日立アドバンストサーバ
HA8000シリーズ

HITACHI
Inspire the Next

ユーザーズガイド

～リモートマネジメント編～

HA8000/RS220-h HM1/JM1/KM1/LM1
HA8000/RS210-h HM1/JM1/KM1/LM1

2012年11月～モデル

マニュアルはよく読み、保管してください。
製品を使用する前に、安全上の指示をよく読み、十分理解してください。
このマニュアルは、いつでも参照できるよう、手近な所に保管してください。

R2EAM11600-2

登録商標・商標

Microsoft、Windows、Windows Server、Hyper-V は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

インテル、Intel、Xeon はアメリカ合衆国およびその他の国における Intel Corporation の商標または登録商標です。

Linux は Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

Red Hat は米国およびその他の国における Red Hat, Inc. の商標または登録商標です。

VMware、vCenter、VMware vSphere、ESX、ESXi は米国およびその他の国における VMware, Inc. の登録商標または商標です。

ENERGY STAR と ENERGY STAR マークは、米国の登録商標です。

80PLUS は、米国 Ecos Consulting, Inc. の米国およびその他の国における登録商標または商標です。

そのほか、本マニュアル中の製品名および会社名は、各社の商標または登録商標です。

発行

2012 年 11 月（初 版）（廃 版）
2013 年 6 月（第 2 版）

版権

お知らせ

重要なお知らせ

- 本書の内容の一部、または全部を無断で転載したり、複写することは固くお断わりします。
- 本書の内容について、改良のため予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、万一ご不審な点や誤りなど、お気付きのことがありましたら、お買い求め先へご一報くださいますようお願いいたします。
- 本書に準じないで本製品を運用した結果については責任を負いません。
  なお、保証と責任については保証書裏面の「保証規定」をお読みください。

システム装置の信頼性について

ご購入いただきましたシステム装置は、一般事務用を意図して設計・製作されています。生命、財産に著しく影響のある高信頼性を要求される用途への使用は意図されていませんし、保証もされていません。このような高信頼性を要求される用途へは使用しないでください。
高信頼性を必要とする場合には別システムが必要です。弊社営業部門にご相談ください。

一般事務用システム装置が不適当な、高信頼性を必要とする用途例
・化学プラント制御　・医療機器制御　・緊急連絡制御など

規制・対策などについて

❑ 電波障害自主規制について

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

❑ 電源の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て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。

❑ 高調波電流規格：JIS C 61000-3-2 適合品

JIS C 61000-3-2 適合品とは、日本工業規格「電磁両立性 — 第 3-2 部：限度値 — 高調波電流発生限度値（1 相当たりの入力電流が 20A 以下の機器）」に基づき、商用電力系統の高調波環境目標レベルに適合して設計・製造した製品です。

❑ 雑音耐力について

本製品の外来電磁波に対する耐力は、国際電気標準会議規格 IEC61000-4-3「放射無線周波電磁界イミュニティ試験」のレベル 2 に相当する規定に合致していることを確認しております。

なお、レベル 2 とは、対象となる装置に近づけないで使用されている低出力の携帯型トランシーバから受ける程度の電磁環境です。

❑ 輸出規制について

本製品を輸出される場合には、外国為替および外国貿易法の規制ならびに米国の輸出管理規制など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、お買い求め先にお問い合わせください。

また、本製品に付属する周辺機器やソフトウェアも同じ扱いとなります。

❑ 海外での使用について

本製品は日本国内専用です。国外では使用しないでください。

なお、他国には各々の国で必要となる法律、規格などが定められており、本製品は適合していません。

❑ ENERGY STAR® 適合モデルについて

当社は ENERGY STAR の参加事業者として、ENERGY STAR for Computer Servers Version 1.1 基準を満たしていると判断します。
ENERGY STAR は、米国環境保護庁および米国エネルギー省の定める省エネルギー化推進のためのプログラムです。このプログラムは、エネルギー消費を効率的に抑えるための機能を備えた製品の開発、普及の促進を目的としたもので、事業者の自己判断により参加することができる任意制度となっています。ENERGY STAR を取得した製品は、米国環境保護庁および米国エネルギー省の定める厳しいエネルギー効率ガイドラインを満たすことにより温室効果ガスの排出を抑制します。

❑ システム装置の廃棄について

事業者が廃棄する場合、廃棄物管理表（マニフェスト）の発行が義務づけられています。詳しくは、各都道府県産業廃棄物協会にお問い合わせください。廃棄物管理表は（社）全国産業廃棄物連合会に用意されています。個人が廃棄する場合、お買い求め先にご相談いただくか、地方自治体の条例または規則にしたがってください。

また、システム装置内の電池を廃棄する場合もお買い求め先にご相談いただくか、地方自治体の条例または規則にしたがってください。

システム装置の廃棄・譲渡時のデータ消去に関するご注意

システム装置を譲渡あるいは廃棄するときには、ハードディスク / SSD の重要なデータ内容を消去する必要があります。
ハードディスク / SSD 内に書き込まれた「データを消去する」という場合、一般に

- データを「ゴミ箱」に捨てる
- 「削除」操作を行う
- 「ゴミ箱を空にする」コマンドを使って消す
- ソフトで初期化（フォーマット）する
- OS を再インストールする

などの作業をしますが、これらのことをしても、ハードディスク / SSD 内に記録されたデータのファイル管理情報が変更されるだけです。つまり、一見消去されたように見えますが、OS のもとでそれらのデータを呼び出す処理ができなくなっただけであり、本来のデータは残っているという状態にあります。
したがって、データ回復のためのソフトウェアを利用すれば、これらのデータを読みとることが可能な場合があります。このため、悪意のある人により、システム装置のハードディスク / SSD 内の重要なデータが読みとられ、予期しない用途に利用されるおそれがあります。

ハードディスク / SSD 上の重要なデータの流出を回避するため、システム装置を譲渡あるいは廃棄をする前に、ハードディスク / SSD に記録された全データをお客様の責任において消去することが非常に重要です。
消去するためには、専用ソフトウェアあるいはサービス（共に有償）を利用するか、ハードディスク / SSD を金槌や強磁気により物理的・磁気的に破壊して、データを読めなくすることをお勧めします。

なお、ハードディスク / SSD 上のソフトウェア（OS、アプリケーションソフトなど）を削除することなくシステム装置を譲渡すると、ソフトウェアライセンス使用許諾契約に抵触する場合があるため、十分な確認を行う必要があります。

ソフトウェアのライセンス情報

本製品に組み込まれたソフトウェアは、複数の独立したソフトウェアで構成され、個々のソフトウェアはそれぞれ日立または第三者の著作権が存在します。

本製品に含まれる日立自身が開発または作成したソフトウェアには、日立の所有権および知的財産権が存在します。また、同様にこれらのソフトウェアに付帯したドキュメントなどにも、日立の所有権および知的財産権が存在します。これらについては、著作権法その他の法律により保護されています。

本製品では、日立自身の開発または作成したソフトウェアのほかに、以下のオープンソースソフトウェアをそれぞれのソフトウェア使用許諾契約書にしたがい使用しています。

ソフトウェア名	関連ソフトウェア使用許諾契約書
XML_RPC	BSD-style License 次のリンク先をご確認ください。 http://xmlrpc-c.svn.sourceforge.net/viewvc/xmlrpc-c/trunk/doc/COPYING?view=markup
Net-SNMP	BSD License 次のリンク先をご確認ください。 http://www.net-snmp.org/about/license.html

はじめに

このたびは日立のシステム装置をお買い上げいただき、誠にありがとうございます。このマニュアルは、システム装置に標準搭載されているリモートマネジメント機能と、Web コンソールによる操作方法および設定項目について記載しています。

マニュアルの表記

マニュアル内で使用しているマークの意味は次のとおりです。

⚠警告	これは、死亡または重大な傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
⚠注意	これは、軽度の傷害、あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
通知	これは、人身傷害とは関係のない損害を引き起こすおそれのある場合に用います。
	システム装置の故障や障害の発生を防止し、正常に動作させるための事項を示します。
	システム装置を活用するためのアドバイスを示します。

❑ システム装置の表記について

このマニュアルでは、システム装置を装置と略して表記することがあります。

また、システム装置を区別する場合には次のモデル名で表記します。

- RS220-h HM1/JM1/KM1/LM1 モデル
- RS210-h HM1/JM1/KM1/LM1 モデル

システム装置のモデルすべてを表す場合には

- RS220-h xM1 モデル
- RS210-h xM1 モデル

と表記します。

❑ オペレーティングシステム（OS）の略称について

このマニュアルでは、次の OS 名称を省略して表記します。

- Microsoft® Windows Server® 2012 Standard 日本語版
  （以下 Windows Server 2012 Standard または Windows Server 2012、Windows）
- Microsoft® Windows Server® 2012 Datacenter 日本語版
  （以下 Windows Server 2012 Datacenter または Windows Server 2012、Windows）
- Microsoft® Windows Server® 2008 R2 Standard 日本語版
  （以下 Windows Server 2008 R2 Standard または Windows Server 2008 R2、Windows）
- Microsoft® Windows Server® 2008 R2 Enterprise 日本語版
  （以下 Windows Server 2008 R2 Enterprise または Windows Server 2008 R2、Windows）
- Microsoft® Windows Server® 2008 R2 Datacenter 日本語版
  （以下 Windows Server 2008 R2 Datacenter または Windows Server 2008 R2、Windows）
- Microsoft® Windows Server® 2008 Standard 日本語版
  （以下 Windows Server 2008 Standard または Windows Server 2008、Windows）
- Microsoft® Windows Server® 2008 Enterprise 日本語版
  （以下 Windows Server 2008 Enterprise または Windows Server 2008、Windows）
- Microsoft® Windows Server® 2008 Datacenter 日本語版
  （以下 Windows Server 2008 Datacenter または Windows Server 2008、Windows）
- Microsoft® Windows Server® 2008 Standard without Hyper-V® 日本語版
  （以下 Windows Server 2008 Standard without Hyper-V または
  Windows Server 2008 Standard、Windows Server 2008、Windows）
- Microsoft® Windows Server® 2008 Enterprise without Hyper-V® 日本語版
  （以下 Windows Server 2008 Enterprise without Hyper-V または
  Windows Server 2008 Enterprise、Windows Server 2008、Windows）
- Microsoft® Windows Server® 2008 Datacenter without Hyper-V® 日本語版
  （以下 Windows Server 2008 Datacenter without Hyper-V または
  Windows Server 2008 Datacenter、Windows Server 2008、Windows）
- Microsoft® Windows Server® 2003 R2, Standard Edition 日本語版
  （以下 Windows Server 2003 R2, Standard Edition または
  Windows Server 2003 R2（32 ビット）、Windows Server 2003 R2、Windows）
- Microsoft® Windows Server® 2003 R2, Enterprise Edition 日本語版
  （以下 Windows Server 2003 R2, Enterprise Edition または
  Windows Server 2003 R2（32 ビット）、Windows Server 2003 R2、Windows）
- Microsoft® Windows Server® 2003 R2, Standard x64 Edition 日本語版
  （以下 Windows Server 2003 R2, Standard x64 Edition または
  Windows Server 2003 R2 x64 Editions、Windows Server 2003 R2、Windows）
- Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition 日本語版
  （以下 Windows Server 2003 R2, Enterprise x64 Edition または
  Windows Server 2003 R2 x64 Editions、Windows Server 2003 R2、Windows）
- Microsoft® Windows Server® 2003, Standard Edition 日本語版
  （以下 Windows Server 2003, Standard Edition または
  Windows Server 2003（32 ビット）、Windows Server 2003、Windows）
- Microsoft® Windows Server® 2003, Enterprise Edition 日本語版
  （以下 Windows Server 2003, Enterprise Edition または
  Windows Server 2003（32 ビット）、Windows Server 2003、Windows）

- Microsoft® Windows Server® 2003, Standard x64 Edition 日本語版
  （以下 Windows Server 2003, Standard x64 Edition または
  Windows Server 2003 x64 Editions、Windows Server 2003、Windows）
- Microsoft® Windows Server® 2003, Enterprise x64 Edition 日本語版
  （以下 Windows Server 2003, Enterprise x64 Edition または
  Windows Server 2003 x64 Editions、Windows Server 2003、Windows）
- Microsoft® Windows ® 7 Professional 日本語版
  （以下 Windows 7 Professional または Windows 7、Windows）
- Microsoft® Windows® Vista Business 日本語版
  （以下 Windows Vista Business または Windows Vista、Windows）
- Microsoft® Windows® XP Professional 日本語版
  （以下 Windows XP Professional または Windows XP、Windows）
- Microsoft® Windows® XP Professional x64 Edition 日本語版
  （以下 Windows XP Professional x64 Edition または Windows XP、Windows）
- Red Hat Enterprise Linux Server 6.4（64-bit x86_64）
  （以下 RHEL6.4（64-bit x86_64）または RHEL6.4、RHEL6、Linux）
- Red Hat Enterprise Linux Server 6.4（32-bit x86）
  （以下 RHEL6.4（32-bit x86）または RHEL6.4、RHEL6、Linux）
- Red Hat Enterprise Linux Server 6.2（64-bit x86_64）
  （以下 RHEL6.2（64-bit x86_64）または RHEL6.2、RHEL6、Linux）
- Red Hat Enterprise Linux Server 6.2（32-bit x86）
  （以下 RHEL6.2（32-bit x86）または RHEL6.2、RHEL6、Linux）
- Red Hat Enterprise Linux 5.7（AMD/Intel 64）
  （以下 RHEL5.7（AMD/Intel 64）または RHEL5.7、RHEL5、Linux）
- Red Hat Enterprise Linux 5.7（x86）
  （以下 RHEL5.7（x86）または RHEL5.7、RHEL5、Linux）
- VMware vSphere® ESXi™ 5.1
  （以下 VMware vSphere ESXi 5.1 または VMware vSphere ESXi、VMware）
- VMware vSphere® ESXi™ 5.0
  （以下 VMware vSphere ESXi 5.0 または VMware vSphere ESXi、VMware）
- VMware vSphere® ESX® 4.1
  （以下 VMware vSphere ESX 4.1 または VMware vSphere ESX、VMware）

なお次のとおり、省略した「OS 表記」は、「対象 OS」中のすべてまたは一部を表すときに用います。

OS 表記	対象 OS
Windows Server 2012 Standard *1	· Windows Server 2012 Standard *1
Windows Server 2012 Datacenter *1	· Windows Server 2012 Datacenter *1
Windows Server 2012 *1	· Windows Server 2012 Standard *1 · Windows Server 2012 Datacenter *1
Windows Server 2008 R2 Standard *1	· Windows Server 2008 R2 Standard *1
Windows Server 2008 R2 Enterprise *1	· Windows Server 2008 R2 Enterprise *1
Windows Server 2008 R2 Datacenter *1	· Windows Server 2008 R2 Datacenter *1
Windows Server 2008 R2 *1	· Windows Server 2008 R2 Standard *1 · Windows Server 2008 R2 Enterprise *1 · Windows Server 2008 R2 Datacenter *1
Windows Server 2008 Standard *2	· Windows Server 2008 Standard *2 · Windows Server 2008 Standard without Hyper-V *2
Windows Server 2008 Enterprise *2	· Windows Server 2008 Enterprise *2 · Windows Server 2008 Enterprise without Hyper-V *2
Windows Server 2008 Datacenter *2	· Windows Server 2008 Datacenter *2 · Windows Server 2008 Datacenter without Hyper-V *2
Windows Server 2008 *2	· Windows Server 2008 Standard *2 · Windows Server 2008 Enterprise *2 · Windows Server 2008 Datacenter *2 · Windows Server 2008 Standard without Hyper-V *2 · Windows Server 2008 Enterprise without Hyper-V *2 · Windows Server 2008 Datacenter without Hyper-V *2
Windows Server 2003 R2（32 ビット）	· Windows Server 2003 R2, Standard Edition · Windows Server 2003 R2, Enterprise Edition
Windows Server 2003 R2 x64 Editions	· Windows Server 2003 R2, Standard x64 Edition · Windows Server 2003 R2, Enterprise x64 Edition
Windows Server 2003 R2	· Windows Server 2003 R2, Standard Edition · Windows Server 2003 R2, Enterprise Edition · Windows Server 2003 R2, Standard x64 Edition · Windows Server 2003 R2, Enterprise x64 Edition
Windows Server 2003（32 ビット）	· Windows Server 2003, Standard Edition · Windows Server 2003, Enterprise Edition
Windows Server 2003 x64 Editions	· Windows Server 2003, Standard x64 Edition · Windows Server 2003, Enterprise x64 Edition
Windows Server 2003	· Windows Server 2003, Standard Edition · Windows Server 2003, Enterprise Edition · Windows Server 2003, Standard x64 Edition · Windows Server 2003, Enterprise x64 Edition
Windows 7	· Windows 7 Professional
Windows Vista	· Windows Vista Business
Windows XP	· Windows XP Professional · Windows XP Professional x64 Edition

OS 表記	対象 OS
Windows	・ Windows Server 2012 Standard *1 ・ Windows Server 2012 Datacenter *1 ・ Windows Server 2008 R2 Standard *1 ・ Windows Server 2008 R2 Enterprise *1 ・ Windows Server 2008 R2 Datacenter *1 ・ Windows Server 2008 Standard *2 ・ Windows Server 2008 Enterprise *2 ・ Windows Server 2008 Datacenter *2 ・ Windows Server 2008 Standard without Hyper-V *2 ・ Windows Server 2008 Enterprise without Hyper-V *2 ・ Windows Server 2008 Datacenter without Hyper-V *2 ・ Windows Server 2003 R2, Standard Edition ・ Windows Server 2003 R2, Enterprise Edition ・ Windows Server 2003 R2, Standard x64 Edition ・ Windows Server 2003 R2, Enterprise x64 Edition ・ Windows Server 2003, Standard Edition ・ Windows Server 2003, Enterprise Edition ・ Windows Server 2003, Standard x64 Edition ・ Windows Server 2003, Enterprise x64 Edition ・ Windows 7 Professional ・ Windows Vista Business ・ Windows XP Professional ・ Windows XP Professional x64 Edition
RHEL6.4	・ RHEL6.4（64-bit x86_64） ・ RHEL6.4（32-bit x86）
RHEL6.2	・ RHEL6.2（64-bit x86_64） ・ RHEL6.2（32-bit x86）
RHEL6	・ RHEL6.4（64-bit x86_64） ・ RHEL6.4（32-bit x86） ・ RHEL6.2（64-bit x86_64） ・ RHEL6.2（32-bit x86）
RHEL5.7 RHEL5	・ RHEL5.7（AMD/Intel 64） ・ RHEL5.7（x86）
Linux	・ RHEL6.4（64-bit x86_64） ・ RHEL6.4（32-bit x86） ・ RHEL6.2（64-bit x86_64） ・ RHEL6.2（32-bit x86） ・ RHEL5.7（AMD/Intel 64） ・ RHEL5.7（x86）
VMware vSphere ESXi 5.1	・ VMware vSphere ESXi 5.1
VMware vSphere ESXi 5.0	・ VMware vSphere ESXi 5.0
VMware vSphere ESXi	・ VMware vSphere ESXi 5.1 ・ VMware vSphere ESXi 5.0
VMware vSphere ESX 4.1 VMware vSphere ESX	・ VMware vSphere ESX 4.1
VMware	・ VMware vSphere ESXi 5.1 ・ VMware vSphere ESXi 5.0 ・ VMware vSphere ESX 4.1

*1　64bit 版のみ提供されます。

*2　「OS 表記」および「対象 OS」において、32bit 版のみを対象とする場合、名称末尾に “32bit 版” を追記します。
　　また、64bit 版のみを対象とする場合、名称末尾に “64bit 版” を追記します。

また、Windows の Service Pack についても SP と表記します。

安全にお使いいただくために

安全に関する注意事項は、下に示す見出しによって表示されます。これは安全警告記号と「警告」、「注意」および「通知」という見出し語を組み合わせたものです。

	これは、安全警告記号です。人への危害を引き起こす潜在的な危険に注意を喚起するために用います。起こりうる傷害または死を回避するためにこのシンボルのあとに続く安全に関するメッセージにしたがってください。
	これは、死亡または重大な傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
	これは、軽度の傷害、あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。

通知	これは、人身傷害とは関係のない損害を引き起こすおそれのある場合に用います。

【表記例 1】感電注意

△の図記号は注意していただきたいことを示し、△の中に「感電注意」などの注意事項の絵が描かれています。

【表記例 2】分解禁止

⃠の図記号は行ってはいけないことを示し、⃠の中に「分解禁止」などの禁止事項の絵が描かれています。
なお、⃠の中に絵がないものは、一般的な禁止事項を示します。

【表記例 3】電源プラグをコンセントから抜け

●の図記号は行っていただきたいことを示し、●の中に「電源プラグをコンセントから抜け」などの強制事項の絵が描かれています。
なお、❗は一般的に行っていただきたい事項を示します。

安全に関する共通的な注意について

次に述べられている安全上の説明をよく読み、十分理解してください。

- 操作は、このマニュアル内の指示、手順にしたがって行ってください。
- 本製品やマニュアルに表示されている注意事項は必ず守ってください。
- 本製品に搭載または接続するオプションなど、ほかの製品に添付されているマニュアルも参照し、記載されている注意事項を必ず守ってください。

これを怠ると、人身上の傷害やシステムを含む財産の損害を引き起こすおそれがあります。

操作や動作は

マニュアルに記載されている以外の操作や動作は行わないでください。
本製品について何か問題がある場合は、電源を切り、電源プラグをコンセントから抜いたあと、お買い求め先にご連絡いただくか保守員をお呼びください。

自分自身でもご注意を

本製品やマニュアルに表示されている注意事項は、十分検討されたものです。それでも、予測を超えた事態が起こることが考えられます。操作にあたっては、指示にしたがうだけでなく、常に自分自身でも注意するようにしてください。

一般的な安全上の注意事項

本製品の取り扱いにあたり次の注意事項を常に守ってください。

電源コードの取り扱い

電源コードは付属のものおよびサポートオプションを使用し、次のことに注意して取り扱ってください。取り扱いを誤ると、電源コードの銅線が露出したり、ショートや一部断線で過熱して、感電や火災の原因となります。

- 物を載せない
- 引っ張らない
- 押し付けない
- 折り曲げない
- ねじらない
- 加工しない
- 熱器具のそばで使用しない
- 加熱しない
- 束ねない
- ステップルなどで固定しない
- コードに傷がついた状態で使用しない
- 紫外線や強い可視光線を連続して当てない
- アルカリ、酸、油脂、湿気へ接触させない
- 高温環境で使用しない
- 定格以上で使用しない
- ほかの装置で使用しない
- 電源プラグを持たずにコンセントの抜き差しをしない
- 電源プラグを濡れた手で触らない

なお、電源プラグはすぐに抜けるよう、コンセントの周りには物を置かないでください。

タコ足配線

同じコンセントに多数の電源プラグを接続するタコ足配線はしないでください。コードやコンセントが過熱し、火災の原因となるとともに、電力使用量オーバーでブレーカが落ち、ほかの機器にも影響を及ぼします。

電源プラグの接触不良やトラッキング

電源プラグは次のようにしないと、トラッキングの発生や接触不良で過熱し、火災の原因となります。

- 電源プラグは根元までしっかり差し込んでください。
- 電源プラグはほこりや水滴が付着していないことを確認し、差し込んでください。付着している場合は乾いた布などで拭き取ってから差し込んでください。
- グラグラしないコンセントを使用してください。
- コンセントの工事は、専門知識を持った技術者が行ってください。

電池の取り扱い

電池の交換は保守員が行います。交換は行わないでください。また、次のことに注意してください。取り扱いを誤ると過熱・破裂・発火などでけがの原因となります。

- 充電しない
- ショートしない
- 分解しない
- 加熱しない
- 変形しない
- 焼却しない
- 水に濡らさない

修理・改造・分解

本マニュアルに記載のない限り、自分で修理や改造・分解をしないでください。感電や火災、やけどの原因となります。特に電源ユニット内部は高電圧部が数多くあり、万一さわると危険です。

レーザー光

DVD-ROM ドライブ、DVD-RAM ドライブや LAN の SFP+ モジュールなどレーザーデバイスの内部にはレーザー光を発生する部分があります。分解・改造をしないでください。また、内部をのぞきこんだりしないでください。レーザー光により視力低下や失明のおそれがあります。
（レーザー光は目に見えない場合があります。）

梱包用ポリ袋

装置の梱包用エアーキャップなどのポリ袋は、小さなお子様の手の届くところに置かないでください。かぶったりすると窒息するおそれがあります。

電源コンセントの取り扱い

電源コンセントは、使用する電圧および電源コードに合ったものを使用してください。その他のコンセントを使用すると感電のおそれがあります。
→『ユーザーズガイド ～導入編～』「1.3.3　コンセントについて」

目的以外の使用

踏み台やブックエンドなど、PC サーバとしての用途以外にシステム装置を利用しないでください。壊れたり倒れたりし、けがや故障の原因となります。

信号ケーブル

- ケーブルは足などをひっかけたり、ひっぱったりしないように配線してください。ひっかけたり、ひっぱったりするとけがや接続機器の故障の原因となります。また、データ消失のおそれがあります。
- ケーブルの上に重量物を載せないでください。また、熱器具のそばに配線しないでください。ケーブル被覆が破れ、接続機器などの故障の原因となります。

装置上に物を置く

システム装置の上には周辺機器や物を置かないでください。周辺機器や物がすべり落ちてけがの原因となります。また、置いた物の荷重によってはシステム装置の故障の原因となります。

ラックキャビネット搭載時の取り扱い

ラックキャビネット搭載時、装置上面の空きエリアを棚または作業空間として使用しないでください。装置上面の空きエリアに重量物を置くと、落下によるけがの原因となります。

眼精疲労

ディスプレイを見る環境は 300 ～ 1000 ルクスの明るさにしてください。また、ディスプレイを見続ける作業をするときは1時間に10分から15分程度の休息をとってください。長時間ディスプレイを見続けると目に疲労が蓄積され、視力の低下を招くおそれがあります。

装置の損害を防ぐための注意

装置使用環境の確認

装置の使用環境は『ユーザーズガイド ～導入編～』「1.2　設置環境」に示す条件を満足してください。たとえば、温度条件を超える高温状態で使用すると、内部の温度が上昇し装置の故障の原因となります。

使用する電源

使用できる電源は AC100V または AC200V です。それ以外の電圧では使用しないでください。電圧の大きさにしたがって内部が破損したり過熱・劣化して、装置の故障の原因となります。

温度差のある場所への移動

移動する場所間で温度差が大きい場合は、表面や内部に結露することがあります。結露した状態で使用すると装置の故障の原因となります。
すぐに電源を入れたりせず、使用する場所で数時間そのまま放置し、室温と装置内温度がほぼ同じに安定してから使用してください。たとえば、5 ℃の環境から 25 ℃の環境に持ち込む場合、2 時間ほど放置してください。

通気孔

通気孔は内部の温度上昇を防ぐためのものです。物を置いたり立てかけたりして通気孔をふさがないでください。内部の温度が上昇し、発煙や故障の原因となります。また、通気孔は常にほこりが付着しないよう、定期的に点検し、清掃してください。

装置内部への異物の混入

装置内部への異物の混入を防ぐため、次のことに注意してください。異物によるショートや異物のたい積による内部温度上昇が生じ、装置の故障の原因となります。

- 通気孔などから異物を中に入れない
- 花ビン、植木鉢などの水の入った容器や虫ピン、クリップなどの小さな金属類を装置の上や周辺に置かない
- 装置のカバーを外した状態で使用しない

強い磁気の発生体

磁石やスピーカなどの強い磁気を発生するものを近づけないでください。システム装置の故障の原因となります。

落下などによる衝撃

落下させたりぶつけるなど、過大な衝撃を与えないでください。内部に変形や劣化が生じ、装置の故障の原因となります。

接続端子への接触

コネクタなどの接続端子に手や金属で触れたり、針金などの異物を挿入したりしてショートさせないでください。発煙したり接触不良の故障の原因となります。

煙霧状の液体

煙霧状の殺虫剤などを使用するときは、事前にビニールシートなどでシステム装置を完全に包んでください。システム装置内部に入り込むと故障の原因となります。
また、このときシステム装置の電源は切ってください。

装置の輸送

システム装置を輸送する場合、常に梱包を行ってください。また、梱包する際はマザーボード側（システム装置背面から見てコネクタ類のある側）が下となるよう、向きに注意してください。梱包しなかったり、間違った向きで輸送すると、装置の故障の原因となります。
なお、工場出荷時の梱包材の再利用は 1 回のみ可能です。

サポート製品の使用

流通商品のハードウェア・ソフトウェア（他社から購入される Windows も含む）を使用された場合、システム装置が正常に動作しなくなったり故障したりすることがあります。
この場合の修理対応は有償となります。システム装置の安定稼動のためにも、サポートしている製品を使用してください。

バックアップ

ハードディスク / SSD のデータなどの重要な内容は、補助記憶装置にバックアップを取ってください。ハードディスク / SSD が壊れると、データなどがすべてなくなってしまいます。

ディスクアレイを構成するハードディスク / SSD の複数台障害

リビルドによるデータの復旧、およびリビルド後のデータの正常性を保証することはできません。
リビルドを行ってディスクアレイ構成の復旧に成功したように見えても、リビルド作業中に読めなかったファイルは復旧できません。
障害に備え、必要なデータはバックアップをお取りください。
なお、リビルドによるデータ復旧が失敗した場合のリストアについては、お客様ご自身で行っていただく必要があります。
（リビルドによる復旧を試みる分、復旧に時間がかかります。）

本マニュアル内の警告表示

⚠警告

本マニュアル内にはありません。

⚠注意

本マニュアル内にはありません。

通知

本マニュアル内にはありません。

目次

1

リモートマネジメント機能の概要

この章では、システム装置に標準搭載されるリモートマネジメント機能の概要について説明します。

1.1 リモートマネジメント機能概要と一覧

ここでは、システム装置に標準搭載されるリモートマネジメント機能の概要と、標準・拡張機能の一覧について説明します。

1.1.1 機能概要

本システム装置は、マザーボードに搭載される BMC（Baseboard Management Controller）に、システム装置の稼働状況監視や電源制御を行う機能を付加しております。
また、BMC 専用のマネジメントインタフェースを備えており、LAN 接続によりリモートアクセスし、BMC に対する初期設定を行うことができます。リモートアクセスは標準機能として提供される「Web コンソール」を使用します。

その他、次のオプションを使用することにより機能を拡張することができます。

- 「JP1/ServerConductor/Advanced Agent」、「JP1/ServerConductor/ Blade Server Manager」

  「JP1/ServerConductor/Agent」と組み合わせることにより、電源制御スケジューリング機能（SVP エージェントサービス）やリモートからの障害監視機能（マネージャサービス）が使用でき、より高度なリモート管理環境を構築することができます。

- 「リモートコンソールオプション（VSS7BR20）」

  リモートからシステム装置の画面を表示させ、キーボード・マウス操作を行うリモートコンソール機能を使用することができます。また、バーチャルフロッピーディスク・バーチャル CD/DVD といったリモートデバイス機能を使用することができます。これにより、リモートからシステム装置の BIOS や OS の操作を行ったり、バーチャル CD/DVD からユーティリティなどをインストールすることができます。
  リモートコンソールオプションは、BMC 専用のマネジメントインタフェースを使用してシステムコンソール端末と LAN 接続します。

1.1.2 標準・拡張機能一覧

BMC の標準機能である「Web コンソール」と、「JP1/ServerConductor Advanced Agent」「JP1/ServerConductor/Server Manager」「JP1/ServerConductor/Blade Server Manager」、「リモートコンソールオプション」から使用可能な主な機能は次のとおりです。

凡例：○＝使用可、－＝使用不可

機能	Web コンソール	JP1/ServerConductor			リモートコンソールオプション
		Agent	Advanced Agent *1	Server Manager *1	
リモート電源制御（ON/ 強制 OFF/ ハードリセット）	○	－	○		○
電源制御スケジュール	－	－	○	－	－
ローカル障害監視	－	○	－	－	－
リモート障害監視	－	－	－	○	－
電源 ON/OFF 監視、電源制御リトライ	－	－	○	－	－
OS ハングアップ監視、自動回復	－	－	○	－	－
リモートコンソール / リモートデバイス	－	－	－	－	○
NMI 発行	○	－	－	－	○
Web コンソールのユーザ管理	○	－	－	－	－
IPMI Over LAN の設定	○	－	－	－	－
省電力機能の設定	○	－	－	－	－

*1: 「JP1/ServerConductor/Advenced Agent」、「JP1/ServerConductor/Server Manager」、「JP1/ServerConductor/Blade Server Manager」を使用するには、「JP1/ServerConductor/Agent」が必要になります。

－ MEMO －

2

リモートマネジメント機能使用上の注意事項

この章では、リモートマネジメント機能使用上の注意事項について説明します。

2.1 使用上の注意事項

ここでは、リモートマネジメント機能を使用するにあたってご注意いただきたい内容について説明します。

2.1.1 サーバ管理設定のバックアップ

システム装置の管理のために使用する設定データは、障害が発生した場合の復旧作業時に必要となります。

Web コンソールや「JP1/ServerConductor」による電源制御スケジューリング、リモートコンソールオプションを使用する場合は障害発生時に備え、設定変更時にサーバ管理設定のバックアップを実施し、紛失しないよう大切にデータを保管してください。

詳細は「(2) 「サーバ管理設定のバックアップ」画面」P.56 をご参照ください。

2.1.2 マネジメントインタフェースのネットワーク設定

Web コンソールの使用にはマネジメントインタフェースのネットワーク設定が必要です。お使いになる前に使用環境に合わせて設定してください。

詳細は「3.1 マネジメントインタフェースへの接続」P.8 をご参照ください。

2.1.3 [リモートコンソール起動] ボタンについて

オプションの「リモートコンソールオプション（VSS7BR20)」を適用している場合、コンソール画面に [リモートコンソール起動] ボタンが表示されます。適用していない場合は表示されません。

2.1.4 IPMI Over LAN 機能の設定

IPMI Over LAN 機能の設定は、サーバ管理設定のバックアップおよびリストアの対象にはなっていません。また、保守作業時においてマザーボードを交換した場合、設定の情報が失われる場合があるため設定した内容をメモして保管することをお勧めします。

2.1.5 BMC ネットワークの設定

BMC ネットワークの設定を行う際は、セキュリティ向上のため、接続許可 IP アドレスを設定することを強く推奨します。

接続許可 IP アドレスの設定については、「4.2.4 ネットワークの設定」P.24 をご参照ください。

3

リモートマネジメント機能の使用準備

この章では、Web コンソールを使用するための接続方法について説明します。

3.1 マネジメントインタフェースへの接続

ここでは、マネジメントインタフェースへの接続について説明します。

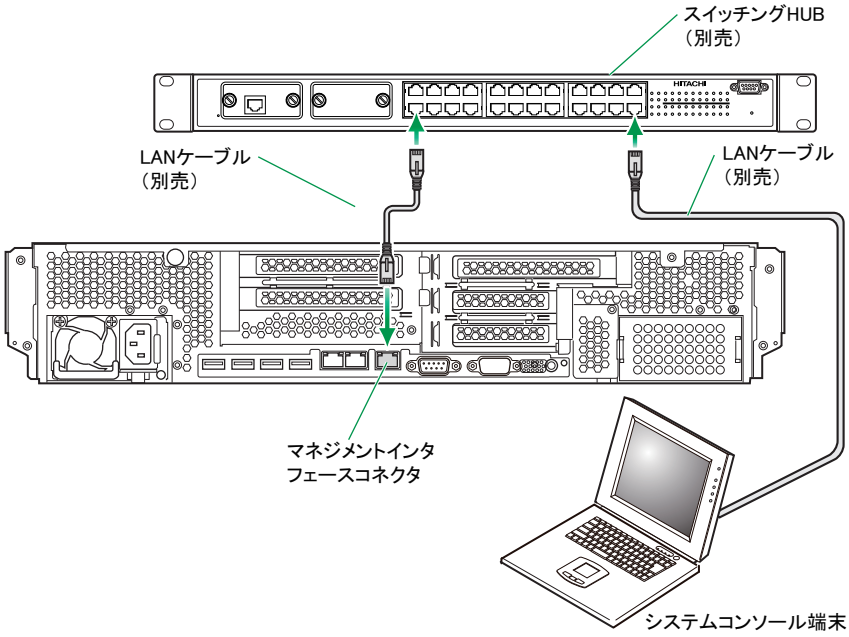
3.1.1 接続時に必要なもの

Web コンソールを使用するために、システム装置背面にあるマネジメントインタフェースコネクタと、システムコンソール端末を LAN ケーブルで接続します。
接続にあたり、次のものが必要になります。

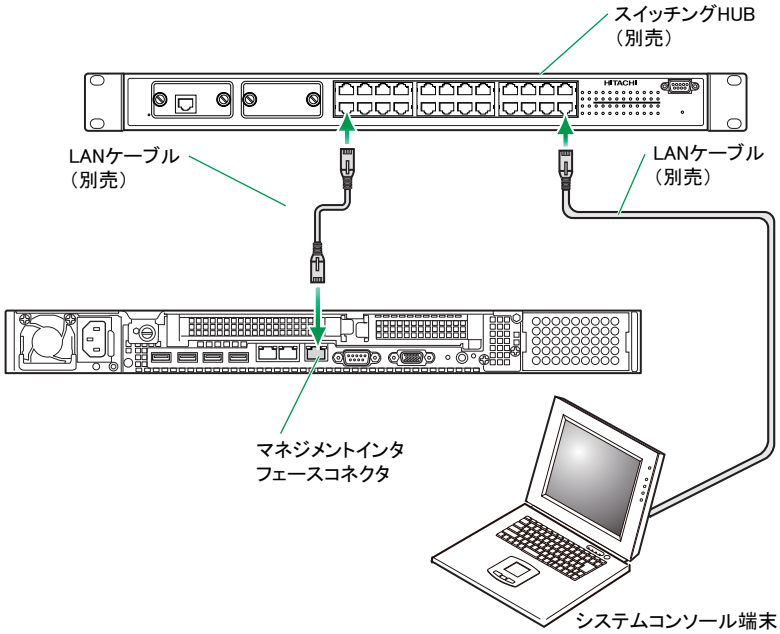
- システムコンソール用の端末（クライアント）（100BASE-TX 対応）
- UTP-5 以上の LAN ケーブルおよびスイッチング HUB（100BASE-TX 対応）
- HTTP のクライアントソフトウェア

各モデルの接続形態は次のとおりです。

RS220-h xM1 モデル



RS210-h xM モデル



制限

マネジメントインタフェースは 100Mbps（100BASE-TX）です。マネジメントインタフェースのリンク速度とデュプレックスはオートネゴシエーション設定となりますので、マネジメントインタフェースに接続するシステムコンソール用端末やスイッチング HUB の LAN ポートはオートネゴシエーションに設定してください。

補足

- システムコンソール端末とマネジメントインタフェースコネクタ間を LAN ケーブルで直結する場合、端末側の仕様によってはクロスケーブルを使用する必要があります。
- BMC を起動（システム装置に AC 供給）する場合、LAN ケーブルを接続し、スイッチング HUB もしくはシステムコンソール端末の電源を入れた状態にしてください。
  BMC 起動後に LAN ケーブルを接続すると、BMC が応答しない場合があります。この場合、LAN ケーブルの接続後、一度システム装置の電源コードを抜いて 30 秒待ってから電源コードを再接続してください。
- マネジメントインタフェースのリンク速度が 10Mbps（10BASE-T：リンク確立時 リンクランプが消灯）となる環境では通信に不具合が発生する場合があります。100Mbps でリンクするよう、マネジメントインタフェースコネクタに接続するネットワーク構成を見直してください。
  また、このときに通信が不安定になった場合、システム装置の電源を切り、システム装置の電源コードを抜くなどして AC 供給を遮断し、30 秒以上経過してから再度 AC 供給をして電源を入れてください。

3.1.2 システムコンソール端末について

マネジメントインタフェースに接続する管理用システムコンソール端末は次の条件を満たすものをご使用ください。

項目	動作条件
OS	・Windows Server 2012 Standard ・Windows Server 2012 Datacenter ・Windows Server 2008 R2 Standard ・Windows Server 2008 R2 Enterprise ・Windows Server 2008 Standard ・Windows Server 2008 Enterprise ・Windows Server 2008 Standard without Hyper-V ・Windows Server 2008 Enterprise without Hyper-V ・Windows Server 2003 R2, Standard Edition ・Windows Server 2003 R2, Enterprise Edition ・Windows Server 2003 R2, Standard x64 Edition ・Windows Server 2003 R2, Enterprise x64 Edition ・Windows Server 2003, Standard Edition ・Windows Server 2003, Enterprise Edition ・Windows Server 2003, Standard x64 Edition ・Windows Server 2003, Enterprise x64 Edition ・Windows 7 Professional ・Windows Vista Business ・Windows XP Professional ・Windows XP Professional x64 Edition
インターネットブラウザ	Internet Explorer 7.0 以降 *1
LAN	100BASE-TX に対応

*1: Internet Explorer7.0 以降は、OS 標準のブラウザを推奨します。

3.1.3 工場出荷時設定

マネジメントインタフェースのネットワークの工場出荷時設定は次のとおりです。

項目	工場出荷時設定
IP アドレス	192.168.100.100
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	未設定
HTTP	有効

また、Web コンソールを使用する前に、次の内容についてシステムコンソール端末（クライアント）のブラウザ設定を確認してください。設定が適切でない場合、Web コンソールが正常に動作しません。

- ポップアップの禁止設定を解除してください。

  ブラウザの機能のほか、ツールバーやアプリケーションによる設定も解除してください。

- Java スクリプトを有効にしてください。

補足

- マネジメントインタフェースは、障害調査のために保守員が保守用端末を接続し、情報収集させていただく場合があります。
- マネジメントインタフェースから得られる情報は障害調査および解析に有益です。お使いのシステム環境にかかわらず、いつでもマネジメントインタフェースが使用できるようネットワーク設定を行っていただくことをお勧めします。
- マネジメントインタフェースをネットワークに接続する場合、IP アドレスが重複していないことを確認してから接続してください。ネットワーク上に IP アドレスが重複する機器が存在する場合、システム装置に障害が発生します。
  複数台のシステム装置のマネジメントインタフェースを同一のネットワークに接続する場合は、1 台ずつマネジメントインタフェースのネットワーク設定を変更してから接続してください。
  →「4.2.4 ネットワークの設定」P.24
- マネジメントインタフェースがLANに接続されていない状態でFUNCTIONスイッチを10秒以上押し続けると、マネジメントインタフェース設定が保守モードに設定され、ERROR ランプが点滅します。
  保守モードは保守作業時に使用するものですので、この操作は行わないでください。万一、誤って保守モードに設定された場合、FUNCTION スイッチをボールペンなどで 10 秒以上押し続け、保守モードを解除してください。保守モードが解除されると、ERROR ランプの点滅が止まります。

3.2 BMC ネットワーク設定

BMC（マネジメントインタフェース）のネットワーク（IP アドレス、サブネットマスク、デフォルトゲートウェイ）は、工場出荷時「3.1 マネジメントインタフェースへの接続」P.8のとおり設定されています。

マネジメントインタフェースのネットワーク設定の変更が必要な場合、システム BIOS を起動してセットアップメニューから行うか、工場出荷時の設定に合わせてシステムコンソール端末のネットワークを設定し、Web コンソールにログインして変更を行ってください。詳細は「4.2.4 ネットワークの設定」P.24 または『ユーザーズガイド ～ BIOS 編～』「Server Mgmt：サーバ管理メニュー」「BMC network configuration：BMC ネットワーク設定サブメニュー」をご参照ください。

また、BMC ネットワーク設定における注意事項があります。設定を行う前に「5 BMC ネットワーク設定の注意事項」P.61をご参照ください。

4

Web コンソールの使用方法

この章では、Web コンソールの使用方法や初期設定、および Web コンソールの機能について説明します。

4.1 Web コンソールのログイン・終了

ここでは、Web コンソールのログインと終了の方法について説明します。

4.1.1 ログイン

1. システム装置に AC が給電されているか確認します。
2. システムコンソール端末のブラウザを起動します。
3. アドレスに URL を入力します。

   HTTP（Hypertext Transfer Protocol）プロトコルを使用して接続する場合は、アドレスに次のように入力します。

   「http://< マネジメントインタフェースの IP アドレス >」

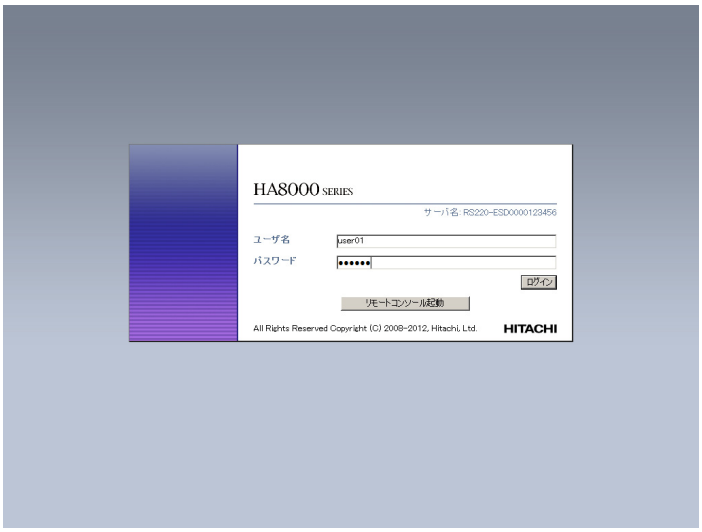
   (例) マネジメントインタフェースの IP アドレスが 192.168.0.2 の場合

   HTTPS（Hypertext Transfer Protocol over Secure Socket Layer）プロトコルを使用して接続する場合は、アドレスに次のように入力します。

   「https://< マネジメントインタフェースの IP アドレス >」

   (例) マネジメントインタフェースの IP アドレスが 192.168.0.2 の場合

4. 接続に成功するとブラウザにログイン画面が表示されます。



5 ログイン画面でユーザ名 / パスワードを入力します。
ユーザ認証に成功しログインすると、「サーバ情報」メニュー画面が表示されます。

補足

- システム装置の出荷時設定では、ログイン画面の「ユーザ名」および「パスワード」に対して、"user01"、"pass01" を入力することで管理者としてログインできます。システム装置に上記と異なるユーザアカウントの設定がされている場合、この方法ではログインできません。設定済みの「ユーザ名」および「パスワード」を入力してログインしてください。
- セキュリティ上、出荷時設定と異なるユーザアカウントの設定を行うことを強く推奨いたします。→「4.2.1　ユーザアカウントの設定」P.16
- [リモートコンソール起動] ボタンは、オプションのリモートコンソールオプション（VSS7BR20）を適用している場合のみ表示されます。[リモートコンソール起動] ボタンをクリックすると、リモートコンソールオプションが起動し、リモートコンソール用のユーザ名およびパスワード入力画面が表示されます。
リモートコンソールオプションの使いかたについては、リモートコンソールオプションに添付されるマニュアルをご参照ください。
- Webコンソールに同時にログインできるのは2ユーザまでとなります。すでに2ユーザがログインしている場合、ログインできません。
- Webコンソールにログインした状態で15分間以上操作が行われなかった場合、自動的にログアウトされます。

4.1.2　終了方法

画面右端にある［ログアウト］ボタンを押すことで、Web コンソールからログアウトできます。

補足

ログアウトせずにブラウザを閉じた場合、15 分後に自動的にログアウトされるまでユーザがログインしている状態となります。このため、ログアウトせずにブラウザを閉じることを繰り返すと、15 分経過するまで新たにログインできなくなります。
ブラウザを閉じる前に、右上のボタンからログアウトを行ってください。

4.2 Web コンソールによる初期設定

ここでは、Web コンソールによるシステム装置の初期設定について説明します。

初期設定が必要なデータは次のとおりです。

- ユーザアカウントの設定
- リモートコンソールのマウスモードの設定
- BMC 時刻の設定
- ネットワークの設定

4.2.1 ユーザアカウントの設定

システム装置をリモート操作するための、ユーザアカウントを設定します。

各登録ユーザには、ユーザ名、パスワードおよび Web コンソールの操作を行うための権限とアカウントの有効 / 無効の設定を行うことができます。

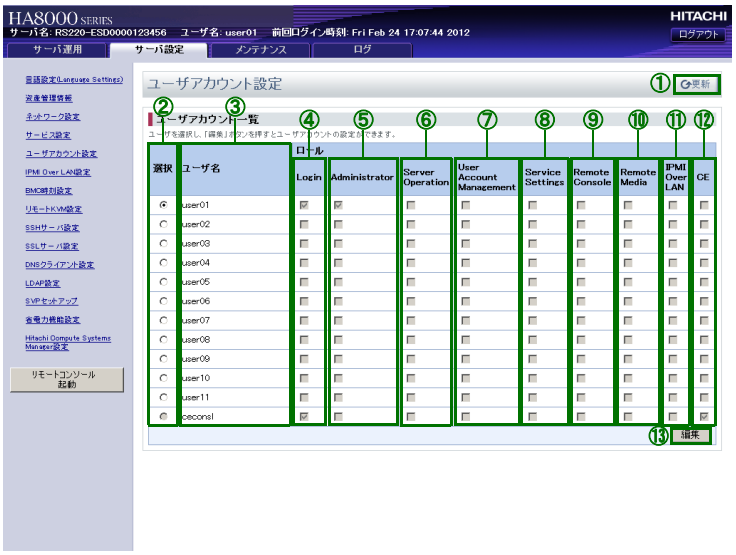
設定は「ユーザアカウント一覧」画面から行います。
上部タブから［サーバ設定］を選択し、左側のツリーメニューから「ユーザアカウント設定」を選択して表示します。

補足

Web コンソールへログインするためのユーザ名、パスワードおよびロールなどを忘れてしまった場合には、システム BIOS のセットアップメニューを起動し、「Server Mgmt」画面の「Reset BMC Web Connection」の設定値を「Yes, On next Reset」に設定し、「Save&Exit」から設定を保存してください。BMC が初期化され、Web コンソールのネットワーク設定の接続先制限、ユーザアカウントの設定が初期化されます。
SERVICE ランプスイッチが 60 秒間程点滅したあと、システム装置が起動されます。
「Reset BMC Web Connection」を実行した場合は、初期のユーザアカウントで Web コンソールにログインし、再度設定し直してください。

(1)「ユーザアカウント一覧」画面

アカウントの設定情報を一覧で表示します。



#	項目名	説明
①	［更新］ボタン	ユーザアカウント情報の再読み込み
②	選択	ユーザアカウント選択用ラジオボタン
③	ユーザ名	ユーザアカウント名称
	ロール	
④	Login	ユーザアカウントに付与されているロールを表示します。
⑤	Administrator	
⑥	Server Operation	
⑦	User Account Management	
⑧	Service Settings	
⑨	Remote Console	
⑩	Remote Media	
⑪	IPMI Over LAN	
⑫	CE	
⑬	［編集］ボタン	「ユーザアカウントの編集」画面へ遷移します。ただし、ラジオボタンにチェックがついていない場合は遷移しません。

◆ ロール

ユーザアカウントにロールを付与することにより、ユーザが行える操作を設定できます。それぞれのロールの意味は次のとおりです。

#	ロール名	説明
1	Login	Web コンソールの提供するサービスにログインするためのロールです。本ロールを持たないユーザは無効とされ、各サービスにログインできません。
2	Administrator	管理者用のユーザ権限を表すロールです。本ロールを持つユーザは Web コンソールの機能のうち、BMC 再起動を除くすべての操作を行うことができます。
3	Server Operation	システム装置の電源、リセット操作を行うためのロールです。
4	User Account Management	ユーザアカウントの設定を行うためのロールです。
5	Service Settings	BMC の提供するサービスの設定を行うためのロールです。
6	Remote Console *1	リモートコンソール機能による、コンソール端末へのシステム装置画面の表示およびキーボード、マウスの遠隔操作を行うためのロールです。
7	Remote Media *1	リモートフロッピーディスク機能 , リモート CD/DVD 機能を使用するためのロールです。
8	IPMI Over LAN	IPMI Over LAN ユーザのアカウント設定と認証タイプ設定を行うためのロールです。
9	CE	保守作業用のユーザ権限を表すロールです。 “ceconsl” 以外のユーザに本ロールを付与することはできません。

*1: オプションの「リモートコンソールオプション（VSS7BR20)」を適用しているときに設定が有効になります。

◆ ユーザアカウントの初期設定

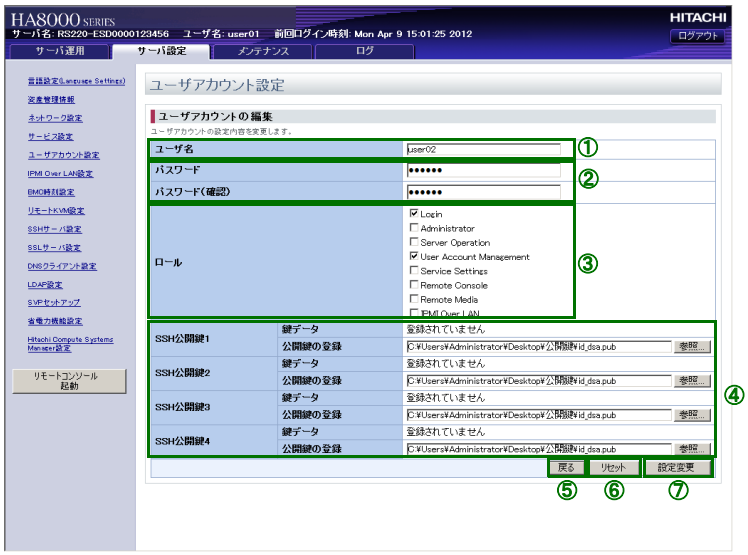
ユーザアカウントの初期設定は次のとおりです。

#	ユーザ名	パスワード	ロール	説明
1	user01	pass01	Login Administrator	システム装置管理者用ユーザです。ロールの変更を行うことはできません。
2	user02	pass02	なし	一般ユーザです。
3	user03	pass03		
4	user04	pass04		
5	user05	pass05		
6	user06	pass06		
7	user07	pass07		
8	user08	pass08		
9	user09	pass09		
10	user10	pass10		
11	user11	pass11		
12	ceconsl	出荷時に設定されます。	Login CE	保守作業用ユーザです。保守員が保守作業時に使用します。設定の変更を行うことはできません。

ユーザアカウントを変更するには、「ユーザアカウント一覧」画面において変更したいユーザアカウントのラジオボタンをチェックし、［編集］ボタンをクリックします。
選択されたユーザアカウントの設定を行う「ユーザアカウントの編集」画面に遷移します。

(2)「ユーザアカウントの編集」画面

ユーザアカウントの設定変更を行います。



#	項目名	説明
①	ユーザ名	ユーザアカウント名称 (最大 32 文字)
②	パスワード	パスワードの入力（最大 32 文字）
	パスワード (確認)	パスワードの再入力
③	ロール	
	Login	チェックされたロールがユーザアカウントに付与されます。
	Administrator	
	Server Operation	
	User Account Management	
	Service Settings	
	Remote Console	
	Remote Media	
	IPMI Over LAN	
④	SSH 公開鍵 1 ～ 4: Secure Shell 接続に用いる公開鍵を設定します。	
	鍵データ	鍵データを表示します。鍵データが設定されていない場合は「登録されていません」と表示されます。
	公開鍵の登録	公開鍵をアップロードし登録します。
⑤	[戻る] ボタン	編集した内容を無効とし、ユーザアカウント一覧画面に戻ります。
⑥	[リセット] ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑦	[設定変更] ボタン	編集した内容を有効とし、確認画面に遷移します。

補足

- ユーザ名は入力必須項目です。
- パスワードを設定する場合は、パスワードとパスワード (確認) は同じ値を入力してください。
- ユーザアカウントを編集する場合にパスワードは必須項目ではありません。入力しない場合はパスワード変更なしとして扱います。
- OpenSSH により作成された SSH 公開鍵ファイルを登録可能です。
- 登録できる SSH 公開鍵ファイルの最大サイズは 2KB です。
- 管理者用ユーザのロールを変更することはできません。
- ロールの変更が行えるのは “Administrator” ロールを持ったユーザのみです。
- “ceconsl” は保守員用のユーザアカウントです。保守サービスを受ける場合に保守員が本ユーザアカウントを使用します。本ユーザアカウントの設定は変更できません。

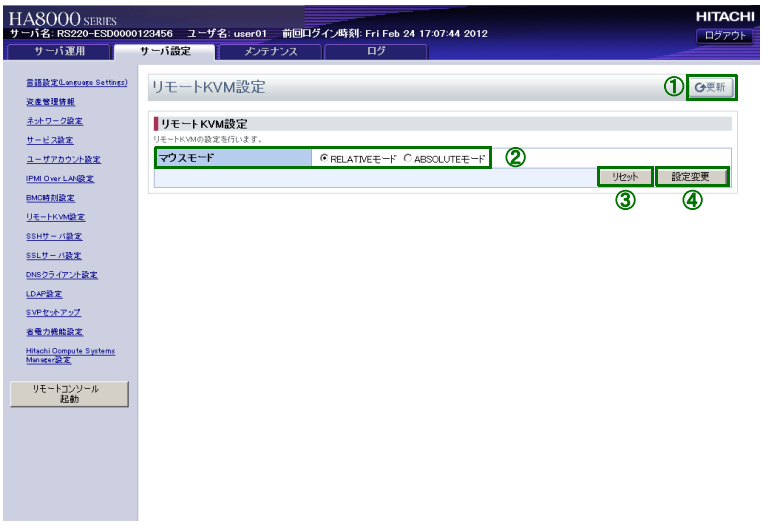
［設定変更］ボタンをクリックすると、「ユーザアカウントの編集（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「ユーザアカウント編集」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「ユーザアカウントの編集」画面に戻ります。

4.2.2 リモートコンソールのマウスモードの設定

システム装置にオプションの「リモートコンソールオプション（VSS7BR20)」を適用している場合、リモートコンソールで操作するためのマウスモードを設定します。「リモートコンソールオプション（VSS7BR20)」を適用していない場合、設定を行う必要はありません。

設定は「リモート KVM 設定」画面から行います。
上部タブから[サーバ設定] を選択し、左側のツリーメニューから「リモートKVM設定」を選択して表示します。

インストールする OS に合わせて、マウスモードを設定してください。



#	項目名	説明
①	[更新] ボタン	情報の表示を更新します。
②	マウスモード	RELATIVE モード： システム装置画面上のマウスカーソルにより、リモートコンソールのマウス操作を行うモードです。システム装置の OS が Windows または RHEL6 以外の場合に設定してください。 ABSOLUTE モード： コンソール端末のマウスカーソルによりリモートコンソールのマウス操作を行うモードです。システム装置の OS が Windows または RHEL6 の場合に設定してください。
③	[リセット] ボタン	編集した内容を無効とし、編集前の状態に戻します。
④	[設定変更] ボタン	編集した内容を有効とし、確認画面に遷移します。

制限

マウスモードを変更する場合は、リモートコンソールを終了した状態で行ってください。リモートコンソール起動中にマウスモードを変更すると、マウスカーソルが正常に動作しなくなるおそれがあります。

補足

- リモートコンソールの使用方法については、「リモートコンソールオプション（VSS7BR20)」に添付されるマニュアルをご参照ください。
- 「リモートコンソールオプション（VSS7BR20)」が適用されているシステム装置には “リモートコンソールオプション内蔵” と記載されたラベルが貼り付けられています。

[設定変更] ボタンをクリックすると、「リモート KVM 設定（確認)」画面が表示されます。表示された画面の [戻る] ボタンをクリックすると編集した内容を保存せずに「リモート KVM 設定」画面に戻り、[確認] ボタンをクリックすると編集した内容を保存して「リモート KVM 設定」画面に戻ります。

4.2.3 BMC 時刻の設定

BMC の時刻を設定します。

設定は「時刻およびタイムゾーンの設定」画面から行います。
上部タブから［サーバ設定］を選択し、左側のツリーメニューから「BMC 時刻設定」を選択して表示します。

BMC の時刻は、障害ログのタイムスタンプ、JP1/ServerConductor/Agent と連動したスケジュール運転に使用されます。

補足

- システム装置の運用前に、時刻設定として Web コンソールおよび、セットアップメニューの両方を実施してください。セットアップメニューの時刻設定は、『ユーザーズガイド ～ BIOS 編～』「Main：メインメニュー」をご参照ください。
- BMC の時刻がシステムクロックに同期する場合は、システムクロックをローカルタイムとみなして同期します。

#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	時計合わせ方式	NTP を使用しない： BMC が定期的にシステム装置のシステムクロックを読み込み、システム装置の時刻に同期します。 NTP による時刻合わせを行う： BMC の時刻は外部 NTP サーバの配信する時刻に同期します。 NTP サーバのアドレスを、項目④により設定してください。
③	年月日 時刻	年月日、および時刻は、現地の時刻を入力してください。
④	NTP 設定	項目②「時計合わせ方式」を「NTP による時刻合わせを行う」に設定する場合に、NTP サーバの IP アドレスを入力します。
⑤	タイムゾーン	システム装置の設置されている現地のタイムゾーンを、システム装置で使用している OS に合わせて設定してください。
⑥	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑦	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

制限

②項を「NTP を使用しない」（BMC の時刻をシステムクロックに同期）に設定して、JP1/ServerConductor 機能によるスケジュール運転を行う場合、システム装置の AC 供給を遮断して再投入すると電源を入れることができない場合があります。
スケジュール運転時に AC 供給を遮断する運用の場合、②項は「NTP による時刻合わせを行う」に設定し、NTP サーバを使用してください。

補足

- JP1/ServerConductor Agent を導入し、NTP サーバを使用されない場合、②項は NTP を使用せず、BMC の時刻を OS の時刻に同期する方法を推奨します。
- 「NTP による時刻合わせを行う」を選択した場合、JP1/ServerConductor Agent による OS 時刻と BMC 時刻との同期機能は有効となりません。

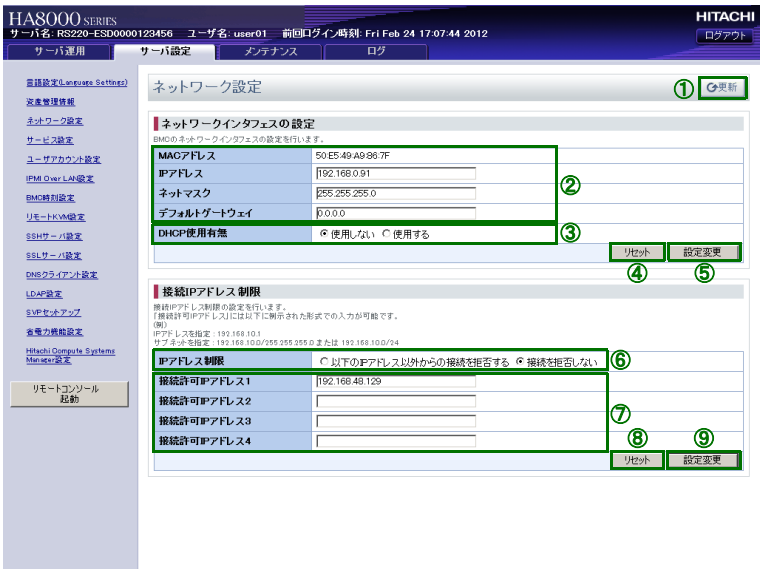
［設定変更］ボタンをクリックすると、「時刻およびタイムゾーンの設定（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「時刻およびタイムゾーンの設定」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「時刻およびタイムゾーンの設定」画面に戻ります。

4.2.4 ネットワークの設定

システム装置の BMC ネットワーク設定を、工場出荷時の状態からお客様の使用環境に合わせて設定変更します。
BMC ネットワーク設定を変更すると、一度ネットワークが切断され、以後は設定変更後の環境でのみ BMC ネットワークに接続が可能になります。BMC ネットワークの設定変更を行う場合は、設定内容に誤りがないことをご確認ください。

また、システム装置に接続できるネットワーク機器の IP アドレスを制限する設定を行うことができます。システム装置に接続を許可するネットワーク機器の IP アドレスは、４つまで指定することができます。

設定は「ネットワーク設定」画面から行います。
上部タブから［サーバ設定］を選択し、左側のツリーメニューから「ネットワーク設定」を選択して表示します。



#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	MAC アドレス（表示のみ） IP アドレス ネットマスク デフォルトゲートウェイ	システム装置の BMC ネットワークを設定します。 BMC の初期 IP アドレス、サブネットマスク、デフォルトゲートウェイ設定は、「3.1　マネジメントインタフェースへの接続」P.8 をご参照ください。 DNS の設定については、「(11)「DNS クライアント設定」画面」P.45 をご参照ください。
③	DHCP 使用有無 *1	DHCP 機能の有効、無効を設定します。
④	［リセット］ボタン	ネットワークインタフェースの設定で編集した内容を無効とし、編集前の状態に戻します。
⑤	［設定変更］ボタン	ネットワークインタフェースの設定で編集した内容を有効とし、確認画面に遷移します。
⑥	IP アドレス制限	接続 IP アドレス制限機能の有効、無効を設定します。
⑦	接続許可 IP アドレス１～４	システム装置への接続を許可する IP アドレスを入力します。単一の IP アドレスまたはサブネットを設定することができます。 （例） 単一 IP アドレス：192.168.10.1 サブネット：192.168.10.0/255.255.255.0 または 192.168.10.0/24
⑧	［リセット］ボタン	接続した IP アドレス制限で編集した内容を無効とし、編集前の状態に戻します。
⑨	［設定変更］ボタン	接続した IP アドレス制限で編集した内容を有効とし、確認画面に遷移します。

*1：DHCP 使用有無の設定を「有効」にした場合、「IP アドレス」、「ネットマスク」、「デフォルトゲートウェイ」に設定されている値は使用されず、DHCP 機能が設定した値が採用されます。

補足

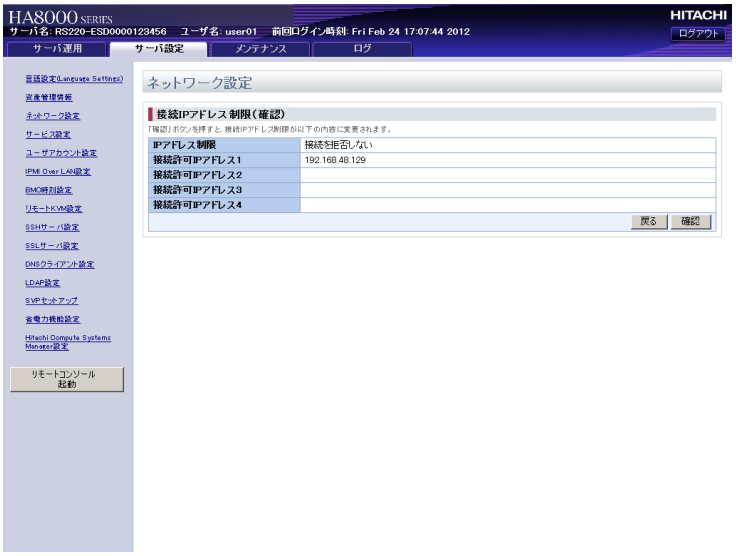
DHCP 使用の有無の設定を「有効」にした場合、DHCP サーバ側の設定より、マネジメントインタフェースの IP アドレスが変更される場合があります。
DHCP サーバの設定は、IP アドレスの初期化など、一時的な使用のみとし、通常は「無効」に設定して運用することをお勧めします。

⑤の［設定変更］ボタンをクリックすると、次の確認画面が表示されます。

［確認］ボタンをクリックすると IP アドレスが変更されるため、Web コンソールからログアウトされ、システム装置との接続が切断されます。

システムコンソール端末のブラウザのアドレスに変更後の IP アドレスを入力し、再接続してから Web コンソールにログインしなおしてください。

⑨の［設定変更］ボタンをクリックすると、次の確認画面が表示されます。



［確認］ボタンをクリックすると設定が保存され、「ネットワーク設定」画面に戻ります。設定を保存しない場合は［戻る］ボタンをクリックします。

4.3 Web コンソールの機能

ここでは、Web コンソールから設定できる機能について説明します。

4.3.1 機能一覧

Web コンソールが提供する機能は次のとおりです。

#	メニュー	機能
「サーバ運用」タブ		
1	サーバ情報	システム装置の情報を表示する。
2	電源および LED	電源、リセット操作および LED 状態の表示を行う。
3	温度および電力蓄積情報	システム装置のマネジメントモジュールに蓄積している温度と消費電力の情報表示を行う。
「サーバ設定」タブ		
4	言語設定	Web コンソールで使用する言語の設定を行う。
5	資産管理情報	資産情報の設定を行う。
6	ネットワーク設定	ネットワーク設定の表示および接続制限の設定を行う。
7	サービス設定	システム装置の提供するサービスの有効化 / 無効化およびポート番号の設定を行う。
8	ユーザアカウント設定	ユーザアカウントの表示および設定を行う。
9	IPMI Over LAN 設定	IPMI Over LAN の設定を行う。
10	BMC 時刻設定	BMC 時刻、タイムゾーンの表示および設定を行う。
11	リモート KVM 設定	リモートコンソールのマウスモードの設定を行う。
12	SSH サーバ設定	SSH の認証方式の設定およびホスト鍵の表示を行う。
13	SSL サーバ設定	SSL サーバ証明書の管理を行う。
14	DNS クライアント設定	DNS サーバの設定を行う。
15	LDAP 設定	LDAP によるユーザ認証の設定を行う。
16	SVP セットアップ	SVP アラートの通報先の表示および設定を行う。
17	省電力機能設定	省電力機能のモード設定を行う。
18	Hitachi Compute Systems Manager 設定	Hitachi Compute Systems Manager（HCSM）の管理サーバ情報の設定を行う。
「メンテナンス」タブ		
19	BMC ファームウェア管理	BMC ファームウェアの情報表示および更新を行う。
20	サーバ管理設定のバックアップ	システム装置設定のバックアップを行う。
21	サーバ管理設定のリストア	システム装置設定のリストアを行う。
22	BMC 再起動 *1	BMC を再起動する。
「ログ」タブ		
23	ログのダウンロード	システム装置のログの採取およびダウンロードを行う。

*1: 機能は、“ceconsl” ユーザ（保守員作業用ユーザ）のみ使用可能です。

4.3.2 操作に必要なロール

Web コンソールでは、ユーザに割り当てられているロールに基づき、操作が制限されます。各ロールで行うことのできる操作は次のとおりです。

#	メニュー	ロールにより可能となる操作					
		Administrator	Server Operation	User Account Management	Service Settings	IPMI Over LAN	CE
「サーバ運用」タブ							
1	サーバ情報	全操作	全操作	情報表示のみ	情報表示のみ	情報表示のみ	全操作
2	電源および LED						
3	温度および電力蓄積情報						
「サーバ設定」タブ							
4	言語設定	全操作	情報表示のみ	情報表示のみ	全操作	情報表示のみ	全操作
5	資産管理情報						なし
6	ネットワーク設定						全操作
7	サービス設定						
8	ユーザアカウント設定		自身のアカウントの設定のみ	一般ユーザの表示および設定	自身のアカウントの設定のみ		なし
9	IPMI Over LAN 設定	なし	なし	なし	なし	全操作	
10	BMC 時刻設定	全操作	情報表示のみ	情報表示のみ	全操作	情報表示のみ	全操作
11	リモート KVM 設定						
12	SSH サーバ設定						なし
13	SSL サーバ設定						
14	DNS クライアント						全操作
15	LDAP 設定		なし	なし	なし	なし	なし
16	SVP セットアップ		全操作	全操作	全操作	情報表示のみ	全操作
17	省電力機能設定		情報表示のみ	情報表示のみ			なし
18	Hitachi Compute Systems Manager 設定						
「メンテナンス」タブ							
19	BMC ファームウェア管理	全操作	情報表示のみ	情報表示のみ	情報表示のみ	情報表示のみ	全操作
20	サーバ管理設定のバックアップ		なし	なし	なし	なし	
21	サーバ管理設定のリストア						
22	BMC 再起動	なし					
「ログ」タブ							
23	ログのダウンロード	全操作	全操作	なし	なし	なし	全操作

補足

「Remote Console」「Remote Media」ロールは Web コンソールの操作に影響しません。
それぞれの機能を有効にするために使われます。

4.4 Web コンソールの設定項目

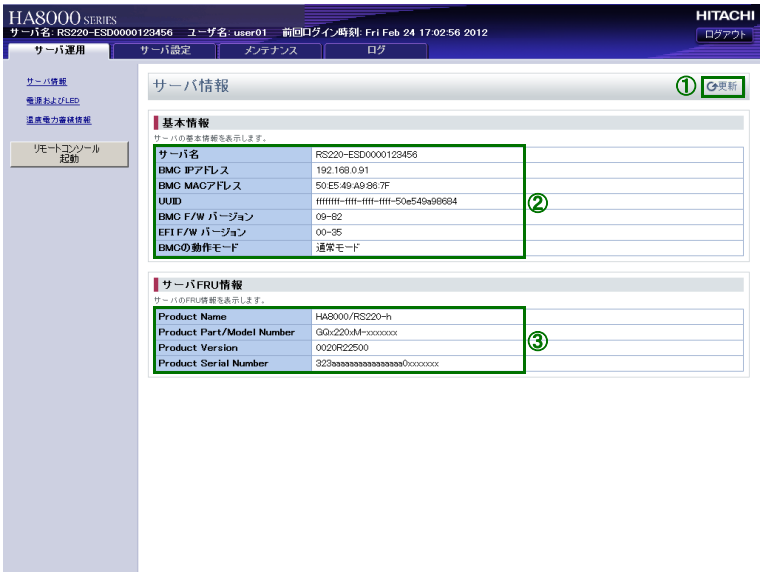
ここでは、Web コンソールの画面および設定項目について説明します。

4.4.1 「サーバ運用」タブ

「サーバ運用」タブでは、システム装置の識別情報の参照や、リモート電源操作に関する設定を行うことができます。

(1) 「サーバ情報」画面

システム装置の識別情報を表示します。



#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	基本情報	サーバ名　：「(2) 「資産管理情報」画面」P.34 により設定された、サーバ名称を表示します。 BMC IP アドレス　：システム装置の BMC の IP アドレスを表示します。BMC の初期 IP アドレス設定は、「3.1　マネジメントインタフェースへの接続」P.8 をご参照ください。 BMC の IP アドレス変更は、「4.2.4　ネットワークの設定」P.24 をご参照ください。 BMC MAC アドレス　：BMC の MAC アドレスを表示します。 UUID　：UUID を表示します。 BMC F/W バージョン　：BMC のファームウェアバージョンを表示します。 EFI F/W バージョン　：EFI のファームウェアバージョンを表示します。 BMC の動作モード　：BMC の動作モードを表示します。
③	サーバ FRU 情報 *1	システム装置の製品情報を表示します。 Product Name　：システム装置の製品名称を表示します。 Product Part/Module Number　：システム装置の形名情報を表示します。 Product Version　：システム装置のハードウェアバージョンを表示します。 Product Serial Number　：システム装置の製造番号を表示します。

*1:　FRU：システム装置の固有情報（Field-Replaceable Unit information）情報が設定されていない場合、「N/A」と表示されます。

補足

「BMC の動作モード」には、通常モードと保守モードがあります。保守モードは保守員が保守作業時にのみ使用するため、「BMC の動作モード」が保守モードと表示されている場合は、FUNCTION スイッチをボールペンなどで 10 秒以上押し続け、保守モードを解除してください。

(2) 「電源および LED 」画面

システム装置の電源状態を表示します。システム装置に対して電源 ON、電源 OFF、リセットのリモート制御を行います。また、システム装置の電源およびランプの状態を表示します。

#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	電源状態	現在のシステム装置の電源状態を表示します。 OFF　　：電源 OFF 状態です ON　　：電源 ON 状態です 強制電源 OFF：電源障害が発生したため電源 ON できない状態です。
③	［電源 ON］ボタン	システム装置の電源を ON にします。
④	［強制電源 OFF］ボタン	システム装置の電源を強制的に OFF にします。 なお、OS のシャットダウンは実施されません。通常の電源 OFF 操作は OS 画面からのシャットダウン、または JP1/ServerConductor によるシャットダウンを行ってください。
⑤	［ハードリセット］ボタン	システム装置をハードウェアリセットします。 システム装置の電源が ON の状態で有効です。
⑥	［NMI］ボタン	NMI 割り込み信号を発行します。 OS の設定によりダンプ処理が起動されます。システム装置の電源が ON の状態で有効です。
⑦	［点灯］ボタン	識別ランプを点灯します。 ボタンをクリックすると SERVICE ランプスイッチを押下した場合と同じ動作をします。
⑧	［消灯］ボタン	識別ランプを消灯します。 ボタンをクリックすると SERVICE ランプスイッチを押下した場合と同じ動作をします。
⑨	LED 状態 *1	システム装置のランプの状態を表示します。 識別ランプ（LID） エラーランプ（ALT） Mode0 ランプ Mode1 ランプ

*1: 「LED 状態」に表示される各ランプとシステム装置のランプの対応は次のとおりです。
識別ランプ（LID）：SERVICE ランプスイッチ
エラーランプ（ALT）：ERROR ランプ
Mode0 ランプ：MAINTENANCE ランプ左側のドットランプ（RS220-h xM1 モデル）
：MODE0 ランプ（RS210-h xM1 モデル）
Mode1 ランプ：MAINTENANCE ランプ右側のドットランプ（RS220-h xM1 モデル）
：MODE1 ランプ（RS210-h xM1 モデル）
各ランプの詳細は、各モデルの『ユーザーズガイド ～導入編～』「2.2　システム装置各部の名称と機能」をご参照ください。

(3)「温度および電力蓄積情報」画面

システム装置のマネジメントモジュールに蓄積している温度と消費電力の情報を表示します。

#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	ソートの種類	蓄積情報の表示順序を設定します。 日付順：蓄積情報の「Date time」が一番新しい情報から順に最大 12 件まで表示します。 電力順：蓄積情報の「MAX」の値で「***W」が一番大きい情報から順に最大 12 件まで表示します。 温度順：蓄積情報の「MAX」の値で「** ℃」が高い情報から順に最大 12 件まで表示します。
③	［実行］ボタン	「ソートの種類」で選択した順序に表示を変更します。
④	蓄積情報 *1	システム装置の温度および消費電力の情報を表示します。

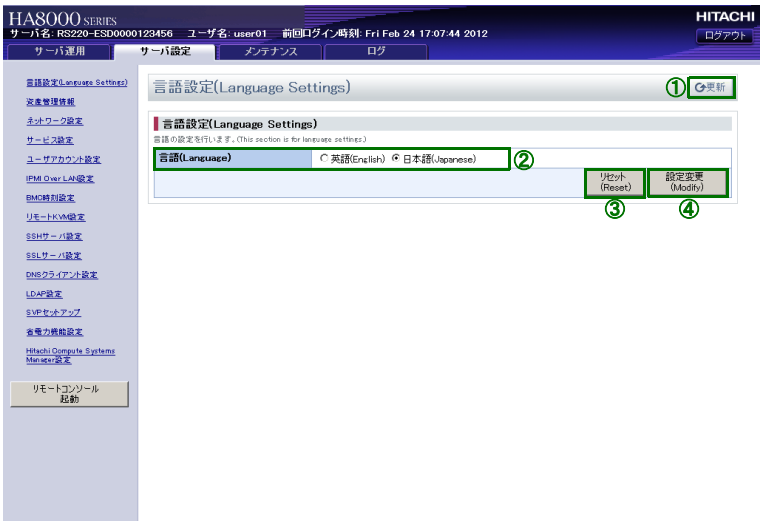
*1: 約 2 時間ごとに記録され最大 2 年分の情報を蓄積することが可能です。

4.4.2 「サーバ設定」タブ

「サーバ設定」タブでは、システム装置を管理するための機能の設定を行うことができます。

(1)「言語設定」画面

Web コンソールの表示言語を設定します。



#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	言語設定	英語　：Web コンソールの表示言語を英語に設定します。 日本語：Web コンソールの表示言語を日本語に設定します。
③	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
④	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

［設定変更］ボタンをクリックすると、「言語設定（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「言語設定」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「言語設定」画面に戻ります。

(2) 「資産管理情報」画面

システム装置の管理情報を設定することができます。

#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	サーバ名 *1	システム装置の名称を設定します。（半角英数字記号 63 文字） 本設定の内容は画面左上の「サーバ名：」欄および、「サーバ運用」タブの「サーバ情報」画面に表示されます。
③	サーバ資産情報 *1	文章を登録することができます。（半角英数字記号 63 文字） システム装置の設置場所、管理者などの情報を記録するために使用できます。
④	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑤	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

*1:サーバ名の入力文字数は半角英数字記号 20 文字、サーバ資産情報の入力文字数は半角英数字 25 文字を推奨します。
合計 45 文字以上入力すると、タイトル部分に表示されるサーバ名、ユーザ名、前回ログイン時刻が正常に表示されなくなる場合があります。

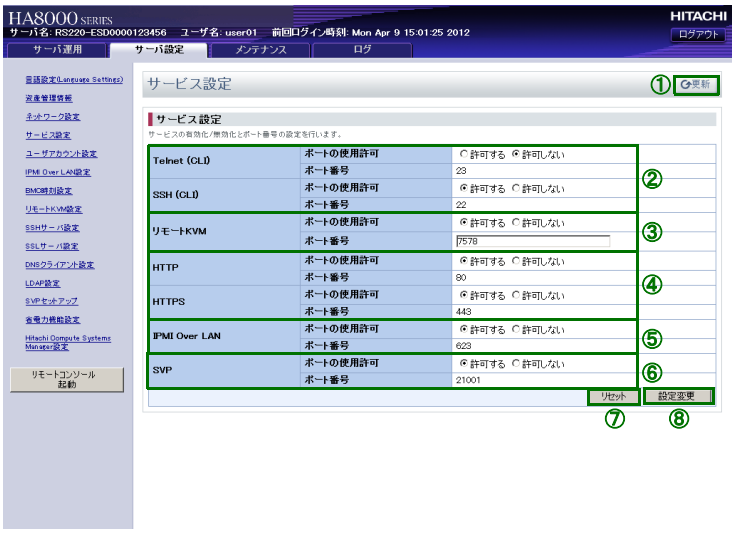
［設定変更］ボタンをクリックすると、「資産管理情報（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「資産管理情報」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「資産管理情報」画面に戻ります。

(3) 「ネットワーク設定」画面

「Web コンソールによる初期設定」－「4.2.4　ネットワークの設定」P.24 をご参照ください。

(4)「サービス設定」画面

システム装置の提供するサービスについて、有効／無効、使用するポート番号を設定します。



#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	Telnet（CLI） SSH（CLI）	Telnet および SSH で使用するポートの使用可否を設定します。 サポートしておりません。
③	リモート KVM	リモートコンソールアプリケーションの使用可否と、システム装置に接続する際に使用するポート番号を設定します。
④	HTTP HTTPS	Web コンソールで使用する HTTP ポートおよび HTTPS ポートの使用可否を設定します。
⑤	IPMI Over LAN *1	IPMI Over LAN 機能で使用するポートの使用可否を設定します。
⑥	SVP	SVP 機能で使用するポートの使用可否を設定します。
⑦	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑧	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

*1: IPMI Over LAN 機能は、一部のコマンドに制限して使用可能としています。

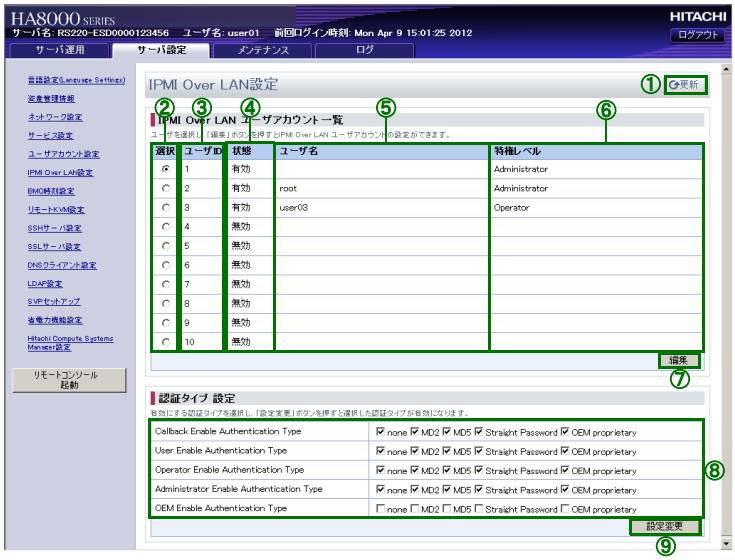
［設定変更］ボタンをクリックすると、「サービス設定（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「サービス設定」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「サービス設定」画面に戻ります。

(5)「ユーザアカウント設定」画面

「Web コンソールによる初期設定」－「4.2.1　ユーザアカウントの設定」P.16 をご参照ください。

(6)「IPMI Over LAN 設定」画面

IPMI Over LAN 機能を設定する権限が付与されている、ユーザーアカウントの IPMI Over LAN 機能の認証タイプを設定します。



#	項目名	説明
①	［更新］ボタン	ユーザアカウント情報の再読み込み
②	選択	ユーザアカウント選択用ラジオボタン
③	ユーザ ID	ユーザアカウントの ID
④	状態	ユーザアカウントの有効／無効を表示
⑤	ユーザ名	ユーザアカウント名称
⑥	特権レベル	ユーザアカウントに付与されている特権レベルを表示
⑦	［編集］ボタン	「IPMI Over LAN ユーザーアカウントの編集」画面へ遷移します。ただし、ラジオボタンにチェックがついていない場合は遷移しません。
⑧	認証タイプ	各特権レベルの認証タイプを設定します。
⑨	［設定変更］ボタン	「認証タイプの編集（確認）」画面へ遷移します。

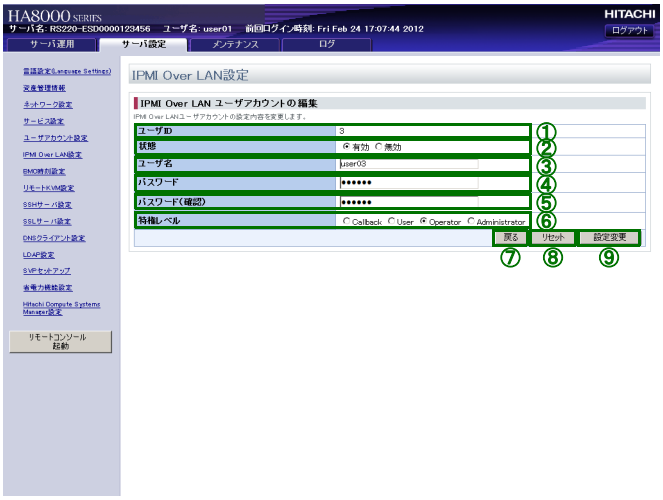
補足

■ ユーザ ID1、2 は状態の変更のみ可能です。

■ ユーザ ID1、2 は工場出荷時に設定されています。設定値は次のとおりです。

- ユーザ ID1 の場合：
「状態」は「有効」、「ユーザ名」は「空白」、パスワードは「空白」、「特権レベル」は「Administrator」にそれぞれ設定されています。
- ユーザ ID2 の場合：
「状態」は「有効」、「ユーザ名」は「root」、パスワードは「superuser」、「特権レベル」は「Administrator」にそれぞれ設定されています。

［編集］ボタンをクリックすると、「IPMI Over LAN ユーザーアカウントの編集」画面が表示されます。



#	項目名	説明
①	ユーザ ID	ユーザ ID を表示
②	状態 *1	ユーザアカウントの有効／無効を設定
③	ユーザ名 *2	ユーザアカウント名称 （半角英数字最大 32 文字）
④	パスワード *2 *3 *4	パスワードの入力（半角英数字最大 16 文字）
⑤	パスワード（確認） *2 *3 *4	パスワードの再入力
⑥	特権レベル *2	特権レベルを設定
⑦	［戻る］ボタン	編集した内容を無効とし、ユーザアカウント一覧画面に戻ります。
⑧	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑨	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

*1: 無効に設定した場合、「IPMI Over LAN 機能の設定」画面の「ユーザ名」および「特権レベル」が「N/A」と表示されます。

*2: ユーザ ID1、2 は変更できません。

*3: ユーザ ID8、9、10 は、パスワードに空白を設定することはできません。

*4: 設定可能なパスワードは、IPMI1.5 と互換性のある 16byte password です。

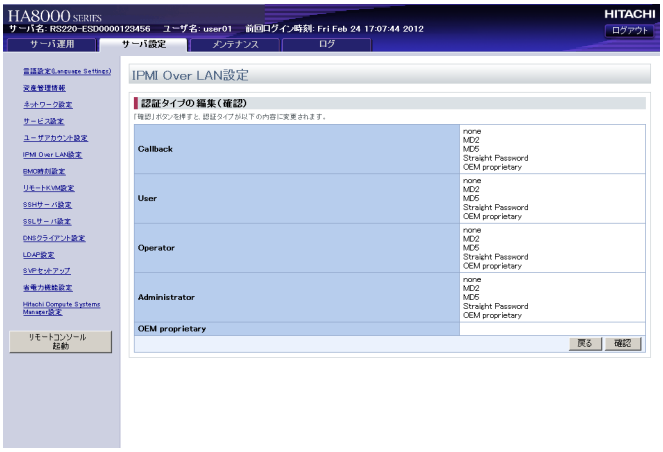
「IPMI Over LAN ユーザーアカウントの編集」の［設定変更］ボタンをクリックすると、次の確認画面が表示されます。

画面上の［戻る］ボタンをクリックすると編集した内容を保存せずに「IPMI Over LAN ユーザーアカウントの編集」画面に戻り、［確認］ボタンをクリックすると、内容を保存し「IPMI Over LAN 設定」画面に戻ります。

補足

- IPMI Over LAN 機能の設定情報は、システム装置から電源コードを抜いても保持されます。
- 「メンテナンス」タブでバックアップおよびリストアを実施しても、IPMI Over LAN 機能の設定情報はバックアップ、リストアされません。障害などでマザーボードを交換した場合は、再度設定し直してください。

認証タイプを設定して［設定変更］ボタンをクリックすると、「認証タイプの編集（確認）」画面が表示されます。



画面上の［戻る］ボタンをクリックすると編集した内容を保存せずに「IPMI Over LAN 設定」画面に戻り、［確認］ボタンをクリックすると、内容を保存し「IPMI Over LAN 設定」画面に戻ります。

(7)「BMC 時刻設定」画面

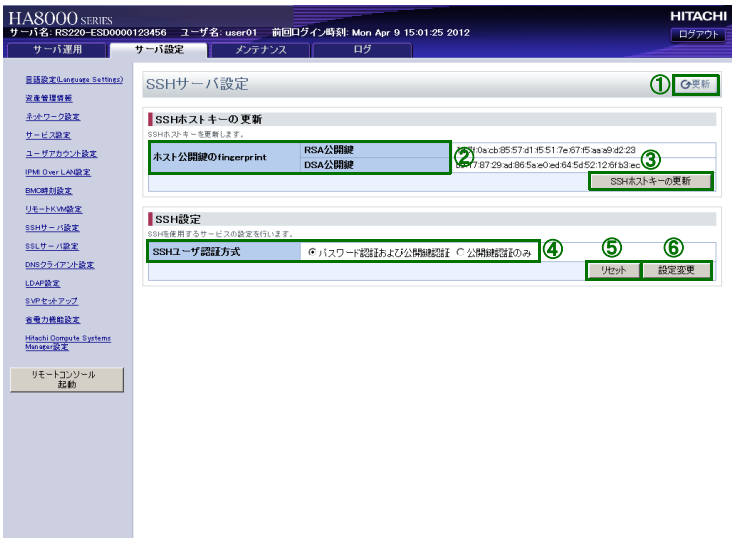
「Web コンソールによる初期設定」－「4.2.3　BMC 時刻の設定」P.22 をご参照ください。

(8)「リモート KVM 設定」画面

「Web コンソールによる初期設定」－「4.2.2　リモートコンソールのマウスモードの設定」P.21 をご参照ください。

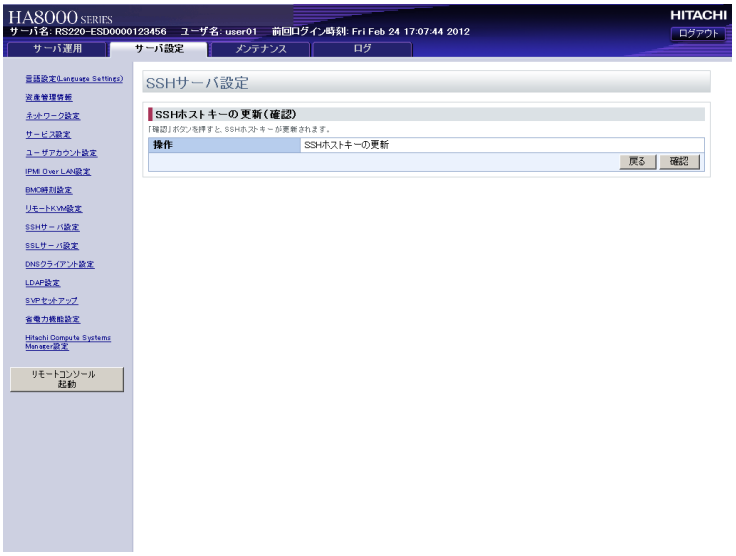
(9) 「SSH サーバ設定」画面

SSH サーバのホストキーの表示および認証方式の設定を行うことができます。



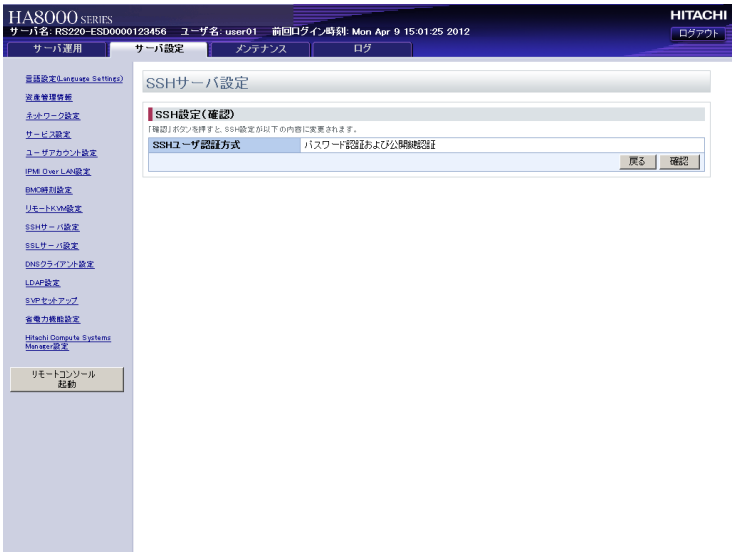
#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	ホスト公開鍵の fingerprint	SSH サーバが使用しているホストキー（公開鍵）のフィンガープリントを表示します。
③	［SSH ホストキーの更新］ボタン	SSH サーバが使用しているホストキー（公開鍵）を更新します。ボタンをクリックしたあと、確認画面に遷移します。
④	SSH ユーザ認証方式	SSH サーバが使用するユーザ認証方式を選択します。
⑤	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑥	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

［SSH ホストキーの更新］ボタンをクリックすると、次画面が表示されます。



［戻る］ボタンをクリックするとキーを更新せずに「SSH サーバ設定」画面に戻ります。［確認］ボタンをクリックするとキーを更新して「SSH サーバ設定」画面に戻ります。

［設定変更］ボタンをクリックすると、次画面が表示されます。



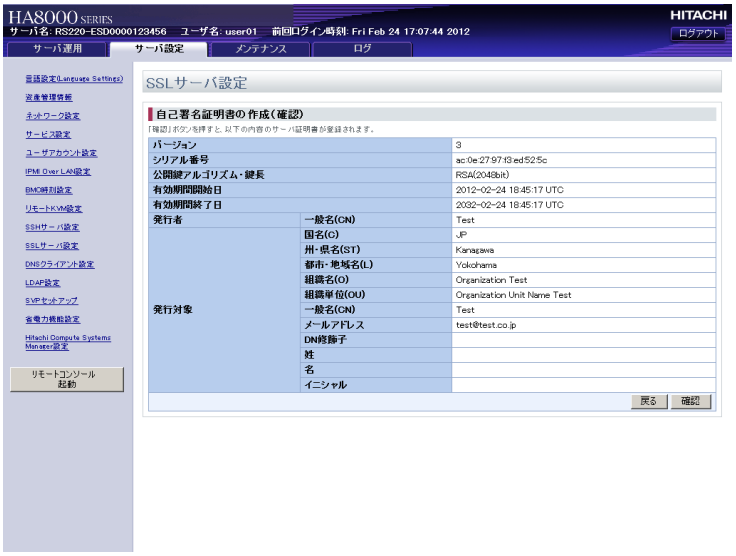
［戻る］ボタンをクリックするとキーの認証方式を変更せずに「SSH サーバ設定」画面に戻ります。［確認］ボタンをクリックすると認証方式を変更して「SSH サーバ設定」画面に戻ります。

(10)「SSL サーバ設定」画面

SSL サーバ証明書の管理を行います。登録されているサーバ証明書の表示、自己署名サーバ証明書の作成、CSR の作成、サーバ証明書のインポートおよびサーバ証明書のダウンロードを行うことができます。

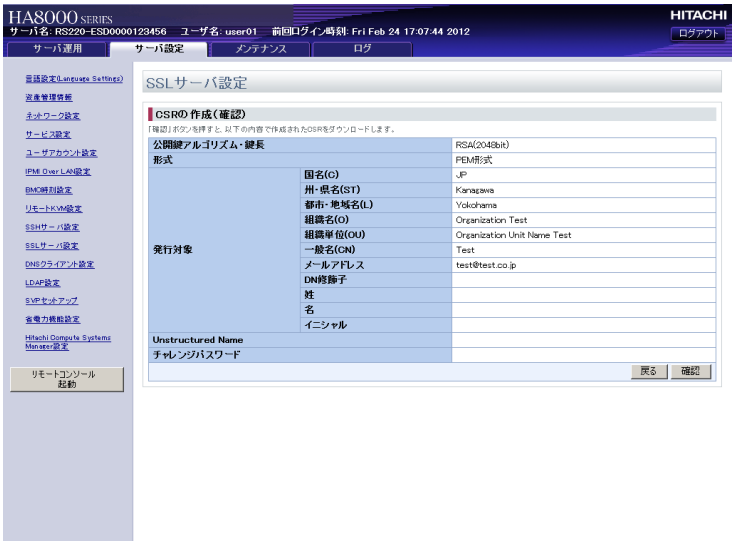
#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	サーバ証明書の情報	マネジメントインタフェースが使用するサーバの証明書情報を表示します。 バージョン：サーバ証明書のバージョンを表示します。 シリアル番号：シリアル番号を表示します。 公開鍵アルゴリズム・鍵長：公開鍵アルゴリズム・鍵長の情報を表示します。 有効期間開始日：有効期間の開始日を表示します。 有効期間終了日：有効期間の終了日を表示します。 発行者：一般名（CN）の情報を表示します。 発行対象：発行対象の情報を表示します。 SHA1 Fingerprint：SHA1 フィンガープリントの情報を表示します。
③	自己署名証明書の作成	自己署名サーバ証明書の作成に必要な情報を入力します。 入力項目は、公開鍵アルゴリズム・鍵長および次の項目となります。 国名（C）：大文字アルファベット 2 文字を入力できます。 州・県名（ST）、都市・地域名（L）、組織名（O）、組織単位（OU）：最大 60 文字の英数字、記号を入力できます。 一般名（CN）：1 ～ 60 文字の英数字、-（ハイフン）、.（ピリオド）を指定できます。 メールアドレス：最大 60 文字の ASCII 文字列を入力できます。 DN 修飾子、姓、名：最大 60 文字の英数字、記号を入力できます。 イニシャル：最大 30 文字の英数字、記号を入力できます。 一般名（CN）以外の項目は省略可能です。 州・県名（ST）、都市・地域名（L）、組織名（O）、組織単位（OU）、DN 修飾子、姓、名、イニシャルに使用できる記号は次のとおりです。 空白記号、'（アポストロフィ）、-（ハイフン）、,（カンマ）、＝（イコール）、/（スラッシュ）、()（括弧）、.（ピリオド）、:（コロン）、＋（プラス）、？（クエスチョン）
④	［リセット］ボタン	③にて編集した内容を無効とし、編集前の状態に戻します。
⑤	［自己署名証明書の作成］ボタン	③にて編集した内容を有効とし、自己署名サーバ証明書を作成します。 ボタンを押すと確認画面に遷移します。
⑥	CSR の作成	CSR の作成に必要な情報を入力します。入力項目は、③の項目および以下となります。 形式：ダウンロードする CSR の形式を設定します。「PEM 形式」または「DER 形式」を選択できます。 Unstructured Name：最大 60 文字の英数字、記号を入力できます。 チャレンジパスワード：最大 30 文字の英数字、記号を入力できます。 Unstructured Name およびチャレンジパスワードは省略可能です。 これらの項目に使用できる記号は③に示したものと同一です。
⑦	［リセット］ボタン	⑥にて編集した内容を無効とし、編集前の状態に戻します。
⑧	［CSR の作成とダウンロード］ボタン	⑥にて編集した内容を有効とし、CSR を作成します。 ボタンを押すと確認画面に遷移します。
⑨	サーバ証明書のインポート	インポートするサーバ証明書を指定します。 形式：インポートしようとするサーバ証明書の形式を設定します。「PEM 形式」または「DER 形式」を選択できます。 インポートする証明書：サーバ証明書のファイルを指定します。
⑩	［サーバ証明書のインポート］ボタン	⑨で指定したサーバ証明書のファイルをインポートします。ボタンを押すと確認画面に遷移します。
⑪	サーバ証明書のダウンロード	ダウンロードするサーバ証明書の形式を設定します。 「PEM 形式」または「DER 形式」を選択することができます。
⑫	［サーバ証明書のダウンロード］ボタン	登録されているサーバ証明書を⑪で指定された形式でダウンロードします。

［自己署名証明書の作成］ボタンをクリックすると、次画面が表示されます。



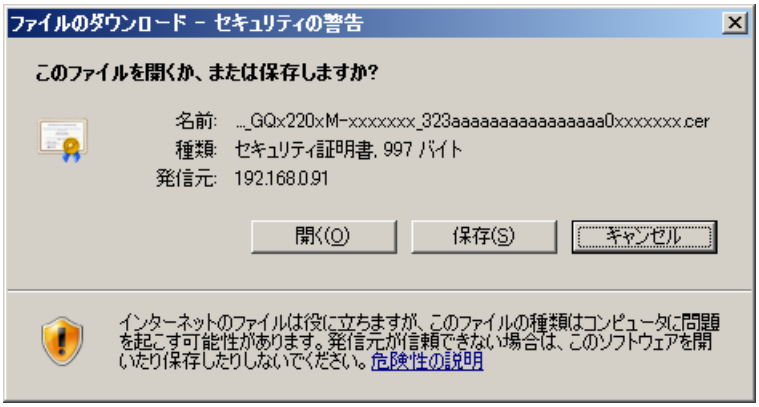
［戻る］ボタンをクリックすると自己証明書をサーバに登録せずに「SSL サーバ設定」画面に戻ります。
［確認］ボタンをクリックすると自己証明書をサーバに登録して「SSL サーバ設定」画面に戻ります。

［CSR の作成とダウンロード］ボタンをクリックすると、次画面が表示されます。

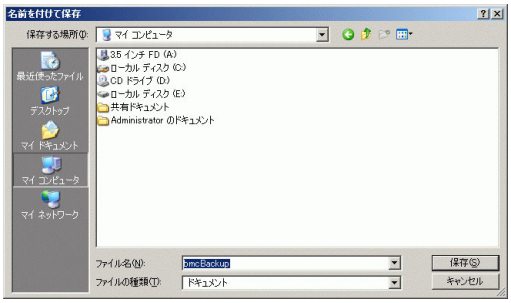


［戻る］ボタンをクリックすると作成した CSR をダウンロードせずに「SSL サーバ設定」画面に戻ります。
［確認］ボタンをクリックすると作成した CSR をダウンロードして「SSL サーバ設定」画面に戻ります。

［サーバ証明書のダウンロード］ボタンをクリックすると、次画面が表示されますので、［保存ボタン］をクリックします。



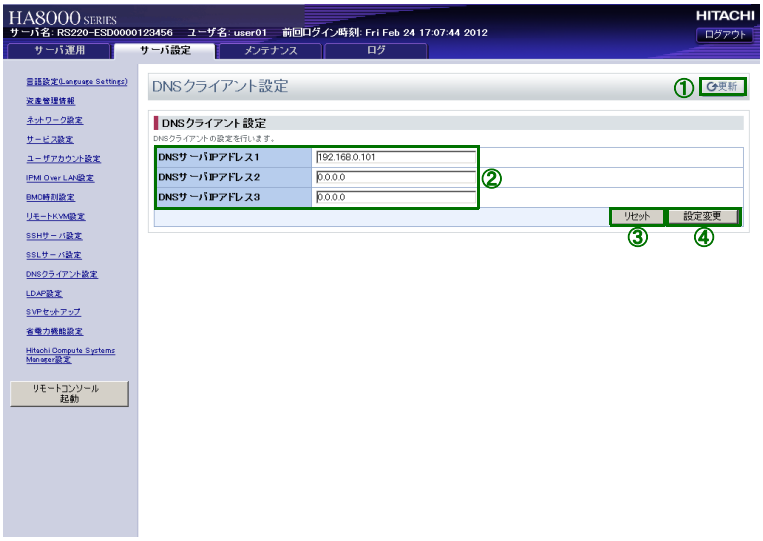
次の画面が表示されますので、保存先を選択したあと［保存］ボタンをクリックします。



サーバ証明書が保存され「ダウンロードの完了」画面が表示されますので、［閉じる］ボタンをクリックします。

(11)「DNS クライアント設定」画面

DNS サーバの IP アドレスを設定し、DNS を使用して名前解決をさせることができます。
DNS サーバの IP アドレスは 3 つまで設定できます。

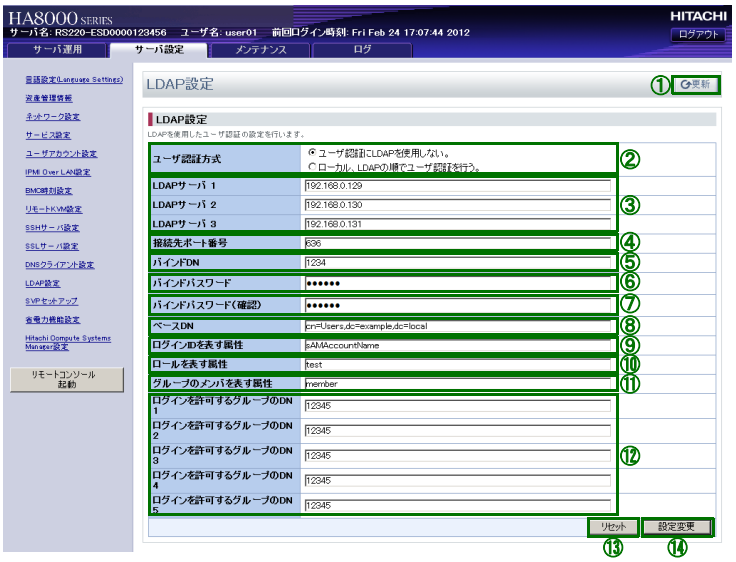


#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	DNS サーバ IP アドレス 1 ～ 3	DNS サーバの IP アドレスを入力します。 DNS サーバの IP アドレスは 3 つまで設定でき、上のものから順に使用されます。2 番目、3 番目の DNS サーバを設定しない場合、"0.0.0.0" を入力してください。 DNS を使用しない場合、3 つとも "0.0.0.0" に設定してください。
③	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
④	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

［設定変更］ボタンをクリックすると、「DNS クライアント設定（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「DNS クライアント設定」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「DNS クライアント設定」画面に戻ります。

(12)「LDAP 設定」画面

LDAP サーバを使用したユーザ認証の設定を行います。



#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	ユーザ認証方式	LDAP を使用したユーザ認証方式を設定します。 ユーザ認証に LDAP を使用しない： 設定されたユーザアカウントによるユーザ認証を行います。 ローカル、LDAP の順でユーザ認証を行う： 設定されているユーザアカウントによるユーザ認証を行い、ユーザ認証に失敗した場合、LDAP サーバ上のユーザアカウントによるユーザ認証を行います。
③	LDAP サーバ 1 ～ 3	LDAP サーバを IP アドレスまたは FQDN で指定します。（最大 127 文字）
④	接続先ポート番号	接続先ポート番号を 10 進数で指定します。（1 ～ 65535）
⑤	バインド DN	LDAP サーバへのバインド時に使用する DN を指定します。（最大 256 文字）入力無しの場合は Anonymous バインドとなります。
⑥	バインドパスワード	LDAP サーバへのバインド時に使用するパスワードを指定します。 （最大 32 文字）入力無しの場合はパスワード無しとなります。
⑦	バインドパスワード（確認）	バインドパスワードの確認入力を行います。
⑧	ベース DN	ユーザ検索のベースとなる DN を指定します。（最大 256 文字）
⑨	ログイン ID を表す属性	ユーザエントリの属性の中でログイン ID として使用するものを指定します。（最大 64 文字）
⑩	ロールを表す属性	ユーザエントリの属性の中でロールを表す文字列が埋め込まれているものを指定します。（最大 64 文字）
⑪	グループのメンバを表す属性	グループエントリの属性の中でメンバとなるユーザを表すものを指定します。（最大 64 文字）
⑫	ログインを許可するグループの DN1 ～ 5	ログインを許可するグループの DN を指定します。（最大 256 文字） すべての DN が入力無しの場合グループ認証を行いません。
⑬	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑭	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

［設定変更］ボタンをクリックすると、「LDAP 設定（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「LDAP 設定」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「LDAP 設定」画面に戻ります。

(13)「SVP セットアップ」画面

SVP アラートの通報先を設定します。
SVP アラート通報先の IP アドレスは、４つまで指定することができます。

#	項目名	説明
①	［更新］ボタン	SVP アラートの通報先設定の表示を更新します。
②	通報先 1 ～ 4 　名称 　IP アドレス 　ポート番号	SVP アラートの通報先を設定します。 通報先の名称、IP アドレス、ポート番号を入力します。
③	［リセット］ボタン	「SVP アラート通報先設定」で編集した内容を無効とし、編集前の状態に戻します。
④	［設定変更］ボタン	「SVP アラート通報先設定」で編集した内容を有効とし、確認画面に遷移します。
⑤	SVP アラート通知	SVP アラート通知のレベルを設定します。 障害通知　：注意、警告、障害レベルのアラートを通知します。 情報通知　：インフォメーションレベルのアラートを通知します。 全通知　　：すべてのレベルのアラートを通知します。 なし　　：アラート通知しません。
⑥	［リセット］ボタン	「SVP アラート通知設定」で編集した内容を無効とし、編集前の状態に戻します。
⑦	［設定変更］ボタン	「SVP アラート通知設定」で編集した内容を有効とし、確認画面に遷移します。

補足

SVP アラートの通報先のポート番号は、通報先の設定に合わせて入力してください。
「JP1/ServerConductor/Blade Server Manager」の場合、ポート番号のデフォルト値は「20079」です。

SVP アラート通報先設定の［設定変更］ボタンをクリックすると、次の確認画面が表示されます。

SVP アラート通知設定の［設定変更］ボタンをクリックすると、次の確認画面が表示されます。

いずれの画面も［確認］ボタンをクリックすると編集した内容が保存され、「SVP セットアップ」画面に戻ります。編集内容を保存しない場合は［戻る］ボタンをクリックします。

(14)「省電力機能設定」画面

省電力機能の設定を行います。
省電力機能は、システムの最大消費電力を指定した電力以下に抑制する機能です。抑制可能な電力は、搭載されているプロセッサのタイプにより異なります。

#	項目名	説明
①	［更新］ボタン	省電力機能設定の表示を更新します。
②	モード設定	省電力機能の有効・無効および、モードを設定します。 DCMI モード：DCMI コマンドにより電力制御を実行するモードです。 DCMI コマンドを使用する場合は別途ソフトウェアが必要になります。 DCMI+NM モード：DCMI コマンドと Node Manager(NM) コマンドを有効とするモードです。 NM コマンドは、マネジメント LAN から、BMC をブリッジして Node Manager へ発行されます。 本モードに設定すると、DCMI コマンドと NM コマンドを使用するソフトウェアから、BMC のファームウェアが設定している Node Manager の Poclicy 設定を書き換えることができますが、Poclicy 設定が書き換えられることにより、BMC による電力管理機能が使用できなくなります。 通常の使用、特に BMC による電力管理機能を使用する場合は、DCMI+NM モードに設定しないでください。 また、NM コマンドによる Policy のパラメータの設定によっては、温度や消費電力の値によってシステムの電源を強制的にオフさせる設定も可能になりますが、誤って設定すると良好なシステム運用を妨げるおそれもあります。 このため、本モードを使用される場合には、DCMI コマンドと NM コマンドを使用するソフトウェアの評価を充分に実施したうえで、ご使用されることを強く推奨します。 一度、DCMI+NM モードでご使用されたあとに他のモードへ切り替えて使用される場合には、ご使用のソフトウェアで設定された NM の Policy をすべて削除したあと、モード切り替えを実施してください。 動的キャッピングモード：動的キャッピングを有効にします。 無効：動的キャッピングを無効にします。DCMI コマンドの使用も抑止します。
③	入気温度	システム装置の入気温度を表示します。
④	現在の電力	現在の電力を表示します。
⑤	過去最大電力	「モード設定」または「消費電力上限設定値」を設定したあとの最大消費電力を表示します。
⑥	過去平均電力	「モード設定」または「消費電力上限設定値」を設定したあとの平均消費電力を表示します。
⑦	消費電力上限設定値	電力を抑制するための目標とする消費電力を設定します。

#	項目名	説明
⑧	［リセット］ボタン	編集した内容を無効とし、編集前の状態に戻します。
⑨	［設定変更］ボタン	編集した内容を有効とし、確認画面に遷移します。

［設定変更］ボタンをクリックすると、「省電力機能設定（確認）」画面が表示されます。表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「省電力機能設定」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「省電力機能設定」画面に戻ります。

▸「消費電力上限設定値」について

「消費電力上限設定値」を低い値に設定しすぎると、常にパワーキャッピングが働いた状態となり、CPU のパフォーマンスは常に低い状態になります。この状態では、実際の消費電力を「消費電力上限設定値」付近以下となるよう制御することはできません。
また、「消費電力上限設定値」をシステム装置の最大消費電力以上の値に設定した場合、パワーキャッピングは機能しません。

パワーキャッピングの機能を有効に利用するには、次の関係式が成り立つように「消費電力上限設定値」を設定する必要があります。

システム装置の最大消費電力 ≧ 消費電力上限設定値 ≧
システム装置の最大消費電力 − パワーキャッピングにより抑制可能な消費電力の最大値

- 消費電力上限設定値 ≧
  システム装置の最大消費電力 − パワーキャッピングにより抑制可能な消費電力の最大値
  この条件を満たせない場合、パワーキャッピングによる省電力機能は働きますが、実際の消費電力が「消費電力上限設定値」を超えてしまう可能性があります。
- システム装置の最大消費電力 ≧ 消費電力上限設定値
  この条件を満たせない場合、実際の消費電力が「消費電力上限設定値」を超えることはありませんが、省電力の効果はありません。

■ システム装置の最大消費電力

システム装置の最大消費電力は、見積り段階では機器仕様に記載された最大消費電力を参考にしてください。ただし、システム装置の消費電力は、温度条件など動作させる環境や実行するプログラムによって左右されます。きめ細かい調整のために、システム装置の最大消費電力は実際に使用する環境でテスト運用を行い確認されることを推奨します。

システム装置の最大消費電力は、「省電力機能設定」画面の「モード設定」を「無効」にし、システム装置に最大の負荷をかけて連続運転した間に表示される「過去最大電力」の値によって確認できます。温度条件によってファンの回転数が上昇しシステムの消費電力が増える場合もありますので、実運用時に近い温度条件で確認する必要があります。

■ パワーキャッピングにより抑制可能な消費電力の最大値

消費電力の抑制の程度は、システム装置のモデルや搭載している CPU の種類、実行するプログラムの負荷条件によって異なります。

抑制可能な消費電力の最大値の目安は次のとおりです。

CPU	動作周波数	抑制可能な消費電力の最大値（目安）*1	
		CPU1 個搭載時	CPU2 個搭載時
Xeon プロセッサー E5-2690	2.90 GHz	120 W	240 W
Xeon プロセッサー E5-2670	2.60 GHz	85 W	170 W
Xeon プロセッサー E5-2640	2.50 GHz	55 W	110 W
Xeon プロセッサー E5-2637	3 GHz	25 W	50 W
Xeon プロセッサー E5-2620	2 GHz	30 W	60 W
Xeon プロセッサー E5-2609	2.40 GHz	25 W	50 W
Xeon プロセッサー E5-2603	1.80 GHz	10 W	20 W
Xeon プロセッサー E5-2630L	2 GHz	30 W	60 W

*1　抑制可能な消費電力は測定結果に基づいた値です。
　　抑制可能な消費電力には、CPUの消費電力が低減されることによって周辺回路の消費電力が低減される効果を含みます。

(15)「Hitachi Compute Systems Manager 設定」画面

Hitachi Compute Systems Manager（HCSM）の設定を行います。

補足

HCSM をサポートしていないバージョンの BMC ファームウェアがシステム装置に適用されている場合、本画面は表示されません。HCSM をご使用になる場合は、BMC ファームウェアをバージョン「09-41」以降にアップデートしてください。
BMC ファームウェアのバージョンは「サーバ運用」タブー「サーバ情報」画面の「BMC F/W バージョン」で確認できます。

#	項目名		説明
①	［更新］ボタン		情報の表示を更新します。
②	管理サーバ数		接続可能な HCSM の数を表示します。
③	管理サーバ情報 1、管理サーバ情報 2、管理サーバ情報 3、管理サーバ情報 4		
		登録番号	対象管理サーバの登録番号を表示します。
		サーバ名	対象管理サーバのサーバ名を設定します。
		IP アドレス	対象管理サーバの IP アドレスを設定します。
		アラートポート番号	アラートに使用するポート番号を設定します。
		アラート通知ポリシー	アラート通知のレベルを設定します。 ・通知せず：アラートを通知しません。 ・障害のみ：障害レベルのアラートを通知します。 ・警告と障害：警告、障害レベルのアラートを通知します。 ・情報と警告と障害：情報、警告、障害レベルのアラートを通知します。
		アラートリトライ間隔（秒）	アラートのリトライ間隔を設定します。 設定可能範囲は 60 ～ 240 秒です。
		アラート再送接続時間（分）	アラートの再送接続時間設定します。 設定可能範囲は 4 ～ 15 分です。
		接続状態	管理対象サーバの接続状態を表示します。
④	［リセット］ボタン		編集した内容を無効とし、編集前の状態に戻します。
⑤	［設定変更］ボタン		編集した内容を有効とし、確認画面に遷移します。

［設定変更］ボタンをクリックすると、「Hitachi Compute Systems Manager 設定」の確認画面が表示されます。
表示された画面の［戻る］ボタンをクリックすると編集した内容を保存せずに「Hitachi Compute Systems Manager 設定」画面に戻り、［確認］ボタンをクリックすると編集した内容を保存して「Hitachi Compute Systems Manager 設定」画面に戻ります。

制限

問題が発生時など、Web コンソールから HCSM との接続を強制的に切断したい場合には、IP アドレスを「0. 0. 0. 0」に設定することにより強制切断することができます。ただし、強制切断する管理サーバのその他の設定項目もすべて削除されます。

補足

- 管理サーバ情報の設定は、対象となる管理サーバの「接続状態」が「未接続」となっているときに行ってください。
- HCSM アラートのアラートポート番号は、通報先の設定に合わせて入力してください。
  HCSM のアラートポート番号のデフォルト値は「22611」です。
- VMware vSphere ESXiではシステムBIOSの時刻をUTCと判断して動作しますが、システム装置は運用上ローカルタイム（現地時間）で管理します。
  このため、VMware vSphere ESXi のインストール後に vSphere クライアントを使用して時刻の設定を行うと、現地時間と UTC の差分だけずれた時間がシステム BIOS の時刻に設定されます。
  この時間は、システム BIOS のセットアップメニューで確認してください。
  HCSM に通知されるアラートの発生時刻や Web コンソール上で表示される時刻は、システム BIOS の時刻で表示され、VMware vSphere ESXi の設定時刻からずれた時刻となります。
- HCSM の詳細は、「Hitachi Command Suite Compute Systems Manager Software ユーザーズガイド」をご参照ください。

4.4.3 「メンテナンス」タブ

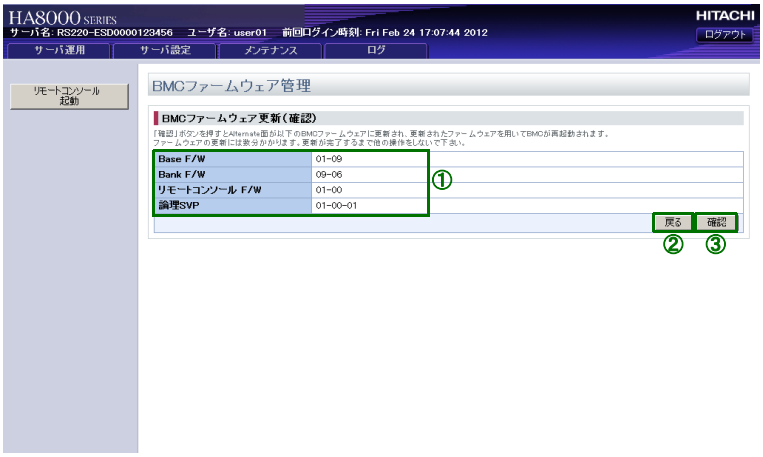
「メンテナンス」タブでは、ファームウェアの更新、ファームウェアで管理しているデータのバックアップ、リストアおよび BMC の再起動を行います。

(1) 「BMC ファームウェア管理」画面

BMC ファームウェアの情報表示および更新を行います。

#	項目名	説明
①	［更新］ボタン	情報の表示を更新します。
②	Base F/W	ベースファームウェアのバージョンを表示します。
③	SDR バージョン	SDR のバージョンを表示します。
④	Bank F/W	ファームウェアのバージョンを表示します。
⑤	リモートコンソール F/W	リモートコンソール機能のバージョンを表示します。
⑥	論理 SVP	論理 SVP 機能のバージョンを表示します。
⑦	BMC F/W イメージファイル	アップロードする BMC ファームウェアイメージファイルを指定します。
⑧	［BMC ファームウェア更新］ボタン	指定したイメージファイルをアップロードします。アップロードには数分かかります。アップロード後、確認画面に切り替わります。

BMC F/W イメージファイルを指定したあと［BMC ファームウェア更新］ボタンをクリックすると、次の確認画面が表示されます。



#	項目名	説明
①	Base F/W Bank F/W リモートコンソール F/W 論理 SVP	アップロードしたイメージファイルに含まれる BMC ファームウェアの情報を表示します。
②	［戻る］ボタン	アップロードしたイメージファイルを破棄し、元の画面に戻ります。
③	［確認］ボタン	アップロードしたイメージファイルを書き込みます。 書き込みには数分かかります。書き込み終了後、BMC が再起動されます。

［確認］ボタンをクリックすると BMC F/W イメージファイルの書き込みが行われます。

制限

BMC F/W イメージファイルの書き込み中は、他の操作はしないでください。
イメージファイルが正常に書き込めなくなる場合があります。

補足

BMC F/W イメージファイルの書き込み中は、「JP1/ServerConductor」や BIOS との通信が遮断されます。このため、BMC F/W のアップデートの前にシステム装置の電源を切る必要があります。もし BMC F/W のアップデート後にシステム装置が起動しない場合、システム装置の電源を切り、電源コードを外すことにより AC 供給を遮断して 30 秒以上待ち、再度電源コードを接続してシステム装置の電源を入れてください。

書き込みが完了すると BMC が再起動されるため、Web コンソールからログアウトされ、システム装置との接続が切断されます。

BMC が再起動されると、システム装置の SERVICE ランプスイッチが 30 秒から 60 秒ほどの間点滅します。SERVICE ランプスイッチの点滅が終了してから、システム装置の電源を切ってください。

補足

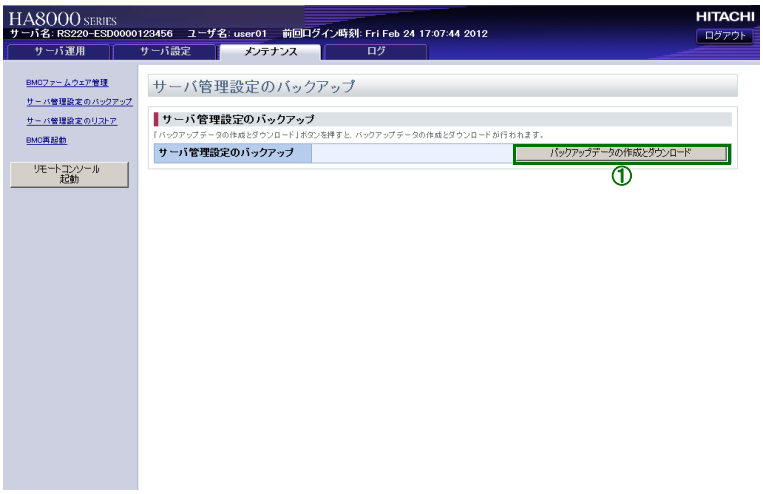
- BMC を再起動すると、「JP1/ServerConductor」、BIOS などとの通信や、Web コンソール、リモートコンソールなどの BMC の機能が停止します。BMC 再起動中（30 秒～ 90 秒）は、これらの通信や機能が使えません。
  BMC と通信を行うプログラムによっては、BMC の再起動時サービスが停止することによって、エラーメッセージを表示するなど問題が発生する可能性があります。
  また、システム BIOS の起動中やセットアップメニューの操作中に BMC を再起動しないでください。BMC と BIOS 間の通信ができない状態となって、システム異常が発生することがあります。
  BMC を再起動する場合は、システム装置をシャットダウンした状態で実行することをお勧めします。
- システム装置がサポートしていない BMC F/W イメージファイルを指定した場合、イメージファイルの書き込みは行われずに BMC が再起動されます。

(2)「サーバ管理設定のバックアップ」画面

システム装置の管理のために使用する設定のバックアップを行います。
Web コンソールの設定を変更した場合は忘れずにバックアップを行ってください。

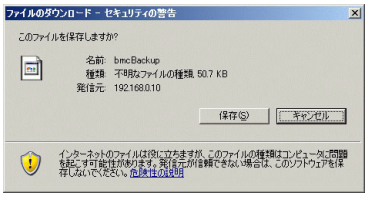
補足

BMC F/W イメージ、SDR などを更新した場合、ファームウェアの設定情報のバックアップを実施し、以降は新しく取得したバックアップファイルをご使用ください。

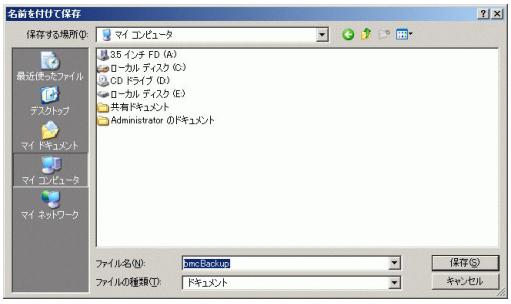


#	項目名	説明
①	［バックアップデータの作成とダウンロード］ボタン	バックアップデータファイルを作成し、ダウンロードします。

［バックアップデータの作成とダウンロード］ボタンをクリックすると次の画面が表示されますので、［保存］ボタンをクリックします。



次の画面が表示されますので、保存先を選択したあと［保存］ボタンをクリックします。



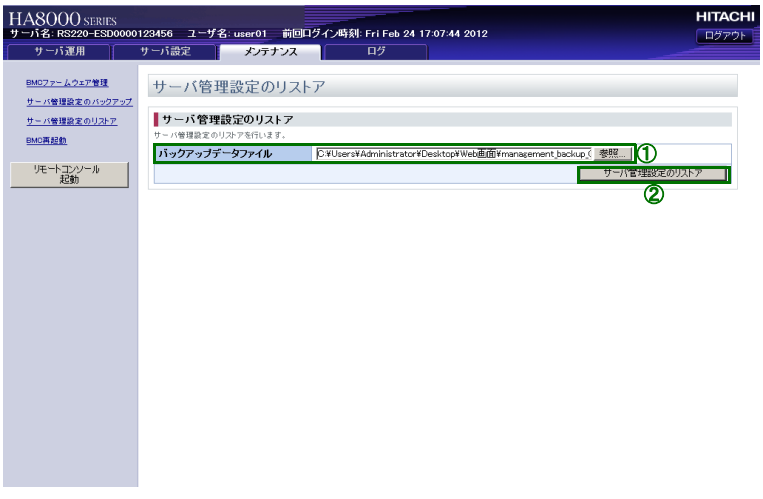
バックアップデータが保存され、「ダウンロードの完了」画面が表示されますので、［閉じる］ボタンをクリックします。

(3) サーバ管理設定のリストア画面

「サーバ管理設定のバックアップ」画面でダウンロードしたバックアップデータファイルを使用して設定を復元します。
復元後、BMC の再起動を行う必要があります。

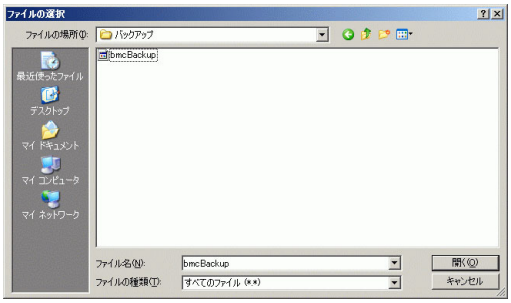
制限

- IPMI Over LAN 機能の設定情報および、BMC ネットワークの IP アドレス、デフォルトゲートウェイ、サブネットマスク設定情報は、バックアップおよびリストアされません。
  障害などでマザーボードを交換した場合は、これらを設定しなおしてください。
- Web コンソールでバックアップしたファームウェア設定情報を、ほかのシステム装置へリストアしないでください。
  システム装置固有のモデル名、製造番号、ハードウェア構成などの情報がほかの装置へ書き込まれ、正常に動作しないおそれがあります。
  バックアップ時のファイル名には、システム装置のモデル名、製造番号が含まれますので、ファイル名を確認して、バックアップを実施した装置へリストアしてください。

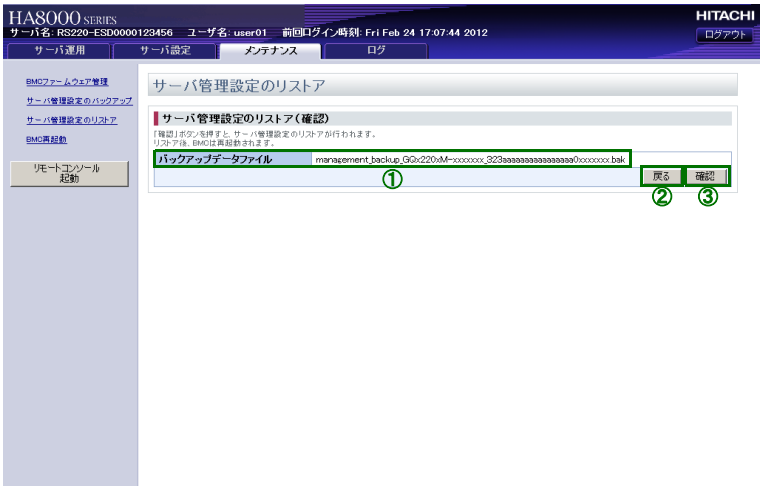


#	項目名	説明
①	バックアップデータファイル	「サーバ管理設定のバックアップ」画面でダウンロードしたバックアップデータファイルを指定します。
②	［サーバ管理設定のリストア］ボタン	指定したバックアップデータファイルをアップロードし、確認画面に遷移します。

［参照］ボタンをクリックすると次の画面が表示されますので、サーバ管理設定のバックアップデータファイルを選択し［開く］ボタンをクリックします。



バックアップデータファイルを選択したあとに［サーバ管理設定のリストア］ボタンをクリックすると、次の確認画面が表示されます。



#	項目名	説明
①	バックアップデータファイル	アップロードしたバックアップデータファイルのファイル名を表示します。
②	［戻る］ボタン	アップロードしたバックアップデータファイルを破棄し、元の画面に戻ります。
③	［確認］ボタン	アップロードしたバックアップデータファイルを用いて設定を復元します。設定を復元したあとで BMC が再起動されます。

選択したファイルが正しいことを確認して［確認］ボタンをクリックすると、設定の復元が開始されます。

補足

サーバ管理設定のリストア中は、「JP1/ServerConductor」や BIOS との通信が遮断されます。このため、サーバ管理設定のリストア前にシステム装置の電源を切る必要があります。
もしサーバ管理設定のリストア後にシステム装置が起動しない場合、システム装置の電源を切り、電源コードを外すことにより AC 供給を遮断して 30 秒以上待ち、再度電源コードを接続してシステム装置の電源を入れてください。

設定の復元が行われ、BMC が再起動されるため、Web コンソールからログアウトされ、システム装置との接続が切断されます。

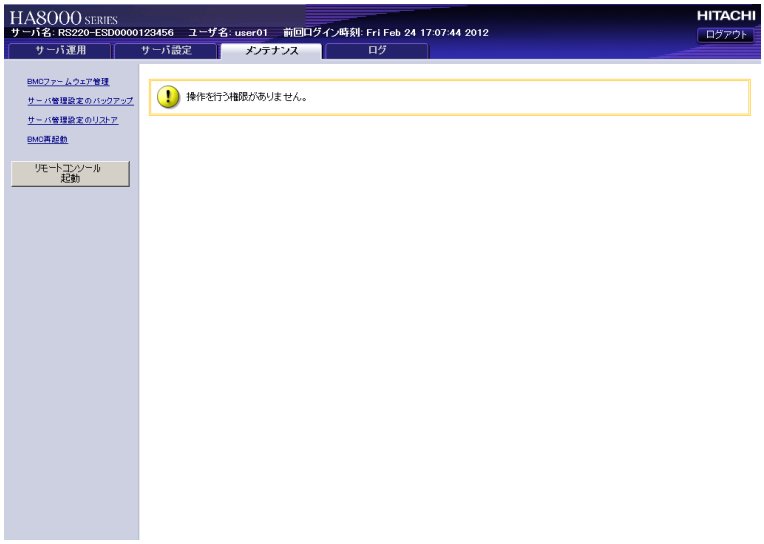
BMC が再起動されると、システム装置の SERVICE ランプスイッチが約 30 秒から 60 秒ほどの間点滅します。SERVICE ランプスイッチの点滅が終了してから、システム装置の電源を切ってください。

補足

BMC を再起動すると、「JP1/Server Conductor」、BIOS などとの通信や、Web コンソール、リモートコンソールなどの BMC の機能は停止します。BMC 再起動中（30 秒～ 90 秒）は、これらの通信や機能が使えません。
BMC と通信を行うプログラムによっては、BMC の再起動時サービスが停止することによって、エラーメッセージを表示するなど問題が発生する可能性があります。
また、システム BIOS の起動中やセットアップメニューの操作中に BMC を再起動しないでください。BMC と BIOS 間の通信ができない状態となって、システム異常が発生することがあります。
BMCを再起動する場合は、システム装置をシャットダウンした状態で実行することをお勧めします。

(4) 「BMC 再起動」画面

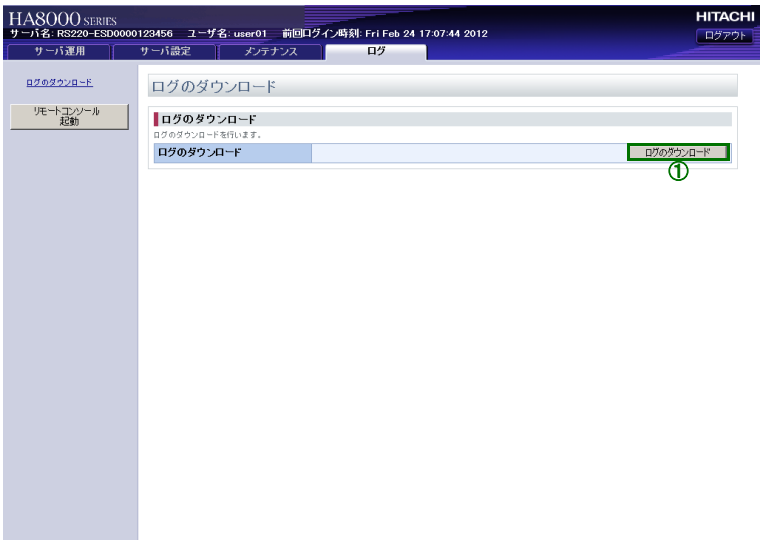
本画面は“ceconsl”ユーザ（保守員作業用ユーザ）のみ使用可能です。権限のないユーザでは使用できません。



4.4.4 「ログ」タブ

「ログ」タブでは、BMC が採取したログをダウンロードすることができます。

(1)「ログのダウンロード」画面



#	項目名	説明
①	［ログのダウンロード］ボタン	BMC が採取したログをダウンロードします。

補足

本ログは、ハードウェアの障害調査時に使用します。通常の運用では、ログを採取する必要はありません。
なお、障害が発生した場合、原因調査のために Web コンソールを使用しログの採取をお願いする場合があります。

5

BMC ネットワーク設定の注意事項

この章では、BMC のネットワーク設定方法と設定値および設定上の注意事項について説明します。

5.1 BMC ネットワーク設定方法の種類と設定値

ここでは、BMC ネットワーク設定方法の種類と設定値について説明します。

5.1.1 BMC ネットワーク設定方法の種類

リモートマネジメント機能をご使用になる場合の BMC ネットワークの設定方法は、次の 3 種類があります。

- SVP エミュレート機能を使用する場合の BMC ネットワーク設定
  （「JP1/ServerConductor/Advanced Agent」の「SVP PCI 設定ユティリティ」による設定）
- システム BIOS のセットアップメニューによる BMC ネットワーク設定
- Web コンソールによる BMC ネットワーク設定
  （初期のネットワーク設定により BMC ネットワークに接続し、クライアントから設定）

リモートマネジメント機能の主な設定項目と、設定を行うためのツールの関係を次の表に示します。（太枠は、その機能を設定する推奨ツールであることを示します。）
特に、BMC ネットワーク設定には複数の方法がありますが、ほかの設定項目と同じ方法で設定されることをお勧めします。

○：設定可能　×：使用禁止　－：機能なし

機能	主な設定項目	設定可能な方法（ツール）		
		SVP PCI 設定ユティリティ	Web コンソール	システム BIOS セットアップ
SVP エミュレート *1（JP1/ServerConductor/Advanced Agent 環境下で使用）	BMC ネットワーク設定	○ *2	× *2	○ *2
	SVP アラート接続先設定	○	○	－
	SVP アラート通知レベル	○	○	－
	障害監視の詳細設定	○	－	－
SVP エミュレート *1（VMware などの環境下で使用）	BMC ネットワーク設定	－	○	○
	SVP アラート接続先設定	－	○	－
	SVP アラート通知レベル	－	○	－
	障害監視の詳細設定	－	－	－
Web コンソール	BMC ネットワーク設定	○	○	○
	接続先アドレス制限	－	○	－
	ユーザアカウント設定	－	○	－
リモートコンソール	BMC ネットワーク設定	○	○	○
	マウスモードの設定	－	○	－
	接続先アドレス制限	－	○	－
	ユーザアカウント設定	－	○	－
IPMI Over LAN	BMC ネットワーク設定	○	○	○
	接続先アドレス制限	－	○	－

機能	主な設定項目	設定可能な方法（ツール）		
		SVP PCI 設定ユティリティ	Web コンソール	システム BIOS セットアップ
ネットワーク接続不可時の設定回復	BMC ネットワーク設定	○	−	○
	接続先アドレス制限	−	−	○
	ユーザアカウント設定	−	−	○

*1: SVP エミュレート機能とは、「リモート電源制御」、「電源制御スケジュール」、「リモート障害監視」など、BMC のファームウェアでエミュレートすることによりサポートしている機能を示します。

*2: 「JP1/ServerConductor/Advanced Agent」から SVP エミュレート機能を使用する場合は、Web コンソール、リモートコンソールオプションなど、ほかの機能の使用有無とは無関係に、「SVP PCI 設定ユティリティ」を使って BMC のネットワーク設定を行ってください。
Web コンソールから BMC のネットワーク設定を行った場合は、「SVP PCI 設定ユティリティ」を使用してネットワークを設定し直してください。

5.1.2 BMC ネットワークの設定値

BMC ネットワークの設定値（IP アドレス、サブネットマスク、デフォルトゲートウェイ）は、ご使用のネットワーク環境に合わせて、適切に設定してください。

各設定項目について、指定可能な値は次のとおりです。なお、各設定の IP アドレスは、IPv4 の IP アドレスの十進数で表記しております。

■ IP アドレス

「1.0.0.0」～「223.255.255.255」のうち、次のアドレスを除いた値を設定することができます。

- ホスト部を二進数で表記したときすべて “1” となるアドレス（ブロードキャストアドレスと重複します）
- ホスト部を二進数で表記したときすべて “0” となるアドレス（ネットワークアドレスと重複します）
- 127.0.0.0 ～ 127.255.255.255 の範囲のアドレス

なお、同一ネットワーク内に Windows のシステムが存在する場合、「xxx.xxx.xxx.255」のように下位 8bit の二進数表記がすべて “1” になるアドレスは使用しないでください。

たとえば、IP アドレスが「192.168.0.0」でサブネットマスクが「255.255.252.0」の場合、ブロードキャストアドレスが「192.168.3.255」となるため使用できません。同様にアドレス「xxx.xxx.0.255」、「xxx.xxx.1.255」、「xxx.xxx.2.255」も使用しないでください。

■ サブネットマスク

「255.0.0.0」～「255.255.255.255」のうち、二進数で表記したときにマスクするビットが連続している値を設定することができます。

たとえば、255.255.255.64（二進数表記：1111 1111 1111 1111 1111 1111 0100 0000）は、マスクするビットが連続していませんので設定できません。

また、指定されたホスト部（サブネット内）に設定可能な IP アドレスが 2 個以上存在しないような値は設定できません。
たとえば、255.255.255.254（二進数表記：1111 1111 1111 1111 1111 1111 1111 1110）は、ホスト部（サブネット内）に IP アドレスとして設定可能な値が存在しないので設定できません。（ネットワークアドレスとブロードキャストアドレスで 2 つ使用されるため、ホストを指定する IP アドレスが割り当てできません。）

■ デフォルトゲートウェイ

IP アドレスとサブネットマスクから定義されるネットワーク（サブネット）に存在するアドレスで、かつ、IP アドレスとして設定可能な値を設定することができます。

たとえば、次の組み合わせは設定できません。

- IP アドレスとサブネットマスクから定義されるネットワーク（サブネット）に存在しないアドレス

IP アドレス	192.168.0.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.20

  ※サブネット内で設定可能なアドレスは 192.168.0.1 ～ 192.168.0.254 であるため。

- IP アドレスとして設定できないアドレス

IP アドレス	192.168.0.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.0.255

  ※192.168.0.255 はブロードキャストアドレスであるため。
  また、同様に 192.168.0.0 はネットワークアドレスとなるため、設定できません。

なお、各設定ツール側では、上記以外の値を指定した場合に必ずしも設定可否を判断するとは限りません。したがって誤った値を指定した場合、設定ツールとしては正常に受け付け処理がされますが、BMC 側に設定しようとしたときに初めて異常と判断され、正常に設定されないことがあります。
BMC のネットワーク設定後に正しく動作しない場合は、設定したツールでネットワークの設定を再確認し、正しい値に設定し直してください。

5.2 SVP エミュレート機能を使用する場合の BMC ネットワーク設定について

ここでは、SVPエミュレート機能を使用する場合のBMCネットワークの設定について説明します。

5.2.1 SVP PCI 設定ユティリティについて

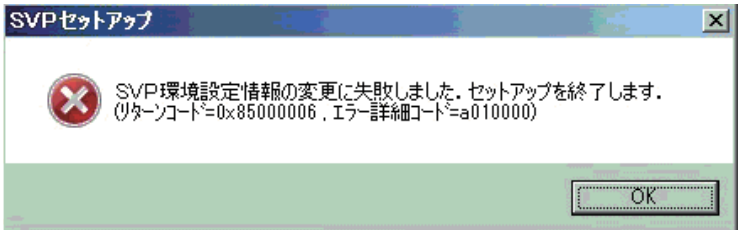
「JP1/ServerConductor/Advanced Agent」および「JP1/ServerConductor/Blade Server Manager」により、「リモート電源制御」、「電源制御スケジュール」、「リモート障害監視」の機能をご使用になる場合には、「JP1/ServerConductor/Advanced Agent」の「SVP PCI 設定ユティリティ」から、BMC ネットワークの設定を行ってください。

Web コンソールから BMC ネットワークの設定を行った場合でも、「JP1/ServerConductor/Advanced Agent」の「SVP PCI 設定ユティリティ」による設定が必要となります。

ただし、VMware による運用など「JP1/ServerConductor/Advanced Agent」をご使用にならない場合は、システム BIOS のセットアップメニューおよび Web コンソールを使って BMC ネットワークの設定を行う必要があります。

「SVP PCI 設定ユティリティ」から設定を行う場合、次の制限があります。

- デフォルトゲートウェイの設定を、IP アドレスとサブネットマスクにより定義されるネットワークセグメント（サブネット）外のアドレスにした場合、次のようなメッセージを表示して「SVP PCI 設定ユティリティ」が異常終了することがあります。



  この場合「SVP PCI 設定ユティリティ」を再起動し、正しいネットワークに設定し直してください。

- サブネットマスクに“255.0.255.0”や“255.255.255.64”のような、マスクするビットが不連続となる値を設定した場合、「SVP PCI 設定ユティリティ」の画面では正しく設定されたように表示されますが、実際には BMC に設定が反映されません。

  この場合「SVP PCI 設定ユティリティ」を再起動し、正しいネットワークに設定し直してください。

- BMCのネットワーク設定を変更した場合（WebコンソールでBMCのネットワーク設定を変更した場合を含む）には、「JP1/ServerConductor/Advanced Agent」の「環境設定ユティリティ」を起動してサービスを再起動するか、システム装置を再起動する必要があります。

索引

－ MEMO －

日立アドバンストサーバ　HA8000 シリーズ

ユーザーズガイド

～リモートマネジメント編～

HA8000/RS220-h HM1/JM1/KM1/LM1　HA8000/RS210-h HM1/JM1/KM1/LM1

2012 年 11 月～モデル

初　版　2012 年 11 月
第 2 版　2013 年 6 月

株式会社　日立製作所
ITプラットフォーム事業本部

〒259-1392　神奈川県秦野市堀山下1番地

http://www.hitachi.co.jp

R2EAM11600-2