

N8115-02
アドバンスドマネージメントカード
Advanced Remote Management Card
ユーザーズガイド
User's Guide

2005年 11月 三版
3rd Edition 11-2005

商標/特許について

EXPRESSBUILDERとESMPRO は日本電気株式会社の登録商標です。

DianaScopeは日本電気株式会社の商標です。

MicrosoftおよびWindows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。AVOCENTおよびDVC(DAMBRACKAS VIDEO COMPRESSION)は米国AVOCENT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。

Mozilla は Mozilla Foundation の商標です。

Netscapelは、Netscape Communications Corporationの米国及び諸外国における商標または登録商標です。Javaの名称はSun Microsystems, Incの米国及び諸外国における商標または、登録商標です。

本製品は、米国AvocentのDAMBRACKAS VIDEO COMPRESSION技術を採用しています。
米国特許番号 5,732,212/5,937,176/6,633,905/6,681,250/6,701,380 その他申請中。

台湾特許番号 173784

ヨーロッパ特許番号 0 740 811

Trademarks and Patents

NEC ESMPRO , NEC EXPRESSBUILDER and NEC DianaScope are trademarks of NEC Corporation. Microsoft , Windows are registered trademarks of Microsoft Corporation in the United States and other countries. DAMBRACKAS VIDEO COMPRESSION is a trademark of Avocent Corporation in the United States and other countries.

Mozilla is trademarks of the Mozilla Foundation.

Netscape is registered trademarks of Netscape Communications Corporation in the United States and other countries. Java is registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

The DAMBRACKAS VIDEO COMPRESSION technology from Avocent Corporation is used for this equipment.

U.S. Patent Numbers: 5,732,212/5,937,176/6,633,905/6,681,250/6,701,380
and "Other Patents Pending"

Taiwanese Patent Number 173784

European Patent Number 0 740 811

ご注意

- (1) 本書の内容の一部または全部を無断転載することは禁止されています。
- (2) 本書の内容に関しては将来予告なしに変更することがあります。
- (3) NEC の許可なく複製・改変などを行うことはできません。
- (4) 本書は内容について万全を期して作成しましたが、万一ご不審な点や誤り、記載漏などお気づきのことがありましたら、お買い求めの販売店にご連絡ください。落丁、乱丁本はお取替えいたします。
- (5) 運用した結果の影響については(4)項にかかわらず責任を負いかねますのでご了承ください。

Notes:

- (1) No part of this manual may be reproduced in any form without the prior written permission of NEC Corporation.
- (2) The contents of this use's guide may be revised without prior notice.
- (3) The contents of this User's Guide shall not be copied or altered without the prior written permission of NEC Corporation.
- (4) All efforts have been made to ensure the accuracy of all information in this User's Guide. If you notice any part unclear, incorrect, or omitted in this User's Guide, contact the sales agent where you purchased this product.
If you find any missing pages or pages out of order in this manual, please contact your dealer for a replacement.
- (5) NEC assumes no liability arising from the use of this product, nor any liability for incidental or consequential damages arising from the use of this User's Guide regardless of Item (4).

本書について

本書は、本製品を本体装置に正しく接続し、使用できるようにするための手引きです。本製品を使用して本体装置のHW管理/監視,リモートマネージメントを行う上で、わからないことや具合の悪いことが起きたときは、取り扱い上の安全性を含めてご利用ください。また本書は必要なときにすぐ参照できるよう、お手元に置いておくようにしてください。なお、本書は和英併記となっております。日本語での説明はiページから60ページを、英語での説明はiページから xvii ページおよび、61ページから118ページを参照してください。

About This User's Guide



This User's Guide is intended to help the user install and use the N8115-02 Advanced Remote Management Card properly. When encountering any questions and troubles in controlling/monitoring H/W and Remote Management with this product, use this guide and also refer to safety precautions in it.

Keep this User's Guide at hand for quick reference at anytime necessary.

This User's Guide is written in both Japanese and English. For Japanese, refer to pages i to 60. For English, refer to pages i to xvii and 61 to 118.

日本語版 Japanese Edition



See page 19 for English version.

| | |
|---|-----------|
|  使用上のご注意 ~必ずお読みください~ | i |
| 安全に関わる表示について | i |
|  SAFETY PRECAUTIONS | ii |
| Safety Indications | ii |
| 本書で使用する記号 | iii |
| Symbols Used in This User's Guide | iii |
| 安全上のご注意 | iv |
| Notes on Safety | iv |
| 本文中の記号について | x |
| Note on Handling ~ For Proper Operation~ | xi |
| はじめに | xii |
| Preface | xii |
| 付属品の確認 | xiii |
| Check of Accessories | xiv |
| 第三者への譲渡について | xv |
| Transfer to Third Party | xv |
| 製品の廃棄について | xv |
| Disposal | xv |
| 本書を紛失してしまったら | xv |
| 1. 各部の名称と機能 | 1 |
| マネージメント カード本体 | 2 |
| 管理用ネットワークカード | 3 |
| ネットワーク デフォルト設定値 | 4 |
| 2. 取り付け/取り外し | 6 |
| 静電気対策について | 7 |
| 取り付け / 取り外しの準備 | 7 |
| 本製品の取り付け/取り外し | 8 |
| 3. 本体装置側の設定 | 15 |
| 本製品の初期設定 | 15 |
| ビデオドライバの組み込み | 15 |
| マウスのプロパティの変更 | 16 |
| 4. 管理 PC 側の設定 | 17 |
| ブラウザの設定 | 17 |
| 動作対応ブラウザ | 17 |
| Java2 Runtime Environment | 17 |
| 5. リモートマネージメントの使い方 | 18 |
| 概要 | 18 |
| 接続方法 | 18 |
| ログイン・ログアウト | 19 |
| メインウィンドウ | 21 |
| コントロールパネル | 22 |
| リモート KVM コンソール | 23 |
| IPMI 情報 | 26 |
| BMC に対する各種設定 | 29 |

| | |
|-----------------------------|-----------|
| ファームウェアアップデート..... | 42 |
| 6. トラブルシューティング | 47 |
| エラーメッセージ..... | 47 |
| その他 | 58 |

英語版 English Edition

See page 1 for Japanese version.

| | |
|---|-----------|
|  使用上のご注意 ~必ずお読みください~ | i |
| 安全に関わる表示について | i |
|  SAFETY PRECAUTIONS | ii |
| Safety Indications | ii |
| 本書で使用する記号 | iii |
| Symbols Used in This User's Guide | iii |
| 安全上のご注意 | iv |
| Notes on Safety | iv |
| 本文中の記号について | x |
| Note on Handling ~ For Proper Operation~ | xi |
| はじめに | xii |
| Preface | xii |
| 付属品の確認 | xiii |
| Check of Accessories | xiv |
| 第三者への譲渡について | xv |
| Transfer to Third Party | xv |
| 製品の廃棄について | xv |
| Disposal | xv |
| 本書を紛失してしまったら | xv |
| 1. Overview | 61 |
| Management Main Card | 62 |
| Management LAN Card | 63 |
| Default Network Settings | 64 |
| 2. Installation | 66 |
| Safety Precautions | 66 |
| Anti-static Measures | 67 |
| Preparing for Installation and Removal | 67 |
| Installation and Removal | 68 |
| Installation | 69 |
| Removal | 73 |
| 3. Server Setup | 75 |
| Initial setting of Advanced Remote Management Card | 75 |
| setting of Video Driver | 75 |
| setting of Mouse properties | 76 |
| 4. Configuring Management PC | 78 |
| Setting your browser | 78 |
| Supported browsers | 78 |
| Java2 Runtime Environment | 78 |
| 5. Using Remote Management Console | 80 |
| Overview | 80 |
| Connecting to the web server from a web browser on the management pc | 80 |
| Login and logout | 81 |
| Main window | 83 |
| Control panel | 84 |
| Remote KVM console | 85 |

| | |
|---------------------------------|------------|
| IPMI Information | 88 |
| BMC configuration | 91 |
| firmware update | 104 |
| 6. Troubleshooting | 109 |
| Error messages | 109 |
| Others | 117 |

本製品の使用につきましては、本書および、本体装置に添付のユーザーズガイドを参照の上ご使用願います。また、ご使用前に「使用上のご注意」を必ずお読みください。本書をお読みになった後は、必要なときにすぐに参照できるようお手元においておくようにしてください。

使用上のご注意 ～必ずお読みください～



本製品を安全に正しくご使用になるために必要な情報が記載されています。

安全に関わる表示について




本製品を安全にお使いいただくために、このユーザーズガイドの指示に従って取り扱ってください。

本書には、ご使用時にどこが危険であるか、どのような危険にあうか、どうすれば危険を避けられるかなどについて説明されています。

本書では、危険の程度を表す用語として、「警告」と「注意」を使用しています。それぞれの用語は、次のような意味を持つものとして定義されています。

| | |
|---|--|
|  警告 | この表示は、使用者が死亡または重傷を負うおそれがあること、および物的損害による火災等の拡大のおそれがあることを示します。 |
|  注意 | この表示は、使用者が負傷を負うおそれがあること、および物的損害のみのおそれがあることを示します。 |

危険に対する注意・表示には次の3種類の記号を使用しています。それぞれの記号は次のような意味を持つものとして定義されています。

| | | |
|---|-------|---|
|  | 注意の喚起 | この記号は、危険が発生するおそれがあることを表しています。記号の中の絵表示は危険の内容を図案化したものです。 |
|  | 行為の禁止 | この記号は行為の禁止を表しています。記号の中や近くの絵表示は、してはならない行為の内容を図案化したものです。 |
|  | 行為の強制 | この記号は行為の強制を表しています。記号の中の絵表示はしなければならない行為の内容を図案化したものです。危険を避けるためには、この行為が必要です。 |

Read this "Safety Precautions" and separately provided User's Guide thoroughly before getting started to use this product safely. After you have read this brochure, store it in the place that is easy to access.

SAFETY PRECAUTIONS



This section describes the information necessary to use this product safely.

Safety Indications




Follow the instructions described in this User's Guide for your safety to use this product.

This product contains components with possible danger, hazards that may cause by ignoring warnings, and preventive actions against such hazards.

In the User's Guide, "WARNING" or "CAUTION" is used to indicate a degree of danger. These terms are defined as follows:

| | |
|--|---|
|  WARNING | This symbol indicates that using the product improperly in defiance of this symbol is likely to result in death, serious injury, fire, or damage to the device and peripherals. |
|  CAUTION | This symbol indicates that using the product improperly in defiance of this symbol may result in injury or only damage to property. |

Precautions and notices against hazards are presented with one of the following three symbols. The individual symbols are defined as follows:

| | | |
|---|-------------------|---|
|  | Attention | This symbol indicates the presence of a hazard if the instruction is ignored. An image in the symbol illustrates the hazard type. |
|  | Prohibited Action | This symbol indicates prohibited actions. An image in the symbol illustrates a particular prohibited action. |
|  | Mandatory Action | This symbol indicates mandatory actions. An image in the symbol illustrates a mandatory action to avoid a particular hazard. |

本書で使用する記号

注意の喚起

| | | | |
|---|------------------------|---|--------------------------|
|  | 感電のおそれがあることを示します。 |  | 高温による傷害を負うおそれがあることを示します。 |
|  | 指などが挟まれるおそれがあることを示します。 |  | 発煙または発火のおそれがあることを示します。 |
|  | 特定しない一般的な注意・警告を示します。 | | |

行為の禁止






| | | | |
|---|-------------------|---|--------------------------------------|
|  | 特定しない一般的な禁止を示します。 |  | 本製品を分解・修理・改造しないでください。感電や火災のおそれがあります。 |
|---|-------------------|---|--------------------------------------|

行為の強制



| | | | |
|--|---|--|---------------------------------------|
|  | 本体装置の電源プラグをコンセントから抜いてください。火災や感電のおそれがあります。 |  | 特定しない一般的な使用者の行為を指示します。説明に従った操作をして下さい。 |
|--|---|--|---------------------------------------|

Symbols Used in This User's Guide



Attentions

| | | | |
|---|---|---|--|
|  | Indicates the risk of electric shock. |  | Indicates the risk of an injury due to high temperature. |
|  | Indicates the risk that your fingers may be caught. |  | Indicates the risk of smoke emission or fire outbreak. |
|  | Indicates a general notice or warning that cannot be specifically identified. | | |

Prohibited Actions

| | | | |
|---|--|---|---|
|  | Indicates the notification of general prohibition. |  | Do not disassemble, repair, or modify this product. Otherwise, an electric shock or fire may be caused. |
|---|--|---|---|

Mandatory Action

| | | | |
|---|---|---|---|
|  | Unplug the AC cord of the server. Otherwise, an electric shock or fire may be caused. |  | Indicates a mandatory action that cannot be specifically identified. Make sure to follow the instruction. |
|---|---|---|---|

安全上のご注意

本製品を安全にお使いいただくために、ここで説明する注意事項をよく読んでご理解し、安全にご活用ください。記号の説明については巻頭の『安全に関わる表示について』の説明を参照してください。

注意

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラス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。

Notes on Safety

To enable you to use this product safely, read the notes described below carefully to understand them. See "Safety Indications" described earlier for the descriptions of symbols.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Statement

Warning: This is a Class A product. In domestic environment this product may cause radio interference in which case the user may be required to take adequate measures (EN55022).

BSMI Statement

警告使用者：
這是甲類的資訊產品、在居住的環境中使用時、可能會造成射頻干擾、在這種情況下、使用者會被要求採取某些適當的對策。

全般的な注意事項

警告



人命に関わる業務や高度な信頼性を必要とする業務には使用しない。

本装置は、医療機器・原子力設備や機器、航空宇宙機器・輸送設備や機器など、人命に関わる設備や機器および高度な信頼性を必要とする設備や機器などへの組み込みやこれらの機器の制御などを目的とした使用は意図されていません。これらの設備や機器、制御システムなどに本装置を使用した結果、人身事故、財産損害などが生じても当社はいかなる責任も負いかねます。

注意



本体装置内に水や異物を入れない

本体装置内に水などの液体、ピンやクリップなどの異物を入れないでください。火災や感電、故障の原因となります。もし入ってしまったときは、すぐ電源をOFFにして、ACコードをコンセントから抜いてください。分解しないで販売店または保守サービス会社にご連絡ください。

General

WARNING



Do not use the server for services where critical high availability may directly affect human lives.

This product is not intended to be used with or control facilities or devices concerning human lives, including medical devices, nuclear facilities and devices, aeronautics and space devices, transportation facilities and devices; and facilities and devices requiring high reliability. NEC assumes no liability for any accident resulting in personal injury, death, or property damage if this product has been used in the above conditions.

CAUTION



Keep water or foreign matter away from the server.

Do not let any form of liquid (water etc.) or foreign matter (e.g., pins or paperclips) enter the server. Failure to follow this warning may cause an electric shock, a fire, or a failure of the server. When such things accidentally enter the server, immediately turn off the power and disconnect the AC cord from the outlet. Do not disassemble the server. Contact your service representative.

設置・移動・保管・接続に関する注意事項

注意



不適切な場所に設置・保管しない

本製品を次に示すような場所や本書で指定している場所以外に設置しないでください。故障の原因となるおそれがあります。

- ほこりの多い場所
- 直射日光が当たる場所
- 給湯器のそばなどの湿気の多い場所
- 磁気を帯びた場所
- 設置・移動・保管・接続に関する注意事項

腐食性ガスの存在する環境で使用または保管しない

腐食性ガス（二酸化硫黄、硫化水素、二酸化窒素、塩素、アンモニア、オゾンなど）の存在する環境に設置し、使用しないでください。また、ほこりや空気中に腐食を促進する成分（塩化ナトリウムや硫黄など）や導電性の金属などが含まれている環境へも設置しないでください。装置内部のプリント板が腐食し、故障および発煙・発火の原因となるおそれがあります。もしご使用の環境で上記の疑いがある場合は、販売店または保守サービス会社にご相談ください。



本体装置やの電源がONのままや、ACコードを接続したままインタフェースケーブルの取り付けや取り外しをしない

インタフェースケーブルの取り付け／取り外しは本体装置の電源をOFFし、ACコードをコンセントから抜いてから行なってください。たとえ、本体装置の電源がOFFされていてもACコードを接続したままケーブルに触ると感電したり、ショートによる火災を起こしたりするおそれがあります。



指定以外のインタフェースケーブルを使用しない

インタフェースケーブルは、NEC が指定するものを使用し、接続する装置やコネクタを確認した上で接続してください。指定以外のケーブルを使用したり、接続先を誤ったりすると、ショートにより火災を起こすことがあります。

また、インタフェースケーブルの取扱いや接続について次の注意をお守りください。

- 破損したケーブルコネクタを使用しない。
インタフェースケーブルを接続する前に、ケーブルコネクタが破損していたり、コネクタピンが曲がっていたり汚れたりしていないことを確認してください。
- ケーブルを履まない。
- ケーブルの接続がゆるんだまま使用しない。
- ケーブルの上にものを載せない。
- ネジ止めなどのロックを外したまま使用しない。



指を挟まない

カードの取り付け・取り外しの際にレールなどで指を挟んだり、切ったりしないよう十分注意してください。

Installation, Relocation, Storage, and Connection

CAUTION



Do not install this product in any other place than specified.

Do not install this product in the following places or any other places than specified in this User's Guide. Failure to follow this instruction may cause a failure.

- a dusty place
- a humid place such as near a boiler
- a place exposed to direct sunlight
- a place in magnetic field
- Do not use the equipment in the place where corrosive gases exist.

Make sure not to locate or use the server in the place where corrosive gases (sulfur dioxide, hydrogen sulfide, nitrogen dioxide, chlorine, ammonia, ozone, etc) exist.

Also, do not set it in the environment where the air (or dust) includes components accelerating corrosion (ex. sulfur, sodium chloride) or conductive metals. There is a risk of a fire due to corrosion and shorts of an internal printed board.



Do not connect any interface cable to the server with the system being powered or the AC cord being connected.

Make sure to power off the server and unplug the AC cord from an outlet before connecting/disconnecting the interface cable. If the server is off-powered but its AC cord is plugged to a power source, touching the cable may cause an electric shock or a fire resulted from a short circuit.



Do not use any unauthorized interface cable.

Use only interface cables specified by NEC and locate a proper device and connector before connecting a cable. Using an unauthorized cable or connecting a cable to an improper destination may cause a short circuit, resulting in a fire.

Also, observe the following notes on using and connecting an interface cable.

- Do not use any damaged cable connector. Before connecting an interface cable, confirm that any cable connector is not damaged and any connector pin is not bent or dirt.
- Do not step on the cable.
- Do not use this product with loose cable connections.
- Do not place any object on the cable.
- Do not disable the locking mechanism of the connectors.



Do not pinch your finger with rails or other components.

Note sufficiently that your fingers may not be caught between a rail and another mechanical part or cut when install/removal of the board.

お手入れに関する注意事項

警告



自分で分解・修理・改造はしない



絶対に分解したり、修理・改造をおこなったりしないでください。本体装置が誤動作したり感電や火災の危険があります。



電源プラグを抜かずに取り扱わない

お手入れの際は、本体装置の電源をOFFにして、ACコードをコンセントから抜いて行なってください。本体装置の電源がONになっていたり、ACコードを接続したままコネクタに触れると感電したりショートによる火災を起こすおそれがあります。また、本体装置のACコードはときどき抜いて、乾いた布でほこりやゴミをよくふき取ってください。ほこりがたまったままで水滴などが付くと、発熱し、火災の原因となるおそれがあります。

注意



中途半端に取り付けない

ACコードやインタフェースケーブルは確実に取り付けてください。中途半端に取り付けると接触不良を起こし、発煙や発火の原因となるおそれがあります。

Cleaning

WARNING



Do not disassemble, repair, or alter this product.

Do not attempt to disassemble, repair, or alter this product. Failure to follow this instruction may cause an electric shock or fire as well as malfunctions of the server.



Disconnect the AC cord before cleaning the server.

Make sure to power off the server and disconnect the AC cord from a power outlet before cleaning. Touching any connectors with the disk expansion unit's power being on or with the AC cord being connected to a power source may cause an electric shock or a fire due to short circuit.

Also, disconnect the AC cord from the outlet occasionally and clean the plug with a dry cloth. Heat will be generated if condensation is formed on a dusty plug, which may cause a fire.

CAUTION



Make sure to complete cable and AC cord installations.

Always install the AC cord and an interface cable firmly. An incomplete installation may cause a contact failure, resulting in smoking or fire.

本文中の記号について

本書の日本語で表記されている部分には、先に示した安全にかかわる注意事項記号の他に4種類の記号を使用しています。これらの記号と意味をご理解になり、本製品を正しくお取り扱いください。



本製品の取り扱いや、操作で守らなければならない事柄や特に注意すべき点を示します。



本製品やソフトウェアを操作する上で確認をしておく必要がある点を示します。



知っておくと役に立つ情報や、便利なことなどを示します。



発生したトラブルの事例を示します。

Text Conventions

The following conventions are used throughout this manual written in English. For safety symbols, see "SAFETY INDICATIONS" described earlier.



Items to be observed or points to be noted when using this product.



Items to be checked when using this product or software.



Information useful or convenient for you.



Example of troubles occurred.

取り扱い上のご注意 ～本製品を正しく動作させるために～

本製品を正しく動作させるために、次に示す注意事項をお守りください。これらの注意を無視した取り扱いをすると、誤動作や故障の原因となります。

- 本体装置やカード間のケーブルの接続／取り外しは、電源が OFF になっていることを確認し、AC コードをコンセントから外した後に行ってください。
- 定期的に本製品を清掃してください。定期的な清掃はさまざまな故障を未然に防ぐ効果があります。



保守サービスについて

本製品の保守に関して専門的な知識を持つ保守員による定期的な診断・保守サービスを用意しています。

本製品をいつまでもよい状態でお使いになるためにも、保守サービス会社と定期保守サービスを契約されることをお勧めします。

Note on Handling ~ For Proper Operation~

Observe the following notes for successful operation of this product. Use of this product ignoring the notes will cause malfunctions or failures of the Advanced Remote Management Card.

- Make sure to power off the server. And disconnect the AC cord from the power outlet before connecting or disconnecting cables.
- Clean this product on a regular basis. Regular cleaning proactively prevents various failures of this product.

はじめに

このたびは、本製品をお買い求めいただき、まことにありがとうございます。

本製品を本体装置内に接続することにより、本製品に搭載されたシステム管理用LSIであるBMC(Baseboard Management Controller)を用い本体装置内の電源、ファン、温度等本体装置の状態を監視や、管理用ネットワークによるリモートからのキーボード、ビデオ、マウス(KVM)制御など、遠隔地から本体装置の制御が可能となります。

本書は本製品を正しく使用できるようにするための手引きです。本書に記載されている内容を良く理解された上で本装置を正しく、確実に操作してください。

PREFACE

Welcome to our N8115-02 Advanced Remote Management Card.

Connecting your server and client PC with this product enabled your system to monitor the status of power supply unit, fan and temperature of servers by BMC(Baseboard Management Controller) and a remote KVM (Keyboard, Video, Mouse)console feature by communicating through a management LAN PORT feature.

This manual is a guidance to use this product properly. Read well the manual to operate the product properly and surely.

付属品の確認

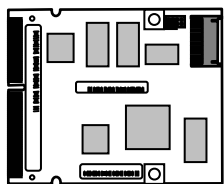
本製品の梱包箱の中には、以下の付属品が入っています。付属品がすべてそろっていることを確認し、それぞれ点検してください。万一足りないものや損傷しているものがある場合は、販売店に連絡してください。



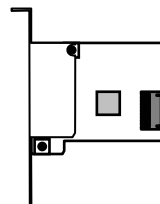
付属品について

添付品はセットアップをするときに必要となりますので大切に保管してください。

□ マネージメント カード本体×1



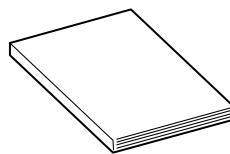
□ 管理用ネットワークカード×1



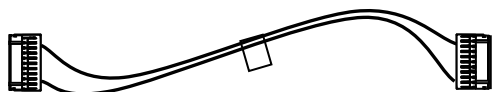
□ 緩衝材×2



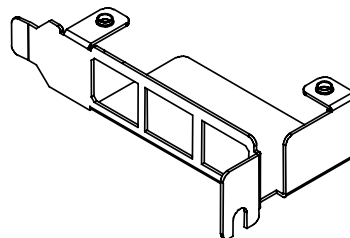
□ ユーザーズガイド（本書）×1



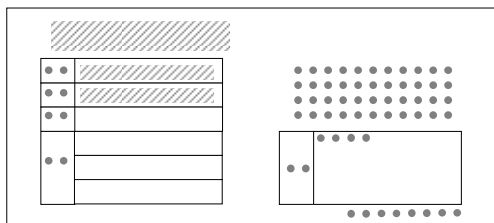
□ 内部接続ケーブル×1



□ PCI ロープファイル用リアパネル×1



□ 保証書 ×1



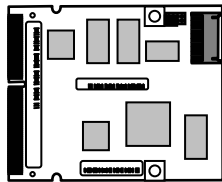
CHECK OF ACCESSORIES

The carton of this product contains several accessories. Make sure that all items listed below are provided and then inspect them. If one or more items are missing or defective, contact your sales representative.

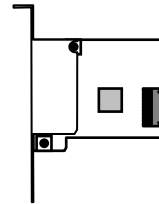


The accessories are required for the setup. Store them carefully.

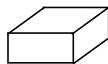
Management Main Card×1



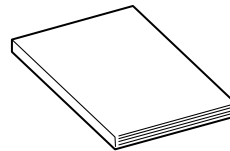
Management LAN Card×1



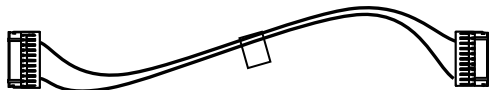
Spacer x2



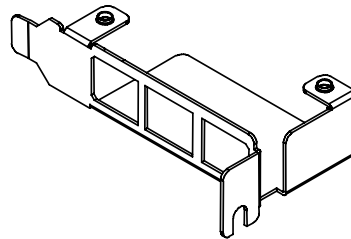
User's Guide (this document) ×1



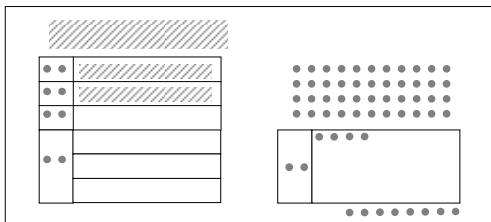
Internal Cable ×1



PCI Low Profile Rear Panel ×1



Warranty ×1



This accessory is available only for using in Japan.

Do not use it in any other country than Japan.

第三者への譲渡について

本製品を第三者に譲渡（または売却）するときは、本書を一緒にお渡してください。

TRANSFER TO THIRD PARTY

To transfer or sell this product to a third party, make sure to provide this User's Guide together with the product to a third party.

製品の廃棄について

本製品の廃棄については、各自治体の廃棄ルールに従ってください。詳しくは、各自治体へお問い合わせください。

DISPOSAL

Dispose this product according to all laws and regulations of the local government.

本書を紛失してしまったら

もし本書を紛失された場合は、弊社ホームページ (<http://www.express.nec.co.jp/care/option/rmc.html>)より本書のデータファイル(pdf形式)をダウンロードすることができます。

1. 各部の名称と機能

本章では本製品の各部の名称とその機能について説明します。

本製品は、2枚組みのカードで構成されサーバ監視機能やリモートKVMコンソール機能を実現します。

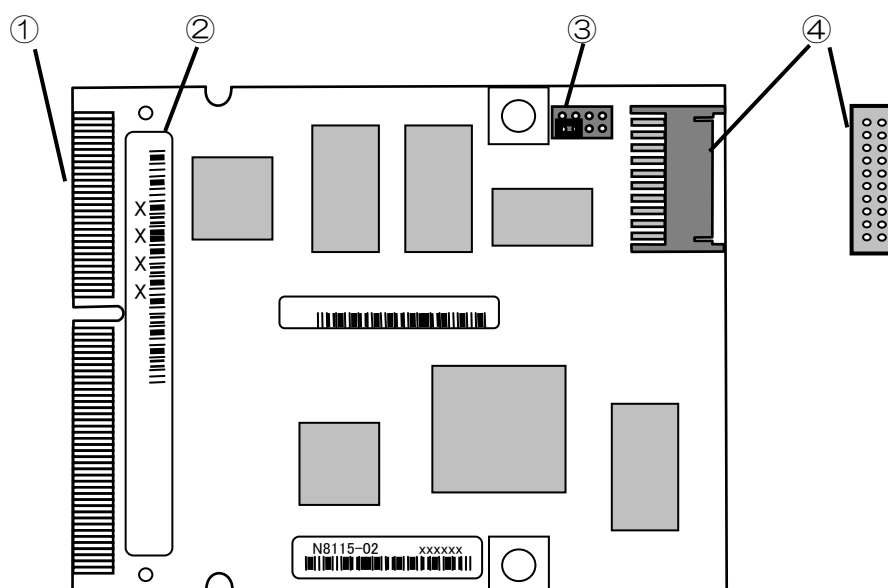


チェック

リモートKVMコンソールで表示できる画面は、解像度1024x768、リフレッシュレート75Hz以下になります。これ以上の設定を行った場合、リモート側で画面が表示されませんので、注意してください。
また本体装置側の画面色数を多く設定すると、リモート側で正確な色が表示できない場合があります。

ブロードキャストが頻発するネットワークに本製品を接続した場合、リモート制御に関する性能に影響が出る場合があります。

マネージメント カード本体



① 本体装置との接続部

本カードを本体装置内部の専用コネクタと接続するカードエッジ部です。
実装するコネクタ位置及び内部ケーブルのルートは、本体装置により異なりますので、実装される本体装置のユーザズガイドを参照してください。

② MAC(Media Access Control)アドレス ラベル

本カードで使用するネットワーク固有の MAC アドレスを示します。
DHCP サーバ機能を使用する場合、ホスト名の一部として使用されますので書き留めて置いてください。

③ 設定クリア用ジャンパ

WEB ブラウザから利用するリモートマネージメント機能のログイン パスワード設定を忘れてしまったときにジャンパ実装位置を変更することにより、パスワードを含む各設定を工場出荷時の状態に戻すことができます。詳細は60ページを参照してください。

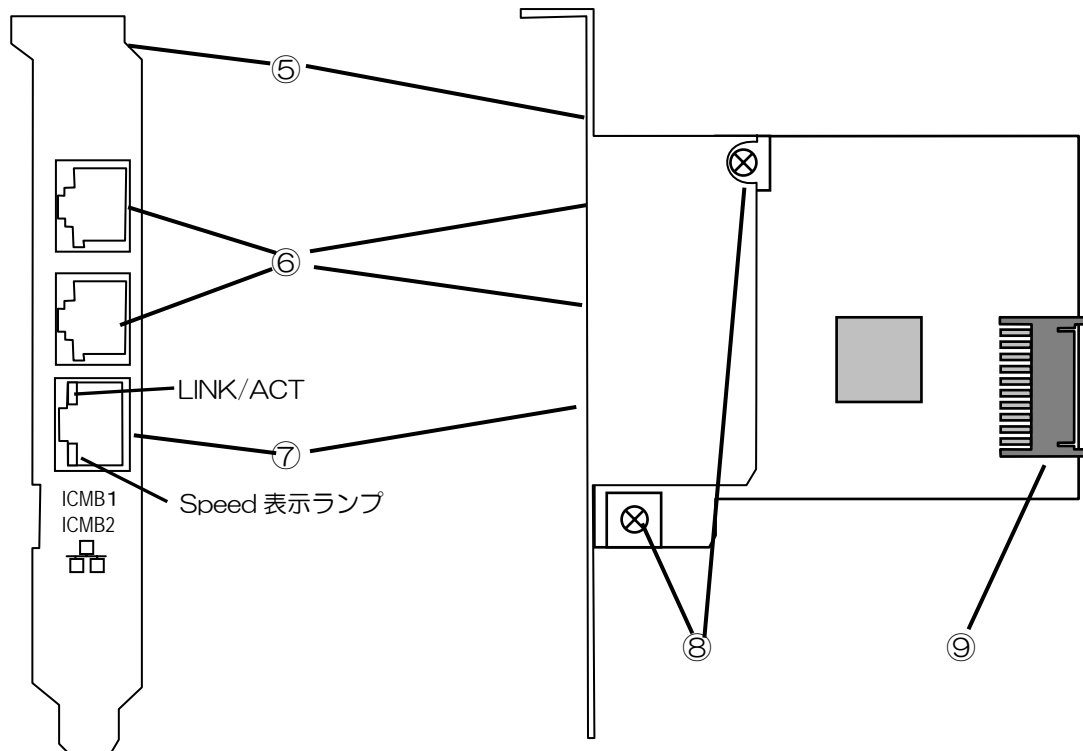


指定箇所以外の場所に実装しないでください、この場合、装置および部品の破損または運用した結果の影響についてはその責任を負いかねます。指定以外の場所における変更の結果起きた装置の誤動作または故障・破損についての修理は有料となります。

④ カード間 接続コネクタ

本製品(2枚組)のカード間を接続するためのコネクタです。添付の内部接続ケーブルにてお互いを接続してください。

管理用ネットワークカード



⑤ PCI スロット取り付けリアパネル

出荷時には、PCI スロット固定用にフルハイトのリアパネルが付いております。
ロープロファイルの slots に固定したい場合には、添付のロープロファイル用 PCI リア
パネルと付け替えてください。
PCI バスを、使用しませんので PCI バスの種類による制約はありません。空いている PCI
スロットに実装してください。

⑥ ICMB 1 コネクタ(上)、ICMB 2 コネクタ(下)

ICMB(Intelligent Chassis Management Bus) インターフェースを持つサーバや周辺機
器と接続します。

⑦ 管理 LAN 用 ポート

ネットワークシステムと接続し、100Mbps/10Mbps に対応。電話回線に直接接続する
ことは出来ません。本体装置に添付されている管理ソフト DianaScope を使った管理を行
う場合にも、このポートが使用されます。

・ LINK/ACT ランプ

ネットワークポートの状態を示します。本製品とハブなどの接続機器に電力が供給されて
いて、かつ正常に接続されている間、緑色に点灯します (LINK)。ネットワークポートが
正常に送受信を行っているときに、緑色に点滅します (ACT)。

・ Speed 表示ランプ

ネットワークポートの通信モードがどのネットワークインタフェースで動作しているかを
示します。アンバー色に点灯しているときは、100Mbps で動作していることを
示します。消灯しているときは、10Mbps で動作していることを示します。

⑧ リアパネル固定ネジ

リアパネルを固定するネジです。ロープロファイル用リアパネルへ交換時には、このネジ 2本によりリアパネルの交換が出来ます。

⑨ カード間 接続コネクタ

本製品(2枚組)のカード間を接続するためのコネクタです。添付の内部接続ケーブルにて、お互いを接続してください。

ネットワーク デフォルト設定値

本装置をネットワークに接続する場合のデフォルト設定値を以下に記載します。

| | |
|---------|-------------------|
| IP アドレス | :192.168.1.1 |
| ユーザ名 | :administrator |
| パスワード | :(なし) |
| ホスト名 | :ARMCXXXXXXXXXXXX |

★DHCP 機能を使用し、DNS サーバに自動登録を行う場合のホスト名が上記ホスト名になります。

XXXXXXXXXXXXには、各々のマネジメントカード本体上に貼られたシールに、書かれているMACアドレスが入ります。

MACアドレスシールは、2ページのマネジメントカード説明における項番②のシールに書かれています。

★DHCP サーバを使用せず接続いただく場合は、上記デフォルトのIPアドレス“192.168.1.1”が使用可能なローカルなネットワーク内で、このアドレスにアクセスしてください。デフォルトで設定されているIP“192.168.1.1”が使用出来ない環境では、サーバ本体からEXPRESSBUILDER CD-ROMを起動し、「ツール」→「システムマネジメント機能」→「システムマネジメントの設定」→「コンフィグレーション」画面から新規を選択し、→「BMC 登録情報の編集」より管理用LANのIPアドレスを設定/登録願います。



重要

セキュリティ上の理由から、お客様のネットワーク環境に合わせたホスト名・パスワード・IPアドレスに設定し直してください。

設定方法に関しましては、5章を参照願います。

2. 取り付け/取り外し

本製品の本体装置への取り付け方法および注意事項について説明します。

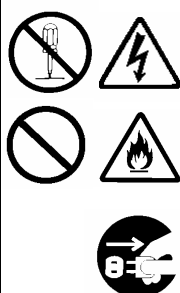


重要

- 本製品の取り付け/取り外しはお客様個人でも行えますが、この場合、装置および部品の破損または運用した結果の影響についてはその責任を負いかねますのでご了承ください。本装置について詳しく、専門的な知識を持った保守サービス会社の保守員に取り付け/取り外しを行わせるようお勧めします。
- 本製品に接続するケーブルはNECの純正品を使用してください。指定以外の部品を取り付けた結果起きた装置の誤動作または故障・破損についての修理は有料となります。

安全にオプションの取り付け・取り外しをするために次の注意事項を必ず守ってください。

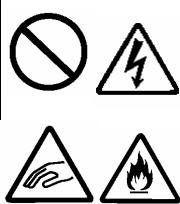
警告



装置を安全にお使いいただくために次の注意事項を必ずお守りください。人が死亡する、または重傷を負うおそれがあります。詳しくはvページ以降の説明をご覧ください。

- 自分で分解・修理・改造はしない。
- プラグを抜かずに取り扱わない。

注意



装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがを負うおそれや物理的損害を負うおそれがあります。詳しくはvページ以降の説明をご覧ください。

- 本体装置を一人で持ち上げない。
- 中途半端に取り付けない。
- 指をはさまない。
- 高温注意。

静電気対策について

本製品や、本体装置内部の部品は静電気に弱い電子部品で構成されています。本製品の取り付け・取り外しの際は静電気による製品の故障に十分注意してください。

- リストストラップ（アームバンドや静電気防止手袋など）の着用
リスト接地ストラップを手首に巻き付けてください。手に入らない場合は部品を触る前に本体装置の塗装されていない金属表面に触れて身体に蓄積された静電気を放電します。また、作業中は定期的に金属表面に触れて静電気を放電するようにしてください。
- 作業場所の確認
 - ー静電気防止処理が施された床、またはコンクリートの上で作業を行います。
 - ーカーペットなど静電気の発生しやすい場所で作業を行う場合は、静電気防止処理を行った上で作業を行ってください。
- 作業台の使用
静電気防止マットの上に本装置を置き、その上で作業を行ってください。
- 着衣
 - ーウールや化学繊維でできた服を身につけて作業を行わないでください。
 - ー静電気防止靴を履いて作業を行ってください。
 - ー取り付け前に貴金属（指輪や腕輪、時計など）を外してください。
- 部品の取り扱い
 - ー取り付ける部品は本装置に組み込むまで静電気防止用の袋に入れておいてください。
 - ー各部品の縁の部分を持ち、端子や実装部品に触れないでください。
 - ー部品を保管・運搬する場合は、静電気防止用の袋などに入れてください。

取り付け / 取り外しの準備

部品の取り付け／取り外しの作業をする前に準備をします。

1. 本体装置のOSのシャットダウン処理を行う。
2. 本体装置の電源をオフにする。
本体装置の電源のオフ手順は、本体装置のユーザズガイドを参照してください。
3. 本体装置からACコードを抜きます。
4. プラスドライバを用意する。



チェック

DHCP 機能を使用し、DNS サーバに自動登録を行う場合、ホスト名に「ARMC の文字に続けてMACアドレス」を使用しますので、マネージメントカード本体に、貼ってあるMACアドレスの番号(2ページ②を参照)を書き写しておくことをお勧めします。

本製品の取り付け/取り外し

本製品の取り付け/取り外しの作業は本体装置の電源を落した後、ACコードを抜き、筐体が安定している状態にて行ってください。

ラックからの引き出し作業は必ず複数の人数で行ってください。

手順は本体装置のユーザーズガイドに詳細に記載していますので参照してください。

注意



装置を安全にお使いいただくために次の注意事項を必ずお守りください。火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、v ページ以降の説明をご覧ください。

- 一人で搬送・設置をしない
- 指を挟まない
- 高温注意
- ラックが不安定な状態でデバイスをラックから引き出した状態にしない
- 複数台のデバイスをラックから引き出した状態にしない

本製品を本体装置内にある専用コネクタ及び PCI スロットに取り付けます。



重要

オプションカードは大変静電気に弱い電子部品です。サーバの金属フレーム部分などに触れて身体の静電気を逃がしてからオプションカードを取り扱ってください。取り付け、取りはずしは、必ずAC コードを抜いて5秒以上待ってから行ってください。

また、オプションカードの端子部分や部品を素手で触ったり、カードを直接机の上に置いたりしないでください。静電気に関する説明は7ページで詳しく説明しています。

取り付け

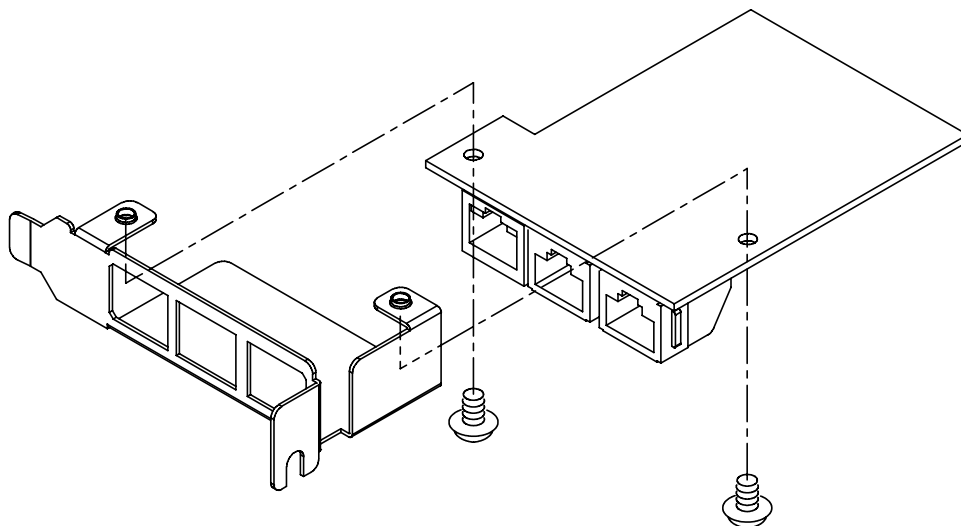
次の手順に従って本製品の取り付けを行います。



重要

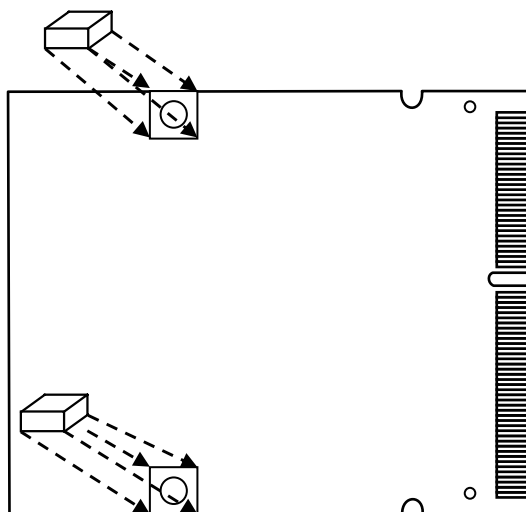
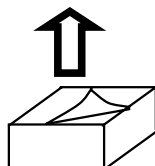
カードを取り付けるときは、本体装置がN8115-02アドバンスドリモートマネージメントカードをサポートしているかを確認し、カードの接続部分の形状とコネクタ形状が合っていることを確認してください。

1. 前記の取り付け/取り外しの準備を行ってください。
2. 実装する本体装置のユーザーズガイドを参照し、筐体カバーを外し、コネクタ位置の確認とPCIスロットからのケーブルルートの確認を行ってください。
3. 管理用ネットワークカードを固定するPCIスロットを決定し、ロープロファイルのPCI スロットに固定するときには、リアパネルの変更を行います。工場出荷時は、フルハイトのPCIスロットに対応したリアパネルになっています。2個のねじで取り付けられているので、下記の手順により添付のロープロファイル対応リアパネルに変更してください。取り外したリアパネルは、大切に保管してください。



4. マネージメントカード本体への緩衝材の貼り付け。
マネージメントカード本体と本体装置のマザーボードとの接触を避けるために緩衝材を貼り付けます。
実装する本体装置のユーザーズガイドを参照し、指定された位置に貼り付けてください。
特に本体装置側に指定がない場合にはマネージメントカード本体以下の裏面2箇所
所に貼り付けてください。

粘着面の保護シートをはがします。



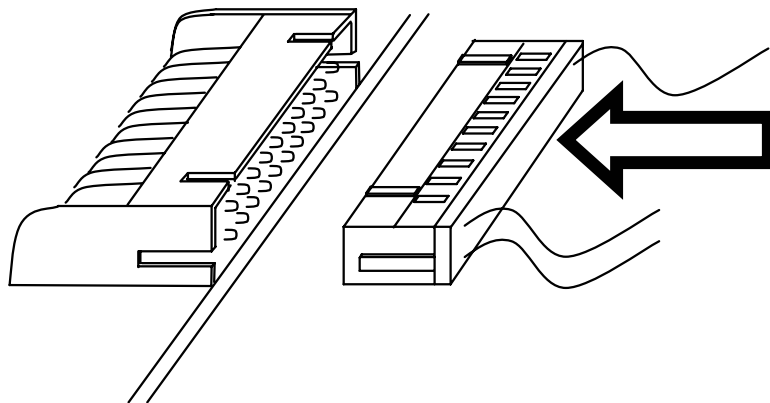
重要

緩衝材を、貼り付けないと、振動によりマザーボードと本装置で接触が発生し、本体装置及び本装置の故障・破損が発生する可能性があります。必ず緩衝材を貼り付けてください。

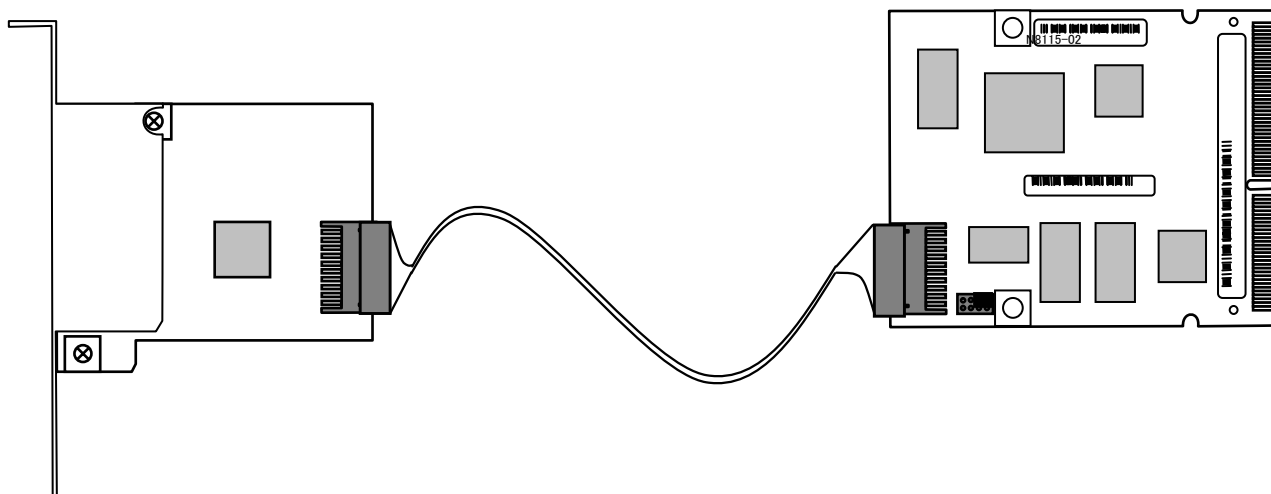
5. 内部ケーブル接続

添付の内部接続ケーブルでマネージメントカード本体と管理用ネットワークカードを接続します。

内部接続ケーブルと、コネクタの組み合わせはどちらに接続しても構いません。ただし、コネクタ上下の組み合わせはありますので注意願います。

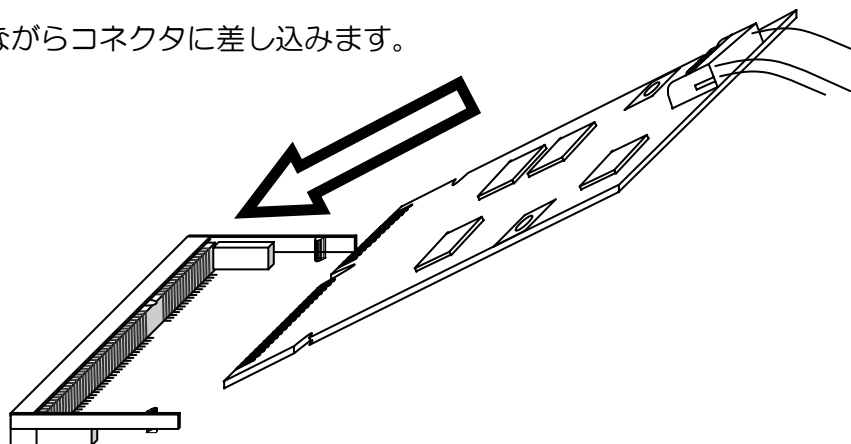


カード間の内部ケーブル接続

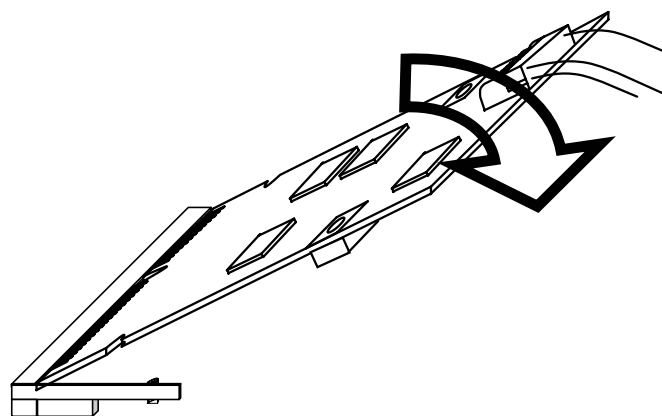


6. 本体装置に専用コネクタにマネージメントカード本体を取り付ける。

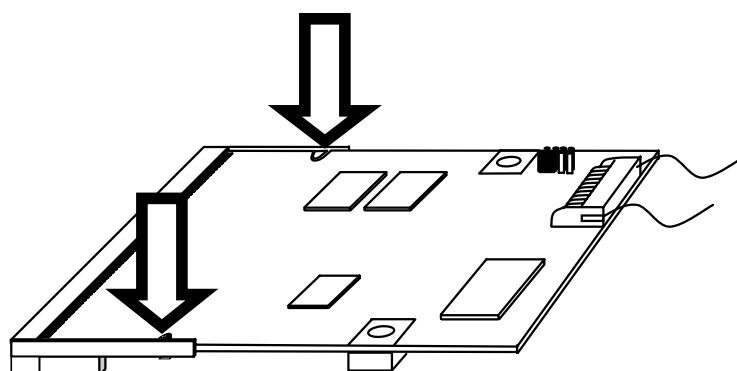
本カードを斜めにしながらコネクタに差し込みます。



コネクタに押し当てカードをマザーボード側に倒します。

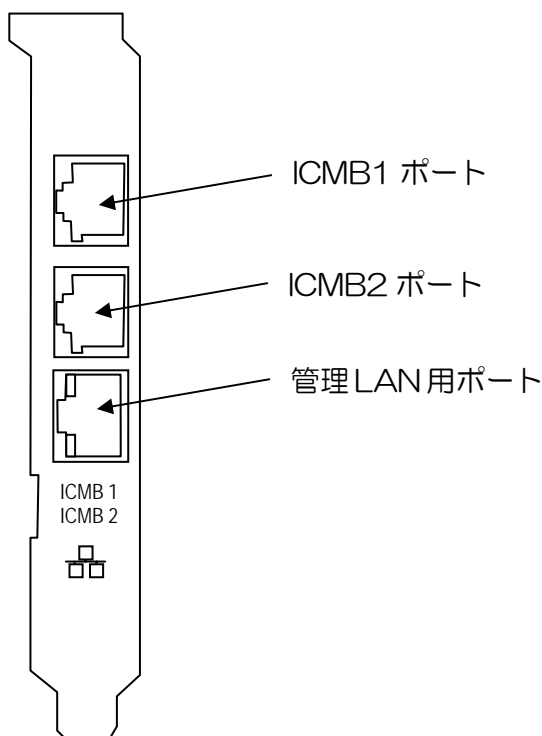


コネクタの左右にあるツメで固定されたことを確認してください。



7. 管理用ネットワークカードの固定。
本体装置内での内部ケーブルのルートを確認し、PCIスロットのブランクカバーを外します。外したスロットに管理用ネットワークカードを固定する。
8. 管理用ネットワークカードに外部接続のLAN/ICMBケーブルを接続する。

ICMB対応機器に接続しない場合は、ICMBケーブルの接続する必要はありません。管理用LANポートには、本製品のリモートマネージメント機能を使用するためネットワークに接続してください。本体装置に添付されている管理ユーティリティDianaScopeを使った管理を行う場合にも、このポートが使用されます。



重要

うまくカードを取り付けられないときは、カードをいったん取り外してから取り付け直してください。カードに過度の力を加えるとカードを破損するおそれがありますので注意してください。

取り外し

カードの取り外しは、取り付けと逆の手順を行い取り外してください。

3. 本体装置側の設定

本章では本製品を本体装置で使用するにあたり、搭載する本体装置側で実施しなければならない内容について説明します。

本製品の初期設定

(1) 装置毎の詳細な監視を実現するために、本体装置毎に異なる固有情報を本製品に書き込む必要があります。

本装置に本体装置の固有情報が書き込まれていない場合には、本体装置の立ち上げ時NECのロゴ表示中あるいは、本体装置の固有情報が書き込まれていない旨を伝える以下のメッセージを表示し一時停止します。

H/W Configuration of BMC is corrupted.

!! Update BMC H/W Configuration by configuration tool !!

!! Refer to BMC configuration manual !!

POST 中、NECのロゴを表示して停止している場合には、別画面で上記メッセージが表示されていることがありますので、ESCキーを押し診断画面を表示し上記メッセージが表示されていないか確認してください。別のエラーメッセージが表示されている場合には、本体装置のユーザーズガイドを参照してください。

(2) 初期設定方法

上記メッセージ後しばらく待つか、Enterキーを押すとPOSTが進みますので、本体装置添付のCD-ROM EXPRESSBUILDERを起動し、「ツールメニュー」から「リモートマネジメントカードの初期設定」を選択すると自動的に、各本体装置固有情報の設定が書き込まれます。

書き込みが終了すると下記メッセージが表示されます。いずれかのキーを入力すると本体装置が再起動し使用することが出来ます。

Programing complete , reboot server for normal operation.

Strike a key when ready...

ビデオドライバの組み込み

- 本体装置のOSがWindowsの場合

本体装置によっては、本体装置添付のEXPRESSBUILDERから専用のビデオドライバのインストールをおこなう必要があります。本体装置のユーザーズガイドを参照し必要な場合には、本体装置添付EXPRESSBUILDERから専用のビデオドライバをインストールしてください。適用しないと管理PCへの画像が転送されない場合があります。

適用に関する詳細な情報は、本体装置のユーザーズガイドを参照してください。

- 本体装置の OS が Linux の場合



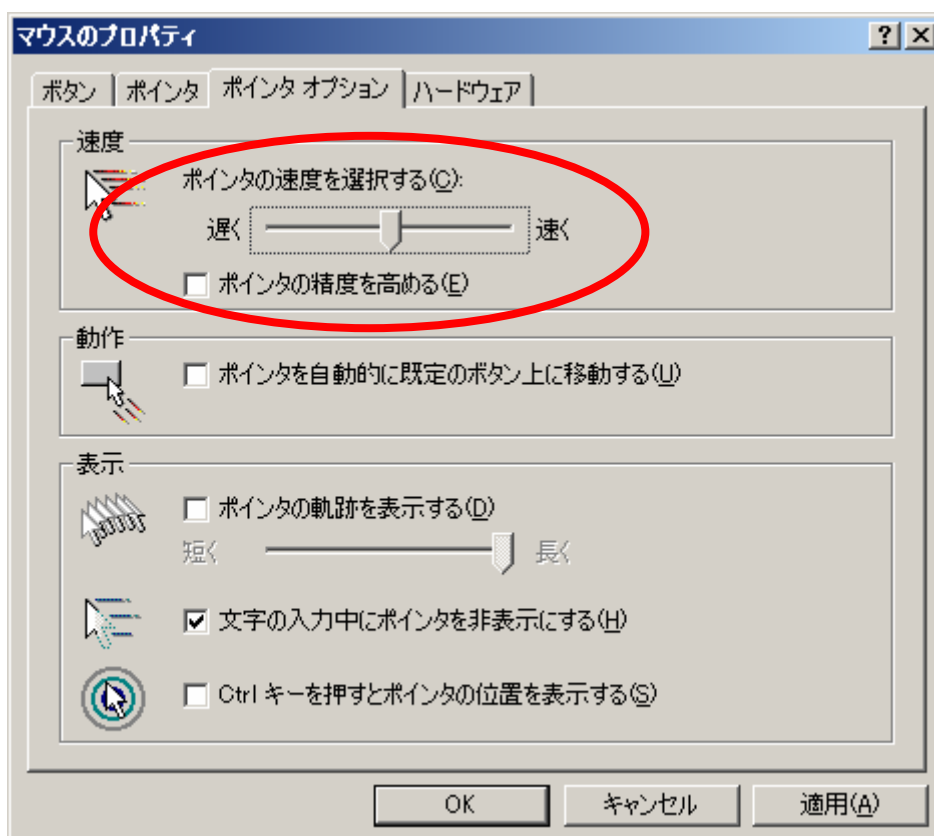
Linux の場合、構成により自動でモニタ/Driver/ビデオメモリの設定が反映されない場合がありますので、テキストモードでの運用をお勧めします。

Linuxの対応については、『8番街』: <http://nec8.com/> の“Linux on Express5800”から最新/詳細情報を入手してください。

マウスのプロパティの変更

本体装置の OS が Windows Server 2003 の場合、下記に示す「マウスのプロパティ」の「ポインタオプション」にあります「速度」の設定で、「ポインタの精度を高める」のチェックボックスを外してください。

また、リモート KVM コンソールにて、マウスカーソルが画面右下まで動かせないときは、ここの「ポインタの速度を選択する」を調節してください。



4. 管理 PC 側の設定

本章では本製品が搭載された本体装置との接続を行うにあたり、クライアントPC側で考慮しなければならない内容について説明します。

ブラウザの設定

以下の設定を行ってください。

- SSL を有効にしてください。

動作対応ブラウザ

以下のブラウザについて、動作を確認しております。

- Microsoft Internet Explorer 6.0
- Netscape 7.0
- Mozilla 1.6

Java2 Runtime Environment

Java2 Runtime Environment, Standard Edition 1.4.2_04 以降が必要です。

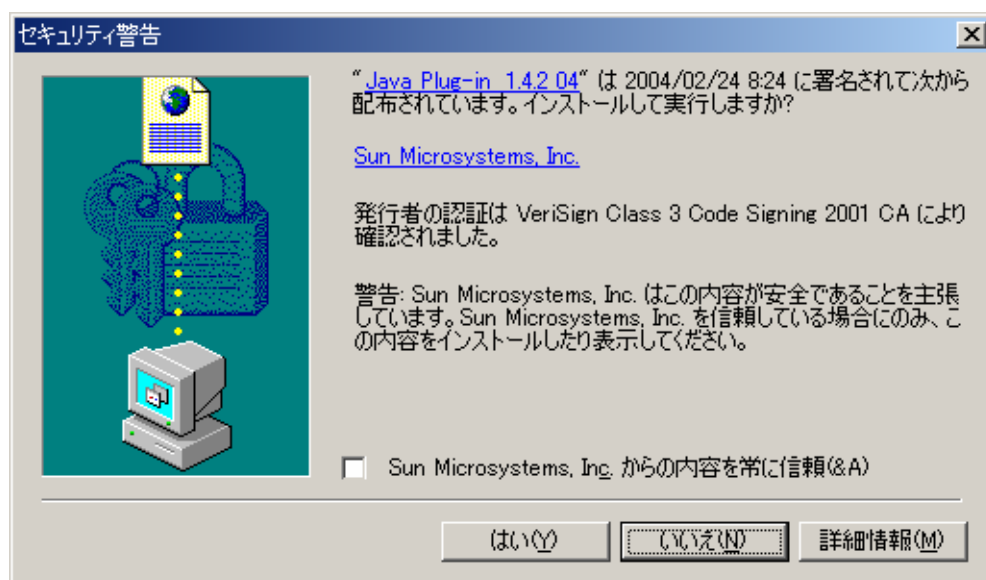
EXPRESSBUILDER を使ってインストールする場合には以下の手順で行ってください。

- (1) インストールしたい管理PC上で、Windows を立ち上げCR-ROM EXPRESSBUILDER をセットします。
- (2) 自動起動機能により EXPRESSBUILDER のマスターコントロールメニューが表示されます。

「ソフトウェアのセットアップ」-「DianaScope」の順にクリックすると DianaScope のインストールメニューの中に、JRE のインストールのインストーラを用意しておりますので、実行してください。

※最新の Java Runtime をインストールするときは、以下の場所よりダウンロードしてください。
<http://java.sun.com/j2se/>

インストールせずにログインページにアクセスすると、以下のようなメッセージが表示される場合があります。内容を確認して、実行してください。



5. リモートマネージメントの使い方

概要

BMC の WEB サーバ機能を使用し、WEB ブラウザからサーバ本体装置の電源制御やリモート KVM コンソールがご利用いただけます。

本機能は Java Applet で実現しております。

接続方法

管理 PC 上の WEB ブラウザから下記の URL にアクセスしてください。

URL: http://BMC_HostPort/index.htm



“BMC_HostPort”は、BMC の IP アドレスもしくはホスト名の後に、コロンと http のポート番号を加えたものです。

http のポート番号が 80(デフォルト)の場合は、ポート番号は省略可能です。



DHCP 機能を使用し、かつ、DNS サーバに自動登録を行う場合、BMC のデフォルトのホスト名は、ARMC の文字に MAC アドレスを追加した名前になります(MAC アドレスは 2 ページを参照)。

| | |
|---------|-------------------|
| IP アドレス | : 192.168.1.1 |
| ユーザ名 | : administrator |
| パスワード | : (なし) |
| ホスト名 | : ARMC00004C9FXXX |

デフォルトのホスト名



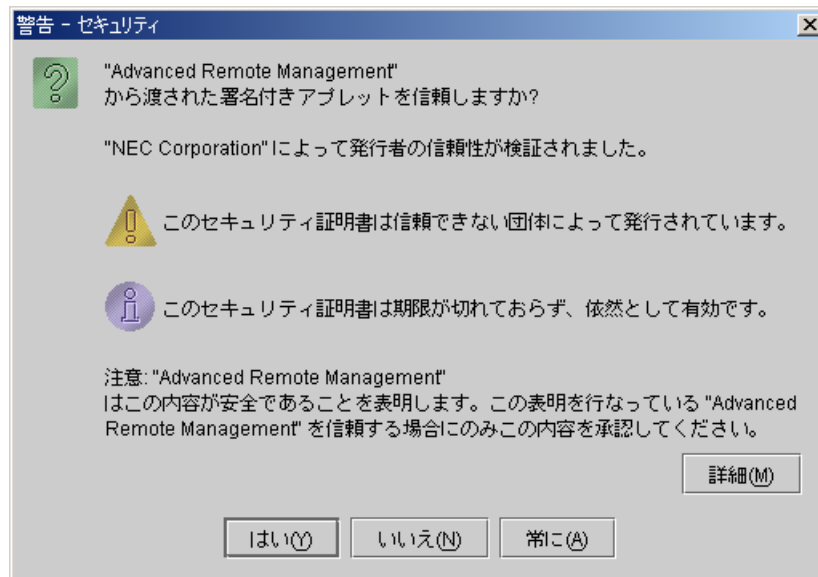
- DHCP を無効化してご利用いただく場合は、初めに、デフォルトの IP アドレス “192.168.1.1” が使用可能なローカルなネットワーク内で、このデフォルトの IP アドレスでアクセスしてください。

次に、後述する「BMC に対する各種設定」を参照して、IP アドレスなどをお客さまのネットワーク環境に合わせて設定してください。

IP アドレスなどの設定が済みましたら、ご使用になれるネットワークに接続して、設定なされた IP アドレスもしくはホスト名でアクセスしてください。

- デフォルト設定されている IP “192.168.1.1” が使用出来ないネットワーク環境の場合には、サーバ本体から EXPRESSBUILDER CD-ROM を起動し、「ツール」→「システムマネージメント機能」→「システムマネージメントの設定」→「コンフィグレーション」画面から新規または編集を選択し、→「BMC 登録情報の編集」より LAN1 の IP アドレスを設定/登録願います。

初めてご利用いただく際に、以下のような「セキュリティの警告」ダイアログボックスが表示される場合がございます。メッセージを良くお確かめの上、「はい」、もしくは「常に」をクリックしてください。ログインページが表示されます。内容に不審な点が見られる場合は、「いいえ」をクリックしてください。



SSL で接続を行った場合は、上記以外に、SSL のためのサーバ証明書に関する「セキュリティの警告」ダイアログボックスがいくつか表示される場合があります。

ログイン・ログアウト

ログイン

ログインページが表示されましたら、ユーザ名／パスワードを入力し、「ログイン」をクリックしてください。

初めてログインする場合は、下記のデフォルトのユーザ名／パスワードを入力してログインしてください。

デフォルトのユーザ名 : administrator

デフォルトパスワード : なし (何も入力しない)



デフォルトではパスワードが設定されておきませんので、ログイン後、速やかにパスワードを設定くださいますよう、お願い致します。

セキュリティ上、デフォルトのユーザ名も合わせて変更することを推奨いたします。

設定・変更の方法に関しましては、後述する「BMC に対する各種設定」をご参照ください。


パスワード認証を通ると、下記のようなライセンスアグリーメントが表示されます。



内容を良く確認してください。

内容に同意できる場合は、「同意します」をクリックしてください。本機能がご利用頂けます。

内容に同意できない場合は、「同意しません」をクリックしてください。ログイン画面に戻ります。本機能をご利用になることはできません。

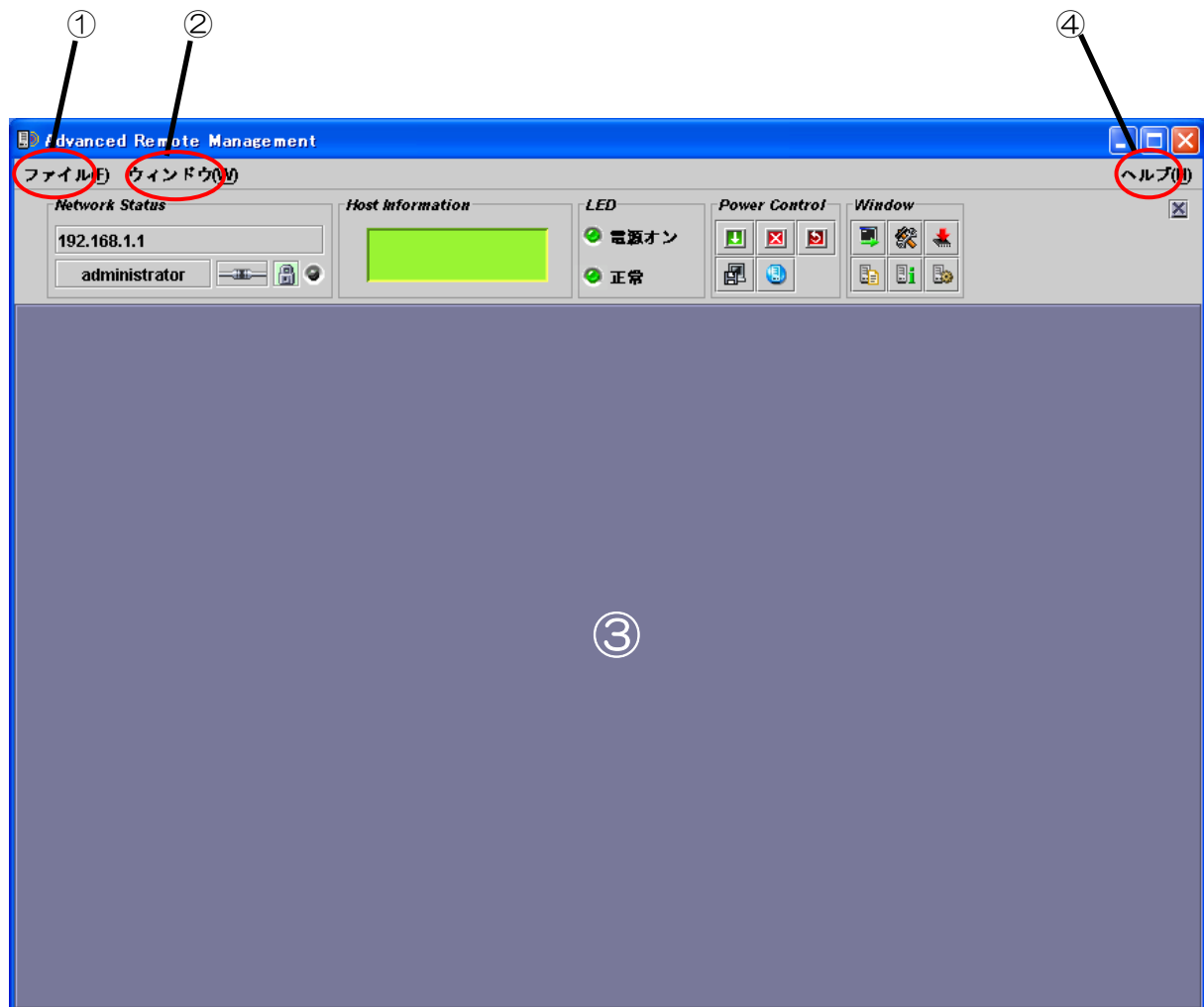
 「同意します」をクリックすると、管理 PC 上に情報が保存されますので、次回以降、このメッセージは表示されなくなります。

ログアウト

左上のファイルメニューをクリックし、「終了」を選択することでログアウトできます。

ログアウトすると、メインウィンドウをクローズし、ブラウザ上のログインページに戻ります。

メインウィンドウ



- ① クリックするとファイルメニューが表示されます。

「終了」を選択すると、本アプレットを終了させることができます。

- ② クリックするとウィンドウメニューが表示されます。

ウィンドウメニューからリモート KVM コンソールウィンドウなど、各種ウィンドウを開くことができます。

- ③ メインフレームです。

ここに、各種ウィンドウを表示します。

- ④ クリックするとヘルプメニューが表示されます。

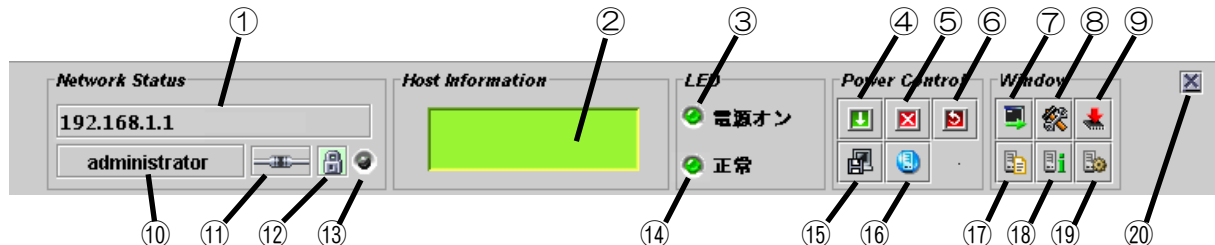
「バージョン情報」をクリックすると、本アプレットのバージョン情報を確認することができます。

コントロールパネル

本体装置の状態表示や電源制御を行うことができます。

また、リモート KVM コンソールなど、各種ウィンドウを起動します。

各部の機能



- ① BMC のホスト名あるいは IP アドレスが表示されます。
- ② 本体装置の LCD が表示されます。
- ③ 本体装置のパワーランプです。本体装置の電源状態を示します。
- ④ 本体装置の POWER スイッチです。(本体装置の POWER スイッチを押すのと同様です)
- ⑤ 本体装置を強制電源オフします。
- ⑥ 本体装置を強制リセットします。
- ⑦ リモート KVM コンソールを起動します。
- ⑧ BMC コンフィグレーションを起動します。
- ⑨ ファームウェアアップデートを起動します。
- ⑩ ユーザ名が表示されます。
- ⑪ BMC との接続状態が表示されます。
- ⑫ 通信のセキュリティ状態が表示されます。
- ⑬ ネットワークアクセスの状態を示します。
- ⑭ 本体装置のステータスランプです。本体装置の状態を示します。
- ⑮ 本体装置でメモリダンプします。(本体装置の DUMP スイッチを押すのと同様です)
- ⑯ 本体装置のユニット ID ランプを点滅させます。
- ⑰ システムイベントログ(SEL)を表示するウィンドウを開きます。
- ⑱ センサ装置情報(SDR)を表示するウィンドウを開きます。
- ⑲ 保守交換部品情報(FRU)を表示するウィンドウを開きます。
- ⑳ コントロールパネルを隠します。

リモート KVM コンソール

BMC のリモート KVM コンソール機能により、本体装置のローカルコンソールを、ネットワークを介して管理 PC のブラウザに転送することができます。

管理 PC から本体装置に対して、ビデオ、キーボード、およびマウスを使用して完全にアクセスできるようになります。



チェック

リモート KVM コンソールは、以下の 5 種類の解像度をサポートしています。

1024 × 768

800 × 600

640 × 480

720 × 400

720 × 350

本体装置の解像度は、これらのいずれかに設定してください。

サポート外の解像度の場合、リモート KVM コンソールには表示されません。



ヒント

KVM とは、キーボード(Keyboard)、ビデオ(Video)、マウス(Mouse)の頭文字を採ったものです。

リモート KVM コンソールは、従来のシリアルコンソールをリモートで使用するものとは違い、グラフィックスをそのままリモートで使用できるものです。




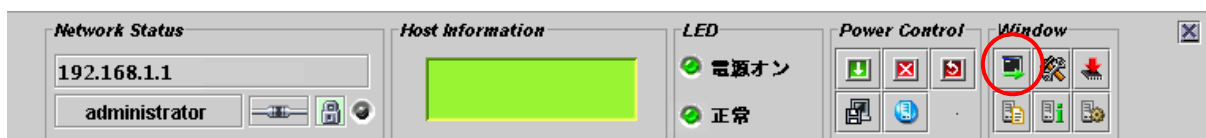
チェック

リモート KVM コンソールは、プロキシを経由した接続ではご利用になれません。

リモート KVM コンソールを使用する場合は、プロキシを使用しない設定でログインしてください。

リモート KVM コンソールウィンドウの起動

コントロールパネル上のリモート KVM コンソールの起動アイコン[]をクリックすると、リモート KVM コンソールウィンドウが表示されます。

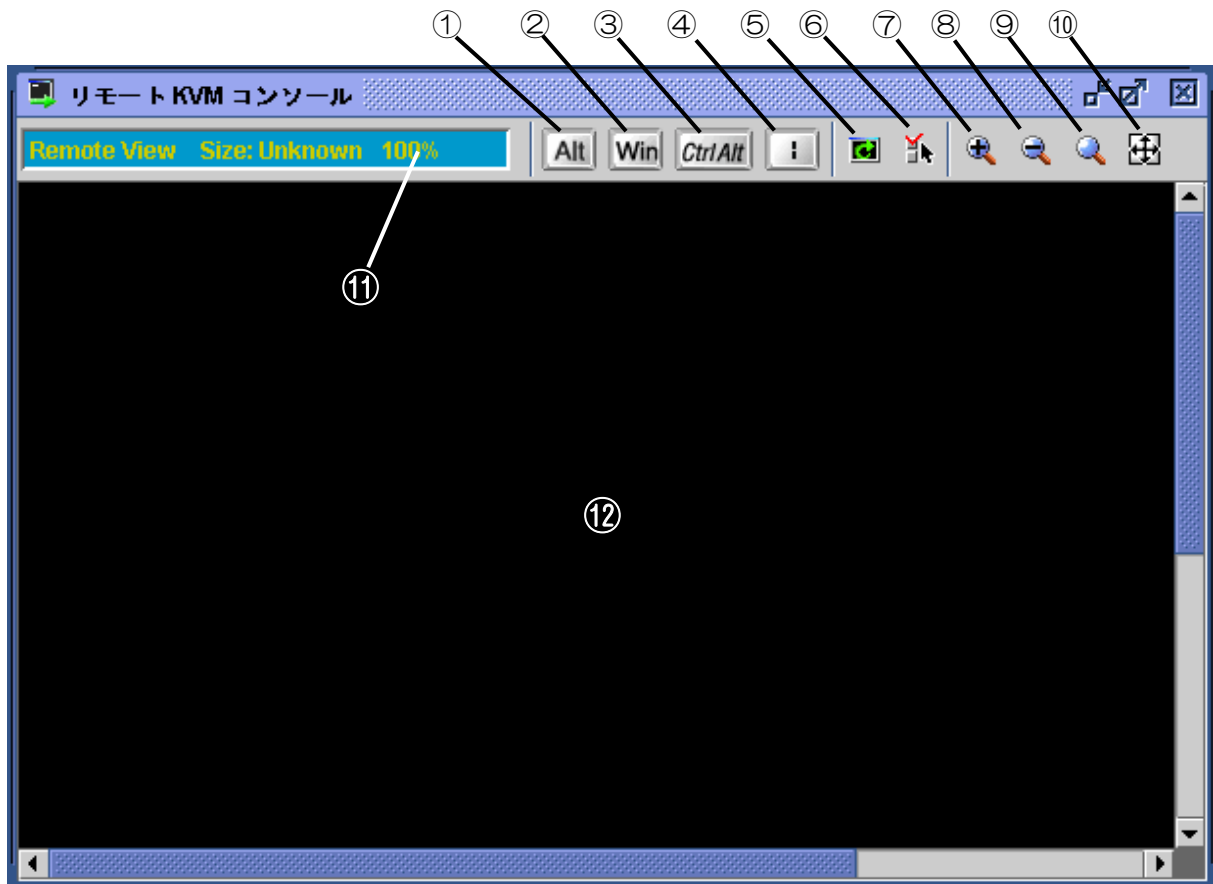


重要

本体装置のローカルコンソールから、自本体装置内の BMC に対してログインした場合、リモート KVM コンソールは絶対に開かないでください。

キーボードやマウスの入力が不可能な状態になってしまいます。

リモート KVM コンソールウィンドウの各部の名称



- ①、②、③、④ 特殊キーアイコンです。特殊キーを入力するときに使用します。
- ⑤画面リフレッシュアイコンです。画面をリフレッシュするときに使用します。
- ⑥KVM プロパティアイコンです。
- ⑦拡大アイコンです。表示を拡大したいときに使用します。
- ⑧縮小アイコンです。表示を縮小したいときに使用します。
- ⑨等倍アイコンです。表示を等倍に戻したいときに使用します。
- ⑩ウィンドウリサイズアイコンです。ウィンドウサイズを画面サイズに合わせます。
- ⑪KVM インジケータです。解像度などの情報が表示されます。
- ⑫リモート KVM コンソール画面です。本体装置の画面が表示されます。



重要



リモート KVM コンソールウィンドウの画面では **Shift+CapsLock** や **NumLock** を押下した場合、管理 PC 側の **CapsLock, NumLock** の LED の状態と実際の動作が一致しなくなることがあります。


また、サーバ側もリモート KVM コンソールウィンドウ使用後に **CapsLock, NumLock** の状態が LED と一致しなくなることがあります。

その場合には、対象装置からキーを押し直し LED の状態と実際の動作を合わせてください。

特殊キーの入力

特殊キーについては、管理 PC のキーボードから入力しても、本体装置には届きません。以下の4種類の特特殊キーアイコンをクリックすることで、ホストサーバに対して入力することができます。

 (開放状態)、 (押下状態)：クリックする毎に変化します。

 (開放状態)、 (押下状態)：クリックする毎に変化します。





例えば、“Ctrl+Alt+Del”を入力する場合は、**[Ctrl+Atl]**アイコンをクリックし、キーボードの Del キーを押下すると、本体装置へ“Ctrl+Alt+Del”が送信されます。入力後、**[Ctrl+Atl]**アイコンを再度クリックして、特殊キー入力を解除してください。


 (Windows キーアイコン)


 (“|”：パイプキーアイコン)

画面の拡大・縮小


拡大アイコンをクリックすると、表示内容が大きくなります。

縮小アイコンをクリックすると、表示内容が小さくなります。


等倍アイコンをクリックすると、ホストサーバ上と同じ大きさの表示となります。

ウィンドウリサイズアイコンをクリックすると、リモート KVM コンソールウィンドウのサイズをリモート画面サイズに合わせます。

画面のリフレッシュ

画面リフレッシュアイコンをクリックすると、リモート KVM コンソール画面のリフレッシュを行います。画面表示が乱れた場合は、リフレッシュを行ってください。

プロパティ変更

KVM プロパティアイコンをクリックすると、KVM プロパティ画面が表示されます。ここで、自動的に行われる画面リフレッシュの間隔を指定できます。

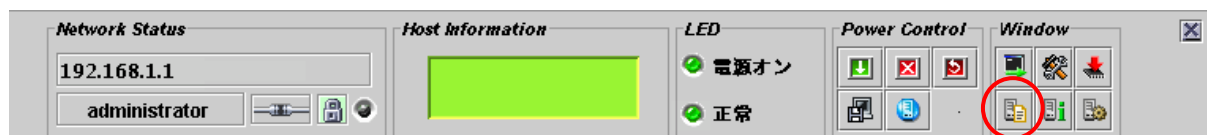



この間隔を短くすることで、画面上に残るゴミを少なくすることができます。ただし、画面のリフレッシュには負荷がかかりますので、あまり短くすると、端末の応答速度が悪くなったり、ネットワーク上のトラフィックに影響を与えることがあります。

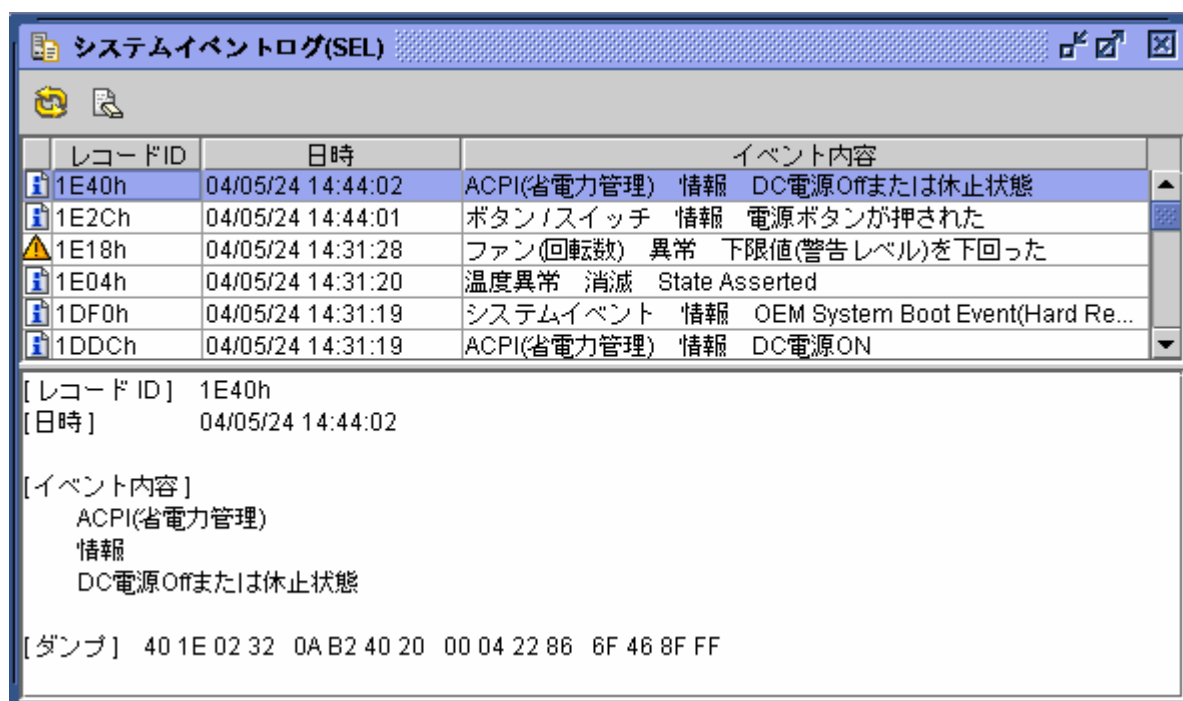
IPMI 情報

システムイベントログ(SEL)、センサ装置情報(SDR)、保守交換部品情報(FRU)をそれぞれ表示することができます。これらを IPMI 情報と呼びます。これらの情報から、本体装置上で起こった障害や各種イベントの発生を調査し、保守交換部品を特定することができます。


システムイベントログ(SEL)の表示




コントロールパネル上のシステムイベントログ(SEL)の起動アイコン[]をクリックすると、BMC から SEL 情報を読み込み、以下のようなシステムイベントログ(SEL)ウィンドウを開いて SEL を表示します。



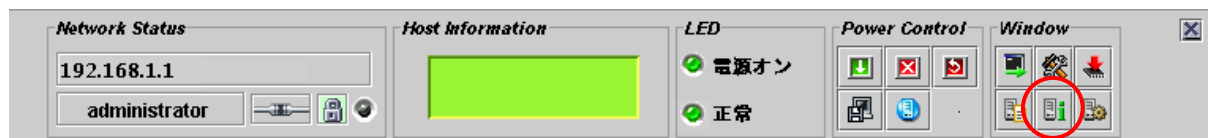
上段に一覧が表示され、下段に一覧表示で選択されたエントリの詳細情報が表示されます。


再読み込みアイコン[]をクリックすることで、BMC から再度 SEL 情報を読み込み、最新情報を表示することができます。

SEL 情報のクリア

SEL クリアアイコン[]をクリックすることで、BMC 上の SEL 情報をクリアすることができます。確認メッセージが表示されますので、良ければ[はい]をクリックしてください。ここで、「いいえ」をクリックすれば、SEL クリアは行われません。

センサ装置情報(SDR)の表示



コントロールパネル上のセンサ装置情報(SDR)の起動アイコンをクリックすると、BMCからSDR情報を読み込み、以下のようなセンサ装置情報(SDR)ウィンドウを開いてSDRを表示します。

センサ装置情報(SDR)


| レコード ID | センサ種別 | オーナー |
|---------|----------------------|------------------|
| 1h | 電圧(Processor 1 VCCP) | Basbrd Mgmt Ctlr |
| 2h | 電圧(Processor 2 VCCP) | Basbrd Mgmt Ctlr |
| 3h | 電圧(Baseboard 3.3V) | Basbrd Mgmt Ctlr |
| 4h | 電圧(Baseboard 3.3VSB) | Basbrd Mgmt Ctlr |
| 5h | 電圧(Baseboard 5V) | Basbrd Mgmt Ctlr |

[レコード ID] 1h
 [センサ種別] 電圧(Processor 1 VCCP)
 [センサ位置] Processor1
 [オーナー] Basbrd Mgmt Ctlr
 [上限値(回復不能レベル)] 監視なし
 [上限値(危険レベル)] 1.64Volts (監視再開値: 1.63Volts)
 [上限値(警告レベル)] 1.56Volts (監視再開値: 1.55Volts)
 [下限値(警告レベル)] 1.15Volts (監視再開値: 1.16Volts)
 [下限値(危険レベル)] 1.06Volts (監視再開値: 1.07Volts)
 [下限値(回復不能レベル)] 監視なし

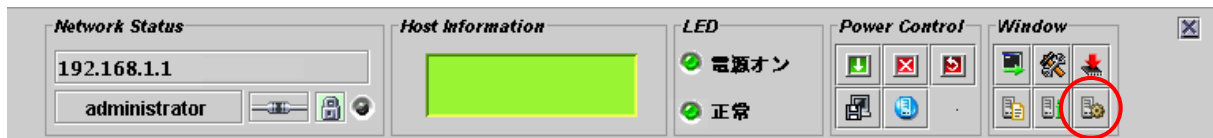
[ダンプ]


```
01 00 51 01    3B 20 00 10    03 01 7F E9    02 01 85 32
85 32 1B 1B    00 04 00 00    EB 42 07 01    00 B4 07 82
B0 5B FF 00    00 BF B0 00    49 5B 02 02    00 00 00 D0
50 72 6F 63    65 73 73 6F    72 20 31 20    56 43 43 50
```

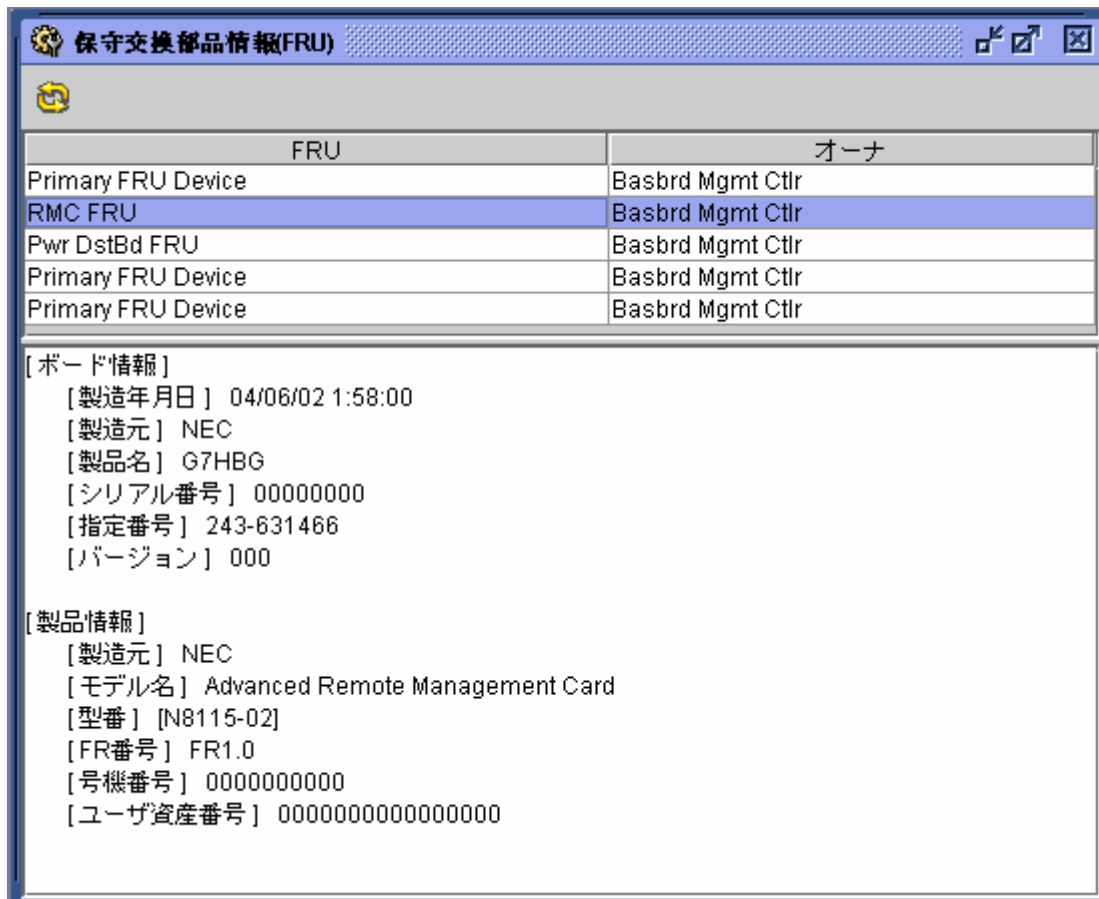
上段に一覧が表示され、下段に一覧表示で選択されたエントリの詳細情報が表示されます。

 **SDR 情報**とは、本体装置上の各種センサについての定義情報です。
 この情報に従って、**BMC** は本体装置のセンサ監視を行います。

保守交換部品情報(FRU)の表示



コントロールパネル上の保守交換部品情報(FRU)の起動アイコン[]をクリックすると、BMC から FRU 情報を読み込み、下記のような保守交換部品情報(FRU)ウィンドウを開いて表示します。




上段に一覧が表示され、下段に一覧表示で選択されたエントリの詳細情報が表示されます。

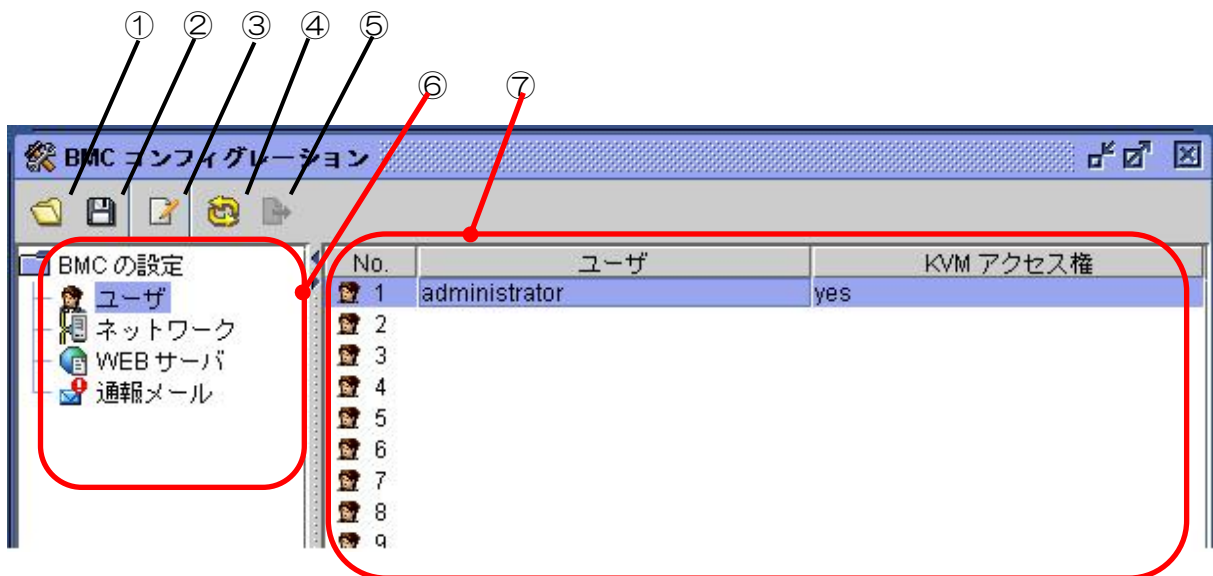
BMC に対する各種設定

BMC に対する各種設定を行うことができます。



BMC コンフィグレーションウィンドウの起動



コントロールパネル上の BMC コンフィグレーションの起動アイコンをクリックすると、以下のような BMC コンフィグレーションウィンドウが表示されます。




- ① BMC コンフィグレーションファイルを読み込みます。
- ② BMC コンフィグレーションをファイルに保存します。
- ③ BMC コンフィグレーションの編集が行えます。
- ④ BMC からコンフィグレーションを再度読み込みます。
- ⑤ ファイルから読み込んだ情報を BMC へ一括して設定します。
- ⑥ 設定項目を選択するツリーです。
- ⑦ 現在の設定値の概要が表示されます。

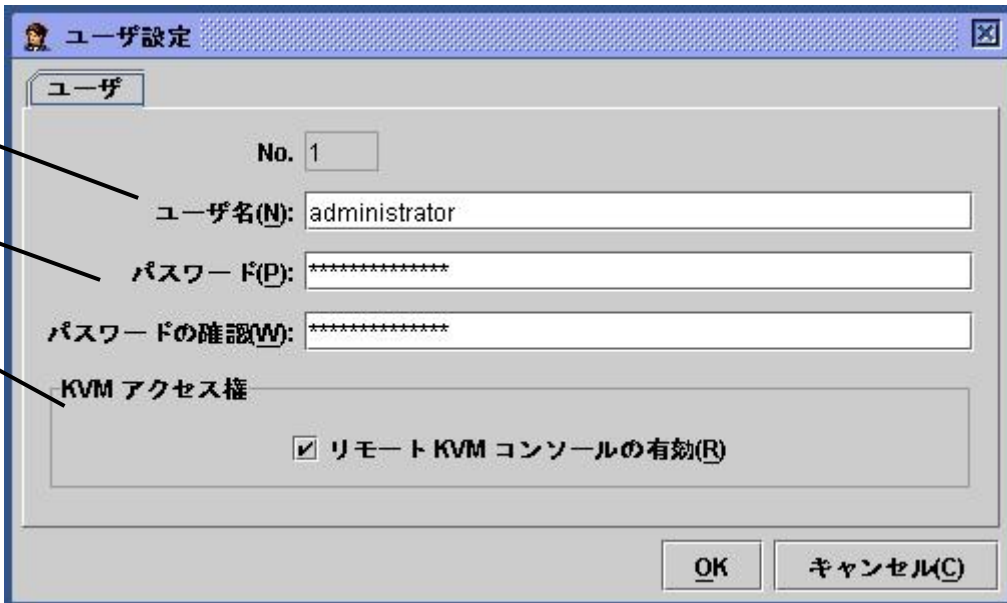
 ファイルからコンフィグレーションを読み込んだ場合は、BMC への一括設定  を使用してください。

ユーザ設定

ユーザアカウントの設定を行います。

BMC コンフィグレーションウィンドウの左欄で「ユーザ」をクリックすると、右欄に全 20 アカウント分の一覧が表示されます。

修正もしくは追加したいアカウントを選択し、編集アイコンをクリックすると、下記のようなユーザアカウント編集ウィンドウが表示されます。



① ユーザ名を入力してください。

② パスワードを入力してください。入力ミス防止のため、2箇所に入力してください。

③ KVM アクセス権を設定します。

① ユーザ名を入力してください。

② パスワードを入力してください。入力ミス防止のため、2箇所に入力してください。

③ KVM アクセス権を設定します。

リモート KVM コンソール…… 有効(許可)/無効(不許可)が指定できます。

チェックボックスをチェックすることにより有効(許可)になります。

「OK」をクリックすると、編集画面の内容が全て BMC に書き込まれます。

「キャンセル」をクリックすると、編集内容を破棄して、編集画面を閉じます。

ネットワークの設定

BMC に対して、IP アドレスなどのネットワーク関連の設定を行います。

本製品では、以下のポートを使用しますので、ファイヤーウォールを設置されているネットワーク環境では、ファイヤーウォールでの対応が必要となります。

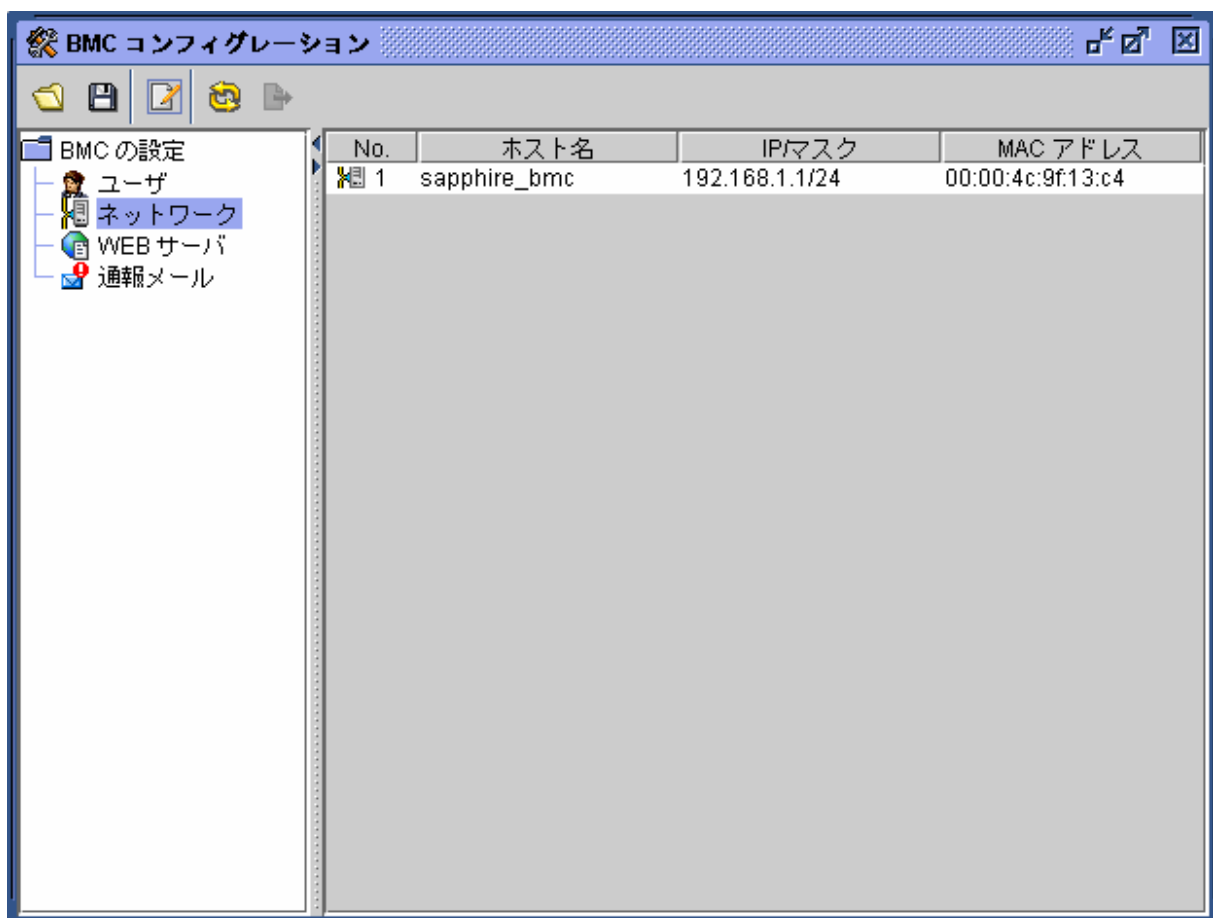
| モジュール名 | ポート番号 | プロトコル | 方向 | モジュール名 | ポート番号 |
|----------------|--------|-------|----|--------|---------|
| リモートKVMクライアント | 不定 | UDP | ⇔ | BMC | 623 |
| メールサーバ | 25(*1) | TCP | ⇔ | BMC | 不定 |
| WEBクライアント | 不定 | TCP | ⇔ | BMC | 80(*2) |
| WEBクライアント(SSL) | 不定 | TCP | ⇔ | BMC | 443(*3) |


*1: [BMC コンフィグレーション]->[通報メール設定]->[SMTP]->[SMTP ポート番号]で変更可能

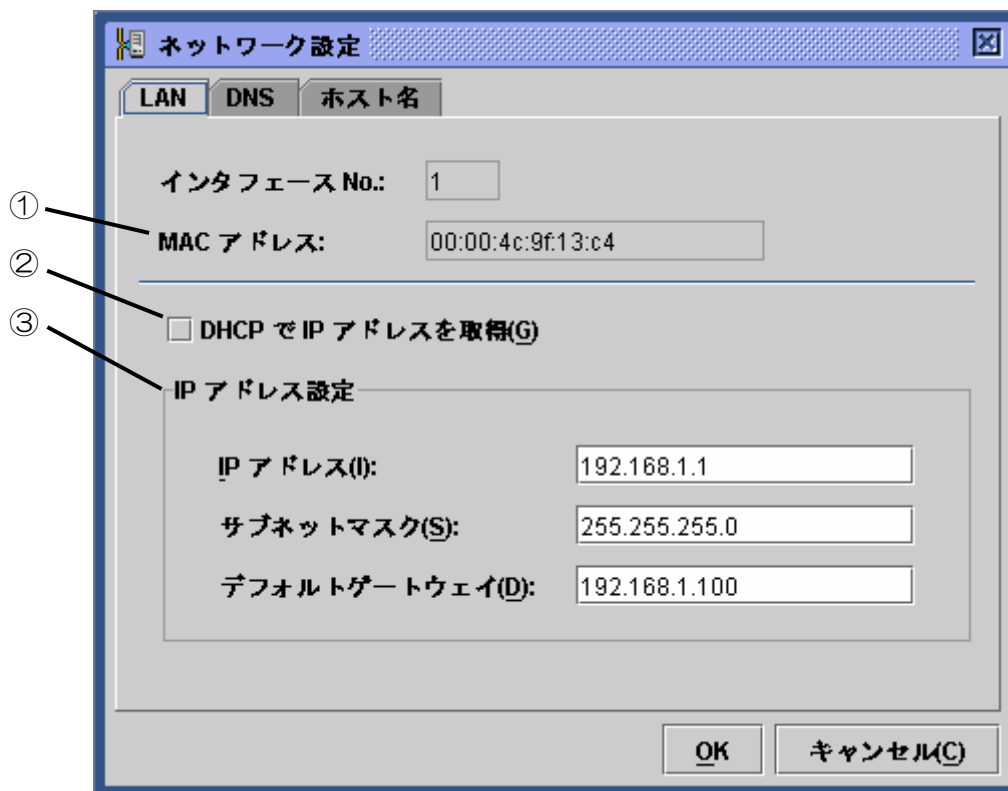
*2: [BMC コンフィグレーション]->[WEB サーバ設定]->[WEB サーバ]->[HTTP ポート番号]で変更可能

*3: [BMC コンフィグレーション]->[WEB サーバ設定]->[WEB サーバ]->[SSL ポート番号]で変更可能

BMC コンフィグレーションウィンドウの左欄で「ネットワーク」をクリックすると、以下のように、右欄がネットワーク設定の概要に切り替わります。



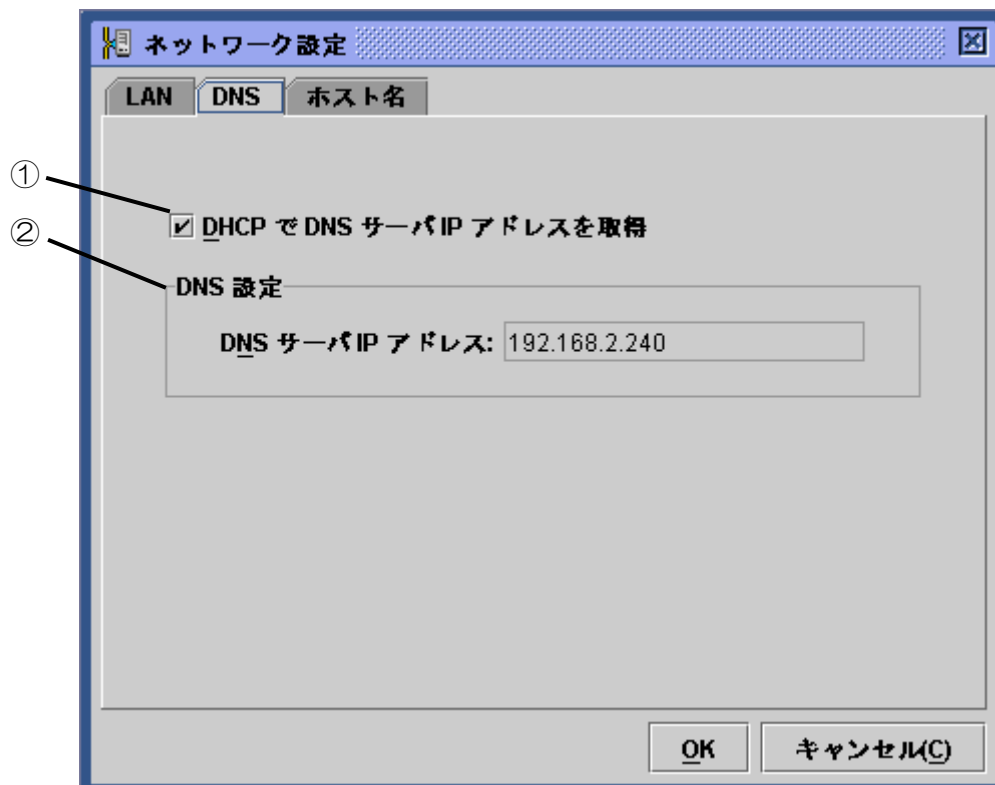
編集アイコンをクリックすると、次に示す様な編集ウィンドウが表示されます。
ネットワーク関連の編集ウィンドウは3つのタブで構成されています。



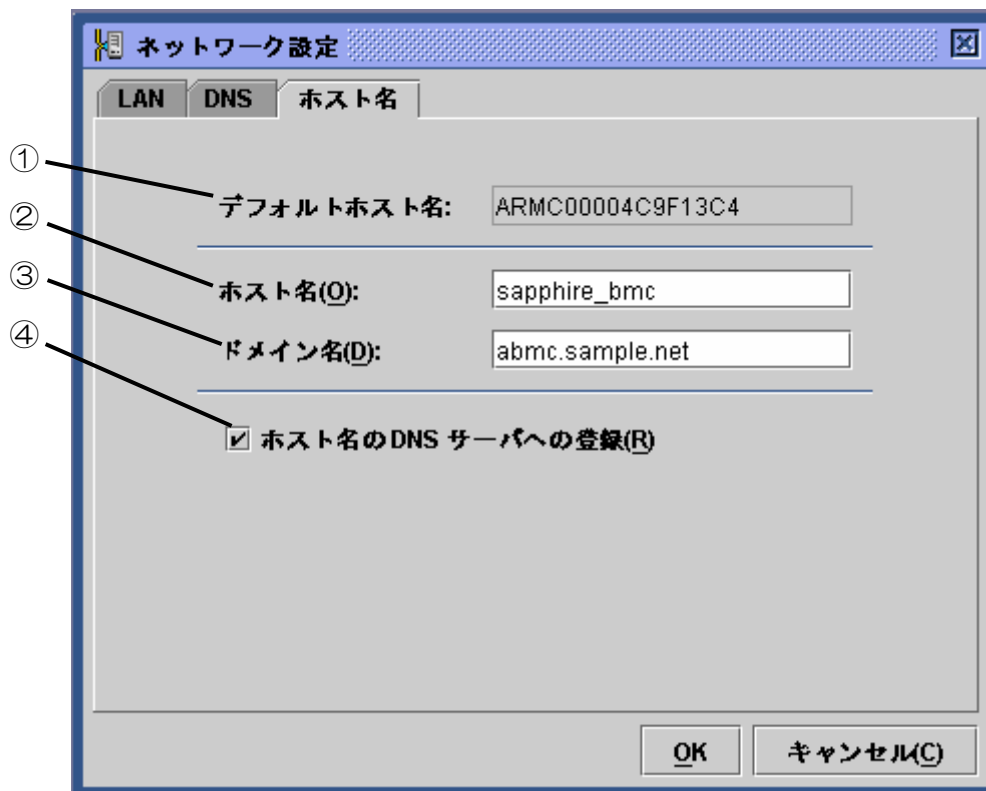
- ① BMC の持つ MAC アドレスが表示されます。
- ② DHCP による IP アドレスの自動取得を行うか否かを選択します。
- ③ DHCP による自動取得を行わない場合には、ここで設定を行います。DHCP で自動取得する場合は、ここに自動取得された内容が表示されます。



- 「デフォルトゲートウェイ」を設定する場合は、ゲートウェイ、本装置、管理用 PC がネットワークで通信できる状態で実施する必要があります。
- 通信できない環境で設定した場合には、設定後 ゲートウェイ、本装置、管理用 PC がネットワークで通信可能な状態で本装置の AC を一度 OFF/ON する必要があります。
- IP アドレスを変更する場合、「OK」をクリックして BMC への設定が完了した時点で、現在の接続は切断されます。
一度ウィンドウを閉じて終了し、再度、新しく設定した IP アドレス(あるいはホスト名)をブラウザに入力してログインしなおしてください。
ブラウザに表示が残っているログインページは、旧アドレスでアクセスした際のものであるので、それでログインすることはできません。



- ① DHCPによるDNSサーバのIPアドレス自動取得を行うか否かを選択します。
- ② DHCPによる自動取得を行わない場合には、ここで設定を行います。DHCPで自動取得する場合は、ここに自動取得された内容が表示されます。



- ① DHCP を使用する際に、ホスト名が未設定な場合に使用される、デフォルトのホスト名です。
- ② BMC のホスト名を設定します。この欄が未設定な場合は、①のデフォルトホスト名が使用されます。
- ③ BMC が所属するネットワークのドメイン名を設定します。
- ④ DNS サーバへのホスト名の登録を行うか否かを選択します。



BMC のホスト名は、本体装置上の OS のホスト名（Windows の場合はコンピュータ名）を容易に類推できるように設定することを推奨します。
例えば、本体装置の OS 上のホスト名が “sapphire” ならば、BMC のホスト名は “sapphire_bmc” などと設定します。



BMC は、本体装置の OS とは独立した LAN コントローラを使用しますので、BMC のホスト名およびドメイン名を本体装置の OS のものと全く同じにすることは出来ません。所属するネットワークドメインが異なるのであれば、ホスト名を同じにすることは可能です。

[OK]をクリックすると、3つのタブで構成された編集画面の内容が、全て BMC に書き込まれます。

[キャンセル]をクリックすると、編集内容を破棄して、編集画面を閉じます。

WEB サーバの設定

BMC に対して、HTTP ポートなど WEB サーバ関連の設定を行います。

BMC コンフィグレーションウィンドウの左欄で「WEB サーバ」をクリックすると、以下のよう、右欄が WEB サーバ設定の概要に切り替わります。




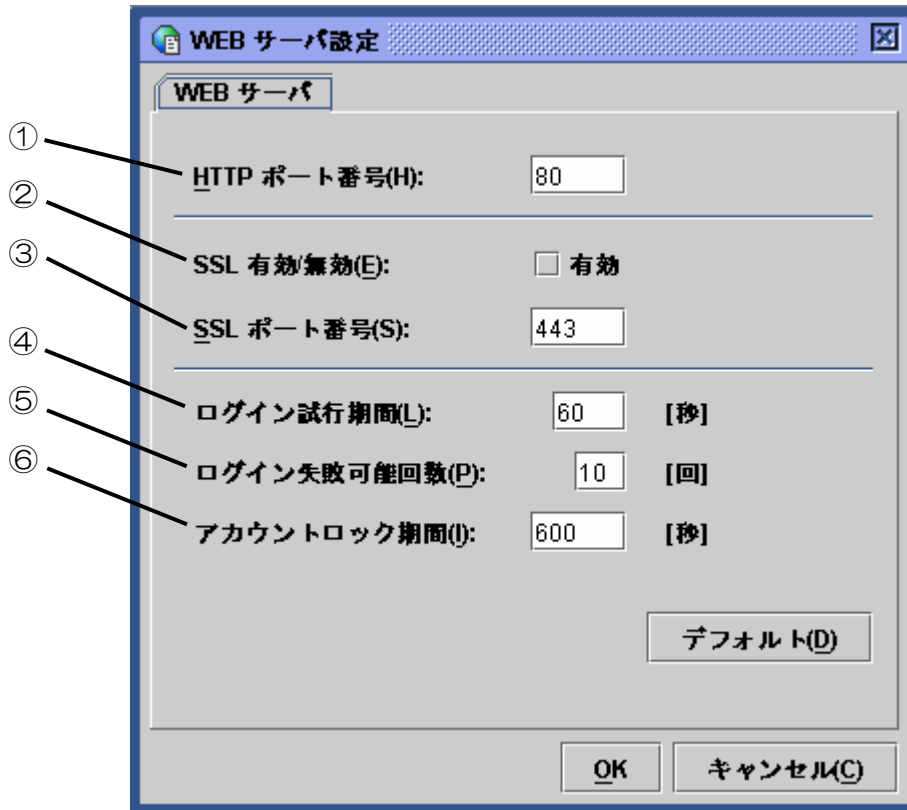
重要

HTTP ポート番号、SSL の有効/無効、SSL ポート番号を変更すると現在の接続は一時的に切断されます。

一度ウィンドウを閉じて終了し、再度、新しく設定したポート番号をブラウザに入力してログインしなおしてください。

ブラウザに表示が残っているログインページは、古い WEB サーバの設定でアクセスした際のものであるため、それでログインすることはできません。

編集アイコンをクリックすると、次に示す様な編集ウィンドウが表示されます。



- ① HTTP のポート番号を指定します。
- ② SSL 通信の有効/無効を指定します。有効のチェックボックスをチェックすると、HTTPS(SSL 有効)での接続となります。チェックを外すことで SSL 無効の設定になります。



SSL が使用できないなどの特別な理由が無い限り、暗号化された HTTPS プロトコルでの接続を推奨します。尚、デフォルトの設定では無効になっております。

- ③ SSL ポート番号を指定します。
- ④ ログイン試行期間は、ログインに失敗した時、再度ログインを試みることが出来る期間を指定します。
- ⑤ ログイン失敗可能回数は、③で指定した期間内に、ここで設定した回数を超えてログインに失敗した場合、以下⑤で指定する期間、ログインを拒否します。
- ⑥ アカウントロック期間は、ログインを拒否する時間を指定します。



上記の3項目は、自動で行われる不正ログインに対して、防御の効果が期待できます。ただし、完全に防げるわけではありません。

[デフォルト]をクリックすると、HTTPポート番号と SSLポート番号、およびログイン試行期間、ログイン失敗可能回数、アカウントロック期間の欄にデフォルト値が表示されます。ただし、SSL 有効/無効のチェック欄は変わりません。

[OK]をクリックすると、編集画面の内容が全て BMC に書き込まれます。


[キャンセル]をクリックすると、編集内容を破棄して、編集画面を閉じます。

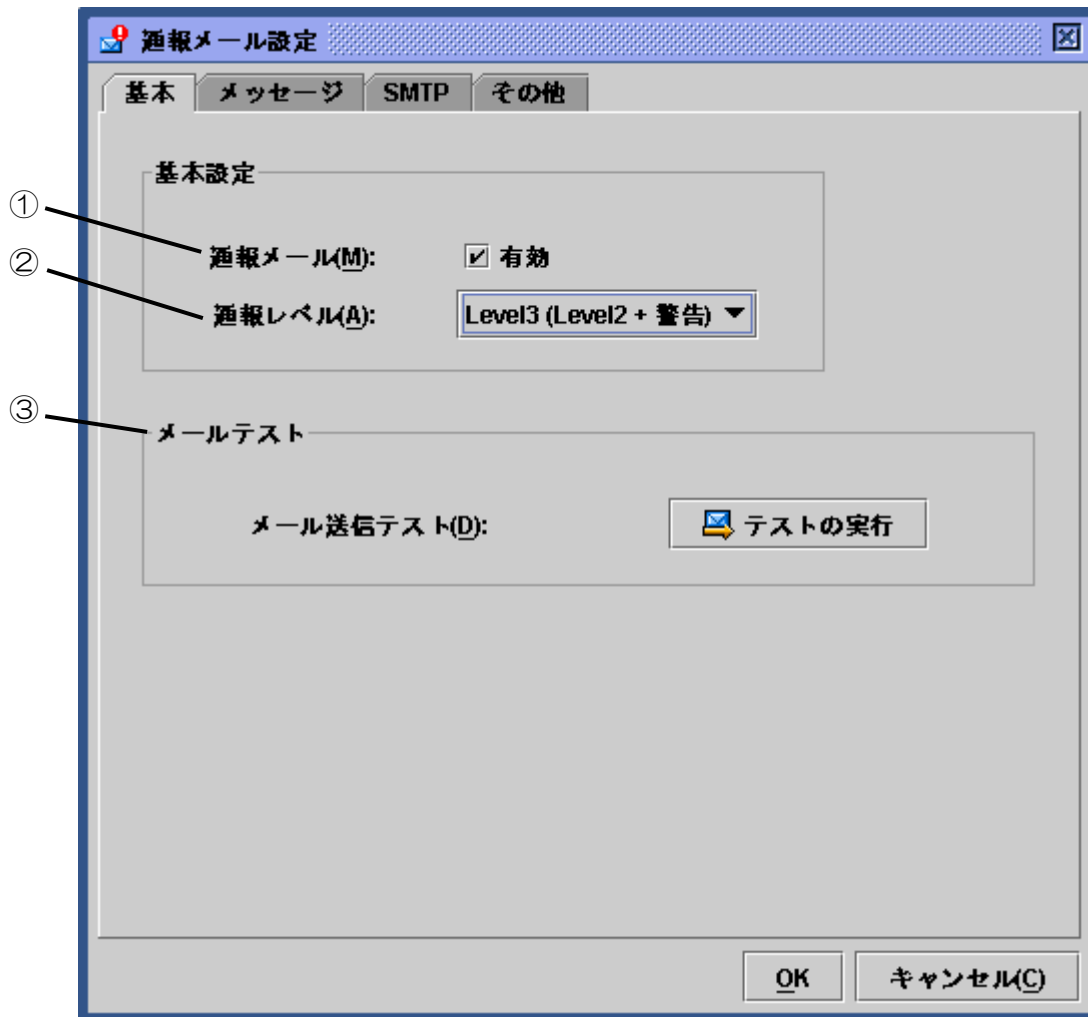
通報メールの設定

BMC に対して、通報メール関連の設定を行います。

BMC コンフィグレーションウィンドウの左欄で「通報メール」をクリックすると、以下のよう
に、右欄が通報メール設定の概要に切り替わります。



編集アイコンをクリックすると、次に示す様な編集ウィンドウが表示されます。編集ウィ
ンドウは4つのタブで分割されています。



- ① 通報メール機能の有効／無効をチェックボックスにて指定します。チェックを入れると、メール関連の設定が可能となります。
- ② 通報レベルを指定します。6段階のレベルで選択可能です。
通報レベルは、その要因となるイベントの重要度によって分けられています。
- ③ テストメールの発信が行えます。



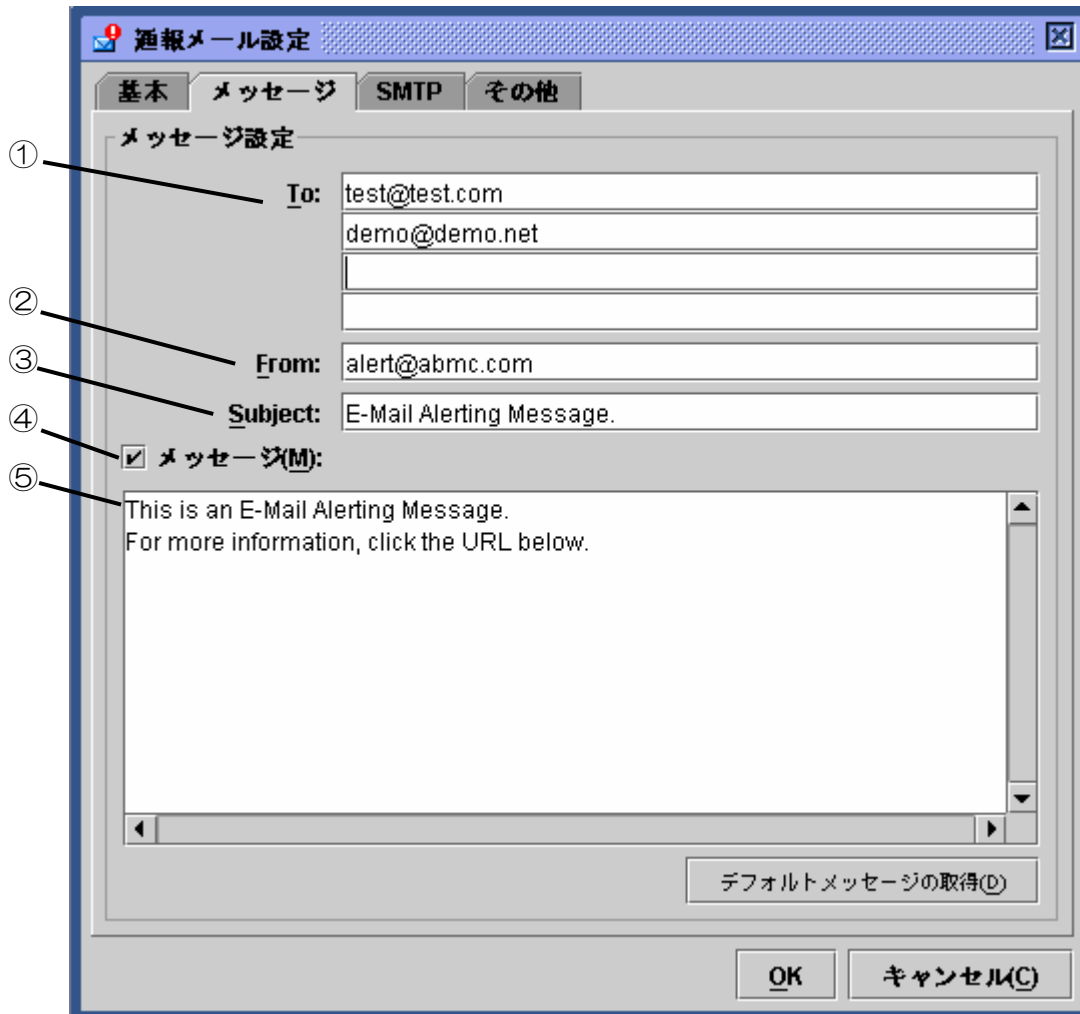
メール送信テストは、次ページ以降に記載する「通報メール設定」を全て完了させた後に行ってください。

なお、編集画面に入力しただけでは、設定は完了になりません。必要事項を入力後、「OK」をクリックして BMC への設定を完了してください。



要因となるイベントの重要度によって、通報メールのメールヘッダの X-Priority: フィールドが変化します。

| | |
|----------|---------------|
| 回復不能・異常 | X-Priority: 1 |
| 警告 | X-Priority: 3 |
| 回復・情報・監視 | X-Priority: 5 |

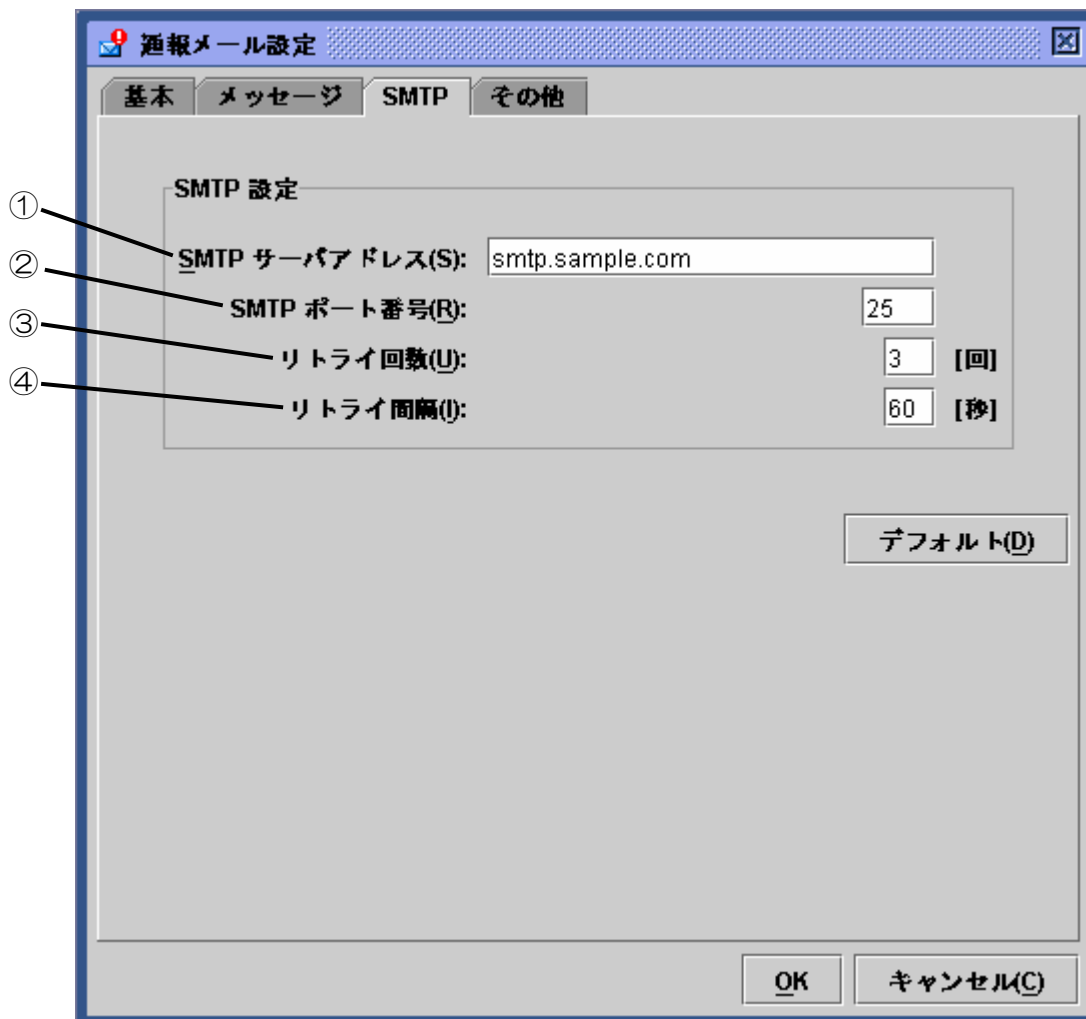


- ① 通報メールの宛先メールアドレスを指定します。4つまで指定できます。
- ② 通報メールの発信メールアドレスを指定します。
- ③ 通報メールに付けるサブジェクトを記入します。
- ④ 下の⑤で指定する通報メールに付ける本文の共通部分の有効/無効を指定します。
- ⑤ 通報メールに付ける本文の共通部分を記入します。不要な場合は、④のチェックを外してください。「デフォルトメッセージの取得」をクリックすると、推奨メッセージが表示されます。



ここで設定したサブジェクトとメッセージが、全ての通報メールに対して付けられます。

なお、サブジェクトとメッセージについては、日本語での入力も可能ですが、メールアドレスについては、日本語での入力はできません。

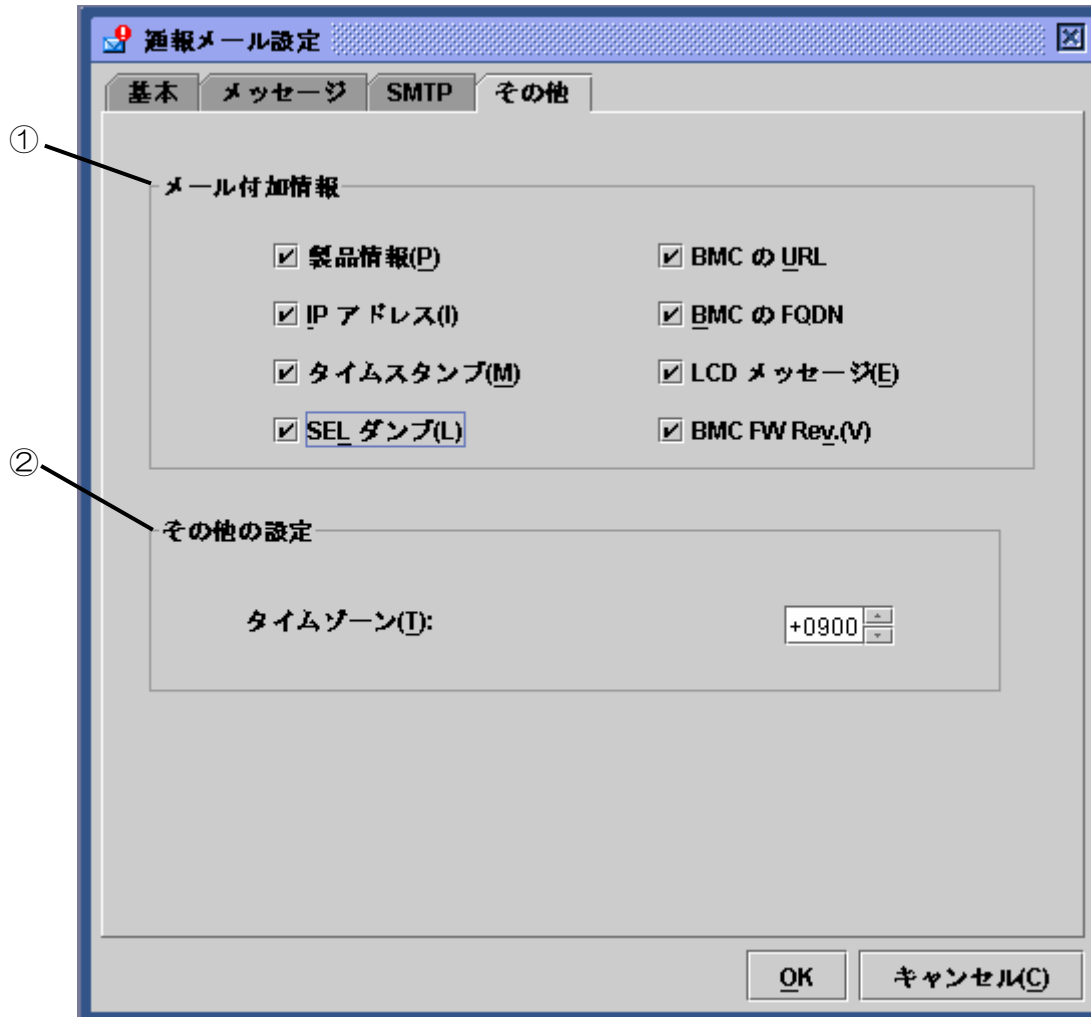


- ① SMTP サーバのアドレスを指定します。IP アドレスまたはホスト名での指定が可能です。
- ② SMTP サーバのポート番号を指定します。
- ③ メール送信失敗時に何回リトライさせるかを指定します。
- ④ メール送信失敗時のリトライを行う際に、何秒待たせるかを指定します。

「デフォルト」をクリックすると、SMTP ポート番号とリトライ回数、リトライ間隔の欄にデフォルト値が表示されます。特に理由が無い限りデフォルト値での設定を推奨します。



本製品は SMTP 認証(SMTP-AUTH)には対応していません。



① 通報メールの本文に付加する情報を指定します。

ここで指定した情報が、メッセージタブのメッセージ欄で指定したメッセージと合わせて、通報メールの本文となります。

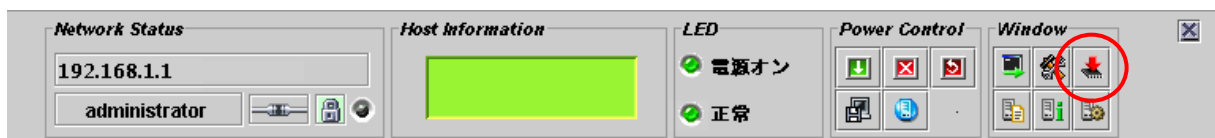
| | |
|-------------|-------------------------------|
| 製品情報 | 本体装置の製品名、型名、号機番号 |
| IP アドレス | BMC の IP アドレス |
| タイムスタンプ | イベントが発生した時刻 |
| SEL ダンプ | システムイベントログ(SEL)を 16 進数で表したデータ |
| BMC の URL | ARMC のログインページへの URL |
| BMC の FQDN | BMC のフルドメイン名 |
| LCD メッセージ | イベント発生時のサーバの LCD メッセージ |
| BMC FW Rev. | BMC ファームウェア/SDR/PIA のレビジョン情報 |


② 通報メールのメールヘッダに付く Date フィールドに使用されます。

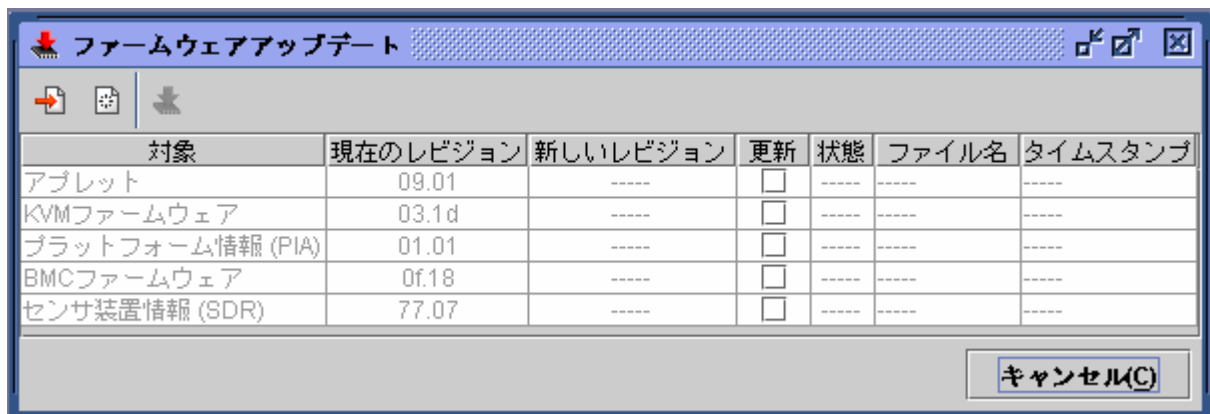
ファームウェアアップデート

アプレットおよび、KVM ファームウェア、BMC ファームウェア、センサ装置情報(SDR)、プラットフォーム情報(PIA)のアップデートを行うことができます。

ファームウェアアップデートウィンドウの起動



コントロールパネル上のファームウェアアップデートの起動アイコン[, 赤い星]をクリックすると、BMC からそれぞれのレビジョン情報を読み込み、以下のようなファームウェアアップデートウィンドウを表示します。

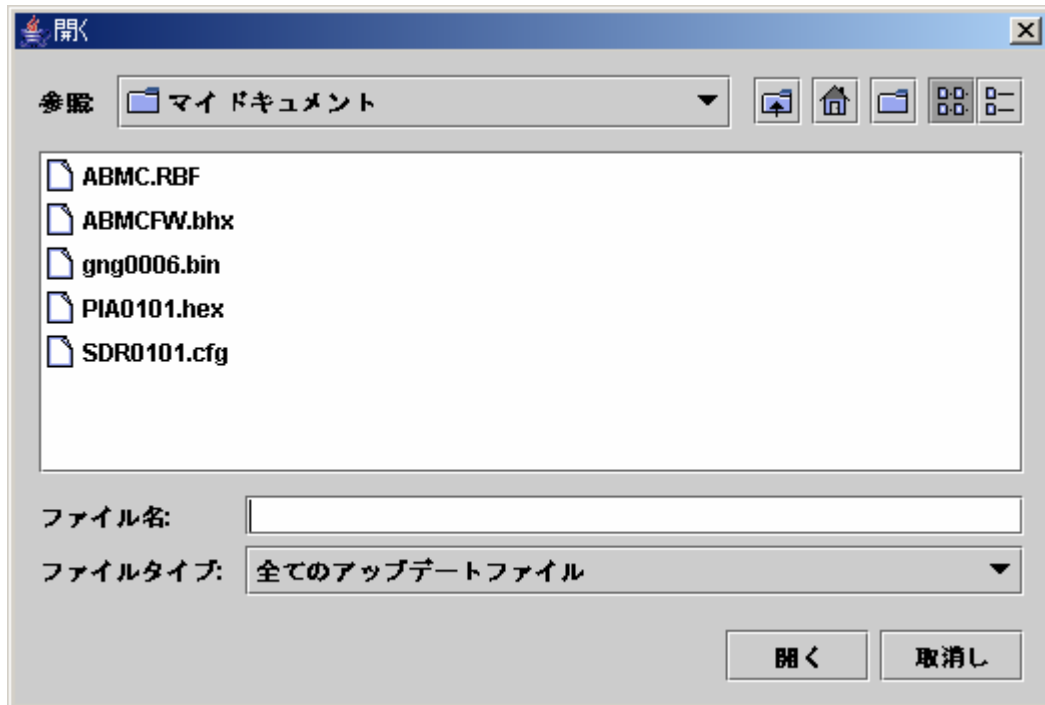


「キャンセル」をクリックすると何もせずに終了し、ファームウェアアップデートウィンドウを閉じます。

次ページ以降で、アップデートの手順について順を追って説明します。

アップデートデータファイルの読み込み

アップデートファイルの追加 [📁] をクリックすると、以下のようなファイル選択画面が表示されます。



アップデートデータのファイルを指定してください。

ファイル指定後、「開く」をクリックすると、ファイルの読み込みを開始します。

読み込みが完了するまで、しばらくお待ちください。

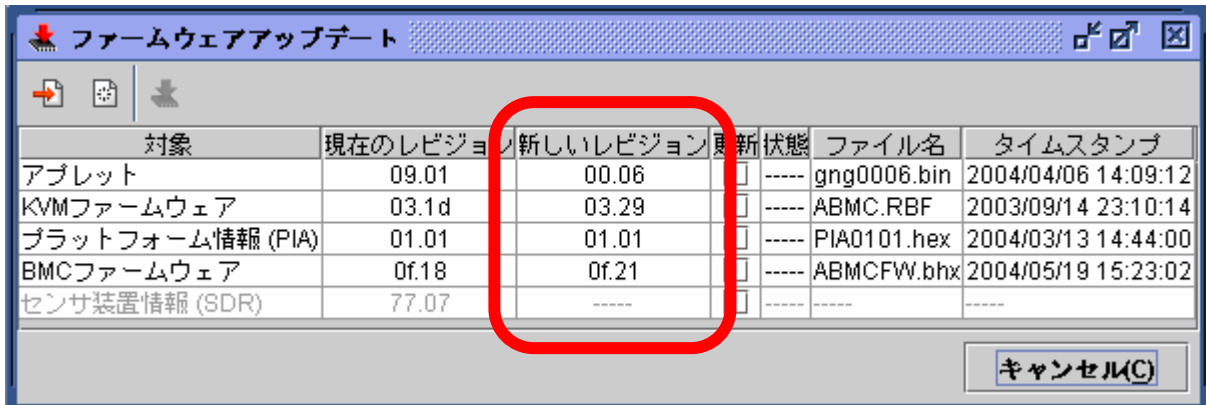


アップデートはまとめて実行可能です。
複数のアップデート対象がある場合は、各対象のアップデート情報を全て読み込んでください。
読み込みファイルを複数同時に選択することも可能です。

レビジョンの確認

データファイルの読み込みが完了すると、画面に現在のレビジョンと読み込んだデータのレビジョン及びファイルの情報(ファイル名とタイムスタンプ)が表示されます。

間違いないかご確認ください



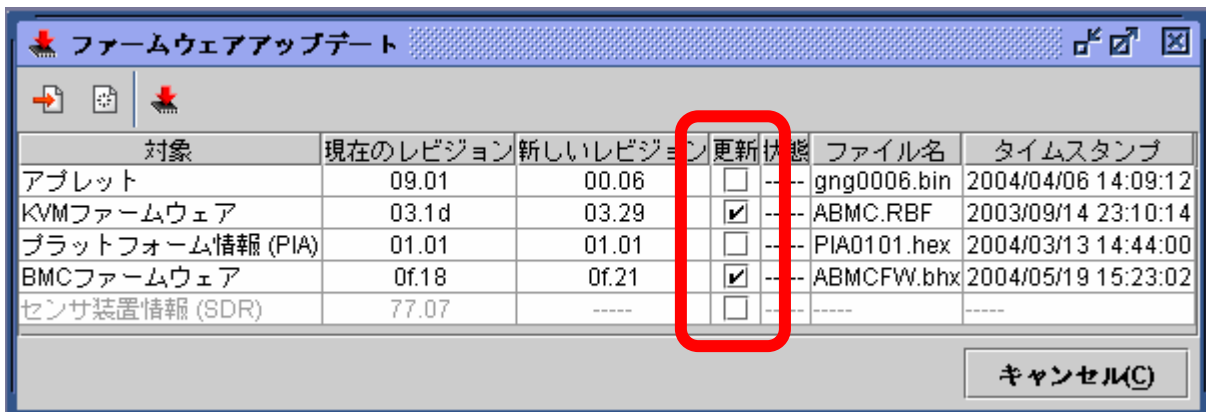
チェック

ダウングレードも可能となっておりますので、それぞれのレビジョンについて良く確認してください。

尚、アップデートデータのクリア [🗑️] をクリックすると、読み込んだデータを全て破棄します。また、「キャンセル」をクリックすると、読み込んだデータを全て破棄して、アップデートウィンドウを閉じます。

アップデート対象の選択

更新チェックボックスにて、アップデートする対象を選択してください。



チェック

ここで指定したものが書き込まれます。

ファイルを読み込ませただけで指定していない項目については、書き込みを行いません。



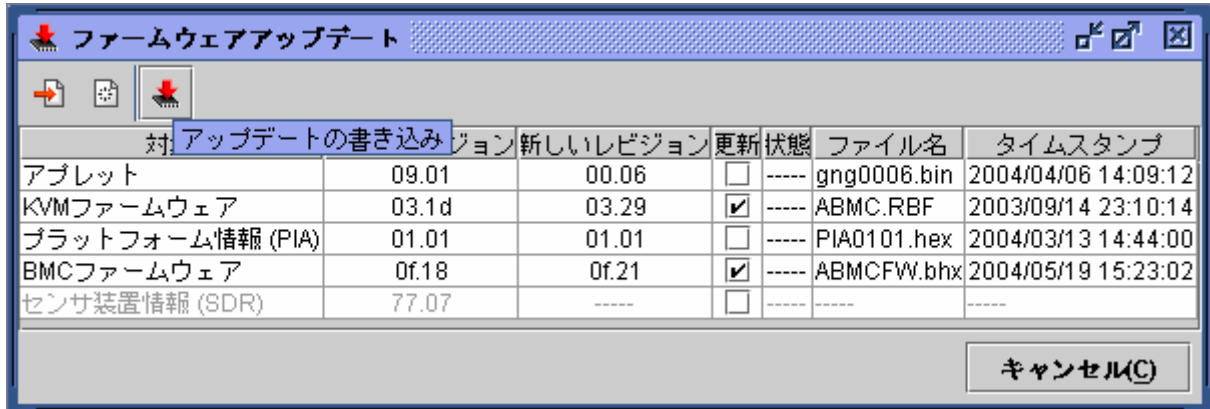
重要

SDR と PIA の双方をアップデートする場合は、必ず、同時に書き込み指定を行ってください。

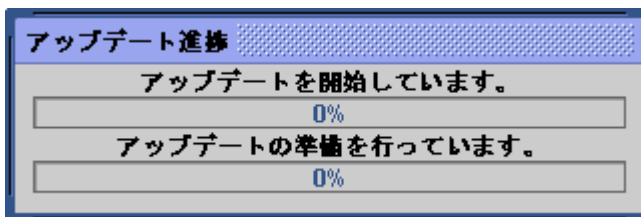
書き込みを2回に分けると、最初に書き込んだ方は無効になります。

アップデートデータの書き込み

アップデートの書き込み [🔥] をクリックすると、BMC へアップデートデータの書き込みを開始します。



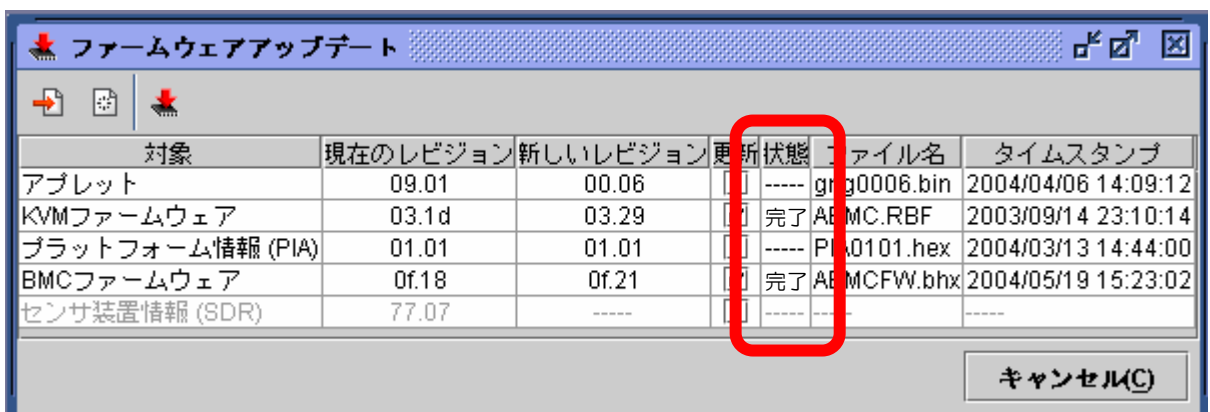
それぞれのアップデート対象毎に以下のような書き込みの進捗を表すウィンドウが表示されます。



途中でエラーを検出するとエラーメッセージを表示して終了します。

完了

書き込みが終了すると、「状態」欄に、それぞれ「対象」毎の結果が表示されます。





チェック

アプレット以外の対象について、実際にアップデートを適用するためには本体装置の再起動、あるいはサーバの電源オフ/オンを行ってください。



チェック

本体装置の再起動あるいは電源オンを行い、**BMC** ファームウェア、**SDR**、**PIA** のアップデートを適用した場合、**BMC** との接続が切断されますので、引き続き使用する場合は、再度ログインしてください。



チェック

アプレットのアップデートを適用するには、一旦、ログアウトして、全てのブラウザを閉じた後に、再度ログインしてください。
本体装置を再起動する必要はありません。

6.トラブルシューティング

エラーメッセージ

リモートマネージメントを使用している際に、何らかの異常が発生して管理 PC 上にエラーダイアログが表示される場合があります。メッセージとそれに対する対処方法を以下に示します。

致命的エラー

| 項番 | エラーメッセージ | 対処方法 |
|----|-----------------------|---|
| 1 | 致命的エラー。JavaVM を終了します。 | 再度ログインしてください。 同様なメッセージが出力される場合はサポート部門にお問い合わせください |
| 2 | 致命的なソフトウェアエラーが発生しました。 | 再度ログインしてください。 同様なメッセージが出力される場合はサポート部門にお問い合わせください |

ログイン時のエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|----------|-----------------------------|
| 1 | 認証エラーです。 | ユーザ名とパスワードを確認して、再度入力してください。 |

アクセス権のエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|-----------------------------|--|
| 1 | 許可されていない操作です。権利レベルが不足しています。 | 管理者 (Administrator) レベルで行ってください。 管理者の方にご相談ください。 |

ネットワーク系のエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|---|--|
| 1 | HTTP 通信に失敗しました。 | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 2 | IP アドレスが解決できませんでした。 | ネットワーク環境を確認してください。 プロキシを経由した接続では、リモート KVM コンソールはご利用頂けません。 |
| 3 | 目的のホストに到達できません。 | ネットワーク環境を確認してください。 プロキシを経由した接続では、リモート KVM コンソールはご利用頂けません。 |
| 4 | ネットワークエラーが発生しました： | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 5 | アプレットのダウンロードに失敗しました。 | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 6 | RMCP+のセッションはクローズされています。 | ネットワーク環境を確認してください。 ネットワークに問題が無い場合は、サポート部門にお問い合わせください。 |
| 7 | RMCP+のセッション確立に失敗しました。 | ネットワーク環境を確認してください。 ネットワークに問題が無い場合は、サポート部門にお問い合わせください。 |
| 8 | RMCP+の送信に失敗しました。 | ネットワーク環境を確認してください。 ネットワークに問題が無い場合は、サポート部門にお問い合わせください。 |
| 9 | 指定された RMCP+プロトコルは利用できません。 | ネットワーク環境を確認してください。 ネットワークに問題が無い場合は、サポート部門にお問い合わせください。 |
| 10 | 新しい RMCP+セッションを確立するための BMC のリソースが不足しています。 | 他のクライアントからの接続が終了した後、再度実行してください。 |
| 11 | RMCP+接続がタイムアウトしました。 | ネットワーク環境やサーバ側を確認してください。 特に問題が見当たらない場合は、サポート部門にお問い合わせください。 |

BMC 関連のエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|--------------------------------|--|
| 1 | IPMI リクエストがアポートされました。 | ネットワークが混雑していることが原因の可能性あります。もう一度、実行してください。何度行っても取得に失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 2 | BMC から不正なレスポンスを受信しました。 | サーバ側を確認してください。BMC が故障している可能性があります。特に問題が見つからない場合は、サポート部門にお問い合わせください |
| 3 | BMC は IPMI 2.0 の機能をサポートしていません。 | サポート部門にお問い合わせください。 |
| 4 | IPMI コマンドの実行に失敗しました。 | サーバ側を確認してください。BMC が故障している可能性があります。特に問題が見つからない場合は、サポート部門にお問い合わせください。 |
| 5 | IPMI メッセージの送信に失敗しました。 | ネットワーク環境を確認してください。ネットワークに問題が無い場合は、サポート部門にお問い合わせください。 |
| 6 | 不正な IPMI コマンドが要求されました。 | サポート部門にお問い合わせください。 |
| 7 | 指定された対象が存在しません。 | サーバ側を確認してください。特に問題が見つからない場合は、サポート部門にお問い合わせください。 |

リモート KVM コンソールでのエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|--|--|
| 1 | リモート KVM コンソールの無効化に失敗しました。 | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 2 | リモート KVM コンソールの有効化に失敗しました。 | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 3 | KVM パケットの送信に失敗しました。 | ネットワーク環境やサーバ側を確認してください。 特に問題が見当たらない場合は、サポート部門にお問い合わせください。 |
| 4 | KVM リクエストがアボートされました。 | 特に問題はありません。「OK」をクリックしてメッセージダイアログボックスを閉じてください。 |
| 5 | UDP パケットの送信に失敗しました。 | ネットワーク環境やサーバ側を確認してください。 特に問題が見当たらない場合は、サポート部門にお問い合わせください。 |
| 6 | リモート KVM コンソールは無効に設定されているため、使用できません。 | 30 ページを参照し、リモート KVM コンソールを有効(許可)にしてください。 |
| 7 | リモート KVM コンソールは既に他のクライアントによって使用されています。 | リモート KVM コンソールを既に使用中のクライアントが、終了した後に再度実行してください |
| 8 | リモート KVM コンソールの終了に失敗しました。 | 3分以上経過してから、リモート KVM コンソールを使用してください。 |
| 9 | BMC コンフィグレーションの設定に失敗しました。 | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 10 | UDP 接続がクローズされました。 | ネットワーク環境やサーバ側を確認してください。 特に問題が見当たらない場合は、サポート部門にお問い合わせください。 |

システムイベントログ(SEL)表示でのエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|-----------------------|--|
| 1 | BMC の SEL クリアに失敗しました。 | ネットワークが混雑していることが原因の可能性あります。もう一度、実行してください。何度行っても取得に失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 2 | SEL の取得に失敗しました。 | ネットワークが混雑していることが原因の可能性あります。もう一度、実行してください。何度行っても取得に失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |

センサ装置情報(SDR)表示でのエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|-----------------|--|
| 1 | SDR の取得に失敗しました。 | ネットワークが混雑していることが原因の可能性あります。もう一度、実行してください。何度行っても取得に失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |

保守交換部品情報(FRU)表示でのエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|-----------------|--|
| 1 | FRU の取得に失敗しました。 | ネットワークが混雑していることが原因の可能性あります。もう一度、実行してください。何度行っても取得に失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |

BMC コンフィグレーションでのエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|--|--|
| 1 | 設定に失敗しました： | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 2 | BMC コンフィグレーションの取得に失敗しました： | ネットワーク環境を確認して、もう一度、実行してください。 何度行っても失敗する場合は、サポート部門にお問い合わせください。 |
| 3 | 他のソフトウェアが使用中です。 しばらくしてから、もう一度、実行してください。 | しばらくしてから、もう一度、実行してください。 |
| 4 | 不正な BMC コンフィグレーションファイルです。 | BMC コンフィグレーションファイルが壊れている可能性があります。ファイルを確認してください。 |
| 5 | 必要な XML タグが見つかりませんでした。 | BMC コンフィグレーションファイルが壊れている可能性があります。ファイルを確認してください。 |
| 6 | ファイルの保存に失敗しました。 | BMC コンフィグレーションファイルが正しく保存できていません。保存先を変更して、もう一度、実行してください。 |
| 7 | ユーザ名が長すぎます。 | 長さは 31 文字以下としてください。 |
| 8 | ユーザ名に不正な文字が含まれています | ユーザ名には英数字および、「-」(マイナス記号)と、「_」(アンダースコア)以外は使用できません。 |
| 9 | パスワードが長すぎます。 | 16 文字以下としてください。 |
| 10 | パスワードが不一致です。 | パスワードを入力し直してください。 |
| 11 | HTTP ポート番号が不正です。 | 数字以外は使用できません。 |
| 12 | SSL ポート番号が不正です。 | 数字以外は使用できません。 |
| 13 | HTTP と SSL のポート番号が同じです。 | 同じポート番号にはできません。異なる値を使用してください。 |

| | | |
|----|-----------------------|---|
| 14 | ログイン試行期間が不正です。 | 数字以外は使用できません。 |
| 15 | ログイン失敗可能回数が不正です。 | 数字以外は使用できません。 |
| 16 | アカウントロック期間が不正です。 | 数字以外は使用できません。 |
| 17 | IP アドレスが不正です。 | 数字とピリオドで指定してください。 |
| 18 | サブネットマスクが不正です。 | 数字とピリオドで指定してください。 |
| 19 | デフォルトゲートウェイが不正です。 | 数字とピリオドで指定してください。 |
| 20 | DNS サーバ IP アドレスが不正です。 | 数字とピリオドで指定してください。 |
| 21 | ホスト名が不正です。 | ホスト名には英数字および、「-」(マイナス記号)と、「_」(アンダースコア)以外は使用できません。また、長さは 64 文字以下としてください。 |
| 22 | ドメイン名が不正です。 | ドメイン名には英数字および、「-」(マイナス記号)と、「_」(アンダースコア)、「.」(ピリオド)以外は使用できません。また、長さは 256 文字以下としてください。 |
| 23 | SMTP サーバアドレスが長すぎます。 | 長さは 256 文字以下としてください。 |
| 24 | SMTP ポート番号が不正です。 | 数字以外は使用できません。 |
| 25 | リトライ回数が不正です。 | 数字以外は使用できません。 |
| 26 | リトライ間隔が不正です。 | 数字以外は使用できません。 |
| 27 | “To”が長すぎます | 長さは 256 文字以下としてください。 |
| 28 | “From”が長すぎます。 | 長さは 256 文字以下としてください。 |
| 29 | “Subject”が長すぎます。 | 長さは 512 文字以下としてください。ただし、日本語で入力する場合は、この半分より少ない文字数となります。 |

| | | |
|----|-------------------|---|
| 30 | メッセージが長すぎます。 | 長さは 4064 文字以下としてください。ただし、日本語で入力する場合は、この半分より少ない文字数となります。 |
| 31 | ファイルのオープンに失敗しました: | 指定のファイルが存在しない可能性があります。ファイル名などに間違いがないか確認してください。 |
| 32 | ファイルのクローズに失敗しました: | 指定のファイルが壊れている可能性があります。 |
| 33 | ディレクトリは開けません。 | 指定のファイルが存在しない可能性があります。ファイル名などに間違いがないか確認してください。 |
| 34 | タイムアウトが発生しました。 | もう一度、実行してください。何度行ってもタイムアウトとなる場合は、サポート部門にお問い合わせください。 |

ファームウェアアップデートでのエラー

| 項番 | エラーメッセージ | 対処方法 |
|----|------------------------------|---|
| 1 | BMC には次のアップデート未完了のイメージがあります: | サーバを再起動して、アップデートを完了させてください。 |
| 2 | アップデートエリアの状態取得に失敗しました。 | ネットワークが混雑していることが原因の可能性があります。もう一度、実行してください。何度行っても取得に失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 3 | アップデートデータが大きすぎます: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 4 | アップデートの準備に失敗しました。 | ネットワークが混雑していることが原因の可能性があります。もう一度、実行してください。何度行っても失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 5 | ファイルサイズが不正です: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |

| | | |
|----|-----------------------------|--|
| 6 | レビジョン情報を発見できませんでした: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 7 | ロールバックイメージの作成に失敗しました。 | もう一度、実行してください。何度行っても失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 8 | 消去に失敗しました。 | もう一度、実行してください。何度行っても失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 9 | 未サポートのフォーマットバージョンです: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 10 | アップデートイメージファイルの読み込みに失敗しました。 | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 11 | アップデートに失敗しました。 | もう一度、実行してください。何度行っても失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 12 | アップデートモードになることが出来ませんでした。 | もう一度、実行してください。何度行っても失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 13 | アップデート対象を検出できませんでした: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 14 | アドレスが不正です: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 15 | 書き込みに失敗しました。 | もう一度、実行してください。何度行っても失敗する場合は、BMC が故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 16 | サポートしていないトークンを検出しました: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 17 | セグメント情報が不正です: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |

| | | |
|----|---------------------------|--|
| 18 | データ長が不正です: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 19 | ファイルのオープンに失敗しました: | 指定のファイルが存在しない可能性があります。ファイル名などに間違いがないか確認してください。 |
| 20 | ファイルのクローズに失敗しました: | 指定のファイルが壊れている可能性があります。 |
| 21 | ファイルのチェックサムが不正です: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 22 | ファイルの解釈に失敗しました。 | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 23 | ファイルの解釈に失敗しました: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 24 | ファイルの読み込みに失敗しました: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 25 | ファイルを発見できませんでした: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 26 | ベリファイに失敗しました。 | もう一度、実行してください。何度行っても失敗する場合は、BMCが故障している可能性がありますので、サポート部門にお問い合わせください。 |
| 27 | 割り込みが発生したので、アップデートを中止します。 | クライアント側を確認してください。お客様が使われている他のソフトウェアによる割り込みの可能性があります。 |
| 28 | 現在オンラインアップデートは使用中です。 | 他のツールで行われているオンラインアップデートが終了した後、必要に応じて再度実行してください。 |
| 29 | 現在のレビジョンの取得に失敗しました。 | ネットワークが混雑していることが原因の可能性があります。もう一度、実行してください。何度行っても取得に失敗する場合は、BMCが故障している可能性がありますので、サポート部門にお問い合わせください。 |

| | | |
|----|--------------------|--|
| 30 | 行の取得に失敗しました: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 31 | 行の長さが不正です: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 32 | 予期しない EOF を検出しました: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 33 | 予期しないトークンを検出しました: | アップデートファイルが壊れている可能性があります。アップデートファイルを再度入手してください。 |
| 34 | PIA がこのサーバに適合しません。 | このサーバ用のプラットフォーム情報 (PIA) ではありません。アップデートファイルを再度入手してください。 |

その他

本製品を用いたリモートKVMコンソール・監視・管理できない場合は、修理に出す前に次の内容に従ってチェックしてください。各項目にある症状に当てはまるものがあるときは、その後の確認、処理に従ってください。尚、システム全般におけるトラブルにつきましては、本体装置に添付のユーザズガイドを参照してください。

該当する項目がない場合や、「対策」を行っても症状が改善しない場合は、保守サービス会社に連絡してください。

❓ 本カードを実装後 POST で警告のメッセージが表示されるようになった。

「リモートマネジメントカードの初期設定」を行いましたか？

→ 本体装置のユーザズガイドにてメッセージを確認してください。

対応した装置情報が書き込まれていない可能性があります。

本体装置添付のEXPRESSBUILDERを起動し、「ツールメニュー」から「リモートマネジメントカードの初期設定」を選択し、本体装置固有の情報を本製品に読み込んで下さい。

❓ 管理 PC から本体装置が認識できない。

「リモートマネジメントカードの初期設定」を行いましたか？

→ 本体装置添付のEXPRESSBUILDERを起動し、「ツールメニュー」から「リモートマネジメントカードの初期設定」を選択し、本体装置固有の情報を本製品に読み込んで下さい。

管理 PC には Java2 Runtime Environment, Standard Edition 1.4.2_04 以降が適用されていますか？

→ Java2 Runtime Environment, Standard Edition 1.4.2_04 以降が必要です。以下の場所よりインストールできます。

インストールしたい管理 PC 上で、Windows を立ち上げ CR-ROM に基本装置添付のEXPRESSBUILDER をセットします。

Autorun 機能によりマスターコントロールメニューが表示されます。

「ソフトウェアのセットアップ」－「DianaScope」の順にクリックする

DianaScope のインストールメニューの中に、JRE のインストールのインストーラがありますので、こちらを実行してください。

※最新の Java Runtime をインストールするときは、以下の場所よりダウンロードしてください。
<http://java.sun.com/j2se/>

マネージメントカード本体と管理用ネットワークカードが内部ケーブルによって接続されていますか？

→ カード間接続コネクタに内部ケーブルを使いカード間を接続されているか確認してください。

LAN/ICMB ケーブルが正しく接続されていますか？

→ LAN/ICMB ケーブルの接続状態を確認してください。ケーブルが正しく接続されていないと本体装置のセンサを正しく参照することができません。
また、接続については、誤ってサーバ本体の LAN コネクタやシリアルポートコネクタに接続していないことを確認してください。

IP アドレスが重なっていませんか？

→ 管理用 LAN ポートの IP アドレスは出荷時、192.168.1.1 に設定されております。同一ネットワーク上に同一の IP アドレスがあると正常に認識されませんので IP アドレスの変更を行ってください。

ESMPRO/ServerAgent において本体装置の監視設定がされていますか？

→ESMPRO/ServerAgent の設定を変更してください。設定方法は Windows コントロールパネルの ESMPRO/ServrAgent を起動し、「システム」タブの [Express5800 本体装置]- [監視する]チェックボックスをチェックしてください。（デフォルトの設定は「監視しない」に設定されています。） 設定変更後、自動的に本体装置の監視が開始されます。 設定変更後サーバを再起動する必要はありませんが、本体装置が参照できない場合はツリーの再構築を実施してください。

ファイヤーウォールやゲートウェイで接続制限されていませんか？

→ファイヤーウォールなどの接続制限に引っかかっている可能性があります。
LANクロスケーブルにて直接クライアントPCを接続し接続問題が解決する場合には、ファイヤーウォールやゲートウェイなどを再確認してください。

 Web のリモート KVM コンソールの画面に、本体装置のコンソール画面が現れない。

本体装置の解像度設定は正しいですか？

→本製品で本体装置画面を表示する場合は、解像度 1024x768,リフレッシュレート 75Hz 以内に収まるように適切な画面設定を行ってください。

本体装置の OS が Windows の場合、専用のビデオドライバの組み込みを行いましたか？

→本体装置に専用のビデオドライバが必要となります。
本体装置のユーザーズマニュアルを参照し、添付されております EXPRESSBUILDER よりビデオドライバを組み込む必要があります。本体装置のユーザーズマニュアルを参照願います。

- 本体装置の OS が Linux の場合、テキストモードで使用していますか？
 → X-Window などグラフィック画面表示を行うとモニタ/ドライバ/ビデオメモリの設定により表示できない場合があります。テキストモードでの運用を、お勧めします。
- Linux 対応については、『8 番街』：<http://nec8.com/> の “Linux on Express5800” から最新/詳細情報を取得してください。

- ❓ WEB ブラウザからリモートマネージメント機能を利用する際のログイン名/パスワードを忘れてしまった。
 → ログイン名やパスワード設定を忘れてしまったときにジャンパ実装位置を変更することにより、パスワードを含む各設定を工場出荷時の状態に戻すことができます。

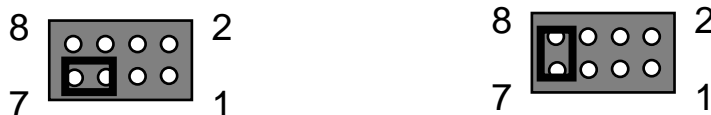


本体装置にバンドルされております管理ソフト DianaScope をご使用の場合は、DianaScope で設定された項目も本操作にてクリアされます。
 DianaScope をご使用の場合には、本操作を行う前に DianaScope の設定情報のバックアップを行って下さい。

手順

1. 本体装置の電源を OFF し、電源コードをコンセントから抜く。
2. マネージメント カード本体の設定クリア用コネクタ(2 ページを参照)に実装しているジャンパを以下のように変更する。

出荷時のジャンパ実装位置 → パスワードクリア実行時のジャンパ実装位置



3. 電源コードを接続する。
4. 電源を OFF のまま、30 秒以上待った後、電源コードをコンセントから抜く。
5. もう一度ジャンパ位置を出荷時の位置に戻します。各種設定が初期設定値に戻りますので、再度設定してください。

1. Overview

This chapter describes the overview of the Advanced Remote Management Card. N8115-02 Advanced Remote Management Card consists of two cards, and realizes a server monitoring feature and a remote KVM feature



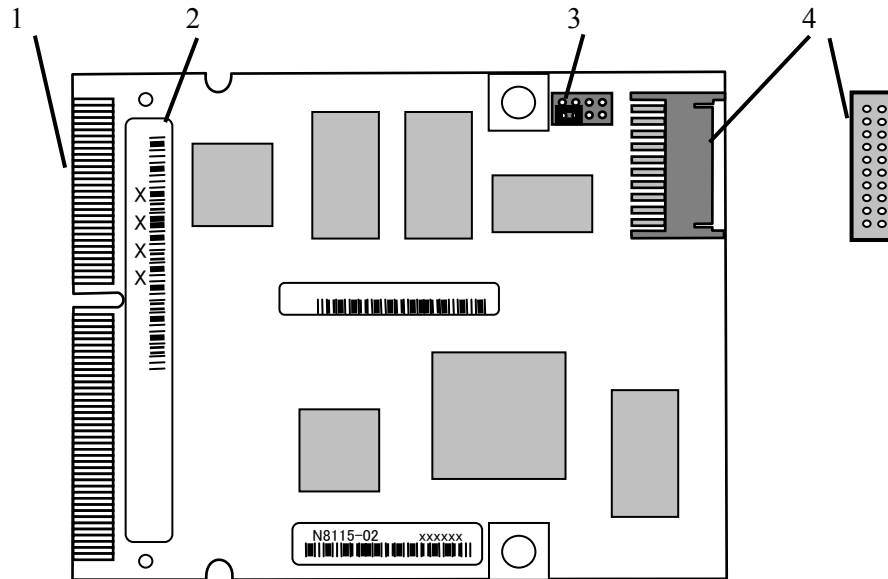
The screen which can be displayed by the remote KVM side becomes resolution 1024x768 and less than refresh rate 75Hz.

Since a screen is not displayed by remote PC when a setup beyond this is performed, please set it as less than this.

Moreover, if many numbers of colors of a screen are set up, an exact color may be unable to be displayed by remote PC.

When this product is connected to the network where broadcasting occurs frequently, the performance about remote control may be affected.

MANAGEMENT MAIN CARD



1. Card edge connector

A Management main card is installed in the connector of exclusive use of a server.

Please refer to the user's guide in your server to mount it since the connector position and the route of an internal cable is different in each server.

2. MAC (Media Access Control) Address

The Media Access Control Address used with this card is shown.

Since this is used as a part of host name when using DHCP server, please write down and place.

3. Clear Jumper

Jumper to reset settings .Login of the remote management function used from a WEB browser when you forget a password setup, by changing a jumper mounting position, it can return to the value at the default settings.



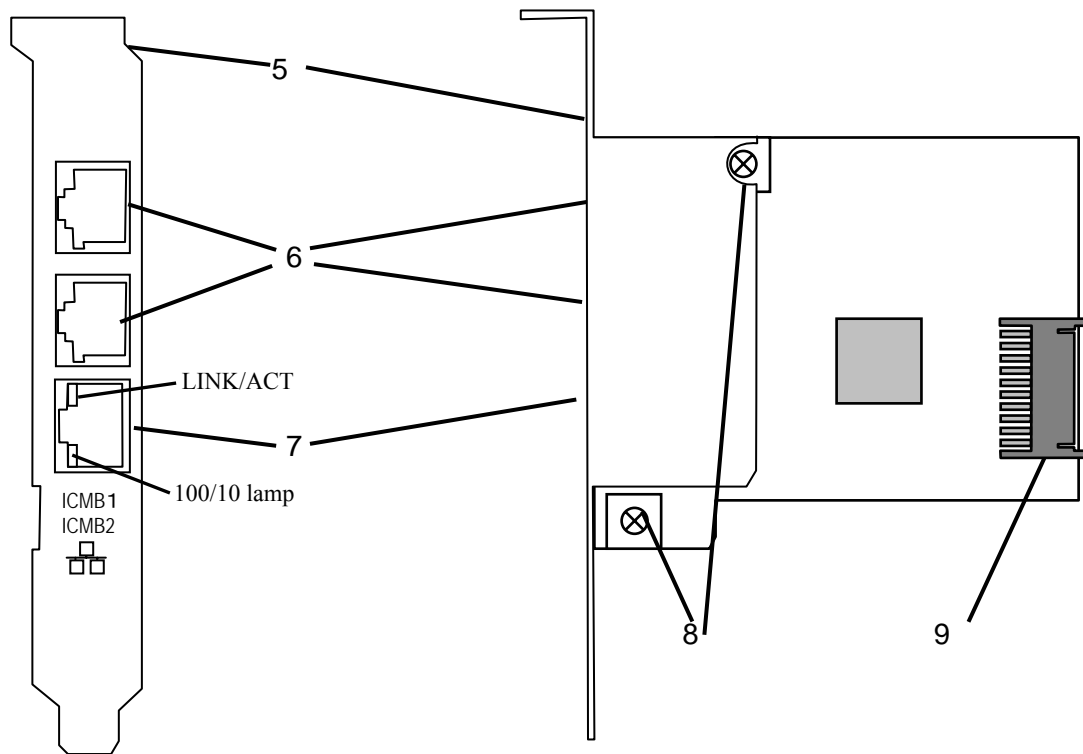
Please do not mount in any places other than the appointed place.

In this case, the responsibility cannot be taken about the influence of the result which equipment and parts damaged or employed.

4. Cards Connection connector

It is a connector for connecting between the cards of an Advanced Remote Management Card (two pieces). Please connect each other by the attached internal connection cable.

MANAGEMENT LAN CARD



5. The rear panel for PCI slot attachment

At the time of shipment, the rear panel of a full height type is attached for PCI slot fixation. Please change to the attached PCI rear panel type of low profile for fix to the slot of a low profile. Since a PCI bus is not used, there are no restrictions by the kind of PCI bus. Please mount in a vacant PCI slot.

6. ICMB-1(Upper)/ICMB-2(lower) connector

The ICMB (Intelligent Chassis Management Bus) connector is connected to a device having the ICMB interface.

You may connect an ICMB cable to whichever among two ICMB connectors.

7. Management LAN Port

This connector is connected with a network system on LAN. This port can be operated through 100Base-TX or 10Base-T interface. Also this port is used when using the NEC DianaScope of the utility appended to the server.

-LINK/ACT lamp

The LINK/ACT lamp shows the LAN access status.

- 100/10 lamp

The 100/10 lamp indicates the LAN transfer rate. Amber lamp is 100Mbps.

8. Screw for Rear Panel Fixation

There are screws that connect a rear panel and Card.

At the time of the exchange to a low profile type, these two screws are removed and exchange of a rear panel can be performed.

9. Cards Connection connector

It is a connector for connecting between the cards of an Advanced Remote Management Card (two pieces). Please connect each other by the attached internal connection cable.

DEFAULT NETWORK SETTINGS

When linking this Advanced Remote Management card to a network, refer to the following for default settings.

| | |
|-------------------|--------------------------|
| IP Address | :192.168.1.1 |
| User Name | :administrator |
| Password | :(None) |
| Host Name | :ARMCXXXXXXXXXXXX |

★Using a DHCP function, the host name in the case of performing automatic registration to a DNS server turns into the above-mentioned host name.

Host Name: ARMCXXXXXXXXXXXX, where the 12Xs are the MAC address of the Management Main Card. (Refer to item2 of Page62)

★When you link without a DHCP server, please access the above-mentioned IP address in the local network which can use a default IP address "192.168.1.1."

If default IP (192.168.1.1) cannot be used in your network.

Please boot NEC EXPRESSBUILDER CD-ROM from the server to set the IP Address at offline.

Select NEC EXPRESSBUILDER Main Menu [Tools]-[System Management]-[Set System Management Parameters]-[Configuration]- select "new" or "Change"-[LAN1]-edit IP Address and save settings(BMC Configuration Menu - OK).



For security reasons, change these default settings(Password, an IP address ,host name)by the your network environment. Refer to the chapter 5 for the setting method.

2. Installation

This chapter describes the installation procedures of the Advanced Remote Management Card and the notes on the installations. Some steps might require the use of the User's Guide that comes with your Advanced Remote Management Card and server.



. The user can install or remove the Advanced Remote Management Card in or from the server. If so, NEC assumes no liability for any damage of the Advanced Remote Management Card and the server and the results from the system operation. It is recommended to ask a maintenance engineer of your sales agent having the expert and detailed knowledge on the system to install or remove the Advanced Remote Management Card.

Use cables authorized by NEC. Repair of the Advanced Remote Management Card due to a failure or damage resulted from use of cables unauthorized by NEC will be charged.

Safety Precautions

Always observe the following cautions to install or remove the Advanced Remote Management Card in or from the server safely.

| ⚠ WARNING | |
|------------------|---|
| | <p>Observe the following instructions to use the Advanced Remote Management Card and server safely. Failure to follow these instructions may result in death or serious personal injury. See the description on pages v through ix for details.</p> <ul style="list-style-type: none">■ Do not disassemble, repair, or modify the Advanced Remote Management Card and server by yourself.■ Disconnect the power plug before working with the server. |

| ⚠ CAUTION | |
|------------------|--|
| | <p>Observe the following instructions to use the Advanced Remote Management Card and server safely. Failure to follow these instructions may cause personal burn or injury and/or physical damages. See the description on pages v through ix for details.</p> <ul style="list-style-type: none">■ Do not attempt to lift the server only by yourself.■ Do not install the Advanced Remote Management Card halfway.■ Do not pinch your fingers with components.■ Take note on a high temperature. |

Anti-static Measures

The almost electric components in the Advanced Remote Management Card and server are composed of electric parts easily affected by static electricity. In the installation or removal of the Advanced Remote Management Card, take sufficient note so that it may be damaged by static electricity.

- Wear a wrist strap (as arm band or anti-static glove).

Wear a wrist strap on your wrist. If no wrist strap is available, touch an unpainted metal part of the chassis before touching an Advanced Remote Management Card to discharge static electricity from your body. In addition, touch a metal part regularly when working with components to discharge static electricity.

- Select a suitable workspace.

- Work with the Advanced Remote Management Card and Server on the anti-static or concrete floor.

- When you work with the Advanced Remote Management Card and Server on a carpet where static electricity is likely to be generated, make sure take anti-static measures beforehand.

- Use a worktable.

Place the Advanced Remote Management Card and Server on an anti-static mat to work with it.

- Cloth

- Do not wear a wool or synthetic cloth to work with the Advanced Remote Management Card and Server.

- Wear anti-static shoes to work with the Advanced Remote Management Card and Server.

- Take off any jewels (a ring, bracelet, or wristwatch) before installing the Advanced Remote Management Card and Server.

- Handling of components

- Keep Advanced Remote Management Card in an anti-static bag until you actually install it to the Server.

- Hold an Advanced Remote Management Card by its edge to avoid touching any terminals or parts.

- To store or carry Advanced Remote Management Card, place it in an anti-static bag.

Preparing for Installation and Removal

Follow the procedure below to prepare for installing or removing components.

1. Shut down the OS in the server.
2. Turn off the power of the server.

Refer to the User's Guide of the server for turning off the power of the server.

3. Unplug the power cord of the server.

4. Prepare a proper Phillips driver. It is not required for the installation or removal of cable connection or disconnection.



Since an "ARMC and MAC Address" is used for a host name when using a DHCP function and performing automatic registration to a DNS server, we recommend you to copy the number of the Media Access Control Address seal stuck on the main part of a management card. Refer to item2 of Page62.

INSTALLATION AND REMOVAL

Before the Advanced Remote Management Card can be installed or removed, the Server should be pulled out from the rack safely, Turn off the power and unplug the power cord. Details of how to pull out the Server from the rack, refer to the User's Guide that comes with the Server

CAUTION



Observe the following instructions to use the Server safely. Failure to follow these instructions may cause personal burn or injury and/or physical damages. See the description on pages v through xi for details.

- Do not leave more than one device being pulled out from the rack.
- Do not install the Server halfway.
- Do not pinch your fingers with components.
- Take care on a high temperature.
- Do not pull out a Server or other server from the rack if the rack is unstable.

INSTALLATION

A Management main card is installed in the connector of exclusive use of a server.

A Management LAN Card is fixed at PCI slot. Since a PCI bus is not used, there are no restrictions by the kind of PCI bus. Please mount in a vacant PCI slot. Please exchange rear panel to low profile rear panel, if you fix in the slot of a low profile.



Please be sure to perform Installation and Removal after pulling out the AC code and waiting 5 seconds or more.

The Advanced Remote Management Card includes electronic parts extremely sensitive to static electricity. Work with the Advanced Remote Management Card after touching a metal frame of the Server to discharge static electricity of your body.

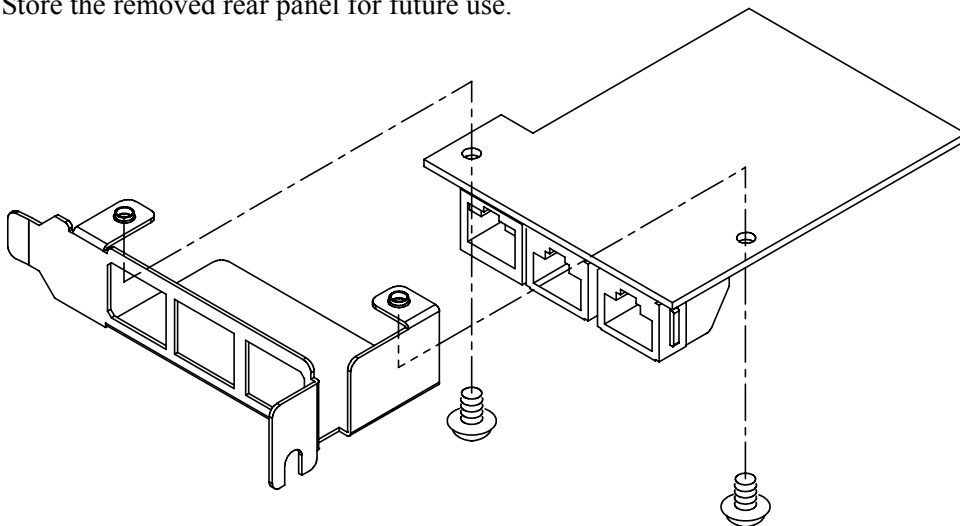
Do not make your bare hands contact with the terminals and components on the Advanced Remote Management Card. Do not put the Advanced Remote Management Card on a table directly. See the section "Anti-Static Measures" for details of the static electricity. Refer to Page67



When you install an Advanced Management Card, please check whether server is supporting it and check that the form and connector form of a connection portion of a card suit.

Install the Advanced Remote Management Card in the following procedure.

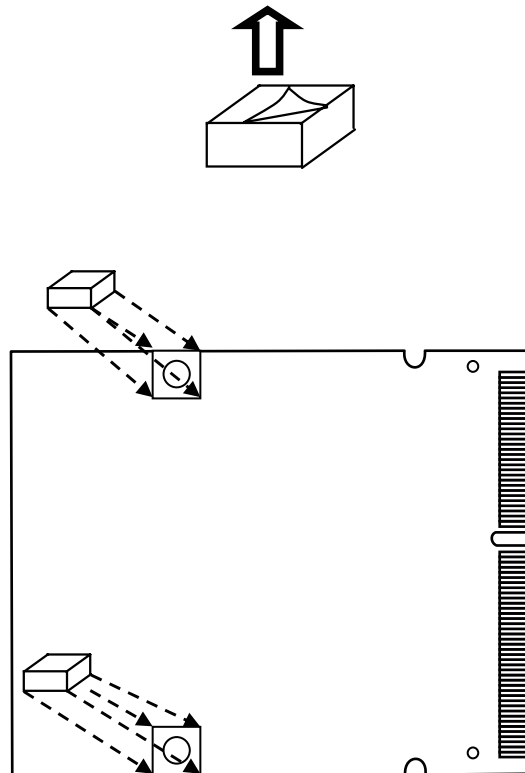
1. See the section "Preparing for Installation and Removal" to prepare.
2. With reference to user's guide of a server to mount, please remove a top cover and check the cable route and PCI slot to fix and a connector position on a Mother Board.
3. When the PCI slot which fixes the Management LAN Card determined. At the time of shipment, the rear panel of a full height type is attached for PCI slot fixation. Rear panel is fixed by two screws. Please change to the attached PCI rear panel type of low profile for fix to the slot of a low profile with the following procedure. Since a PCI bus is not used, there are no restrictions by the kind of PCI bus.
Store the removed rear panel for future use.



4. The spacer to the main management card should stick.

A spacer is stuck in order to avoid interference with the Main Management Card, and the mother board of the server. Please stick on the specified attachment position with reference to user's guide of server. When there is no specification in the server side especially, you must stick two spacers on a back location of the Management Main Card.

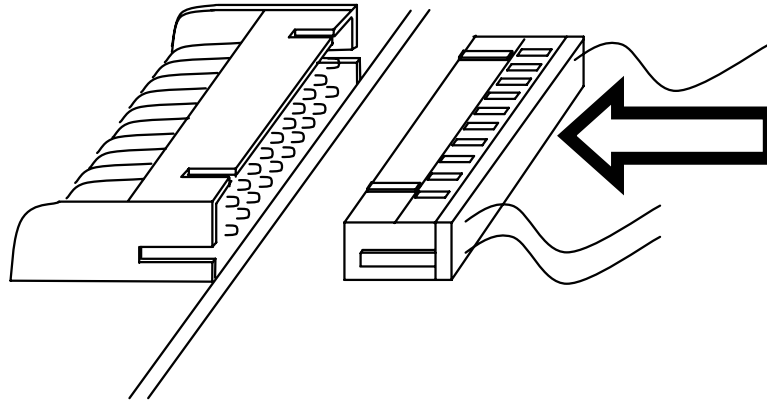
The protection sheet of an adhesion side is removed.



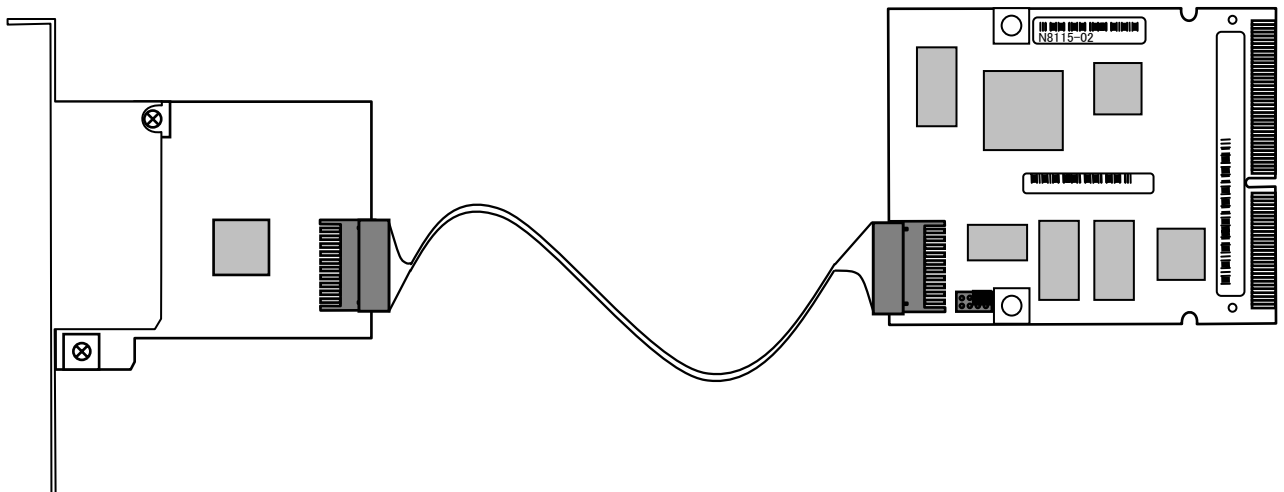
If a spacer is not stuck, interference may occur with a mother board and the Management Main Card by vibration, and failure and breakage of the server and the Management Main Card may occur. You have to stick two spacers certainly.

5. Connection of Internal Cable.

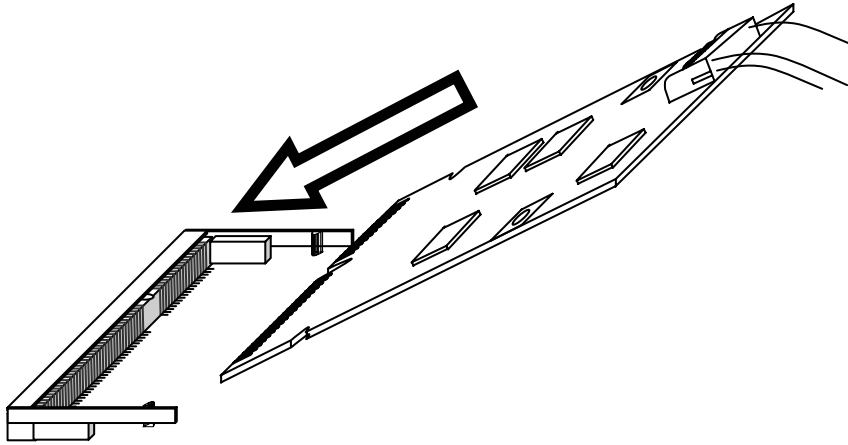
The Management LAN Card is connected with the Main Management Card by the Internal Cable. You may connect an internal connection cable and the combination of a connector to whichever. However, keep in mind that there is distinction of the connector upper and lower sides.



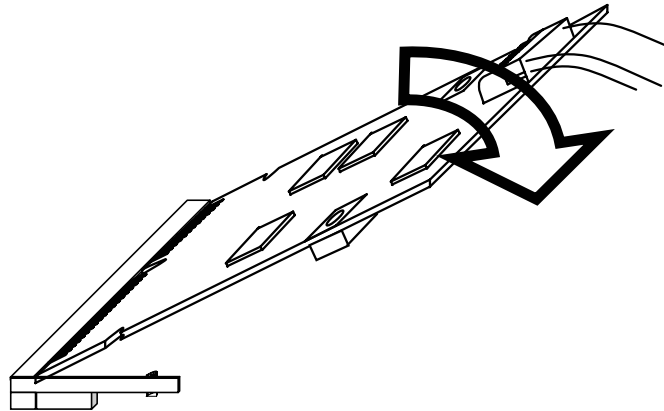
Internal cable connection between cards



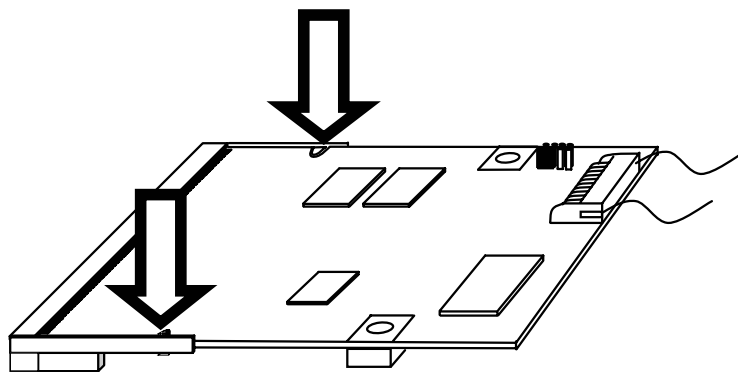
6. Install the Management Main Card to the mother board of the server.
It inserts in a connector, making the Management Main Card slanting.



It presses against a connector and a card is moved to a mother board position.



Please check being fixed by the projection in right and left of a connector.



7. Install the Management LAN Card to the PCI Slot.

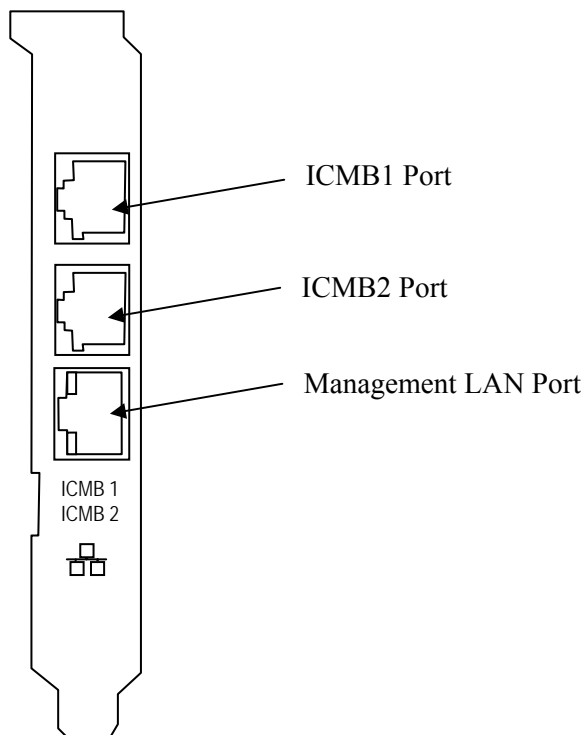
Check the route of the internal cable within the server, and remove the blank cover of a PCI slot. The Management LAN Card is fixed to the removed slot.

8. Connect the LAN/ICMB cable of external connection to the Management LAN Card .

When not connecting with ICMB correspondence apparatus, there is no necessity that an ICMB cable connects.

Management LAN Port is used when using the Remote Management Console.

Also this port is used when using the NEC DianaScope of the utility appended to the server.



When a card cannot be attached well, once you remove a card, please reattach. Keep in mind that there is a possibility of damaging a card if too much power is applied to a card.

REMOVAL

Removal of the Advanced Remote Management Card should remove by performing a procedure contrary to Installation.

3. Server Setup

This chapter explains the contents which must be carried out by the server side, when using an Advanced Remote Management Card by the server.

INITIAL SETTING OF ADVANCED REMOTE MANAGEMENT CARD

In order to realize the detailed surveillance for every servers, it is necessary to make different peculiar information for the server reflect in this Advanced Remote Management Card.

When the server is powered on, the system may be paused for a while by NEC Logo display or the following message display.

H/W Configuration of BMC is corrupted.

!!Update BMC H/W Configuration by configuration tool!!

!!Refer to BMC configuration manual!!

This message indicates the Advanced Remote Management Card need initialization (upload PIA/SDR) by NEC EXPRESSBUILDER. CD-ROM.

If the system is stopped by NEC Logo Screen, confirm whether this message is displayed at the Diagnostic Screen. The Diagnostic Screen is appeared by ESC key press.

If another message is displayed, refer to the User's Guide of the server.

If POST is resumed, it is continued by waiting for a while or Enter Key press.

Insert the NEC EXPRESSBUILDER CD-ROM into the CD-ROM drive to start the EXPRESSBUILDER.

If an EXPRESSBUILDER of server appending is started and "initial setting of a remote management card" is chosen from a "tool menu"- "Initialize Remote Management Card", a setup of server peculiar information (upload PIA/SDR) will be reflected automatically.

SETTING OF VIDEO DRIVER

- When a server's OS is Windows

When the server requires, it is necessary to install a video driver from EXPRESSBUILDER of the server appending. When there is a demand with reference to the user's guide of the server, please install a video driver from the server appending EXPRESSBUILDER. Unless it applies, the picture to Management PC may not be transmitted.

Refer to the user's guide of the server for the detailed information about video driver.

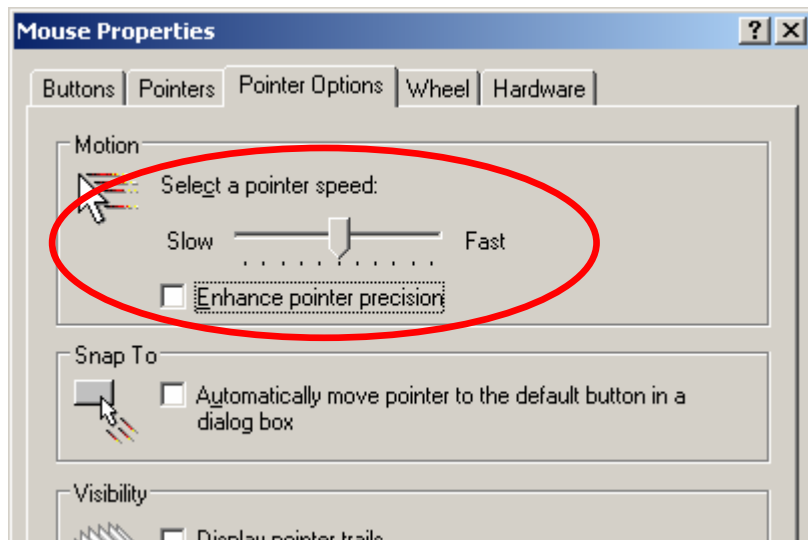
-When a server's OS is Linux

Since it may be automatic and a setup of a monitor/Driver/video memory may not be able to be performed by composition when OS is Linux. We recommend you to use it in text mode.

SETTING OF MOUSE PROPERTIES

Clear a check box of "Enhance pointer precision" in "Motion" in "Pointer Options" in "Mouse properties", when the server OS is Windows Server 2003.

Please adjust "Select a pointer speed", when you cannot move a mouse pointer up to the bottom right side of the host server screen via the remote KVM console.



4. Configuring Management PC

This chapter provides information on what you need to do for management PCs and requirements of the browsers in them to establish connection between them and server.

SETTING YOUR BROWSER

Make the following settings.

- Enable SSL.

SUPPORTED BROWSERS

The following browsers are supported.

- Microsoft Internet Explorer 6.0
- Netscape 7.0
- Mozilla 1.6

JAVA2 RUNTIME ENVIRONMENT

Java2 Runtime Environment, Standard Edition 1.4.2_04 or later, which you can install from EXPRESSBUILDER or download from the following, is required.

- (1) Boot Windows on the PC in which you want to install.
- (2) Insert the NEC EXPRESSBUILDER CD-ROM into the CD-ROM driver.

The master control menu will be displayed by the Autorun function.

Click [Software Setup]-[NEC DianaScope]

The DianaScope installation menu for Windows will appear.

There is JAVA Installer at Menu of NEC DianaScope Manager.

Please download it as follows if you want latest JRE(Java Runtime Environment) distributed free of charge by Sun Microsystems, Inc.

<http://java.sun.com/j2se/>

5. Using Remote Management Console

OVERVIEW

You can control power-on/off of a server and use Remote KVM Console from a web browser by using the web server functions of BMC.

This functionality is achieved through Java Applet.

CONNECTING TO THE WEB SERVER FROM A WEB BROWSER ON THE MANAGEMENT PC

Access the following URL from the web browser in the management PC.

URL: `http://BMC_HostPort/index.htm`



“BMC_HostPort” is a colon and port number added after the BMC address or host name.
If the http port number is 80h (default), you can skip a port number.



When you use DHCP functions as well as performing auto registration to the DNS server, the BMC default name is “ARMC”+MAC Address.
There is the MAC address on the Management Main Card. (See page 62)

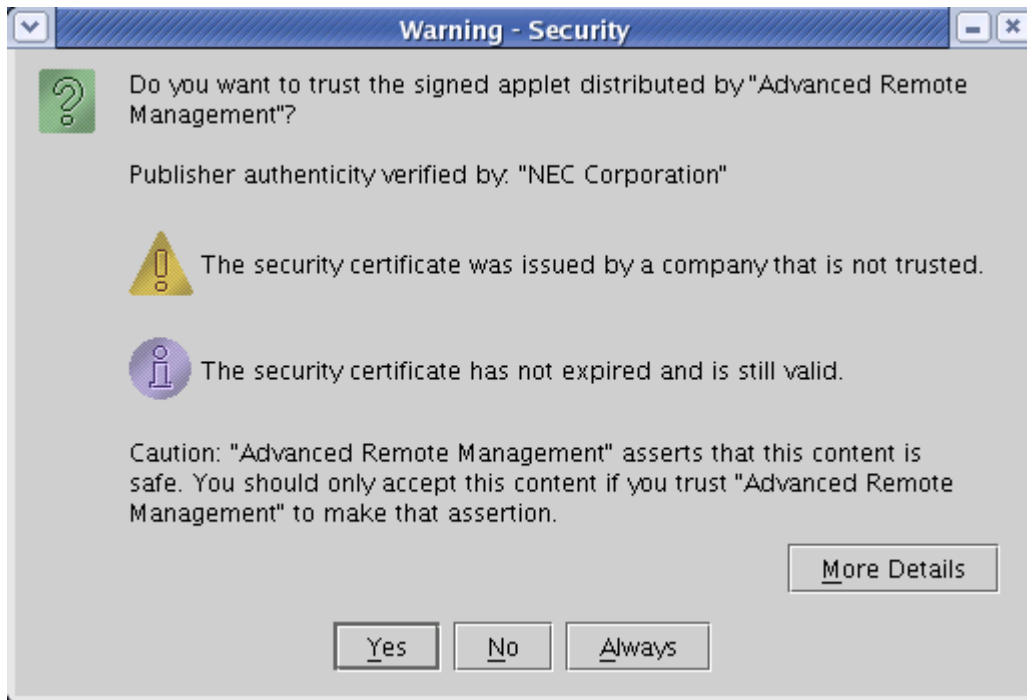
IP address: 192.168.1.1
User name: Administrator
Password : (none)
Host name: ARMC00004C9FXXXX

Default host name



- If you want to use the N8115-02 Advanced Management Card with DHCP disabled, first use the default IP address “192.168.1.1” and make access in a local network where this IP address is available, and then adjust configurations such as IP address according to your network environment. For information on configuration, see “BMC Configuration” described later in this chapter.
- If default IP (192.168.1.1) cannot be used in your network. Please boot NEC EXPRESSBUILDER CD-ROM from the server to set the IP Address at offline.
Select NEC EXPRESSBUILDER Main Menu [Tools]-[System Management]-[Set System Management Parameters]-[Configuration]-select “new” or “Change”-[LAN1]-edit IP Address and save(BMC Configuration Menu - OK).

When you use the N8115-02 Advanced Management Card for the first time, you may see a dialogue box for security warning as shown below. Read the message well and click either “Yes” or “Always.” If you are not sure about the information, select “No.”



When a connection is done with SSL, you may see some dialogue boxes for security warning.

LOGIN AND LOGOUT

Login

When the login page appears, enter the user name and password, and then click [Login].

If you are logging in for the first time, use the following default user name and password.

Default user name : administrator

Default password : None (enter no information)

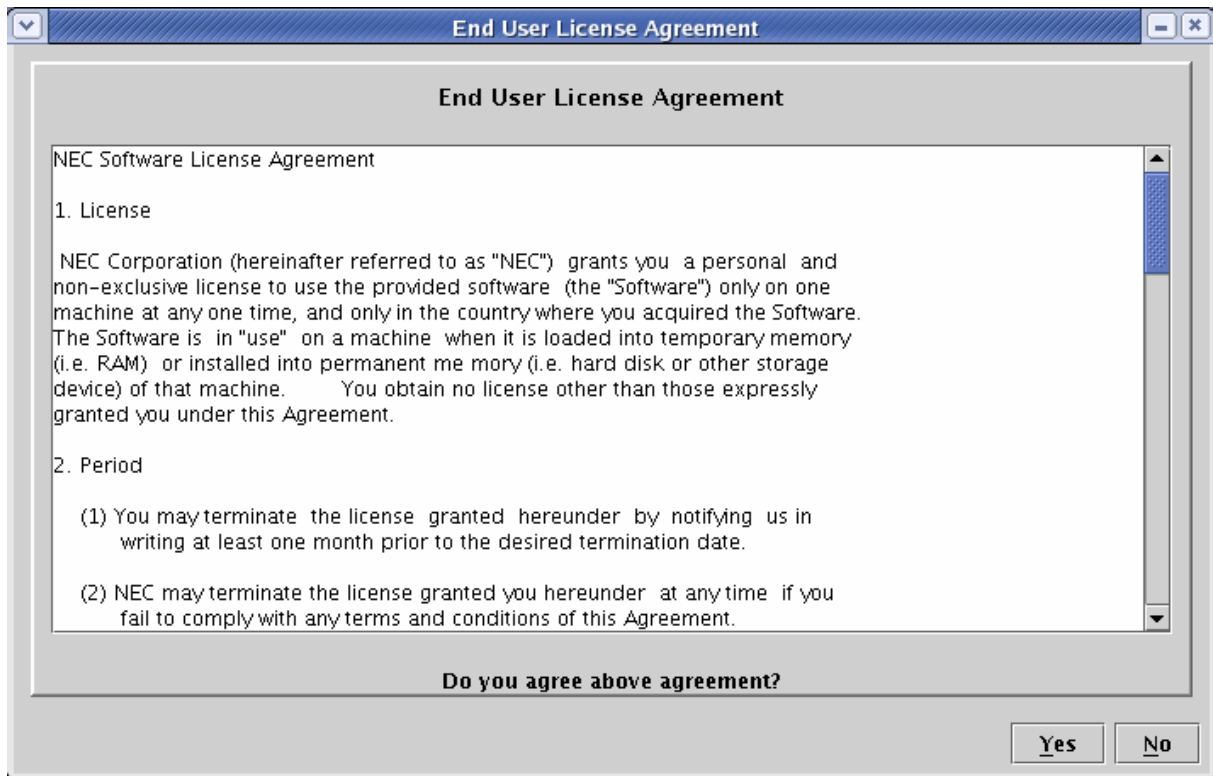


Because no password is set by default, make sure to configure a password immediately after you log in.

For security reasons, it is recommended to change the default user name as well.

For information on configuration and modification, see “BMC Configuration” described later in this chapter.

When the password you entered is authorized, the following licensing agreement appears.



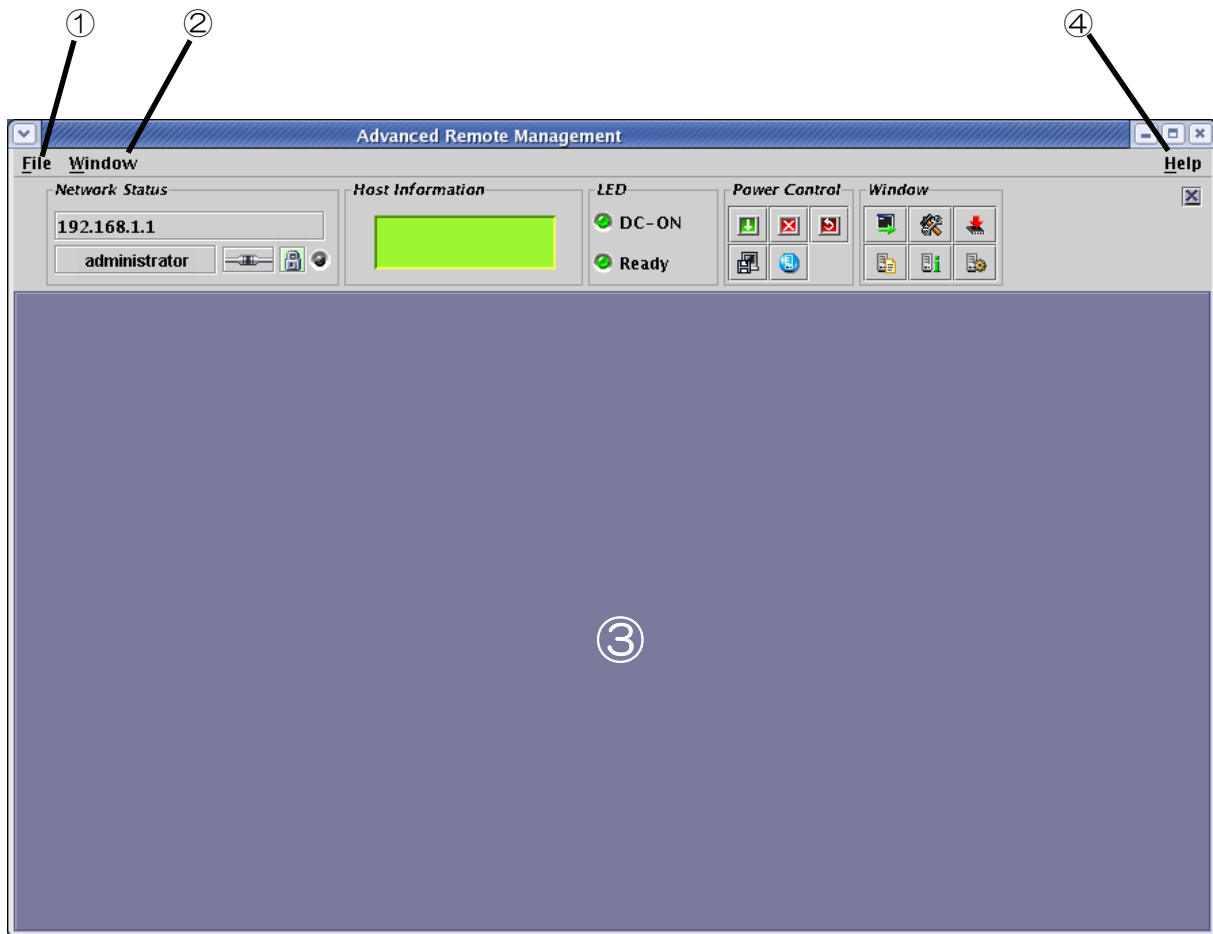
Read the information well and click "Yes" If you cannot agree, click "No", and you will return to the login window.

Logout

To log out, select "Exit" on the File menu.

When you log out, the main window closes and the login window for the browser appears.

MAIN WINDOW



① File menu

The File menu allows you to quit this applet.

② Window menu

The Window menu allows you to open various windows including Remote KVM Console window.

③ Main frame

Various windows open here.

④ Help menu

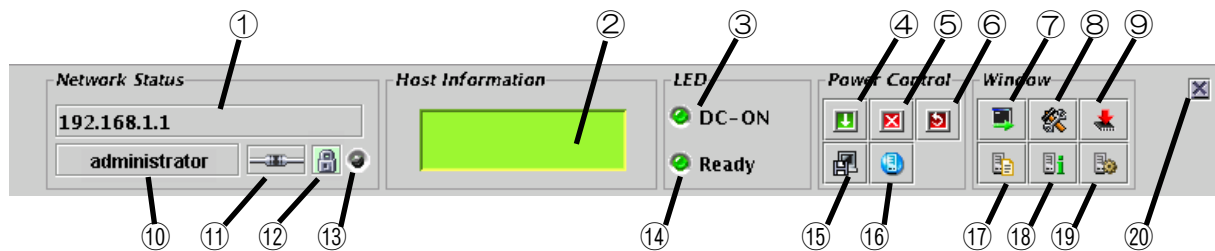
With the Help menu, you can check the version of this applet.

CONTROL PANEL

You can use Control Panel to see server status and to control power-on/off.

Control Panel also starts up various windows including Remote KVM Console.

Functions of Control Panel



- ① Shows the BMC host name.
- ② Shows the server LCD.
- ③ Server power lamp that shows the server power-supply status.
- ④ Server power switch (provides the same function as achieved by pressing the server POWER switch)
- ⑤ Forcefully powers off the server.
- ⑥ Forcefully resets the server.
- ⑦ Starts up Remote KVM Console.
- ⑧ Starts up BMC Configuration.
- ⑨ Starts up Firmware Update.
- ⑩ Displays a user name.
- ⑪ Indicates status of connection with BMC.
- ⑫ Indicates status of communication security.
- ⑬ Indicates network access status.
- ⑭ Server status lamp that shows server status.
- ⑮ Makes the server collect memory dump (provides the same functionality as achieved by pressing the DUMP switch in the server.)
- ⑯ Makes the server unit ID lamp flash.
- ⑰ Opens the window to show system event logs (SEL.)
- ⑱ Opens the window to show sensor data records (SDR).
- ⑲ Opens the window to show field replaceable unit (FRU) information.
- ⑳ Hides Control Panel.

REMOTE KVM CONSOLE

By using Remote KVM Console functions of BMC, you can transfer local console of a server to the browser in the management PC over network.

You can make full access from the management PC to the server by using video, keyboard and mouse.



The following five types of resolution are supported for a server.

1024×768
800×600
640×480
720×400
720×350




KVM is an acronym for Keyboard, Video, and Mouse.

Unlike using a conventional serial console remotely, KVM allows you to remotely use graphics as they are.



The remote KVM console cannot be used for connection via proxy.

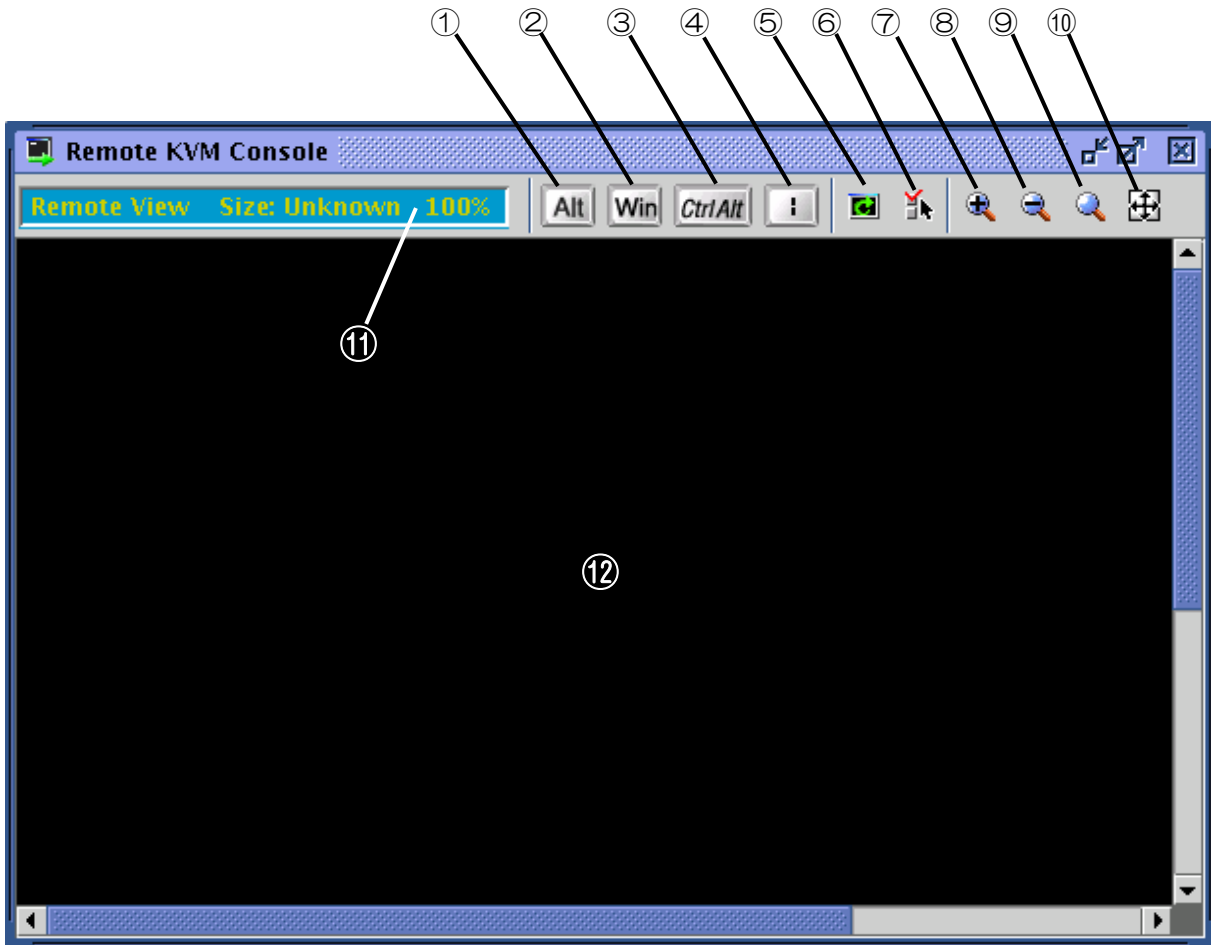
Starting up Remote KVM Console

When you click [], the icon to start up Remote KVM Console, on Control Panel, the Remote KVM Console window opens.



Never open Remote KVM Console if you have logged in BMC of the local server from the local console of a server. Otherwise entry by keyboard or mouse becomes disabled.

Names of components in the Remote KVM Console window



- ①, ②, ③, ④ Special key icon
- ⑤ Screen refresh icon
- ⑥ KVM properties icon
- ⑦ Zoom in icon
- ⑧ Zoom out icon
- ⑨ Default size icon
- ⑩ Window resize icon
- ⑪ KVM indicator
- ⑫ Remote KVM Console screen





When pressing Shift + CapsLock or NumLock on the remote KVM console, the indication may not be the same as the CapsLock or Numlock LED on the management PC. In addition, the CapsLock or NumLock status on the Server may change after the remote KVM console has been used.

In that case, please try to push the key from the target system and match a state of LED and actual operation.

Entry via special keys

For special keys, even if you press these keys in a remote keyboard, it will not take effect in the host server. Using the following three special key icons will take effect in the host server.

 (raised state) and  (pressed-in state) : toggles whenever clicked.

 (raised state) and  (pressed-in state) : toggles whenever clicked.





For example, to enter “Ctrl+Alt+Del” , press the [Ctrl+Atl] icon and press the Del key on your keyboard. By doing so “Ctrl+Alt+Del” takes effect in the host server. When this takes effect, click the [Ctrl+Atl] icon again to release the effect of entry of this special key.


 (Windows key icon)


 (“|” pipe key icon)

Zoom in and zoom out


When you click  to zoom in, what is shown becomes larger.

When you click  to zoom out, what is shown becomes smaller.


When you click , the default size icon, what is displayed will be the same size as the host server.

When you click , the window resize icon, the size of the Remote KVM Console window is adjusted to the remote screen size.

Screen refresh

When you click , the screen refresh icon, the Remote KVM Console screen will be refreshed. When the screen display is disturbed, refresh the screen.

Modifying properties

When you click , the KVM properties icon, the KVM properties window appears. In this window, you can specify the screen refresh interval which is executed automatically.

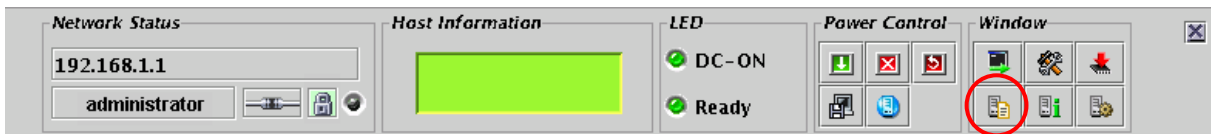


By having a shorter refresh interval, garbage on the screen will be reduced. However, note that screen refresh will give burden. A too short refresh interval can slow response speed of terminals or affect traffic performance of the network.

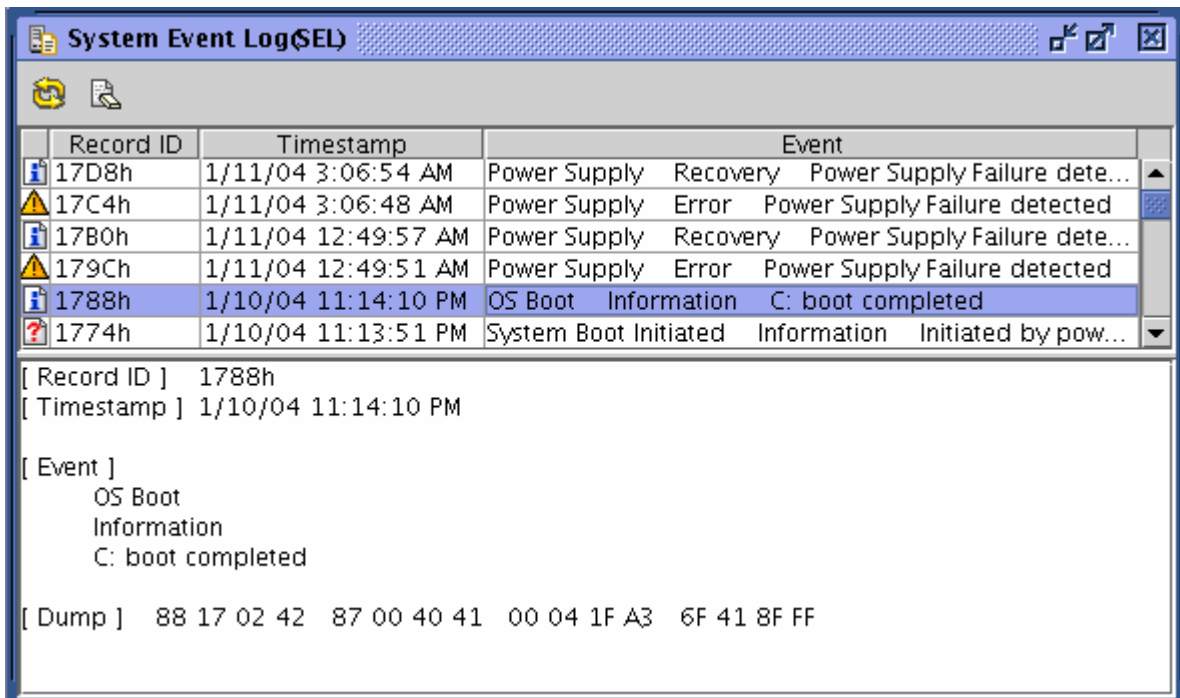
IPMI INFORMATION

You can see system event logs (SEL), sensor data records (SDR), and field replaceable units (FRU) information, which are called IPMI information. By using the IPMI information, you can see and examine troubles and events on the host server, and determine a part to be replaced.

Displaying System Event Logs (SEL)



When you click [SEL] to display system event logs (SEL) on Control Panel, SEL information is loaded from BMC, and the following window showing system event logs (SEL) opens.



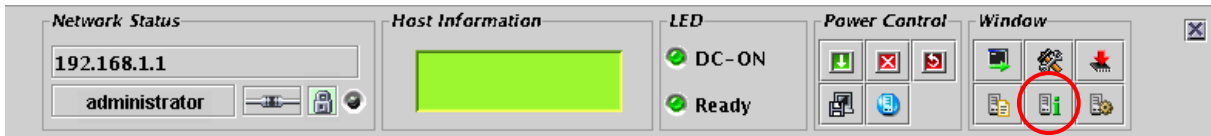
On the upper part of the window, a list of logs appears. On the lower part of the window, detailed information of the entry selected from the list appears.


When you click [Refresh] for reloading, the SEL information is reloaded from BMC, and you can update the information to latest.

Clearing SEL information

You can clear the SEL information on BMC by clicking [Clear], the icon for SEL clearing. When you see the message for confirmation, click [Yes] if you want to clear SEL. If not, click [No] so that SEL clearing will not be performed.

Displaying Sensor Data Records (SDR)



When you click  to display sensor data records on Control Panel, SDR information is loaded from BMC, and the following window showing sensor data records appears.

Sensor Data Record(SDR)

| Record ID | Sensor Type | Owner |
|-----------|---------------------------|------------------|
| 1h | Voltage(Processor 1 VCCP) | Basbrd Mgmt Ctlr |
| 2h | Voltage(Processor 2 VCCP) | Basbrd Mgmt Ctlr |
| 3h | Voltage(Baseboard 3.3V) | Basbrd Mgmt Ctlr |
| 4h | Voltage(Baseboard 3.3VSB) | Basbrd Mgmt Ctlr |
| 5h | Voltage(Baseboard 5V) | Basbrd Mgmt Ctlr |
| 6h | Voltage(Baseboard 5VSB) | Basbrd Mgmt Ctlr |
| 7h | Voltage(Baseboard 12V) | Basbrd Mgmt Ctlr |
| 8h | Voltage(Baseboard VBAT) | Basbrd Mgmt Ctlr |

[Record ID] 1h
 [Sensor Type] Voltage(Processor 1 VCCP)
 [Entity] Processor1
 [Owner] Basbrd Mgmt Ctlr
 [Upper non-recoverable Threshold] ---
 [Upper critical Threshold] 1.64Volts (Hysteresis: 1.63Volts)
 [Upper non-critical Threshold] 1.56Volts (Hysteresis: 1.55Volts)
 [Lower non-critical Threshold] 1.15Volts (Hysteresis: 1.16Volts)
 [Lower critical Threshold] 1.06Volts (Hysteresis: 1.07Volts)
 [Lower non-recoverable Threshold] ---

[Dump]
 01 00 51 01 3B 20 00 10 03 01 7F E9 02 01 85 32
 85 32 1B 1B 00 04 00 00 EB 42 07 01 00 B4 07 82
 B0 5B FF 00 00 BF B0 00 49 5B 02 02 00 00 00 D0
 50 72 6F 63 65 73 73 6F 72 20 31 20 56 43 43 50

On the upper part of the window, a list of sensor data records appears. On the lower part of the window, detailed information of the entry selected from the list appears.

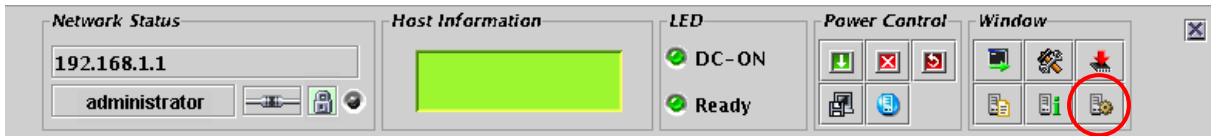



Tips

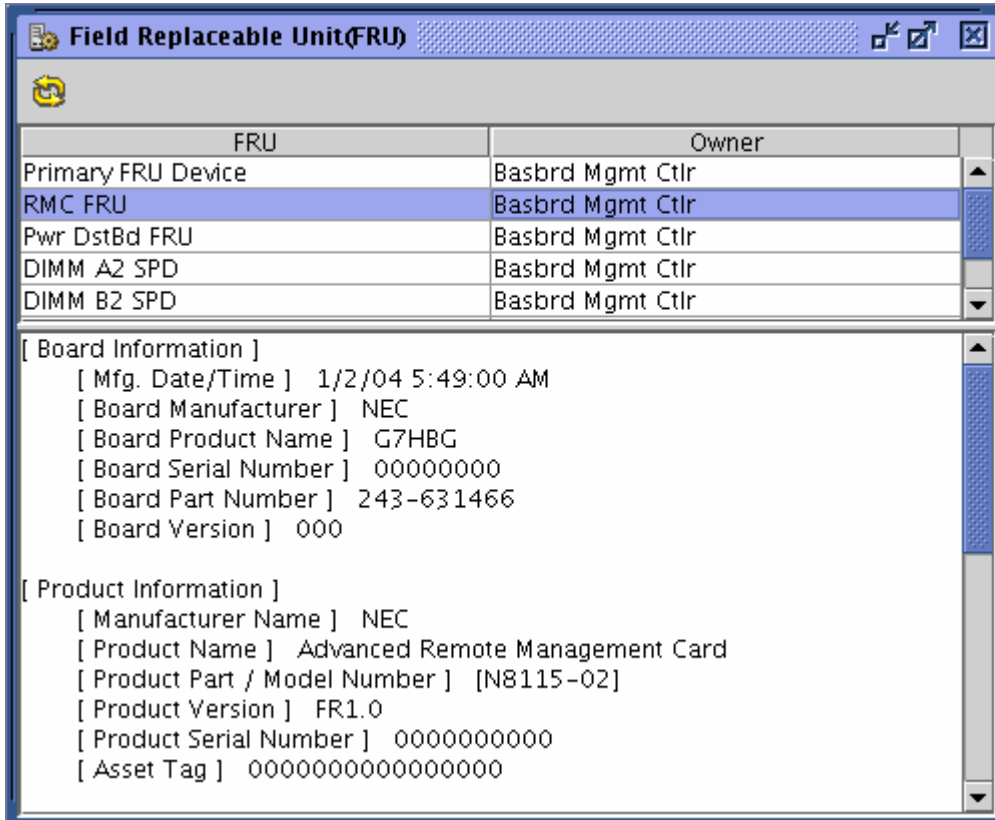
SDR information is information on definitions for each sensor on the server.

BMC monitors server sensors according to this information.

Displaying Field Replaceable Units (FRU) information



When you click [] to display field replaceable units (FRU) information on Control Panel, FRU information is loaded from BMC, and the following window showing field replaceable units (FRU) information appears.

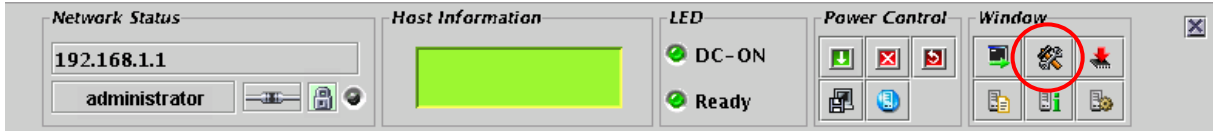



On the upper part of the window, a list of FRUs appears. On the lower part of the window, detailed information of the entry selected from the list appears.

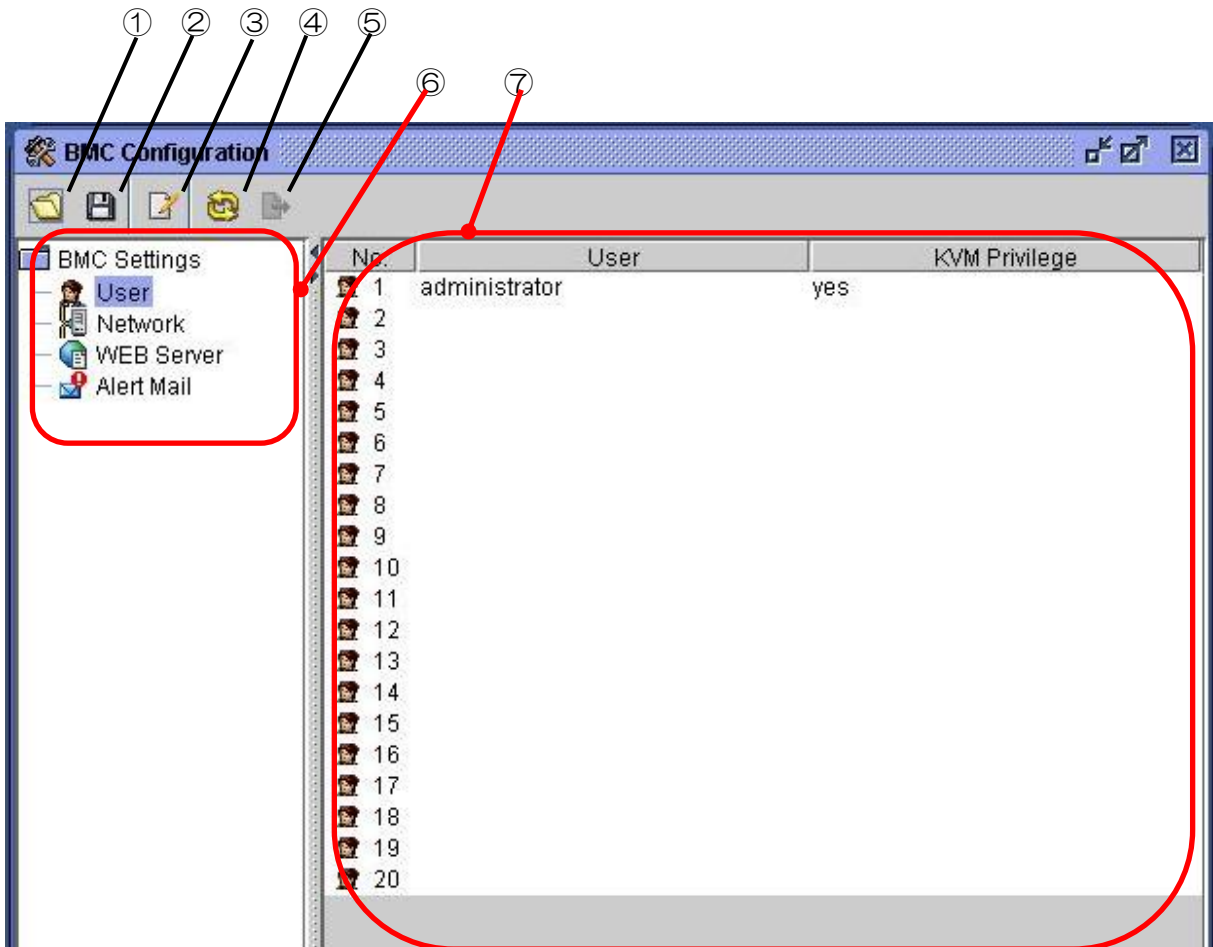
BMC CONFIGURATION

You can configure BMC settings.

Starting up the BMC Configuration window



When you click [], the icon to start up BMC Configuration on Control Panel, the BMC Configuration window appears as shown below.



- ① Loads a file
- ② Saves the file
- ③ Edits information
- ④ Reloads from BMC
- ⑤ Makes global settings of BMC
- ⑥ Item selection tree
- ⑦ Currently configured values



Use “Global settings of BMC” when configuration information is loaded from a file.

User Configuration

By clicking [User Configuration] in the left pane of the BMC Configuration window, a list to show 20 accounts opens in the right pane and you can set up user accounts.

Choose the account you want to modify or add and click [✎] to edit information. The User Configuration window to edit a user account as shown below opens.

The screenshot shows a 'User Settings' dialog box with the following fields and options:

- No.:** 1
- Username:** administrator
- Password:** *****
- Password(Confirm):** *****
- KVM Privilege:** Remote KVM Console Enable

Buttons: OK, Cancel

- ① Enter a user name.
- ② Enter a password. To avoid a mistake, enter a password in two boxes.
- ③ Configure an access privilege.

Remote KVM Console: Specify whether or not to enable Remote KVM Console.

If you select this check box, you can make Remote KVM Console enabled (permit) settings.

When you click [OK], all the information in the User Configuration window will be written into BMC.

When you click [Cancel], the User Configuration window closes discarding what you have configured in the window.

Network Configuration

The ports listed below are used for remote management.

If your network has a firewall, provide setting for firewall appropriately.

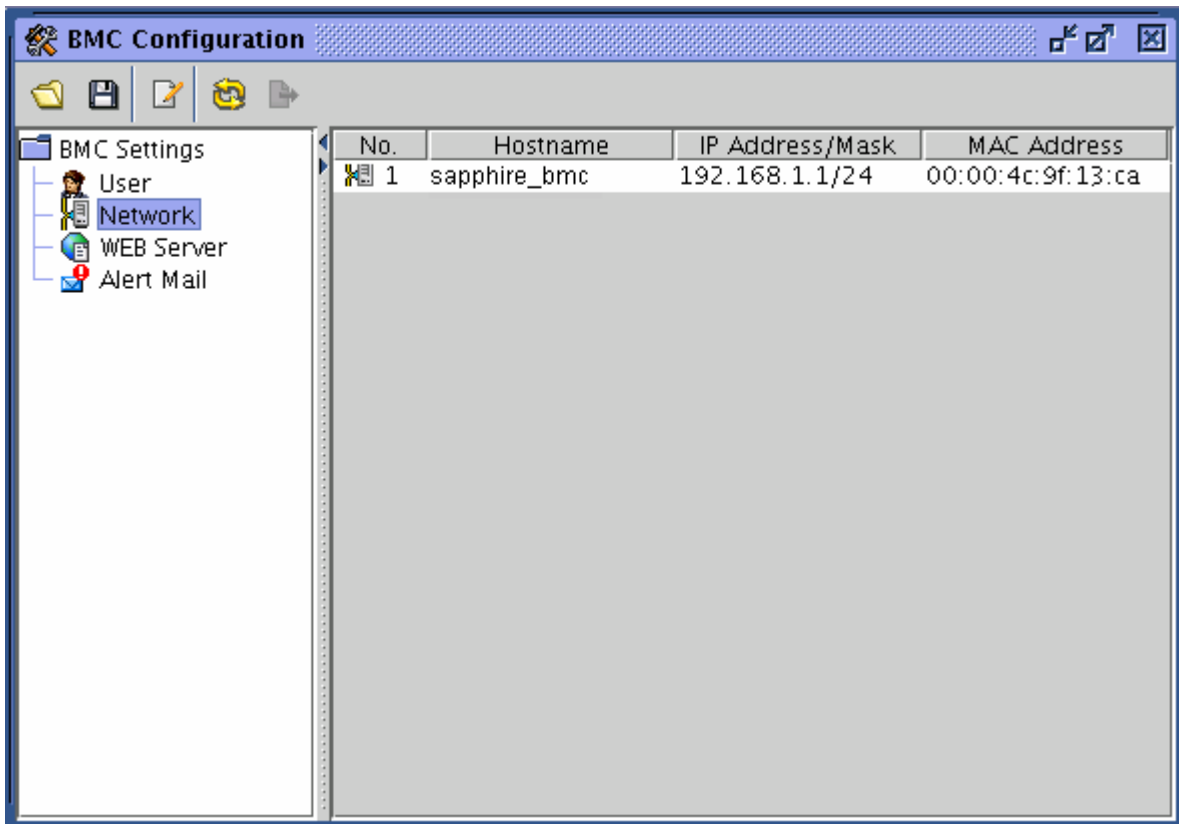
| Module name | Port number | Protocol | Direction | Module name | Port number |
|-------------------|-------------|----------|-----------|-------------|-------------|
| Remote KVM client | Undefined | UDP | ↔ | BMC | 623 |
| Mail server | 25(*1) | TCP | ↔ | BMC | Undefined |
| WEB client | Undefined | TCP | ↔ | BMC | 80(*2) |
| WEB client(SSL) | Undefined | TCP | ↔ | BMC | 443(*3) |

*1:To change the port number, select [BMC Settings]→[Alert Mail]→[E-Mail Alert Settings]→[SMTP]→[SMTP Port Number].

*2:To change the port number, select [BMC Settings]→[WEB Server]→[WEB Server Settings]→[HTTP Port Number].

*3:To change the port number, select[BMC Settings]→[WEB Server]→[WEB Server Settings] → [SSL Port Number].

By clicking [Network Configuration] in the left pane of the BMC Configuration window, you will see a window as shown below and you can make network-related settings for BMC including IP address.

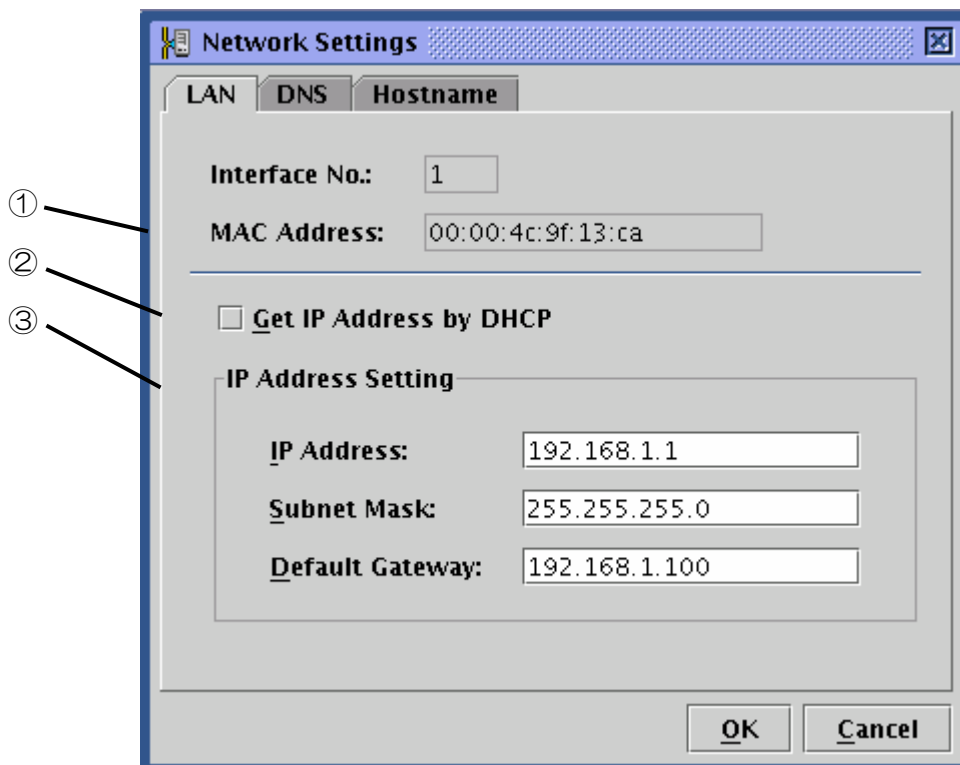


When you click [🔗], the icon for editing information, in this window, the Network Configuration window as shown in the following page appears.

The Network Configuration window has three tabs.



Before setting the default gateway, the gateway, the server, and the management PC must be ready to communicate. If the default gateway is set while they are not ready to communicate, you must cycle the power of the server after they are ready to communicate through network.

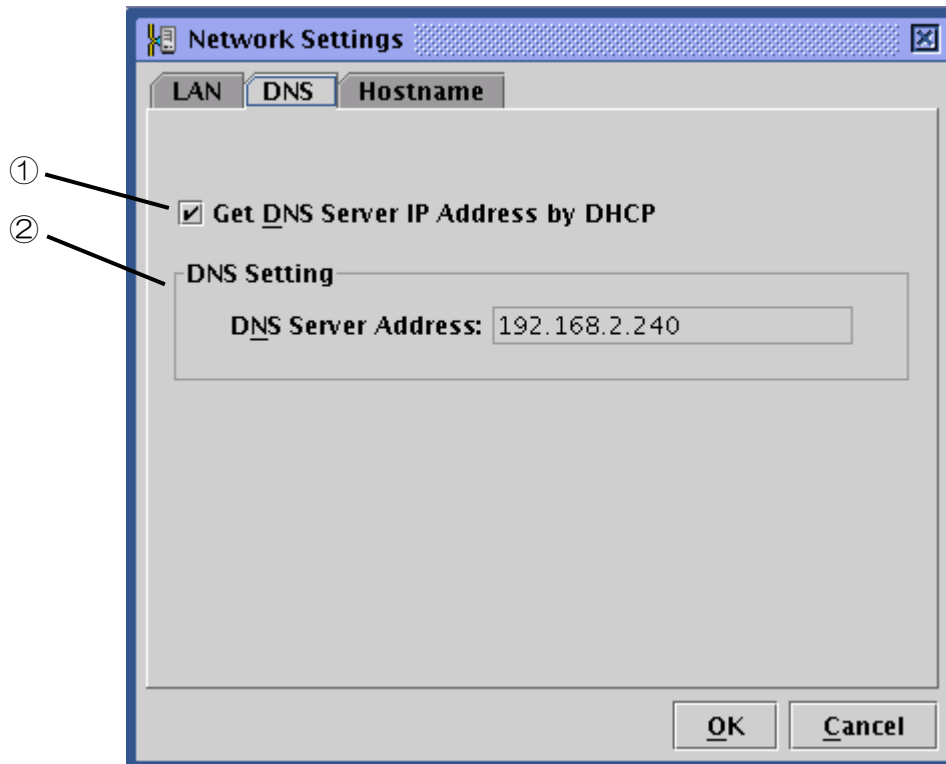


- ① The MAC address owned by BMC appears in this box.
- ② Choose whether or not to acquire an IP address automatically by DHCP.
- ③ If DHCP is not used to automatically acquire an IP address, make settings here. If DHCP is used, information automatically acquired appears here.

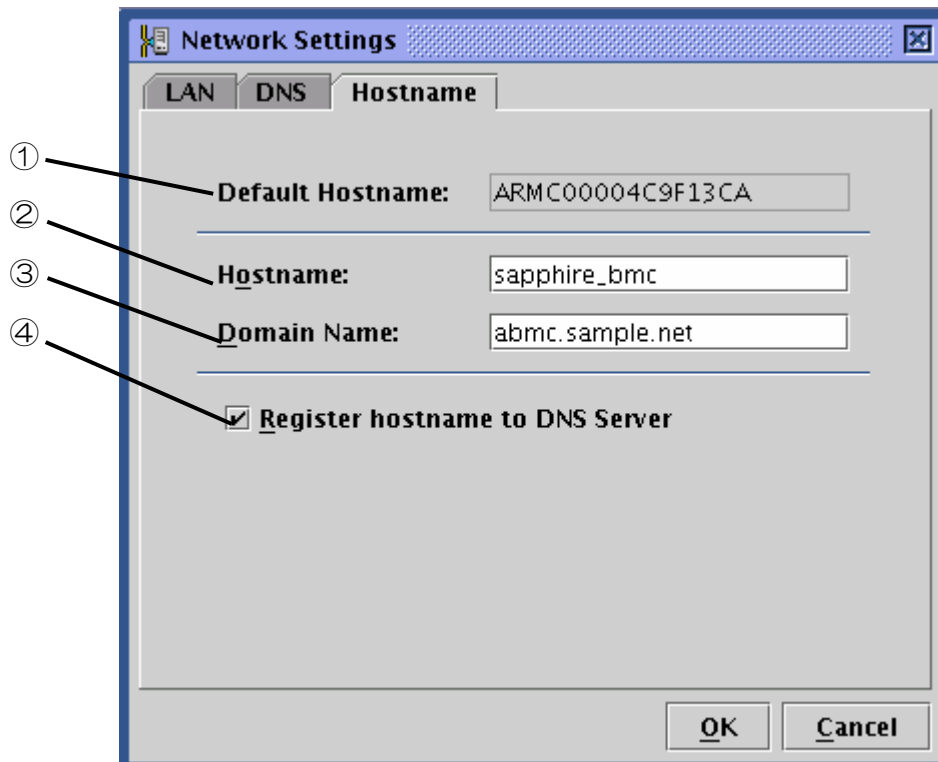


When you change the IP address, the current connection will be disconnected after you click OK and settings of BMC is completed. Close the window once, and then enter the IP address (or host name) that has been newly configured in the browser to log in.

Because the login page that remains to be displayed in the browser has been accessed by the old address, you cannot use it to log in.



- ③ Choose whether or not to acquire the IP address of the DNS server automatically by DHCP.
- ④ If DHCP is not used to automatically acquire the IP address of the DNS server, make settings here. If DHCP is used, information automatically acquired appears here.



- ① The default host name to be used when no host name is configured for using DHCP
- ② Enter the host name of BMC. If nothing is set here, the default host name in the previous step will be used.
- ③ Enter the domain name of the network to which BMC belongs.
- ④ Choose whether or not to register the host name to the DNS server.



Tips

It is recommended to specify a name that is easy to imagine the host name in the server OS (for Windows, a computer name) for a BMC host name.

For example, if the host name on the server OS is “sapphire” , you may set BMC “sapphire_bmc” for a BMC host name.



Notice

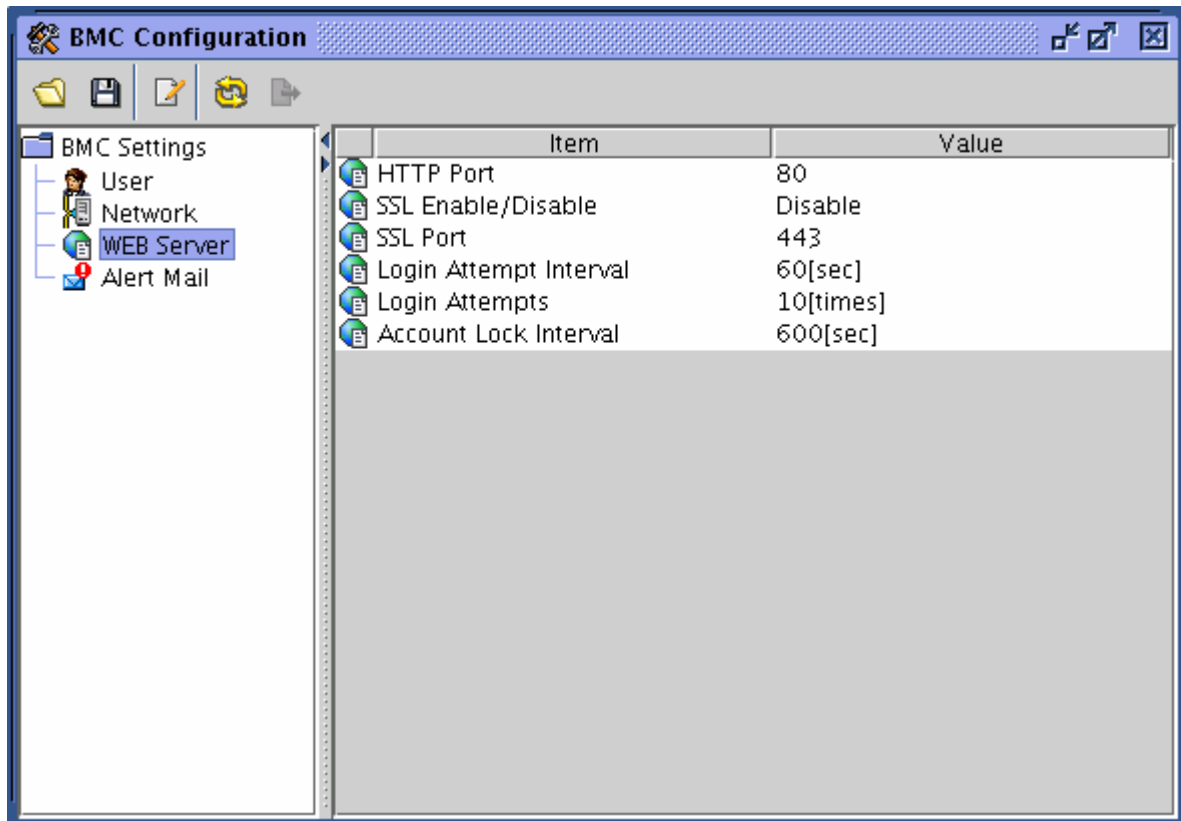
Because BMC uses a LAN controller independent of the server OS, a BMC host name and a domain name cannot be exactly the same as those on the server OS. If BMC belongs to a different network domain, you can have the same host name.

When you click [OK], all the information in the Network Configuration window with three tabs will be written into BMC.

When you click [Cancel], the Network Configuration window closes discarding what you have configured.

HTTP Configuration

By clicking [HTTP Configuration] in the left pane of the BMC Configuration window, you will see a window as shown below and you can make web server-related settings for BMC such as HTTP port.



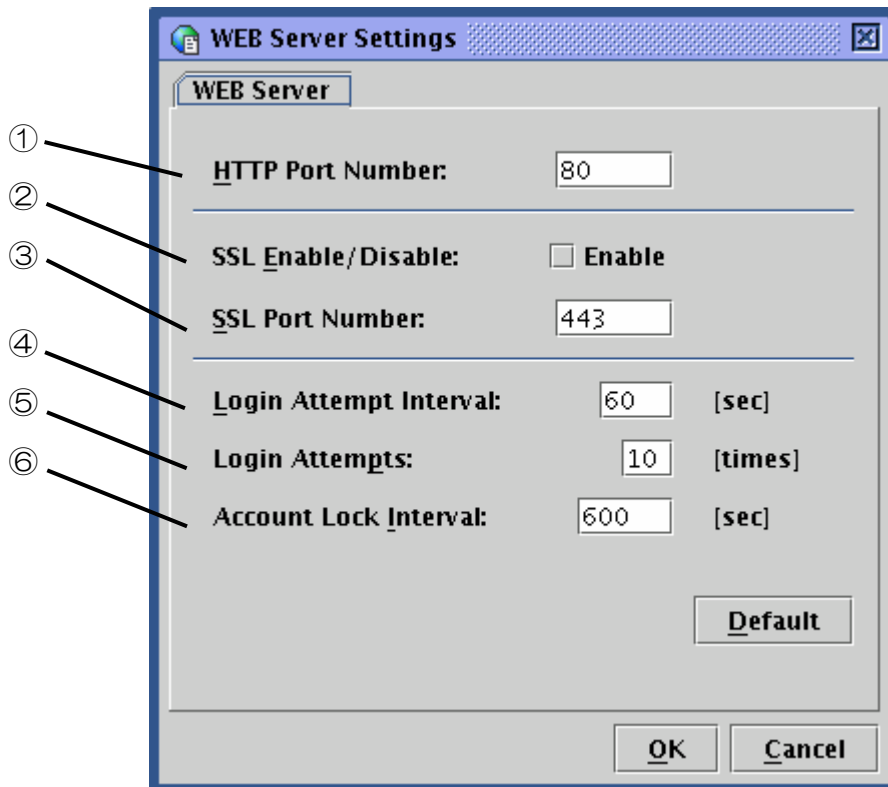
Notice

If you change the settings of HTTP port number, Enable SSL, or SSL Port Number, the current connection will be disconnected.

Close the window once, and then enter the port number that has been newly configured in the browser to log in.

Because the login page that remains to be displayed in the browser has been accessed by the old address, you cannot use it to log in.

When you click [edit icon], the icon for editing information, in this window, the HTTP Configuration window as shown in the following page appears.



- ① Specify an HTTP port number
- ② Choose enable/disable SSL communication. If you select this check box, you can make SSL enabled settings. And, if you clear this check box, you can make SSL disabled settings.



Tips

Unless there is any specific reason such use of SSL not being allowed, it is recommended to use the HTTPS protocol, which is encrypted. By default, SSL is disabled.

- ③ Specify an SSL port number in this box.
- ④ In Login attempt period, specify a time period during which you can retry login if your attempt to log in has failed.
- ⑤ In Failed login attempts, specify the number of login attempts during the period specified in the previous step, exceeding which prompts to denial of login as specified in the following step.
- ⑥ In Account lock period, enter a time period during which login is denied.



Tips

The three configuration items mentioned above are effective to deny unauthorized login accesses that are attempted automatically. However, they cannot prevent such accesses completely.

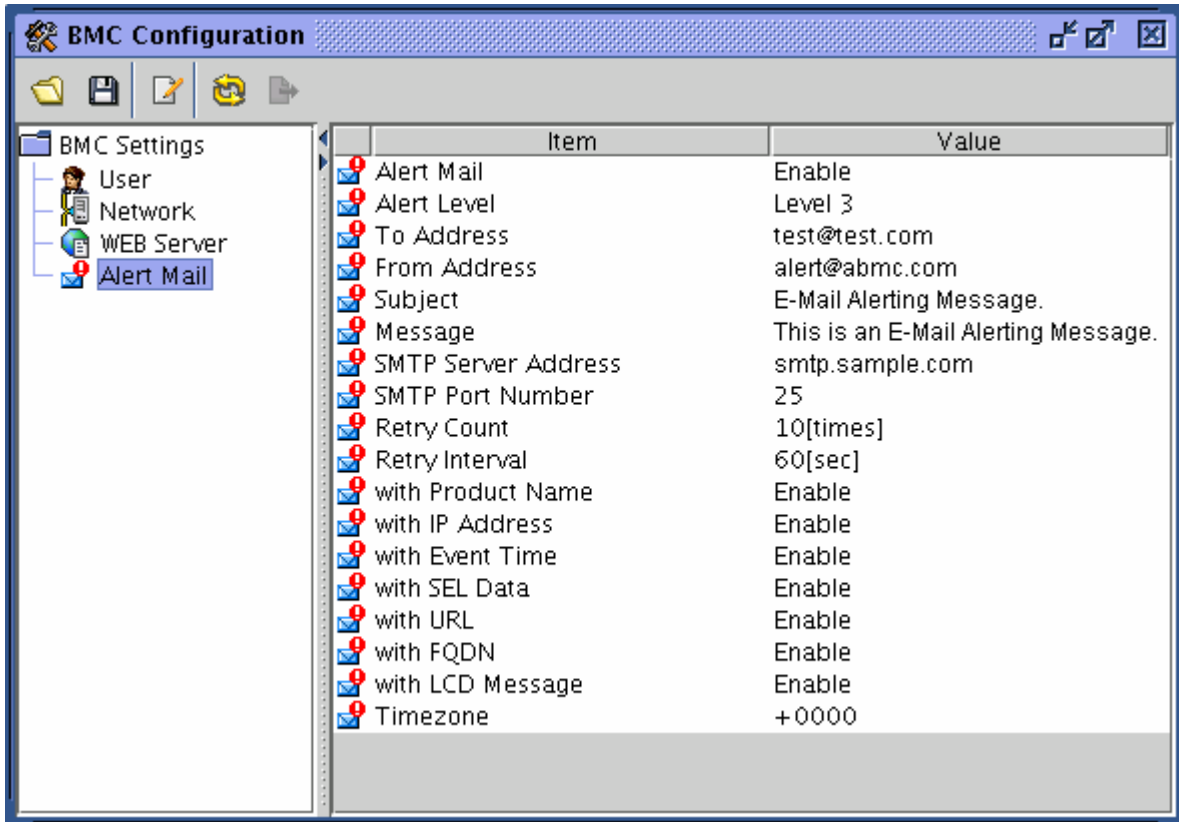
When you click [Default], default values for HTTP port number, SSL port number, Login attempt interval, Login attempts, and Account lock interval appear. But, SSL Enable/Disable check box is not changed.


When you click [OK], all the information in the HTTP Configuration window will be written into BMC.

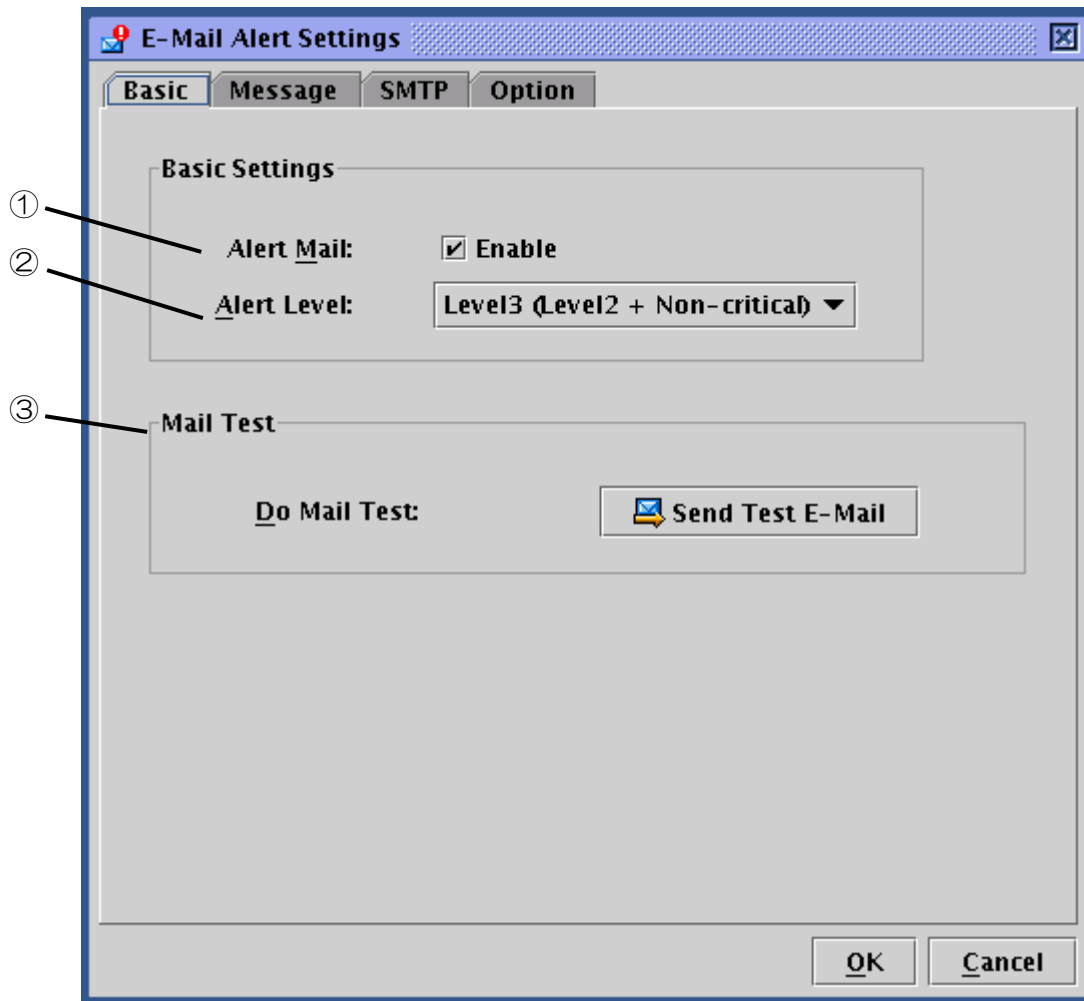
When you click [Cancel], the HTTP Configuration window closes discarding what you have configured in the window.

Alert Mail Configuration

By clicking [Alert Main Configuration] in the left pane of the BMC Configuration window, you will see a window as shown below and you can make alert mail-related settings.



When you click , the icon for editing information, in this window, the Alert Mail Configuration window as shown in the following page appears. The Alert Mail Configuration window has four tabs.



- ① You can choose to enable or disable alert mail functions. If you select this check box, you can make mail-related settings.
- ② Specify an alert level from six levels.
Alert levels are categorized according to severity of event causing an alert.
- ③ You can send a test mail by clicking the button in this box.



Notice

If you want to send a test mail, complete all alert mail settings detailed in the following pages.

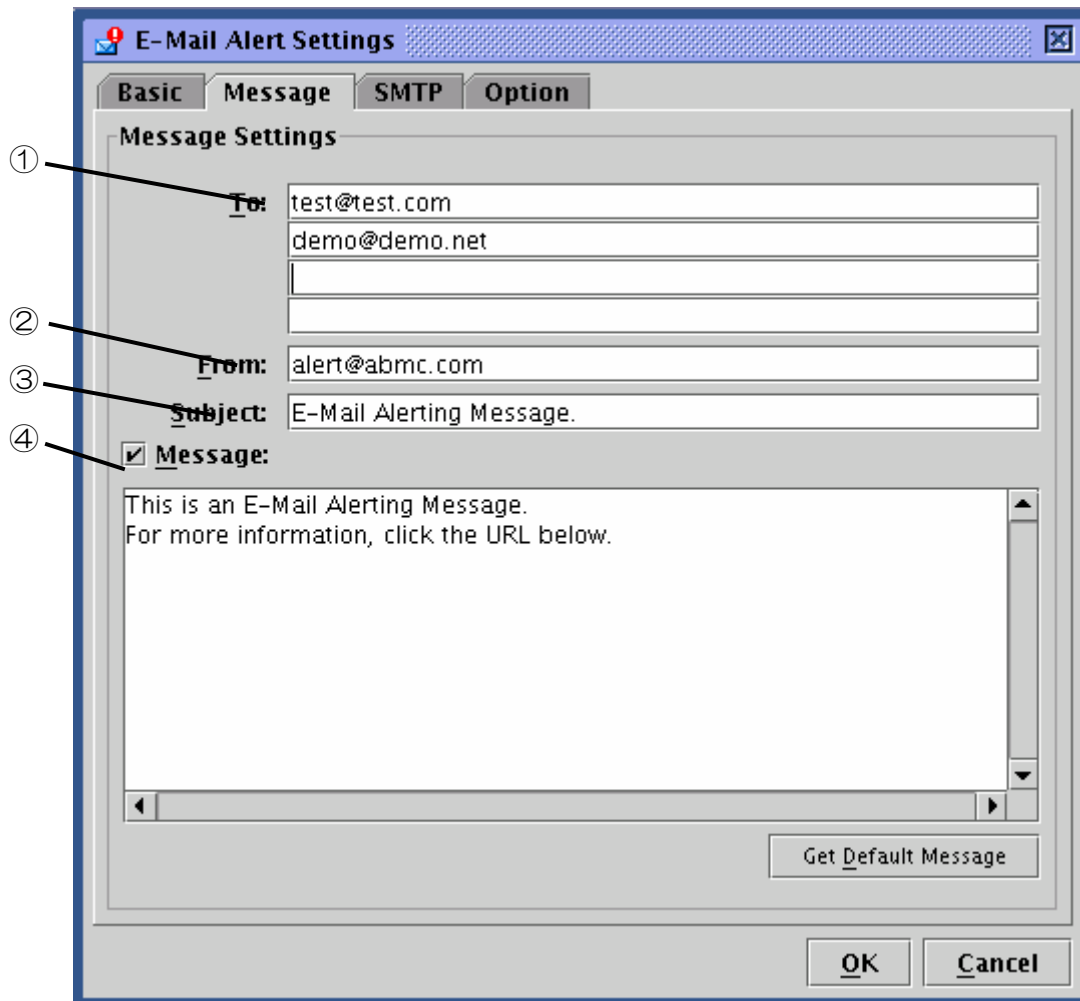
Note that entering information in the Alert Mail Configuration window does not complete settings. When you have entered all the information you need to enter, click [OK], and the information will be written into BMC and settings will be completed.



Tips

According to severity of event causing an alert, X-Priority: field in the alert mail header changes as below.

| | |
|----------------------------------|----------------------|
| Non-recoverable/Critical | X-Priority: 1 |
| Non-critical | X-Priority: 3 |
| OK/Information/Monitoring | X-Priority: 5 |

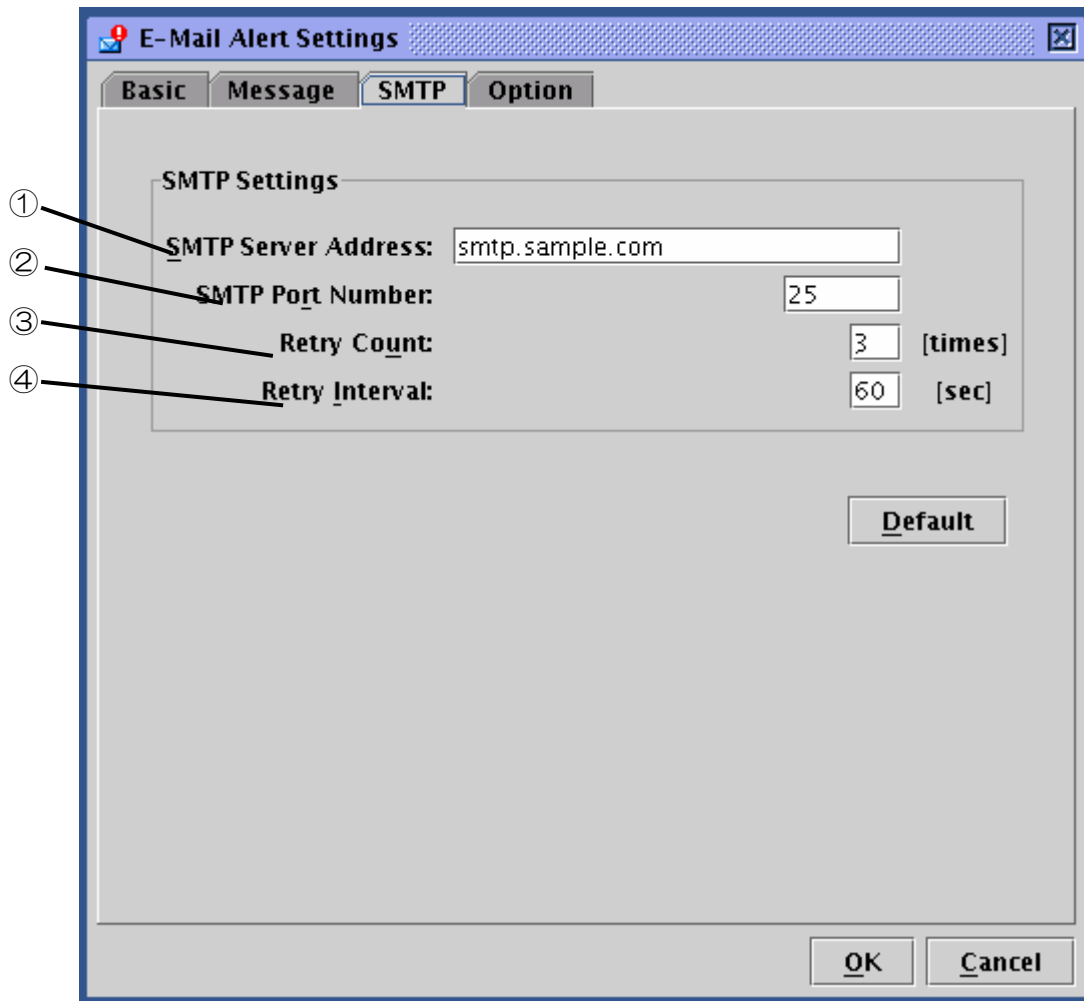


- ① Specify email addresses of alert mail. You can specify up to four addresses.
- ② Specify a sender's email address.
- ③ Type in a subject of alert mail.
- ④ Type in a message that appears in the message body of all alert mails. If you don't need such message, you can clear the check box. If you click "Acquire default message", the recommended message appears.



Tips

The subject and message you configure here will be attached to all alert mails.
You can use Japanese for subject and message but you cannot use Japanese for email addresses.

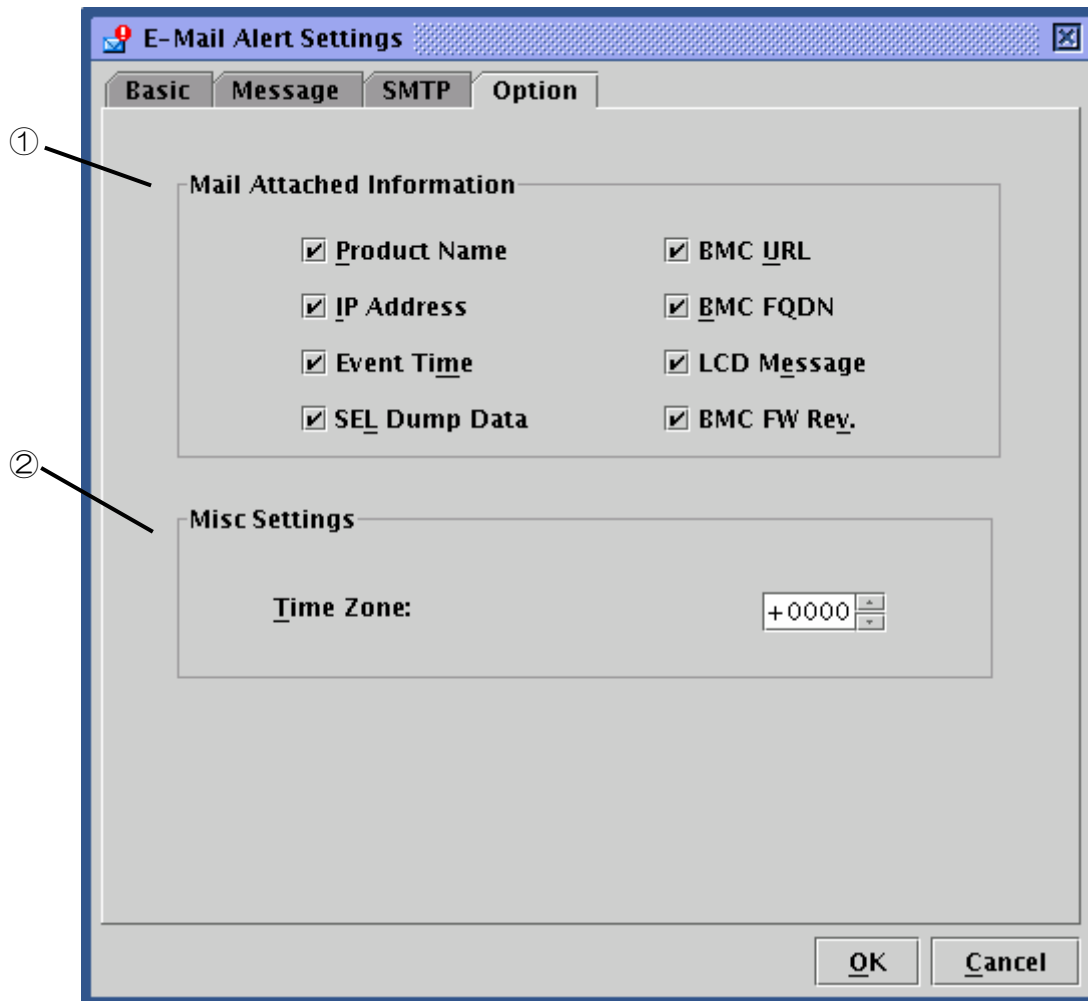


- ① Specify the SMTP server address. You can use the IP address as well.
- ② Specify the port number of the SMTP server.
- ③ Specify how many retries can be made when attempt to send the mail has failed.
- ④ Specify a retry interval that waits for the next retry when attempt to send the mail has failed.

When you click [Default], default values for SMTP port number, retry count, and retry interval appear. Unless there is any specific reason not to, it is recommended to use the default values.



This product doesn't support SMTP Authentication (SMTP-AUTH).



① Specify information to be included in the body of alert mails.

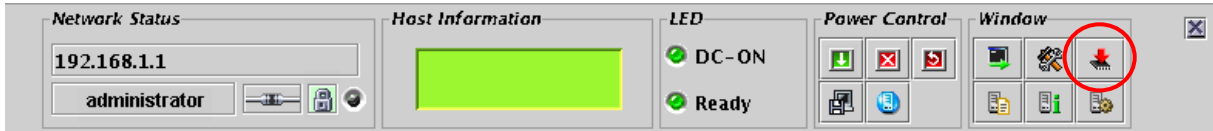
| | |
|---------------------|---|
| Product Information | The product name, code and number of the server |
| IP Address | IP address of BMC |
| Event Time | The time the event occurred |
| SEL Dump Data | Data representing system event logs (SEL) in hexadecimal |
| BMC URL | URL of the ARMC login page |
| BMC FQDN | Full domain name of BMC |
| LCD Message | LCD message in the server at the time of event occurrence |
| BMC FW Rev. | Revision information of BMC firmware/SDR/PIA |

② The information here will appear in the Date field in the header of alert mails.

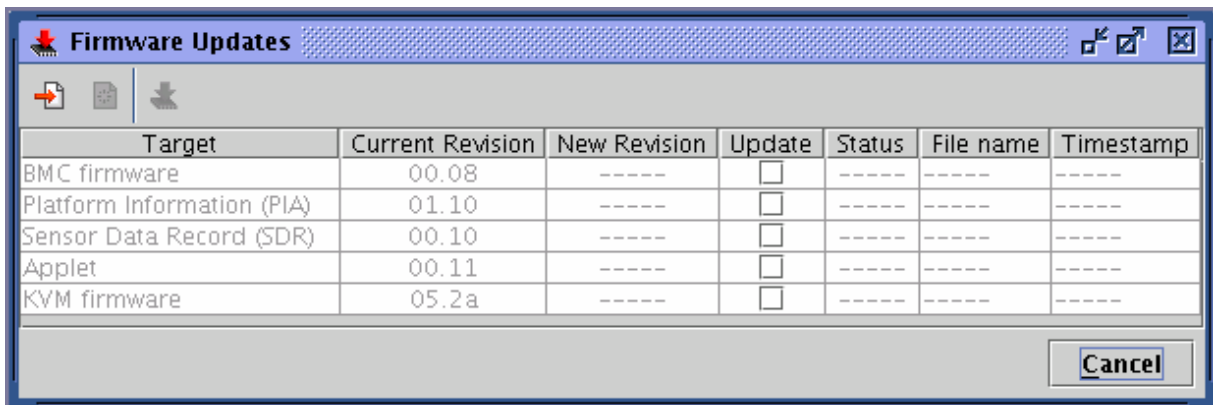
FIRMWARE UPDATE

You can update applet, KVM firmware, BMC firmware, sensor data records (SDR), and platform information (PIA)

Starting up the Firmware Update window




When you click [⚡], the icon to start up Firmware Update, on Control Panel, revision information is loaded from BMC, and the Firmware Update window as shown below appears.

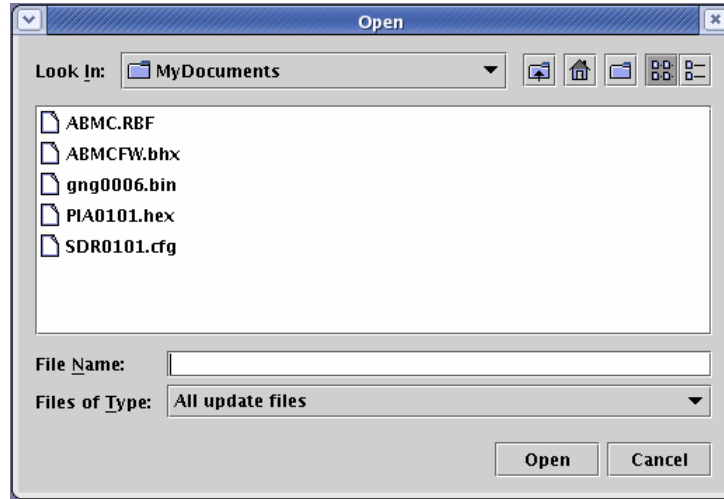


When you click [Cancel], the Firmware Update window closes without any changes made.

The following pages provide information about update procedures.

Loading update data files

When you click  to add update files, a window as shown below opens prompting you to select files.



Select update data files.

When you click [Open] after specifying files, loading of the files begins.

It will take a little while for loading to be completed.



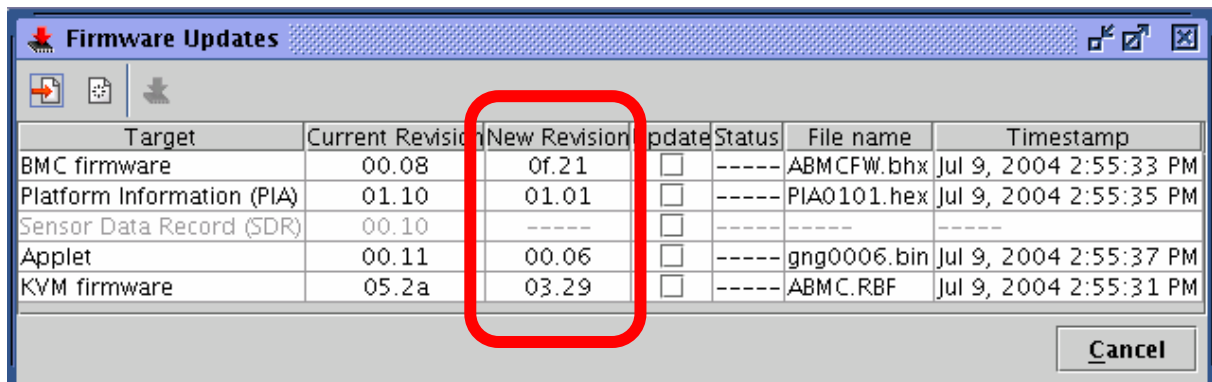
Because update can be made globally for each update target, make sure to load everything you need.

You can specify multiple files to be loaded simultaneously.

Checking revisions

When loading of data files is completed, the current revision and new revisions appear with information on files (file names and time stamps) in the Firmware Update window.


Check the revisions and information.



| Target | Current Revision | New Revision | Update | Status | File name | Timestamp |
|----------------------------|------------------|--------------|--------------------------|--------|-------------|------------------------|
| BMC firmware | 00.08 | 0f.21 | <input type="checkbox"/> | ----- | ABMCFW.bhx | Jul 9, 2004 2:55:33 PM |
| Platform Information (PIA) | 01.10 | 01.01 | <input type="checkbox"/> | ----- | PIA0101.hex | Jul 9, 2004 2:55:35 PM |
| Sensor Data Record (SDR) | 00.10 | ----- | <input type="checkbox"/> | ----- | ----- | ----- |
| Applet | 00.11 | 00.06 | <input type="checkbox"/> | ----- | gng0006.bin | Jul 9, 2004 2:55:37 PM |
| KVM firmware | 05.2a | 03.29 | <input type="checkbox"/> | ----- | ABMC.RBF | Jul 9, 2004 2:55:31 PM |

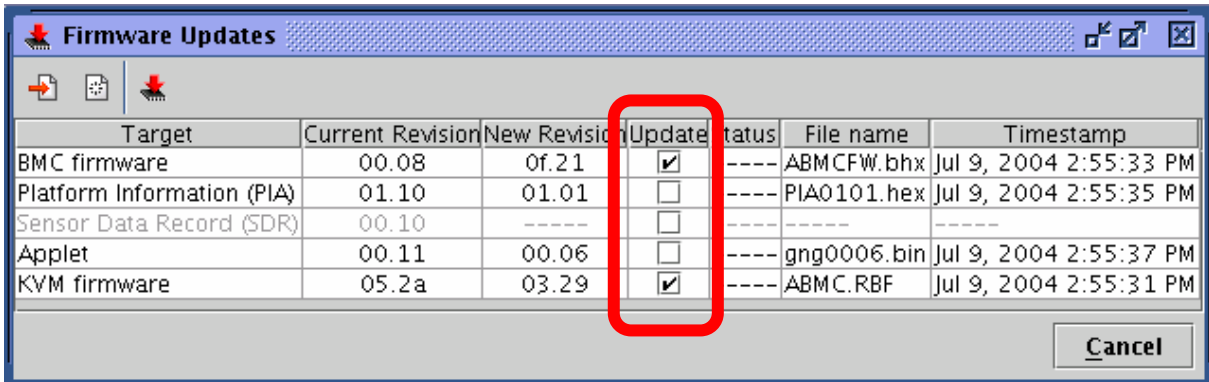


Check each revision well because downgrade can be performed as well.

If you click  to clear update data, all data that has been loaded will be discarded. If you click [Cancel], the Firmware Update window closes discarding all information that has been loaded.

Selecting update target

Select update targets in the Update check boxes.




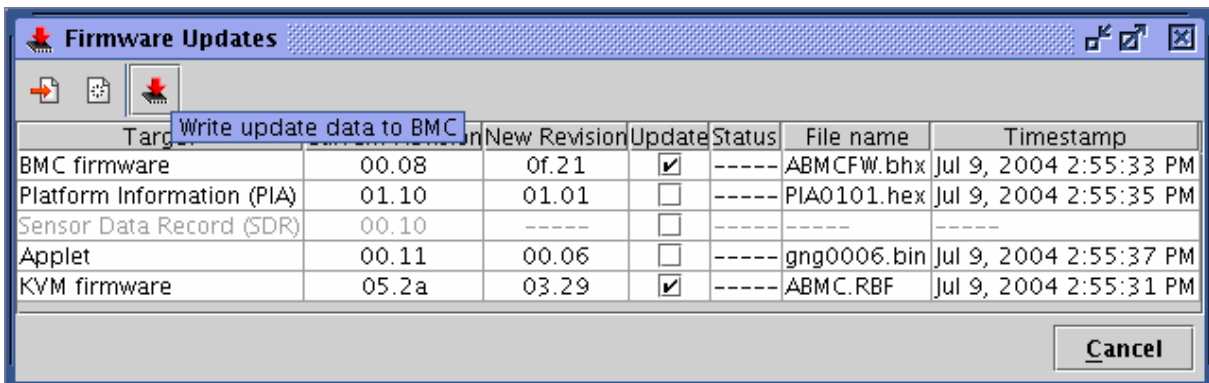
Only what you specify here will be written into BMC.
Data will not be written for those items with file loaded but not specified here.



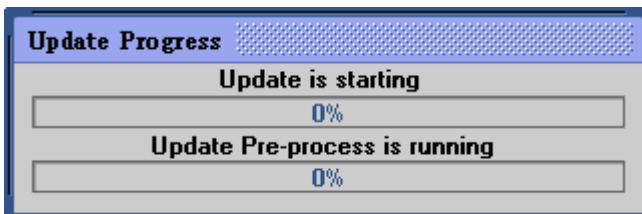
If you want to update both SDR and PIA, perform writing simultaneously. If you update SDR and PIA separately, the first update data will be cleared when the second update is performed.

Writing update data into BMC

When you click  , update data will be written into BMC.



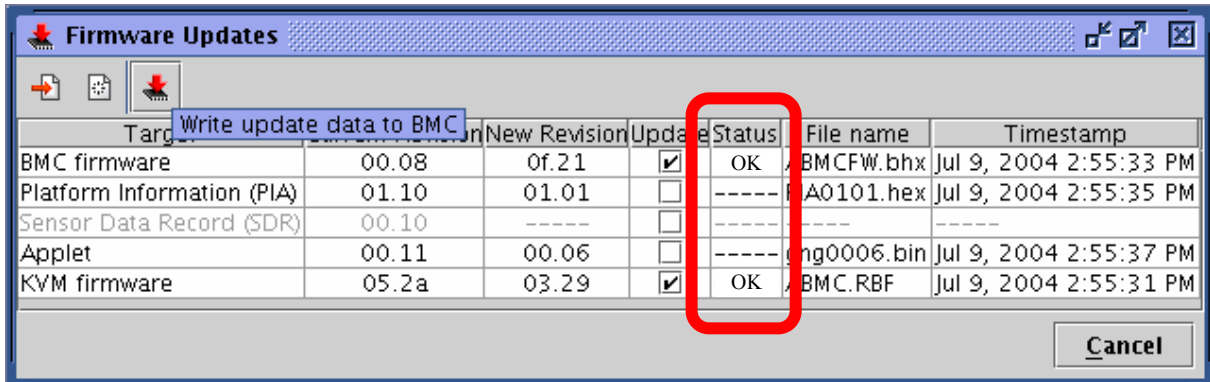
For each update target, the window showing update progress appears.



If any error is detected during update, an error message appears and the update is terminated.

Completion of writing

When writing is completed, results appear in the [Status] column per [Target].



| Target | Current Revision | New Revision | Update | Status | File name | Timestamp |
|----------------------------|------------------|--------------|-------------------------------------|--------|-------------|------------------------|
| BMC firmware | 00.08 | 0f.21 | <input checked="" type="checkbox"/> | OK | BMCFW.bhx | Jul 9, 2004 2:55:33 PM |
| Platform Information (PIA) | 01.10 | 01.01 | <input type="checkbox"/> | ----- | PIA0101.hex | Jul 9, 2004 2:55:35 PM |
| Sensor Data Record (SDR) | 00.10 | ----- | <input type="checkbox"/> | ----- | ----- | ----- |
| Applet | 00.11 | 00.06 | <input type="checkbox"/> | ----- | app0006.bin | Jul 9, 2004 2:55:37 PM |
| KVM firmware | 05.2a | 03.29 | <input checked="" type="checkbox"/> | OK | KVM.RBF | Jul 9, 2004 2:55:31 PM |



For targets other than applet, reboot the server or power off and then on the server to apply the update.



If you reboot the server or power on the server to apply the BMC firmware update, connection to BMC is disconnected. To continue using, log in again.



To apply applet update, log out and shut down all browsers, and then log in again. You do not need to reboot the server.

6. Troubleshooting

ERROR MESSAGES

Fatal errors

| No | Error Message | What to do |
|----|--------------------------------------|--|
| 1 | Fatal error. JavaVM quits. | Try logging in again. If the same message continues to appear, contact your support department. |
| 2 | A fatal software error has occurred. | Try logging in again. If the same message continues to appear, contact your support department. |

Login error

| No | Error Message | What to do |
|----|----------------------|--|
| 1 | Authentication error | Check the user name and password, and then enter them again. |

Access privilege error

| No | Error Message | What to do |
|----|---|---|
| 1 | Unauthorized operation. You have no privilege to perform the operation. | Try performing the operation with administrator's privileges. Consult your administrator. |

Network errors

| No | Error Message | What to do |
|----|-----------------------------------|--|
| 1 | The HTTP communication failed. | Check the network environment and try again. Contact your support department if the error persists. . |
| 2 | Could not resolve the IP address. | Check the network environment. You cannot use Remote KVM Console for connections via proxy. |
| 3 | Unable to reach the target host. | Check the network environment. You cannot use Remote KVM Console for connections via proxy. |

| | | |
|----|--|---|
| 4 | A network error occurred. | Check the network environment and try again. Contact your support department if the error persists. |
| 5 | Failed to download applet. | Check the network environment and try again. Contact your support department if the error persists. |
| 6 | The RMCP+ session is closed. | Check the network environment. If there is no network problem, contact your support department. |
| 7 | Failed to establish the RMCP+ session. | Check the network environment. If there is no network problem, contact your support department. |
| 8 | The RMCP+ transmission failed. | Check the network environment. If there is no network problem, contact your support department. |
| 9 | The specified RMCP+ protocol cannot be used. | Check the network environment. If there is no network problem, contact your support department. |
| 10 | BMC resources to establish a new RMCP+ session are insufficient. | Try again after a connection from other client is finished. |
| 11 | The RMCP+ session time-out occurred. | Check the network environment and server. If you don't find problem, contact your support department. |

BMC-related errors

| No | Error Message | What to do |
|----|--|--|
| 1 | The IPMI request was aborted. | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 2 | Received bad response from BMC. | Check the server. A failure may have occurred in BMC. If you don't find problem, contact your support department. |
| 3 | BMC does not support IPMI 2.0 functions. | Contact your support department. |
| 4 | Failed to run the IPMI command. | Check the server. A failure may have occurred in BMC. If you don't find problem, contact your support department. |
| 5 | Failed to send the IPMI message. | Check the network environment. If the network has no problem, contact your support department. |
| 6 | Illegal IPMI message was requested. | Contact your support department. |
| 7 | Specified target is not present. | Check the server. A failure may have occurred in BMC. If you don't find problem, contact your support department. |

Remote KVM Console errors

| No | Error Message | What to do |
|----|--|---|
| 1 | Failed to disable Remote KVM Console. | Check the network environment and try again. Contact your support department if the error persists. |
| 2 | Failed to enable Remote KVM Console. | Check the network environment and try again. Contact your support department if the error persists. |
| 3 | KVM packet transmission failed. | Check the network environment and server. If you don't find problem, contact your support department. |
| 4 | The KVM request was aborted. | This is not a problem. Click OK and close the message box. |
| 5 | UDP packet transmission failed. | Check the network environment and server. If you don't find problem, contact your support department. |
| 6 | Remote KVM console can not activate because it is disabled | Make a remote KVM console enable Refer to page 91. |
| 7 | Remote KVM Console is used by other client. | Try again after the client using Remote KVM Console finishes using. |
| 8 | Failed to shut down Remote KVM Console. | Use Remote KVM Console after waiting 3 or more minutes. |
| 9 | Failed to make settings. | Check the network environment and try again. Contact your support department if the error persists. . |
| 10 | The UDP connection is closed. | Check the network environment and server. If you don't find problem, contact your support department. |

System event logs (SEL) display errors

| No | Error Message | What to do |
|----|--|--|
| 1 | Failed to clear session event logs of BMC. | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 2 | Failed to acquire system event logs. | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |

Sensor data records (SDR) display error

| No | Error Message | What to do |
|----|--|--|
| 1 | Failed to acquire sensor data records. | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |

Field replaceable unit (FRU) information display error

| No | Error Message | What to do |
|----|--|--|
| 1 | Failed to acquire field replaceable units information. | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |

BMC configuration errors

| No | Error Message | What to do |
|----|---|--|
| 1 | Failed to make settings: | Check the network environment and try again. Contact your support department if the error persists. . |
| 2 | Failed to acquire BMC Configuration: | Check the network environment and try again. Contact your support department if the error persists. . |
| 3 | Used by other software program. Try again after a while. | Try again after a while. |
| 4 | Invalid BMC configuration file. | The BMC configuration file may be corrupted. Check the file. |
| 5 | The required XML tag is not found. | The BMC configuration file may be corrupted. Check the file. |
| 6 | Failed to write the file. | The BMC configuration file is not saved successfully. Change the location to save the file and try again. |
| 7 | Invalid user name | You can use only alphanumeric characters, minus sign (-), and underscore (_) for a user name. A user name should be 31 characters or less. |
| 8 | The user name is too long | A user name should be 31 characters or less. |
| 9 | The password is too long. | Use 16 or less characters. |

| | | |
|----|--------------------------------------|---|
| 10 | Passwords are not matched. | Again, input passwords. |
| 11 | Invalid HTTP port number | You can use only numeric values. |
| 12 | Invalid SSL port number | You can use only numeric values. |
| 13 | HTTP/SSL should not be the same. | The same port number can't do them. Specify different value. |
| 14 | Invalid login attempt period | You can use only numeric values. |
| 15 | Invalid failed login attempts | You can use only numeric values. |
| 16 | Invalid account lock period | You can use only numeric values. |
| 17 | Invalid IP address | Use numerals and periods to specify an IP address. |
| 18 | Invalid subnet mask | Use numerals and periods to specify a subnet mask. |
| 19 | Invalid default gateway | Use numerals and periods to specify a default gateway. |
| 20 | Invalid DNS server IP address | Use numerals and periods to specify the IP address of DNS server. |
| 21 | Invalid host name | You can use only alphanumeric characters, minus sign (-), and underscore (_) for a host name. A host name should be 64 characters or less. |
| 22 | Invalid domain name | You can use only alphanumeric characters, minus sign (-), and underscore (_) for a domain name. A domain name should be up to 256 characters. |
| 23 | The SMTP server address is too long. | Specify within 256 characters. |
| 24 | Invalid SMTP port number. | You can use only numeric values. |
| 25 | Invalid retry count | You can use only numeric values. |
| 26 | Invalid retry interval | You can use only numeric values. |
| 27 | "To" is too long. | Specify within 256 characters. |

| | | |
|----|---------------------------|---|
| 28 | "From" is too long. | Specify within 256 characters. |
| 29 | "Subject" is too long. | Specify within 512 characters. If you use Japanese characters, the number of characters you can use is less than half of 512 characters. |
| 30 | The message is too long. | The message should be up to 4064 characters. If you use Japanese characters, the number of characters you can use is less than half of 4064 characters. |
| 31 | Failed to open the file: | The specified file may not exist. Check the file name. |
| 32 | Failed to close the file: | The specified file may be corrupted. |
| 33 | Can't open the file: | The specified file may not exist. Check the file name. |
| 34 | Timeout has occurred. | Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |

Firmware update errors

| No | Error Message | What to do |
|----|--|--|
| 1 | There are uncompleted update images on BMC as follows: | Reboot the server and complete the update. |
| 2 | Failed to acquire status of the update area. | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 3 | Update data is too large: | Some update files may be corrupted. Acquire update files again. |
| 4 | Failed to prepare update | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 5 | Invalid file size: | The update file may be corrupted. Acquire the update file again. |
| 6 | Could not find the revision information: | Some update files may be corrupted. Acquire update files again. |
| 7 | Failed to create rollback image. | Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 8 | Failed to erase. | Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |

| | | |
|----|---------------------------------------|---|
| 9 | Unsupported format version: | Some update files may be corrupted. Acquire update files again. |
| 10 | Failed to load the update image file. | Some update files may be corrupted. Acquire update files again. |
| 11 | Update has failed. | Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 12 | Could not switch to the update mode. | Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 13 | Could not find the update targets: | Some update files may be corrupted. Acquire update files again. |
| 14 | Invalid address: | Some update files may be corrupted. Acquire update files again. |
| 15 | Writing has failed. | Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 16 | Unsupported token is detected: | Some update files may be corrupted. Acquire update files again. |
| 17 | Invalid segment information: | Some update files may be corrupted. Acquire update files again. |
| 18 | Invalid data length: | Some update files may be corrupted. Acquire update files again. |
| 19 | Failed to open the file: | The specified file may not exist. Check the file name. |
| 20 | Failed to close the file: | The specified file may be corrupted. |
| 21 | Invalid file checksum: | Some update files may be corrupted. Acquire update files again. |
| 22 | Failed to parse files. | Some update files may be corrupted. Acquire update files again. |
| 23 | Failed to parse files: | Some update files may be corrupted. Acquire update files again. |
| 24 | Failed to load files: | Some update files may be corrupted. Acquire update files again. |
| 25 | Could not find files: | Some update files may be corrupted. Acquire update files again. |
| 26 | Failed to verify | Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |

| | | |
|----|---|--|
| 27 | Update will be stopped because interruption has occurred. | Check clients. A software program other than you are using may have interrupted. |
| 28 | Online update is now being used. | Try again as necessary after online update performed by other tool is completed. |
| 29 | Failed to acquire the current revision. | The network may be busy. Try again. If the error persists, contact your support department because a failure may have occurred in BMC. |
| 30 | Failed to acquire lines: | Some update files may be corrupted. Acquire update files again. |
| 31 | Invalid line length: | Some update files may be corrupted. Acquire update files again. |
| 32 | Unexpected EOF is detected: | Some update files may be corrupted. Acquire update files again. |
| 33 | Unexpected token is detected: | Some update files may be corrupted. Acquire update files again. |
| 34 | PIA does not suit this server | It is not Platform Information(PIA) of this server. Acquire update files again. |

OTHERS

Please confirm the following items before sending on repair when remote monitor function does not work.

If you found the same trouble condition, please refer to the comment.

In addition, about a trouble in the system, please refer to attached user's guide to the server.

When there is not an item to fit, and when it is not improved even if I carry out measures,

Please contact a maintenance service company.



After having installed this card, During POST processing, a warning message became display.

Did you do initial setting of a remote management card?

→Please confirm a message with user's guide of the server.

There is a possibility that the system device information is not written in.

Please start EXPRESSBUILDER of the server attachment.

Please choose "initial setting of a remote management card" among "a tool menu". Please do setting of information peculiar to each server to an advanced remote management card.



I cannot recognize a server from a management PC.

Did you do initial setting of an Advanced Remote Management Card?

→Please start EXPRESSBUILDER of the server attachment.

Please choose "initial setting of a remote management card" among "a tool menu".

Please do setting of information peculiar to each server to an Advanced Remote Management Card.

Is JAVA 2 Runtime Environment, Standard Edition 1.4.2_04 or later installed in a management PC?

→Java2 Runtime Environment, Standard Edition 1.4.2_04 is necessary for a management PC.

You can download this software from the following places.

Insert the NEC EXPRESSBUILDER CD-ROM into the CD-ROM driver.

The master control menu will be displayed by the Autorun function.

Click [Software Setup]-[NEC DianaScope] The DianaScope installation menu for Windows will appear.

There is JAVA Installer at Menu of NEC DianaScope Manager.

Please download it as follows if you want latest JRE(Java Runtime Environment) distributed free of charge by Sun Microsystems, Inc.

<http://java.sun.com/j2se/>

Are management card and a network card connected with inside cable?

→Please confirm whether inside cable is connected between cards.

Is a LAN/ICMB cable connected?

→Please confirm a connection state of a LAN/ICMB cable.

You cannot refer to a sensor of the server device justly unless a cable is connected.
In addition, please confirm that you are not connecting a cable to a connector of the server.

Is not an IP address duplicated?

→An IP address of a LAN port for management is set to 192.168.1.1 at the time of shipment. Because it is not recognized that there is the same IP address on the same network normally, please change an IP address.

Are you setting monitor of a main body of Express5800 device of ESMPRO/Server Agent?

→A setting method is as follows. Start ESMPRO/ Server Agent of Windows Control Panel, and please check of [Express5800 device] - [watch it] check box of "a system" tab.

The initial value is "No watch". After a setting change, monitor of a main server device is started automatically.

You do not have to reboot a server after a setting change. Please carry out rebuilding of a tree when you cannot refer to a main server device.

Is not connected limitation done in the fire wall and the gateway?

→There is a possibility of caught to connected limitation such as the fire walls.

This is guessed to be a cause when client PC is connected directly with LAN crossing cable and the problem solves. Please reconfirm the fire wall and the gateway, etc.

To a remote KVM window of Web, a console screen of a server does not emerge. Is resolution setting of a server right?

→A support range of an advanced remote management card, resolution 1024x768, refreshment rate 75Hz are the upper limits. Please set to appropriate screen mode.

Did you apply exclusive Video Driver for Windows?

→When the server requires, please apply a video driver from EXPRESSBUILDER attached to the server. Please refer to user's guide of the server.

Are you using a device with a text mode for Linux OS?

→If you do set a graphic screen, system may not display from condition of monitor/Driver/video memory on x-window. Please set with a text mode.



When a login name/password is forgotten for the password at the time of using a remote management function from a WEB browser.

- When you forget a login name and a password setup, by changing a jumper mounting position, various setup can be returned to the value at the time of shipments.



In the case of using the DianaScope which is the management utility, settings by the DianaScope is also cleared by this operation.

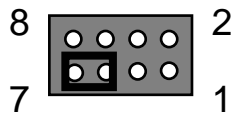
Please back up the setting information on the DianaScope before performing this operation.

→A procedure

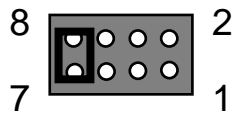
1. Turn off a power supply of a server and pull a power supply cord from outlet.
2. You have to mount the Clear Jumper of the management card as follows.

Refer to page62

Implement position at the time of shipment



Implement position at the time of password clear



3. After that, you connect a power supply cord.
4. You wait more than 30 seconds without switching it on.
You pull power supply cord out of an outlet again.
5. You return a jumper to the position at the time of shipment once again.
Because various setting returns to initial setting value, please set it again.

NEC

N8115-02

アドバンスドリモートマネージメントカード
Advanced Remote Management Card
ユーザーズガイド
User's Guide

2005年11月 三版
3rd Edition, Nov 2005

日本電気株式会社
東京都港区芝五丁目7番1号
TEL (03) 3454-1111 (大代表)

NEC Corporation
7-1 Shiba 5-Chome, Minato-Ku
Tokyo 108-8001, Japan

©NEC Corporation 2004

日本電気株式会社の許可なく複製・改変などを行うことはできません。