています。

– Video
– Mouse
– Options
– Keyboard
– Send Keys
– Hot Keys
– Video Record
– Power
– Active Users
– Help

また、CD imageを指定して、Image Redirection機能を使用できます。

これらのメニュー項目について、次に詳しく説明します。

図 35: KVM function

2.9.1.1 Video

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Pause Video	このオプションを使用して、コンソールリダイレクションを一時停止します
Resume Video	このオプションを使用して、セッションが一時停止の場合にコンソールリダイレクションを再開します。
Refresh Video	このオプションを使用して、「Console Redirection」ウィンドウに表示される画面を更新できます。
Host Display	
Display ON Display OFF	このオプションを使用して、コンソールリダイレクションのディスプレイ表示を ON/OFF することができます。
Capture Screen	このオプションを使用して、コンソールリダイレクション画面をキャプチャーすることができます。

表 21: Video

2.9.1.2 Mouse

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Show Client Cursor	クライアントカーソルを表示することができます。
Mouse Mode	
Absolute Mouse Mode	ホストオペレーティングシステムによっては（すべての Windows バージョン、RHEL6 以降の RHEL Linux バージョン）、マウスモードに「Absolute」を選択します。
Relative Mouse Mode	ホストオペレーティングシステムによっては（RHEL6 より前の RHEL Linux バージョン）、マウスモードに「Relative」を選択します。
Other Mouse Mode	Absolute Mouse Mode でも Relative Mouse Mode でもないホストオペレーティングシステムの場合。

表 22: Mouse

2.9.1.3 Options

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Block Privilege Request	このオプションを使用して、ブロック特権を要求できます。
YUV 420 YUV 444 YUV 444 + 2 color VQ YUV 444 + 4 color VQ	このオプションを使用して、YUV 420、YUV 444、YUV 444 + 2 色 VQ、YUV 444 + 4 色 VQ などのビデオ圧縮モードを選択します。
0 Best Quality 1 2 3 4 5 6 7	このオプションを使用して、8 つのレベルからビデオ品質を選択します。

表 23: Options

2.9.1.4 Keyboard

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Keyboard Layout	
English U.S	キーボードのレイアウトを English U.S に設定できます。
German	キーボードのレイアウトを German に設定できます。
Japanese	キーボードのレイアウトを Japanese に設定できます。

表 24: Keyboard

2.9.1.5 Send Keys

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Hold Down	
Right Ctrl Key	このメニュー項目を使用して、コンソールリダイレクション中に、右側 <Ctrl> キーとして動作します。
Right Alt Key	このメニュー項目を使用して、コンソールリダイレクション中に、右側 <Alt> キーとして動作します。
Right Windows Key	このメニュー項目を使用して、コンソールリダイレクション中に、右側 <Win> キーとして動作します。キーの押し方も指定できます：押したまま / 押してから放す
Left Ctrl Key	このメニュー項目を使用して、コンソールリダイレクション中に、左側 <Ctr> キーとして動作します。
Left Alt Key	このメニュー項目を使用して、コンソールリダイレクション中に、左側 <Alt> キーとして動作します。
Left Windows Key	このメニュー項目を使用して、コンソールリダイレクション中に、左側 <Win> キーとして動作します。キーの押し方も指定できます：押したまま / 押してから放す
Press and Release	
Ctrl+Alt +Del	このメニュー項目を使用すると、リダイレクトしているサーバで <Ctrl>, <Alt> and <Delete> キーを同時に押しているかのように動作させることができます。
Left Windows Key	このメニュー項目を使用すると、リダイレクトしているサーバで左側 <Win> キーを押しているかのように動作させることができます。

表 25: Send Keys

アイテム	説明
Right Windows Key	このメニュー項目を使用すると、リダイレクトしているサーバで右側 <Win> キーを押しているかのように動作させることができます。
Context Menu Key	このメニュー項目を使用すると、リダイレクトしているサーバで <Menu> キーを押しているかのように動作させることができます。
Print Screen Key	このメニュー項目を使用すると、リダイレクトしているサーバで <Prnt Scrn> キーを押しているかのように動作させることができます。

表 26: Send Keys

コンテキストメニュー：
このメニュー項目を使用して、コンソールリダイレクション中に、コンテキストメニューキーとして動作します。

2.9.1.6 Hot Keys

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Add Hot Keys	このオプションを使用して、「Press and Release」により、ユーザー指定の Send Keys マクロを新たに登録することができます。

表 27: Hot Keys

2.9.1.7 Video Record

このオプションは、H5Viewer (HTML5 クライアント) を起動する場合のみ使用できます。

アイテム	説明
Record Video	このオプションを使用して画面の記録を開始します。
Stop Recording	このオプションを使用して記録を停止します。
Record Settings	ビデオの記録に関する設定を行います。

表 28: Video Record

手順

記録を開始する前に、設定を入力する必要があります。

1. 下のスクリーンショットに示すように、「Video Record - Record Settings」をクリックして設定ページを開きます。

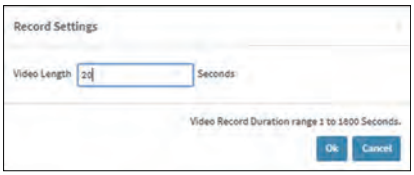

図 36: Record Settings ページ

2. 「Video Length」に秒単位で入力します。
3. 「OK」をクリックしてエントリを保存して、コンソールリダイレクション画面に戻ります。
4. エントリを保存しない場合は、「Cancel」をクリックします。
5. 「Console Redirection」ウィンドウで「Video Record -Record Video」をクリックします。
6. 処理を記録します。
7. 記録を停止するには、「Video Record - Stop Recording」をクリックします。

2.9.1.8 Power

このメニューには、以下のサブメニュー項目があります。

アイテム	説明
Reset Server	サーバを再起動します。
Immediate shutdown	サーバを即時にシャットダウンします。
Orderly shutdown	サーバを正常にシャットダウンします。
Power On Server	サーバの電源を入れる。
Power Cycle Server	サーバを一度シャットダウンしてから電源を入れます。

表 29: Power

2.9.1.9 Active Users

このオプションをクリックすると、アクティブなユーザーとそのシステム IP アドレスが表示されます。

2.9.1.10 Help

H5Viewer：著作権情報とバージョン情報が表示されます。

2.9.1.11 Start Media / Stop Media

ISOファイルを仮想メディアファイルとして、マウント/アンマウントすることができます。

2.9.2 Java sol function

「Remote Control」ページの [Download JAVA SOL] をクリックすると、Java SOL アプリケーションを実行します。

手順

1. 「Remote Control」ページを開いて「Down load Java SOL」をクリックします。
2. BMC から .jnlp ファイルがダウンロードされます。
3. ダウンロードされた .jnlp ファイルを開くときにセキュリティ警告の画面が出る場合は、内容を確認して [実行（R）] を押します。

図 37: セキュリテイ警告画面

.jnlp ファイルを開くときには、最新の JRE バージョン（Javaws）を使用してください。

4. BMC の IP アドレスと、ユーザー名、パスワードを入力するウィンドウが表示されるため、それぞれ入力して [Connect] を押します。

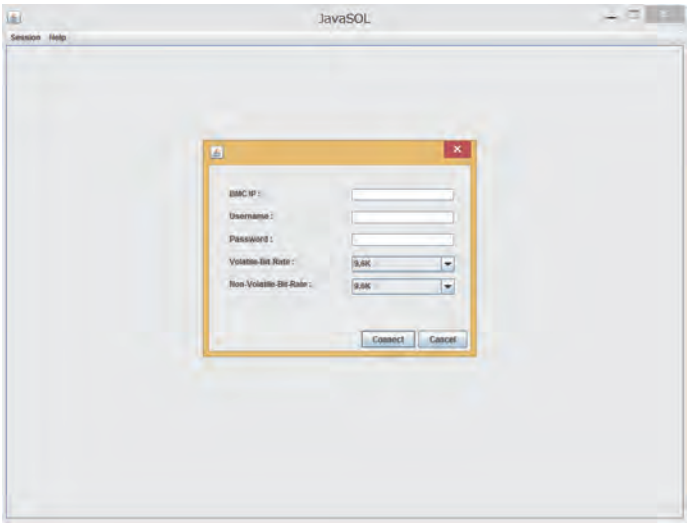

図 38: 入力ウィンドウ

5. Java SOL が起動し、ウィンドウが開きます。

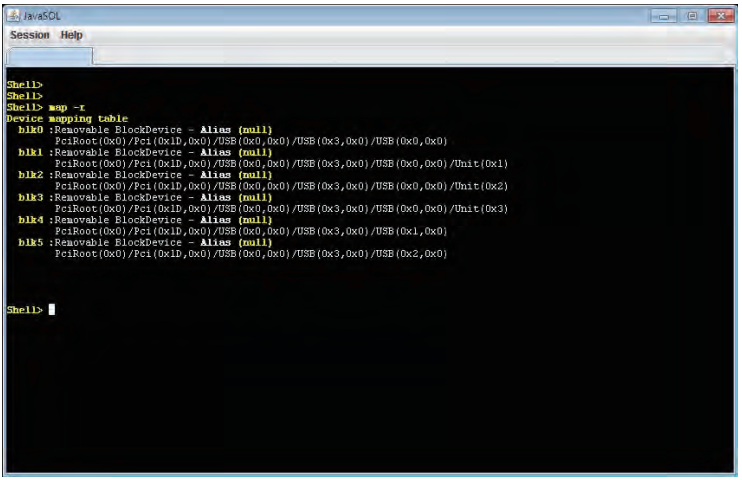

図 39: Java SOL

2.10 Image Redirection

このページを使用して、イメージをリダイレクト用に BMC に構成することができます。

「Image Redirection」ページには「Remote Images」設定があります。

図 40: Image Redirection ページ

2.10.1 Remote Images

この表には、BMC の構成済みイメージが表示されています。リモートメディアサーバのイメージを設定できます。

このページを設定するには、まず「GeneralSetting」ページの（「Settings」、「Media Redirection Setting」、「General Setting」の順にクリックします。）「Remote Media Support」オプションにチェックを入れて、有効にする必要があります。

図 41: Remote Media ページ

2.11 Power Control

このページでは、サーバの電源の表示と制御ができます。

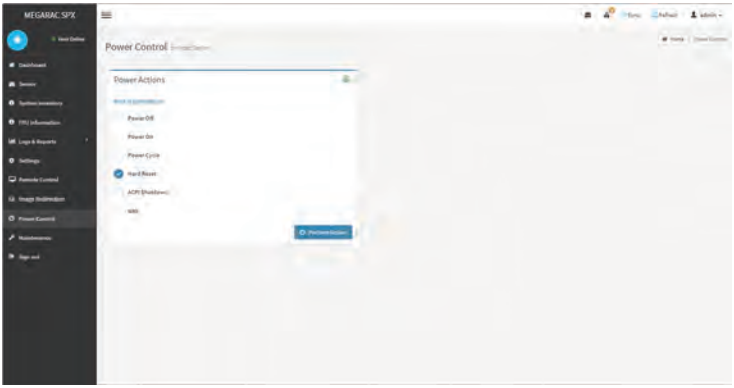

図 42: Power Control ページ

電源制御の各種オプションを次に示します。

アイテム	説明
Power Off	このオプションで、サーバの電源を即座に切断します。
Power on	このオプションで、サーバの電源を投入します。
Power Cycle	このオプションで、電源をいったん切断してからシステムを再起動します（コールドブート）。
Hard Reset	このオプションで、電源をオフにせずにシステムを再起動します（ウォームブート）。
ACPI Shutdown	このオプションで、ACPI のシャットダウンを実行します。
NMI	NMI（マスク不可割り込み）を発生させます。
Perform Action	このオプションをクリックして、選択した操作を実行します。

表 30: Power Actions

手順

アクションを選択して「Perform Action」をクリックすると、選択したアクションを実行します。

選択を確定するメッセージが表示されます。確定すると、コマンドが実行され、ステータスが通知されます。

2.12 Maintenance

このページでは、デバイスの保守作業を行うことができます。この Maintenance ページには「Backup Configuration」、「Firmware Information」、「Firmware Update」、「BIOS update」、「Preserve Configuration」、「Restore Configuration」、「Restore Factory Defaults」の項目があります。

図 43: Maintenance ページ

2.12.1 Backup Configuration

このページでは、「Backup Configuration」時にバックアップする特定の構成項目を選択することができます。

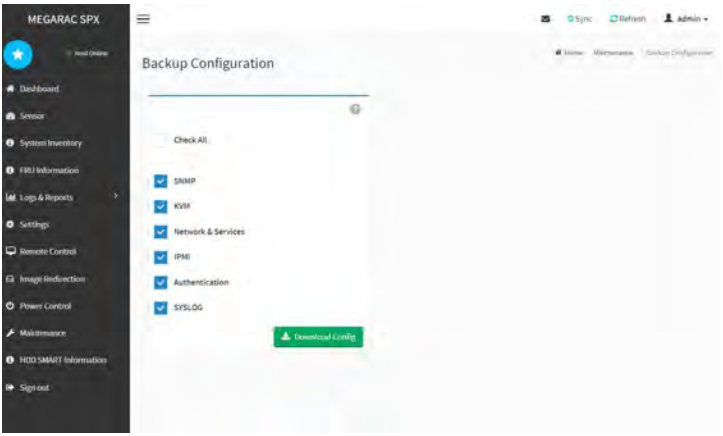

図 44: Backup Configuration ページ

次に「Backup Configuration」ページの各種オプションについて説明します。

アイテム	説明
Check All	このオプションで、すべてを有効にします。
SNMP	このオプションで、SNMPを有効にします。
KVM	このオプションで、KVM を有効にします。
Network & Services	このオプションで、Network & Services を有効にします。
IPMI	このオプションで、IPMI を有効にします。
Authentication	このオプションで、認証を有効にします。
SYSLOG	このオプションで、SYSLOG を有効にします。
Download Config	オプションが有効になった各項目の設定情報を含んだConfig ファイルをダウンロードします。

表31: Backup Configuration

手順

1. アイテムを選択して「Download Config」をクリックすると、設定データ "xxx.bak" ファイルを保存します。

2.12.2 Firmware Information

このページを使用して、ファームウェア情報を表示します。

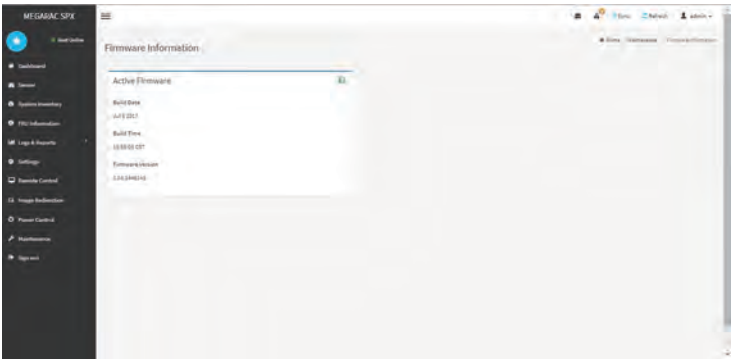

図 45: Firmware Information ページ

次に「Firmware Information」ページのフィールドについて説明します。

アイテム	説明
Active Firmware	
Build Date	作成年月を表示します。
Build Time	作成時間を表示します。
Firmware version	ファームウェアバージョンを表示します。

表 32: Firmware Information

2.12.3 Firmware Update

このページを使用して、ファームウェアアップグレード処理を行うことができます。アップグレードが完了するかキャンセルすると、ボックスのリセットが自動的に行われます。設定を保存するためのオプションが表示されます。

アップグレードを通じて構成された設定を保存するには、このオプションを有効にします。

注意！

アップデートモードウィジェットに移行すると、他の Web ページやサービスが動作しなくなることにご注意ください。開いているすべてのウィジェットは自動的に閉じます。ウィザードの途中でアップグレード処理をキャンセルすると、デバイスがリセットされます。

ファームウェアアップグレード処理は極めて重要な操作です。この操作中は、電力損失や接続損失の可能性を最小限にしてください。

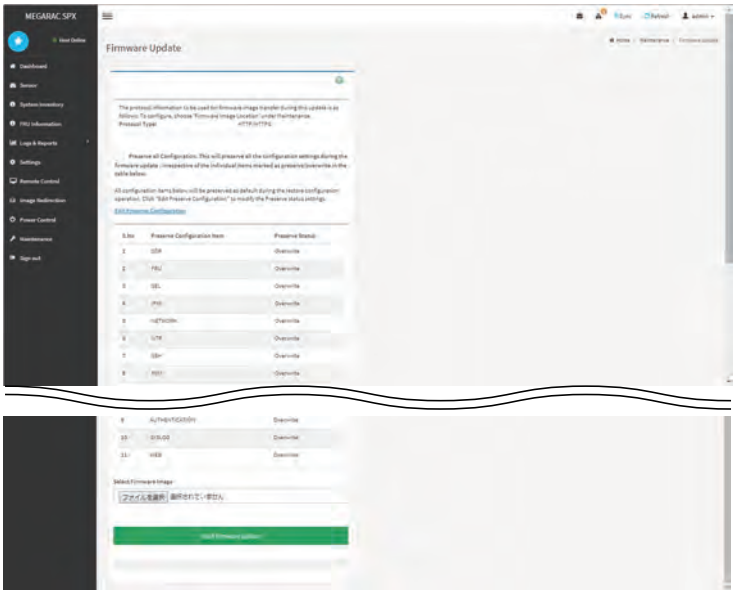

図 46: Firmware Update ページ

手順

「Start firmware update」をクリックして現在のデバイスのファームウェアをアップグレードします。次の手順に従います。

「Preserve Configuration」オプションにチェックを入れると、ファームウェアの更新中はすべての構成設定が保持されます。ページの Preserve Status 欄に preserve/overwrite (保存 / 上書き) とマークされた個々の項目とは無関係です。

1. アクティブなすべてのクライアント要求を終了します。
2. デバイスでファームウェアアップグレードの準備をします。
3. 「Select Firmware Image」フィールドからファームウェアイメージ(.ima)を選択します。
4. ファームウェアイメージを確認します。
5. ファームウェアイメージをフラッシュします。
6. デバイスをリセットします。

適切なBMCファームウェアイメージは以下のWebサイトからダウンロードできます。
http://jp.fujitsu.com/platform/server/primergy/bios/

2.12.4 BIOS update

このページを使用して、BIOSアップグレード処理を行うことができます。アップグレードが完了するかキャンセルすると、ボックスのリセットが自動的に行われます。

注意！

アップデートモードウィジェットに移行すると、他の Web ページやサービスが動作しなくなることにご注意ください。開いているすべてのウィジェットは自動的に閉じます。ウィザードの途中でアップグレード処理をキャンセルすると、デバイスがリセットされます。

BIOSアップグレード処理は極めて重要な操作です。この操作中は、電力損失や接続損失の可能性を最小限にしてください。

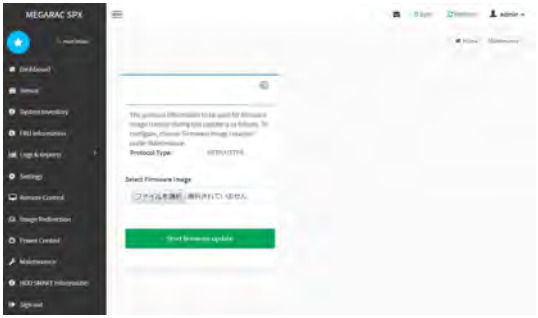

図 47: BIOS update ページ

手順

「Start firmware update」をクリックして現在のデバイスのファームウェアをアップグレードします。次の手順に従います。

1. アクティブなすべてのクライアント要求を終了します。
2. デバイスでファームウェアアップグレードの準備をします。
3. 「Select Firmware Image」フィールドからBIOSイメージ(.bin)を選択します。
4. ファームウェアイメージを確認します。
5. ファームウェアイメージをフラッシュします。
6. デバイスをリセットします。

適切なBIOSイメージは以下のWebサイトからダウンロードできます。
http://jp.fujitsu.com/platform/server/primergy/bios/

2.12.5 Preserve Configuration

このページでは、ファームウェアアップグレードまたは工場出荷時設定へのリストアを行う際に、既存の設定を保持する項目をユーザーが設定できます。

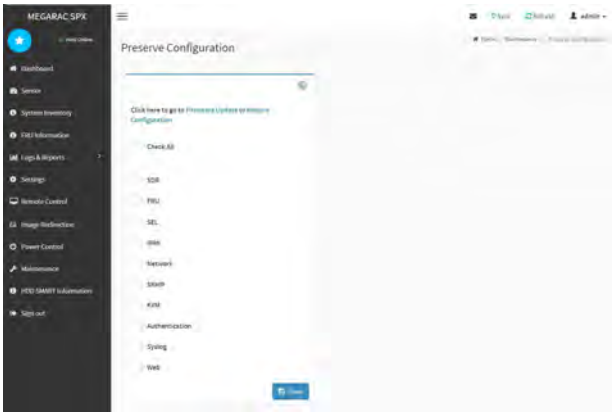

図 48: Preserve Configuration ページ

次に「Preserve Configuration」ページの各種オプションについて説明します。

アイテム	説明
Check All	このオプションで、すべてを有効にします。
SDR	このオプションで、SDR を有効にします。
FRU	このオプションで、FRU を有効にします。
SEL	このオプションで、SEL を有効にします。
IPMI	このオプションで、IPMI を有効にします。
Network	このオプションで、Network を有効にします。
SNMP	このオプションで、SNMP を有効にします。
KVM	このオプションで、KVM を有効にします。
Authentication	このオプションで、Authentication を有効にします。
Syslog	このオプションで、Syslog を有効にします。
Web	このオプションで、Web を有効にします。
Save	設定を保存します。

表 33: Preserve Configuration

手順

アイテムを選択して「Save」をクリックすると、設定データファイルを保存します。

2.12.6 Restore Configuration

このページを使用して、クライアントシステムから BMC に構成ファイルを復元できます。

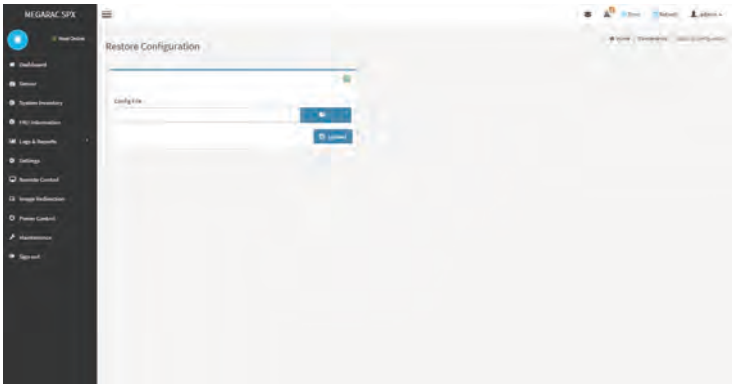

図 49: Restore Configuration ページ

手順

1. 「Config File」フィールドから設定ファイル "xxx.bak" を選択します。
2. 「Upload」をクリックすると、設定データをアップロードします。

2.12.7 Restore Factory Defaults

このページを使用して、デバイスファームウェアを工場出荷時の構成に戻します。

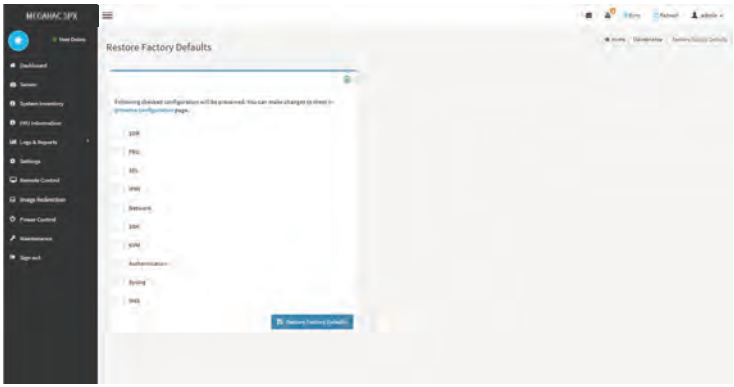

図 50: Restore Factory Defaults ページ

次に「Restore Factory Defaults」ページの各種オプションについて説明します。

アイテム	説明
SDR	このオプションで、SDR を有効にします。
FRU	このオプションで、FRU を有効にします。
SEL	このオプションで、SEL を有効にします。
IPMI	このオプションで、IPMI を有効にします。
Network	このオプションで、Network を有効にします。
SSH	このオプションで、SSH を有効にします。
KVM	このオプションで、KVM を有効にします。
Authentication	このオプションで、Authentication を有効にします。
Syslog	このオプションで、Syslog を有効にします。
Web	このオプションで、Web を有効にします。
Restore Factory Defaults	デバイスファームウェアを工場出荷時の構成に戻します。

表 34: Restore Factory Defaults

手順

アイテムを選択して「Restore Factory Defaults」をクリックすると、デバイスファームウェアを工場出荷時の構成に戻します。

2.13 HDD SMART Information

このページでは、サーバで使用されている HDD/SSD の S.M.A.R.T. 情報の確認ができます。

S.M.A.R.T. 情報を表示するためには、使用 OS 上にDisk agent software がインストールされている必要が有ります。
詳細については、『PRIMERGY CX1430 M1 Disk agent software 取扱説明書』を参照してください。

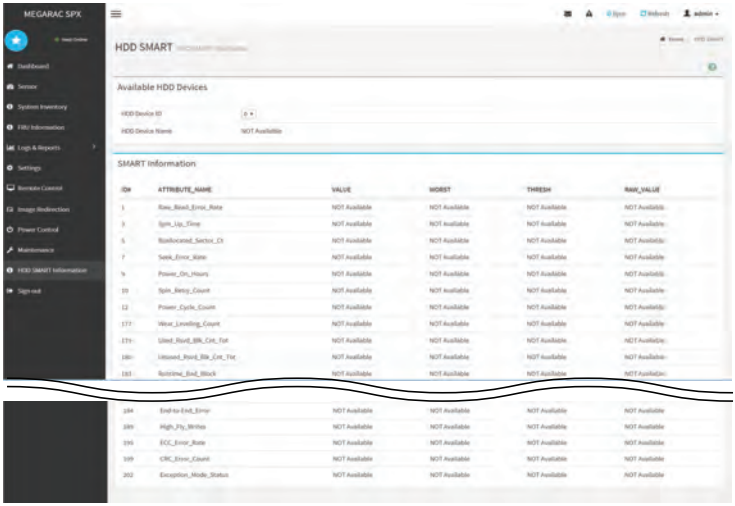

図 51: HDD SMART Information

2.14 Sign out

BMC GUI をサインアウトするには、「Sign out」をクリックします。小ウィンドウの「OK」をクリックしてサインアウトします。

図 52: Sign out

3 Remote BIOS Setup

Remote BIOS Setup 機能を使用することで、Web ブラウザを使用して、システムのシステム機能とハードウェア構成を設定することができます。

各設定メニューの詳細については、『FUJITSU Server PRIMERGY CX1430 M1 用 D3880 BIOS セットアップユーティリティ』を参照してください。
変更した設定はシステムの再起動後に有効となります。

3.1 ログイン

Remote BIOS Setup（Web BIOS）を使用するには、Web ブラウザから以下の URL でアクセスします。

URL：http://BMC_ip_address/bios/Index.html

起動するとユーザー名、パスワードを入力するウィンドウが表示されるため、それぞれ入力して [ログイン] を押します。

フィールド	デフォルト
ユーザー名	Administrator
パスワード	superuser

表 35: デフォルトユーザー名とパスワード

図 53: 入力ウィンドウ

3.2 メニュー画面

Main：Bios のバージョンやメモリ容量などを確認できます。

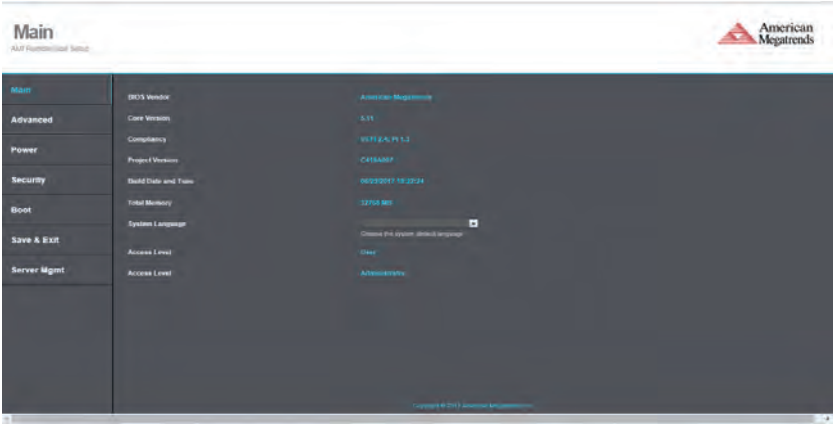

図 54: Main 画面

Advanced：ハードウェアの設定確認、変更ができます。

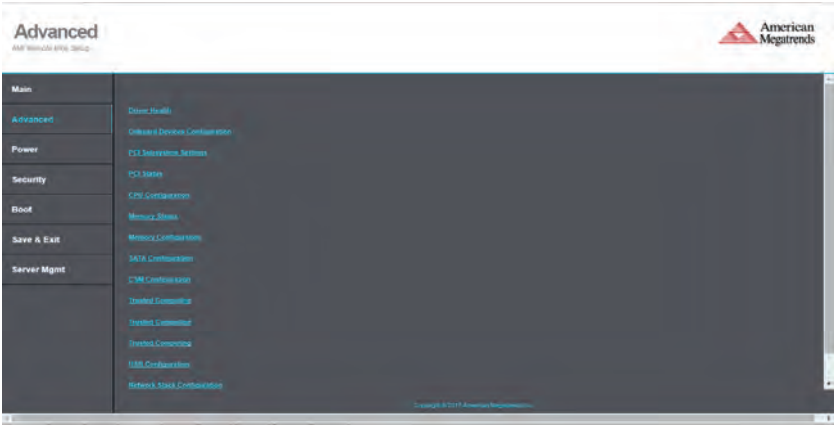

図 55: Advanced 画面

Power：電源に関する設定の確認、変更ができます。

図 56: Power 画面

Security：パスワードの設定、変更ができます。

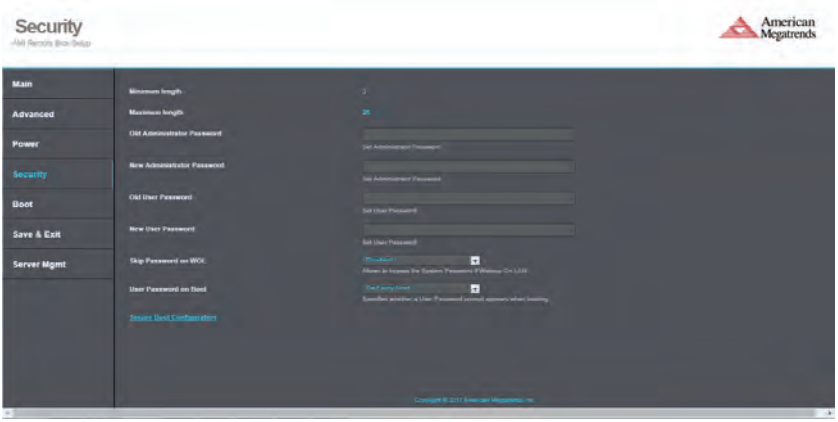

図 57: Security 画面

Boot：起動オプションの設定変更、確認ができます。

図 58: Boot 画面

Save & Exit：変更した設定を保存します。

図 59: Save & Exit 画面

Remote BIOS Setup（Web BIOS）を終了させるには、お使いのブラウザを閉じてください。

Server Mgmt : BMC のバージョンや、デバイス ID を確認できます。
また、イベントログの設定を確認、変更できます。

図 60: Server Mgmt 画面

Remote BIOS Setupに表示されるBIOS設定は、BIOS セットアップユーティリティのセーブ時に更新されます。このため、DIMM の増設など、ハードウェア変更を行った後には、一度BIOS セットアップユーティリティからセーブを実施してください。

4 サポートされる IPMI OEM コマンド

4.1 概要

BMC は標準的な IPMI コマンドに加え、OEM 固有のコマンドをサポートしています。下表は BMC で使用可能なすべての IPMI OEM コマンドです。

次に、BMC ファームウェアでサポートする IPMI OEM コマンドの一覧を示します。

Command Set	Net Function	CMD Code
Set BMC reset options Command	0x30	0x20
Get BMC reset options command	0x30	0x21
Get Board ID command	0x30	0xA8
Get Node Slot ID command	0x30	0xA9
Set CX600 Chassis Fan Duty Command	0x30	0xA4
Get CX600 Chassis Fan Duty Command	0x30	0xA5
Set Power On/Off Time Command	0x30	0xAA
Get Power On/Off Time Command	0x30	0xAB
Clear Power On/Off Time Command	0x30	0xAC
Get SEL Policy Command	0x32	0x7E
Set SEL Policy Command	0x32	0x7F
Get iKVM Option Command	0x30	0x80
Clear Global Error LED Command	0x30	0xAD
Get System MAC Address Command	0x30	0xB7

表 36: IPMI OEM コマンド一覧

4.2 IPMI OEM コマンドの記述

4.2.1 Set BMC Option Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0x20	**Request:** Byte 1 - Disable Mask 0x00= Enable SMI timeout reset action 0x01= Disable SMI timeout reset action **Response:** Byte 1 - Completion code.	「SMI タイムアウトリセットアクション」のデフォルト設定は無効です。 BMC が SMI 信号を検出して 120 秒間 Low に保たれ、「SMI タイムアウトリセットアクション」が有効になっている場合、BMC はシステムをリセットします。

4.2.2 Get BMC Reset Option Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0x21	**Request: N/A** **Response:** Byte 1 - Completion Code Byte 2 - 0x00= Enable SMI timeout reset action 0x01= Disable SMI timeout reset action	「SMI タイムアウトリセットアクション」の状態を読み取ります。

4.2.3 Get Board ID Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xA8	**Request: N/A** **Response:** Byte 1 - Completion Code. Byte 2 - Board ID number.	

4.2.4 Get Node Slot ID Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xA9	**Request: N/A** **Response:** Byte 1 - Completion Code. Byte 2 - Node Slot ID number.	

4.2.5 Set CX600 Chassis Fan Duty Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xA4	**Request:** Byte 1 - PWM value. (0~100%) (0 ~ 0x64) **Response:** Byte 1 - Completion Code.	BMC はこの OEM コマンドを受信した後にファンカーブの制御を停止するので、このコマンドを BMC に送信した後に BMC をリセットしてください。

4.2.6 Get CX600 Chassis Fan Duty Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xA5	**Request: N/A.** **Response:** Byte 1 - Completion Code Byte 2 - Current PWM reading. (0~100%) (0 ~ 0x64)	

4.2.7 Set Power On/Off Time Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xA4	**Request:** Byte 1 - Day. Sunday = 0x00 Monday = 0x01 Tuesday = 0x02 Wednesday = 0x03 Thursday = 0x04 Friday = 0x05 Saturday = 0x0h Byte 2 - Hour (00~23) Byte 3 - Minutes (00~59) Byte 4 - Power On/Off 0x00 = Turn off the power. 0x01 = Turn on the power. **Response:** Byte 1 - Completion Code.	

4.2.8 Get Power On/Off Time Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xAB	**Request:** Byte 1 - 0x00 = Get power off time. 0x01 = Get power on time. **Response:** Byte 1 - Completion Code. Byte 2 - Day. Sunday = 0x00 Monday = 0x01 Tuesday = 0x02 Wednesday = 0x03 Thursday = 0x04 Friday = 0x05 Saturday = 0x06 Byte 3 - Hour (00 ~ 23) Byte 4 - Minutes (00~59)	

4.2.9 Clear Power On/Off Time Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xAC	**Request:** Byte 1 - 0x 00 = Clear power off time. 0x01 = Clear power on time. 0x 02 = Clear power on/off time. **Response:** Byte 1 - Completion Code.	

4.2.10 Get SEL Policy Command

Net Func	CMD Code	Request/Response Data	Description
0x32	0x7E	**Request: N/A** **Response:** Byte 1 - Completion Code. Byte 2 -SEL Policy. 00h = Linear SEL. 01h = Circular SEL.	BMC のデフォルトは循環 SEL ポリシーです。

4.2.11 Set SEL Policy Command

Net Func	CMD Code	Request/Response Data	Description
0x32	0x7F	**Request:** Byte 1 - SEL Policy. 0x00 = Linear SEL. 0x01 = Circular SEL. **Response:** Byte 1 - Completion Code.	BMC のデフォルトは循環 SEL ポリシーです。

4.2.12 Get iKVM Option Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0x80	**Request: N/A** **Response:** Byte 1 - Completion Code. Byte 2 - 0x00 = Disable iKVM. 0x01 = Enable iKVM.	

4.2.13 Clear Global Error LED Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xAD	**Request: N/A** **Response:** Byte 1 - Completion Code.	

4.2.14 Get System MAC Address Command

Net Func	CMD Code	Request/Response Data	Description
0x30	0xB7	**Request:** Byte 1 - 0: X557 Lan1 1: X557 Lan2 2: I210 Lan1 **Response:** Byte 1 - Completion Code. Byte 2 - MAC address Byte 0 Byte 3 - MAC address Byte 1 Byte 4 - MAC address Byte 2 Byte 5 - MAC address Byte 3 Byte 6 - MAC address Byte 4 Byte 7 - MAC address Byte 5	