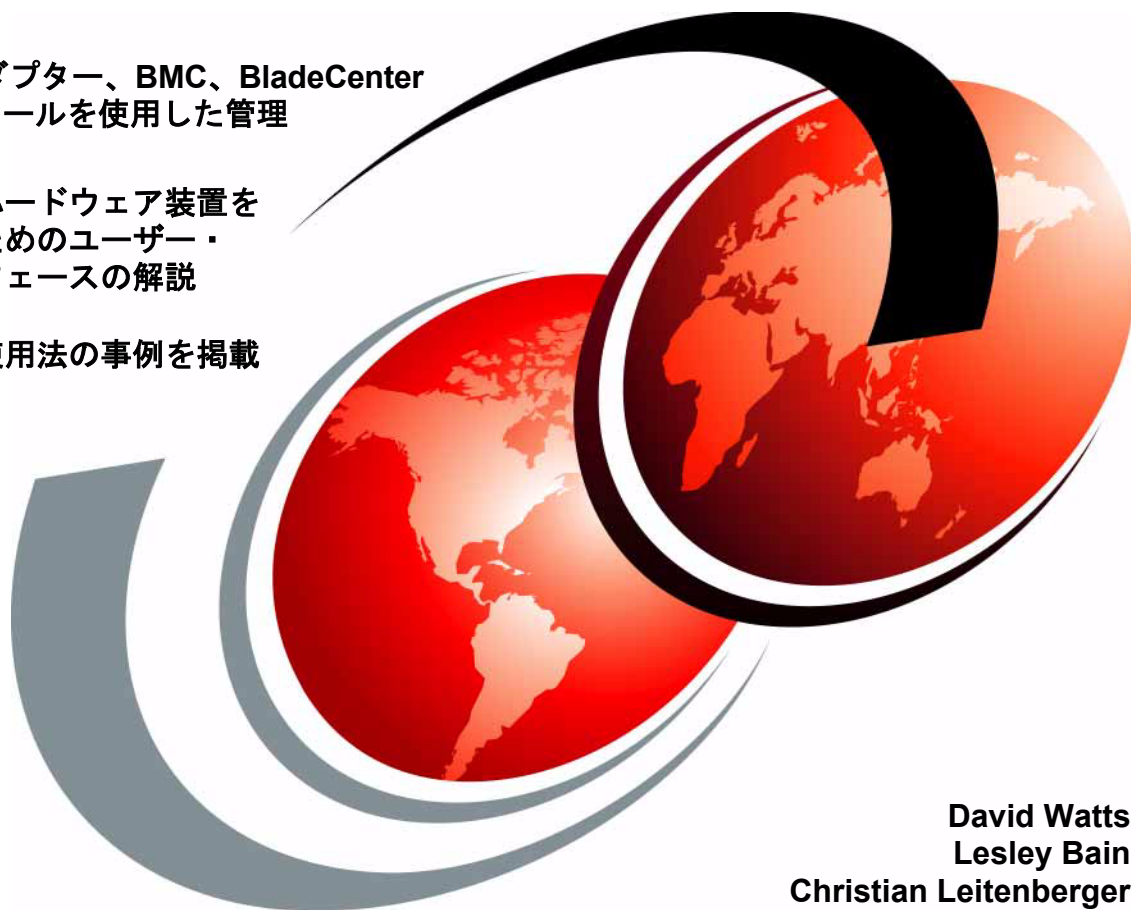


# IBM @server xSeries および BladeCenter サーバー管理

RSA II アダプター、BMC、BladeCenter  
管理モジュールを使用した管理

これらのハードウェア装置を  
使用するためのユーザー・  
インターフェースの解説

ツールの使用法の事例を掲載



David Watts  
Lesley Bain  
Christian Leitenberger





International Technical Support Organization

**IBM @server xSeries および BladeCenter**  
サーバー管理

**お願い :** 本書および本書で紹介する製品をご使用になる前に、『特記事項』 (vii ページ) に記載されている情報をお読みください。

本書は、以下のものに適用されます。

- ▶ xSeries サーバーおよび eServer 325/326 のベースボード管理コントローラー
- ▶ リモート管理アダプター II ( 部品番号 59P2984)
- ▶ リモート管理アダプター II SlimLine ( 部品番号 73P9341)
- ▶ リモート管理アダプター II-EXA ( 部品番号 13N0382)
- ▶ BladeCenter 管理モジュール

IBM 発行のマニュアルに関する情報のページ  
<http://www.ibm.com/jp/manuals/>

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典 :	SG24-6495-00 IBM Eserver xSeries and BladeCenter Server Management
発行 :	日本アイ・ビー・エム株式会社
担当 :	ナショナル・ランゲージ・サポート

第 1 刷 2006.5

# 目次

特記事項.....	vii
商標.....	viii
前書き.....	ix
本書の執筆チーム.....	ix
執筆にご協力ください.....	xi
ご意見をお寄せください.....	xi
<b>第1章 概要.....</b>	<b>1</b>
1.1 xSeries サーバーでサポートされるサービス・プロセッサ.....	2
1.2 業界標準.....	4
1.2.1 Distributed Management Task Force.....	5
1.2.2 IPMI.....	6
1.2.3 SNMP.....	6
<b>第2章 ベースボード管理コントローラー.....</b>	<b>7</b>
2.1 機能の比較.....	8
2.2 e325 および e326 内の BMC.....	9
2.2.1 外部接続.....	9
2.2.2 BMC ファームウェアのアップグレード.....	10
2.2.3 BMC の構成.....	11
2.2.4 OSA IPMI デバイス・ドライバーのインストール.....	17
2.2.5 イベント・ログ.....	18
2.3 xSeries サーバー内の BMC.....	18
2.3.1 機能.....	19
2.3.2 外部接続.....	19
2.3.3 BMC ファームウェアの更新.....	22
2.3.4 BMC_CFG を使用した BMC の構成.....	23
2.3.5 BIOS 内での BMC の構成.....	35
2.3.6 イベント・ログ.....	36
2.3.7 IBM Director による BMC の構成.....	38
2.3.8 リモート制御.....	42
2.3.9 BMC デバイス・ドライバーのインストール.....	42
2.3.10 BMC によって使用されるポート.....	47
2.4 内蔵システム管理プロセッサ.....	47
2.4.1 機能.....	47
2.4.2 制限.....	48
2.4.3 構成.....	48

<b>第3章 リモート管理アダプター II</b> .....	49
3.1 機能および機構 .....	50
3.2 Remote Supervisor Adapter・ファミリーの概要 .....	51
3.2.1 リモート管理アダプター II .....	53
3.2.2 リモート管理アダプター II-EXA .....	54
3.2.3 Remote Supervisor Adapter II SlimLine .....	55
3.3 システム管理ネットワーク .....	57
3.3.1 ASM ゲートウェイの指定 .....	61
3.4 Remote Supervisor Adapter II の基本構成 .....	63
3.4.1 RSA II の取り付け .....	63
3.4.2 ネットワーク設定 .....	64
3.4.3 ファームウェアの更新 .....	66
3.4.4 デバイス・ドライバーのインストール .....	69
3.4.5 MIB ファイル .....	72
3.5 リモート・コンソールとリモート・メディア .....	72
3.5.1 Linux の Remote Control サポート .....	75
3.5.2 リモート・メディアの使用 .....	79
3.5.3 リモート・ディスクット .....	83
3.5.4 リモート CD-ROM および DVD .....	86
3.5.5 リモート・ファイル .....	88
3.6 リモート管理アダプター II によって使用されるポート .....	91
<b>第4章 BladeCenter 管理モジュール</b> .....	93
4.1 機構および機能 .....	94
4.2 管理モジュールの基本構成 .....	97
4.2.1 BladeCenter への取り付け .....	97
4.2.2 ネットワーク設定 .....	98
4.2.3 ファームウェアの更新 .....	101
4.2.4 MIB ファイル .....	103
4.3 リダンダント管理モジュール .....	103
4.3.1 取り付けと配線 .....	103
4.3.2 手動切り替え .....	105
4.4 リモート・コンソールとリモート・メディア .....	106
4.4.1 Linux の Remote Control サポート .....	110
4.4.2 リモート・メディアの使用 .....	112
4.4.3 リモート・ディスクット .....	115
4.4.4 リモート CD-ROM および DVD .....	120
4.4.5 リモート・ファイル .....	123
4.5 ブレード固有の機能の基本構成 .....	127
4.5.1 デバイス・ドライバー .....	127
4.5.2 ブレード・タスク .....	128
4.5.3 入出力モジュール・タスク .....	132
4.6 管理モジュールによって使用されるポート .....	134

4.7 管理モジュールの出荷時のデフォルト値へのリセット .....	136
<b>第5章 セキュリティーおよび認証.....</b>	<b>137</b>
5.1 SSLを使用したセキュリティー .....	138
5.1.1 Secure Sockets Layer (SSL) .....	138
5.1.2 セキュア・シェル (SSH) .....	143
5.2 LDAPを使用した認証 .....	148
5.2.1 LDAP 認証属性 .....	149
5.2.2 LDAP サーバーの構成 .....	151
5.2.3 LDAP サーバー構成のテスト .....	158
5.2.4 LDAP クライアントの構成 .....	160
<b>第6章 システム管理ユーティリティー.....</b>	<b>167</b>
6.1 ツールの比較 .....	168
6.2 Advanced Settings ユーティリティー.....	170
6.2.1 ASU のサポート・リスト .....	171
6.2.2 ASU のサポートされるプラットフォーム .....	171
6.2.3 ASU と定義ファイルのダウンロード .....	173
6.2.4 ASU 定義ファイルの使用 .....	173
6.2.5 ASU コマンドの使用 .....	174
6.2.6 ASU を使用したシステム設定の表示 .....	176
6.2.7 ASU を使用した RSA または RSA II 設定の構成.....	184
6.2.8 ASU バッチ・コマンド .....	185
6.3 管理プロセッサ・コマンド・ライン・インターフェース .....	186
6.3.1 サポートされるサービス・プロセッサ構成.....	186
6.3.2 機能.....	189
6.3.3 制限.....	191
6.3.4 MPCLI のサポートされるプラットフォーム .....	191
6.3.5 MPCLI のインストール .....	191
6.3.6 MPCLI の使用 .....	193
6.4 OSA SMBridge ユーティリティー.....	204
6.4.1 BIOS の構成.....	207
6.4.2 インストール.....	208
6.4.3 Telnet サーバー経由の接続 .....	212
6.4.4 SOL をサポートするための Windows Server 2003 の構成.....	217
6.4.5 SOL をサポートするための Red Hat Linux の構成.....	224
6.4.6 SOL をサポートするための SUSE LINUX の構成.....	227
6.4.7 コマンド・ライン・インターフェースを介した接続.....	229
6.5 Web インターフェース .....	232
6.5.1 Web インターフェースの構造 .....	233
6.6 Telnet インターフェース.....	234
6.7 IBM Director の統合.....	239
6.7.1 管理プロセッサ.....	241

6.7.2 BladeCenter アシスタント .....	242
6.7.3 アラート転送.....	243
<b>第7章 シナリオおよびベスト・プラクティス.....</b>	<b>247</b>
7.1 セキュアな通信と認証 .....	248
7.1.1 一般的な考慮事項.....	248
7.1.2 Web インターフェース .....	249
7.1.3 コマンド・ライン・インターフェース.....	250
7.2 構成のバックアップとリストア .....	251
7.2.1 バックアップ手順.....	251
7.2.2 リストア手順.....	253
7.3 すべての BladeCenter モジュールへのリモート・アクセスの提供 .....	255
7.4 マルチ・サブネット環境.....	259
7.4.1 一般的な考慮事項.....	260
7.4.2 他のサブネットへのアクセス .....	261
7.4.3 異なるサブネット内の DHCP .....	261
7.5 ユーザー ID とパスワードの一括構成.....	262
7.6 RSA II の出荷時のデフォルト値へのリセット .....	264
7.6.1 ASU の使用 .....	265
7.6.2 IBM Director の使用 .....	266
7.6.3 MPCLI の使用 .....	268
7.7 リモート側での ASU の使用法 .....	269
7.8 リモート側での BIOS とファームウェアの更新 .....	273
7.8.1 MPCLI を使用したファームウェアの更新 .....	273
7.8.2 IBM Director を使用したファームウェア更新 .....	275
7.8.3 UpdateXpress RemoteUX を使用したファームウェアの更新 .....	283
7.9 UpdateXpress firmware update scripts for BladeCenter .....	291
<b>省略語および頭字語.....</b>	<b>303</b>
<b>関連資料.....</b>	<b>307</b>
IBM Redbook .....	307
その他の資料.....	307
オンライン・リソース.....	308
IBM Redbook の入手方法.....	311
IBM のヘルプ .....	311
<b>索引.....</b>	<b>313</b>



# 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものであり、

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 ( 特許出願中のものを含む ) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032 東京都港区六本木 3-2-31 IBM World Trade Asia Corporation Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

## 著作権使用許諾：


本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

# 商標

以下は、IBM Corporation の商標です。

BladeCenter™  
@server®  
eServer®  
eServer™  
ibm.com®  
IBM®

Netfinity®  
PowerPC®  
PS/2®  
RETAIN®  
ServerProven®  
ServeRAID™

Wake on LAN®  
Redbooks (logo) ™  
X-Architecture™  
xSeries®

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Intel、Intel Inside (ロゴ)、および Pentium は、Intel Corporation の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

本書の第2章およびセクション6.4の部分の著作権：Copyright (c) 2004-2005 - OSA Technologies, an Avocent Company. All Rights Reserved. 無断複写、転載を禁じます。許可を得てご使用ください。

# 前書き

IBM **@server**<sup>®</sup> xSeries<sup>®</sup> および BladeCenter<sup>™</sup> サーバーに搭載されるシステム管理ハードウェアは、お客様の総合的な管理計画に重要な役割を果たします。このハードウェアは、サーバーまたは BladeCenter シャーシに組み込まれるか、工場アダプターとして取り付けられ、オプションとしても入手可能です。システム管理ハードウェアは、管理者に重要な情報を提供し、オペレーティング・システムが稼働中でなくても、管理者はリモート側でサーバーを制御できるようになります。

この IBM Redbook では、現在 xSeries および BladeCenter システムで使用できる管理ハードウェアの全機種を紹介します。内蔵 Baseboard Management Controller、Remote Supervisor Adapter II ファミリーのアダプター、および BladeCenter 管理モジュールについて説明します。また、このハードウェアにアクセスするために使用するユーザー・インターフェースについて詳しく解説し、セキュリティー機能（SSL など）と認証機能（LDAP など）の構成方法も説明します。

本書は、システム管理ハードウェアの機能、その構成方法、使用法を理解してサーバー管理の向上を目指す、お客様、IBM<sup>®</sup> ビジネス・パートナー、および IBM 社員を対象としています。

## 本書の執筆チーム

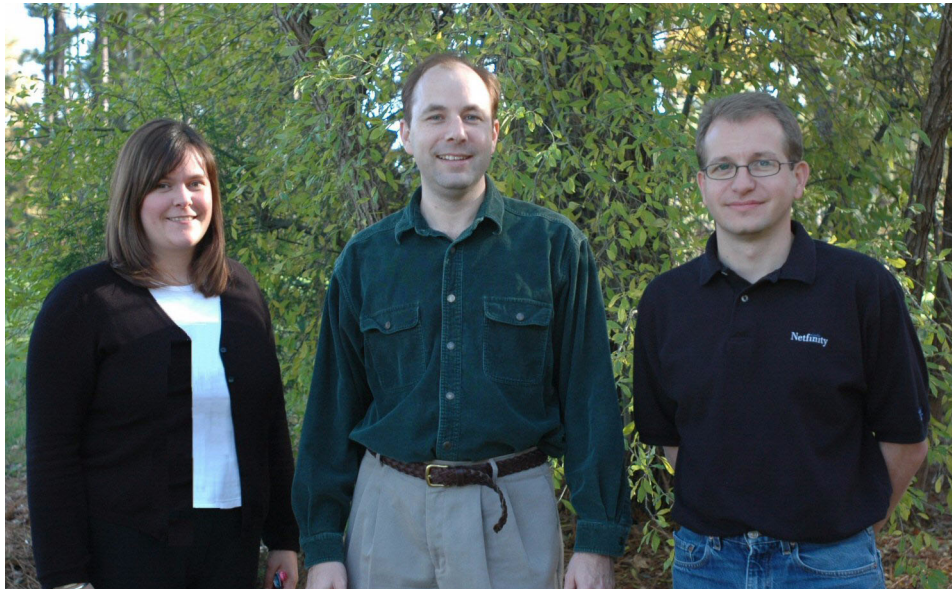
本書は、International Technical Support Organization, Raleigh Center に勤務する世界各国からの専門家チームによって作成されました。

**David Watts** は、ラーレーの IBM ITSO Center の顧問 IT スペシャリストです。研修員を統括し、IBM **@server** xSeries システムおよび関連クライアント・プラットフォームに関係したハードウェアとソフトウェアのトピックを扱う Redbook の制作に携わっています。これまでに、30 冊を超える Redbook および Redpaper の著書があります。クイーンズランド大学（オーストラリア）で工学士号を取得し、IBM に 15 年以上勤務しています。IBM **@server** xSeries 認定スペシャリスト、IBM 認定 IT スペシャリストの資格を取得しています。

**Lesley Bain** は、EMEA Advanced Technical Support Organization に勤務するシステム・エンジニアで、xSeries サーバーのスペシャリストです。スコットランドのグリーンロックの出身です。Presales Technical Support Organization に 5 年、IBM Server Development and Test Organization に 5 年の勤務経験があります。グラスゴー・カレドニア大学でコンピューター情報システムの学位を取得しています。専門分野は、xSeries システム管理ハードウェアとソフトウェアで、Remote

Supervisor Adapter、内蔵管理コントローラー、IBM Director ソフトウェアなどがその対象です。

**Christian Leitenberger** は、PROFI Engineering Systems AG（ドイツにおける IBM のビジネス・パートナー）に勤務するシステム・エンジニアで、xSeries のスペシャリストです。IBM Netfinity<sup>®</sup> と xSeries サーバーの経験が 6 年あり、それを含めて IT 分野で 11 年の経験を積んでいます。University of Cooperative Education (BA)（ドイツ、マンハイム）を卒業し、ビジネス情報テクノロジーの学位を取得しています。Windows<sup>®</sup> NT の MCSE、IBM @server xSeries 認定エキスパートです。専門分野は、xSeries ハードウェア、Windows クラスタリング、Storage Area Network、および VMware ESX Server です。



Redbook チーム (左から右へ): Lesley、David、Christian

このプロジェクトにご協力いただいた方々に感謝いたします。

Jay Bretzmann、Rob Sauerwalt、Bob Zuber  
Worldwide xSeries Product Management

Jason Brunson、Doug Clarke、Craig Elliott  
IBM xSeries Advanced Technical Support

Gerhard Buckler、Gregg Gibson、Raj Kantesaria、Eric Kern、Ed Klodnicki  
IBM xSeries Systems Management Hardware

Jason Almeida、Julia Dees、Danyell Shiflett、Ileana Vila  
IBM xSeries Systems Management Software

Eddy Ciliendo  
IBM Switzerland

Olaf Menke  
IBM Germany

Martin Gudmundsen  
Scribona AS, Norway

Julie Czubik  
International Technical Support Organization, Poughkeepsie Center

Reza Roodsari  
IPMI Systems Architect, OSA Technologies

## 執筆にご協力ください

2週間から6週間の研修プログラムに参加しませんか。特定の製品やソリューションを取り上げた IBM Redbook の制作に携わりながら、最先端のテクノロジーを実地に体験できます。IBM の技術専門家、ビジネス・パートナー、お客様とチームを組んで作業をします。

努力の成果は、製品の受け入れやお客様の満足度の向上に貢献します。さらに、IBM 開発研究所との人脈が築かれ、生産性や市場性の拡大にもつながります。

研修プログラムについての詳細は、研修のインデックスを表示してご確認のうえ、オンラインでお申し込みください。

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## ご意見をお寄せください

皆様のご意見は貴重です。

できるだけ皆様にお役に立つ Redbooks™ を制作したいと考えております。本書または他の Redbooks についてのご意見を、次の方法でお寄せ下さい。

- ▶ 次のサイトにあるオンライン「**Contact us**」レッドブックご意見フォームを使用する。

[ibm.com/redbooks](http://ibm.com/redbooks)

- ▶ ご意見を E メールで送付する。

[redbook@us.ibm.com](mailto:redbook@us.ibm.com)

- ▶ ご意見を郵送する。

IBM Corporation, International Technical Support Organization  
Dept. HZ8 Building 662  
P.O. Box 12195  
Research Triangle Park, NC 27709-2195



## 概要

IBM @server xSeries サーバーと IBM @server BladeCenter 製品ファミリーの重要な差別化要因は、ハードウェア・ベース、ソフトウェア・ベースの両面でのシステム管理機能にあります。システム管理機能は、サーバーの管理を容易にするとともに、包括的なアラート機能を備え、タスク・ベースの管理を可能にします。

エントリー・レベル環境から大規模なハイエンド・エンタープライズ環境にいたるまで、優れた総合的サーバー管理は、総所有コスト (TCO) 削減の鍵となります。

本書では、ハードウェア面での IBM システム管理ソリューションを対象とし、特に次の製品を取り上げます。

- ▶ 内蔵 Baseboard Management Controller
- ▶ Remote Supervisor Adapter II (PCI および SlimLine モデル)
- ▶ BladeCenter 管理モジュール

Web インターフェース、管理プロセッサのコマンド・ライン・インターフェース (MPCLI)、Advanced Settings ユーティリティ (ASU)、OSA System Management Bridge (SMBridge) ユーティリティなど、使用可能なユーザー・インターフェースを使用して xSeries サーバーおよび BladeCenter を管理する方法を説明します。

本書と対になるレッドブック「*Implementing Systems Management Solutions using IBM Director, SG24-6188*」は、IBM システム管理ソリューションのソフトウェア・コンポーネントである IBM Director について詳しく解説しています。

## 1.1 xSeries サーバーでサポートされるサービス・プロセッサ

表 1-1 は、各 IBM @server システムでサポートされるサービス・プロセッサの詳細を示しています。サポートは、3つのカテゴリーに分けられます。

- ▶ なし：このシステムは、このサービス・プロセッサをサポートしません。
- ▶ 標準：このサービス・プロセッサは、システム・プレーナーに組み込まれているか、または工場ですべてにプリインストールされています。
- ▶ オプション：このサービス・プロセッサは、オプションのアップグレード用として注文できます。

ヒント：この一覧表の最新版（旧 Netfinity サーバーのリストを含む）は、次のサイトで IBM 技術情報（IBM Technote）として入手できます。

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

表 1-1 IBM @server xSeries サーバーでサポートされるサービス・プロセッサ

サーバー	ASMP	ISMP	BMC	ASM PCI アダプター	RSA	RSA II	RSA II SlimLine
xSeries 200	なし	なし	なし	なし	なし	なし	なし
xSeries 205	なし	なし	なし	なし	オプション	オプション <sup>1</sup>	なし
xSeries 206	なし	なし	なし	なし	なし	オプション <sup>1</sup>	なし
xSeries 220	なし	なし	なし	なし	オプション	なし	なし
xSeries 225 (8647)	なし	なし	なし	なし	オプション	なし	なし
xSeries 225 (8649)	なし	なし	なし	なし	なし	オプション <sup>1</sup>	なし
xSeries 226	なし	なし	なし	なし	なし	オプション	なし
xSeries 230	標準	なし	なし	オプション	なし	なし	なし
xSeries 232	なし	標準	なし	なし	オプション	なし	なし
xSeries 235	なし	標準	なし	なし	オプション	オプション <sup>1</sup>	なし



サーバー	ASMP	ISMP	BMC	ASM PCI アダプター	RSA	RSA II	RSA II SlimLine
xSeries 236	なし	なし	標準	なし	なし	なし	オプション
xSeries 240	標準	なし	なし	オプション	なし	なし	なし
xSeries 250	標準	なし	なし	オプション	なし	なし	なし
xSeries 255	なし	標準	なし	なし	オプション	オプション <sup>1</sup>	なし
xSeries 300	なし	なし	なし	なし	なし	なし	なし
xSeries 305	なし	なし	なし	なし	オプション	オプション <sup>1</sup>	なし
xSeries 306	なし	なし	なし	なし	なし	オプション <sup>1</sup>	なし
xSeries 330 (8654)	標準	なし	なし	オプション	オプション <sup>2</sup>	なし	なし
xSeries 330 (8674)	標準	なし	なし	なし	オプション <sup>2</sup>	なし	なし
xSeries 330 (8675)	標準	なし	なし	なし	オプション <sup>2</sup>	なし	なし
xSeries 335	なし	標準	なし	なし	オプション	オプション <sup>3</sup>	なし
xSeries 336	なし	なし	標準	なし	なし	なし	オプション
xSeries 340	標準	なし	なし	オプション	なし	なし	なし
xSeries 342	なし	標準	なし	なし	オプション	なし	なし
xSeries 343	なし	なし <sup>4</sup>	なし	なし	なし	なし	なし
xSeries 345	なし	標準	なし	なし	オプション	オプション <sup>1</sup>	なし
xSeries 346	なし	なし	標準	なし	なし	なし	オプション
xSeries 350	標準	なし	なし	オプション	なし	なし	なし
xSeries 360	なし	なし	なし	なし	標準	なし	なし
xSeries 365	なし	なし	なし	なし	なし	標準	なし
xSeries 366	なし	なし	標準	なし	なし	なし	オプション
xSeries 370	なし	なし	なし	標準	なし	なし	なし
xSeries 380	なし	なし	なし	なし	なし	なし	なし
xSeries 382	なし	なし <sup>4</sup>	なし	なし	なし	なし	なし
xSeries 440	なし	なし	なし	なし	標準	なし	なし

サーバー	ASMP	ISMP	BMC	ASM PCI アダプター	RSA	RSA II	RSA II SlimLine
xSeries 445	なし	なし	なし	なし	標準	オプション <sup>5</sup>	なし
xSeries 450	なし	なし	なし	なし	標準	なし	なし
xSeries 455	なし	なし	なし	なし	標準	なし	なし
xSeries 460	なし	なし	標準	なし	なし	なし	標準
eServer™ 325	なし	なし	標準	なし	なし	なし	なし
eServer 326	なし	なし	標準	なし	なし	なし	なし

**表の注：**

1. リモート管理アダプター II をサポートするには、サーバーに最新のシステム BIOS、ISMP ファームウェア、および RSA II ファームウェアが必要です。
2. xSeries 330 (8654、8674、8675) は、リモート管理アダプターをゲートウェイとしてのみサポートします。オンボード ASMP は、すべてのシステム管理機能を提供します。x330 モデル 8674 と 8675 の場合、I2C ケーブル (20 ピン・ケーブル) を取り付ける必要があります。これはリモート管理アダプターに電力を供給するために使用します。外部 AC 電源は、冗長性の目的でのみ使用します。ただし、x330 モデル 8654 の場合は、I2C ケーブル (20 ピン・ケーブル) を取り付けてはなりません。アダプターに付属の外部 AC 電源を使用する必要があります。
3. xSeries 335 は、リモート管理アダプター II をサポートしますが、アダプターのビデオがオンボード・ビデオを使用不可にするため、x335 の C2T 機能は RSA II とは連動しません。RSA II のリモート・ビデオ機能を使用する場合は、お客様がそれぞれの x335 に RSA II をインストールする必要があります。詳細については、<http://www.ibm.com/pc/support/site.wss/MIGR-54747.html> を参照してください。
4. xSeries 343 と xSeries 382 には、システム管理機能を提供するサービス・プロセッサが標準装備されています。これらのシステムに追加のサービス・プロセッサをインストールすることはサポートされません。詳細については、サーバーの資料を参照してください。
5. xSeries 445 は、リモート管理アダプター II-EXA (部品番号 13N0382) をサポートしますが、リモート管理アダプター II (部品番号 59P2984) はサポートしません。

## 1.2 業界標準

業界標準は、今日の IT 環境で重要な役割を果たします。業界標準により、企業はその製品が将来導入される新規ハードウェアをサポートできるかどうかを心配せずに、自社の環境に最適な製品を選択できます。

IBM は、業界標準テクノロジーの使用を強く提唱しており、IBM @server では全面的に業界標準を採用しています。このセクションでは、主要なシステム管理標準について説明します。

## 1.2.1 Distributed Management Task Force

Distributed Management Task Force (DMTF) は、以下に示すように、数多くのシステム管理標準のガイドライン、規格、資料を開発しています。

▶ Common Information Model (CIM)

CIM は、システム、ネットワーク・アプリケーション、およびサービスの管理情報の共通定義を提供し、ベンダーによる拡張を許容しています。この共通定義により、ベンダーはネットワーク全体のシステム間で、豊富な管理情報を交換できます。

▶ Web-based Enterprise Management (WEBEM)

このイニシアチブは、企業コンピューター環境の一元管理を目的として開発された、管理およびインターネット標準テクノロジーの集合です。

▶ Alert Standard Format (ASF)

この仕様は、プリブート環境用のリモート制御およびアラート・インターフェースを定義しています。

▶ Systems Management BIOS (SMBIOS)

この SMBIOS 仕様は、Intel<sup>®</sup> アーキテクチャー・システム上の BIOS インターフェースを拡張することによって、マザーボードおよびシステムのベンダーが、それぞれの製品に関する管理情報を標準形式で提供する方法を示しています。

▶ Desktop Management Interface (DMI)

この標準は、デスクトップ PC、ノートブック、またはサーバー内のコンポーネントを管理し、追跡するための標準枠組みを生成します。

▶ Directory Enabled Network (DEN)

Directory Enabled Network イニシアチブは、CIM (システム、サービス、ポリシーなど) から概念をディレクトリーにマッピングし、この情報を管理インフラストラクチャー内の他の WEBEM エレメントと統合することによって、インテリジェント管理用のビルディング・ブロックを提供するように設計されています。

▶ Systems Management Architecture for Server Hardware (SMASH)

SMASH は、データ・センターを一元管理するための意味体系 (セマンティクス)、業界標準プロトコル、およびプロファイルを提供する一連の仕様です。

上記の標準についての詳しい情報は、次のサイトで入手できます。

<http://www.dmtf.org/standards>

## 1.2.2 IPMI

Intelligent Platform Management Interface (IPMI) は、以下の相互間のインターオペラビリティを可能にする共通プラットフォーム媒介機能インターフェースを定義します。

- ▶ オンボード (ベースボード) 管理コントローラーとシャーシの間
- ▶ ベースボード管理コントローラーとシステム管理ソフトウェアの間
- ▶ サーバーの相互間

IPMI により、次のことが可能になります。

- ▶ プラットフォーム管理情報への共通アクセス。これは次のもので構成されま  
す。
  - システム管理ソフトウェアを介したローカル・アクセス
  - LAN およびシリアル/モデムを介したリモート・アクセス
  - Intelligent Chassis Management Bus (ICMB) を介したシャーシ間アクセス
  - プロセッサがダウンしても使用可能な、LAN、シリアル/モデム、  
IPMB、PCI SMBus、または ICMB を介したアクセス
- ▶ 新規サーバー設計への移植を含めた、幅広いサーバーに対するサポート。
- ▶ IPMI インターフェースは、システム管理ソフトウェアをハードウェアから  
分離します。
- ▶ システム管理ソフトウェアに影響を与えずに、ハードウェアの改良が可能で  
す。
- ▶ IPMI により、クロスプラットフォーム管理ソフトウェアの使用が容易にな  
ります。

IPMI に関する詳しい情報は、次の URL で入手できます。

<http://www.intel.com/design/servers/ipmi>

## 1.2.3 SNMP

Simple Network Management Protocol (SNMP) は、TCP/IP ネットワークに接続された装置 (サーバー、ワークステーション、プリンター、ルーター、スイッチ、ハブなど) と通信するための一連のインターネット標準です。

SNMP メッセージを使用して装置をモニター/制御できる場合、その装置は SNMP 互換であると言います。これらの装置は、SNMP メッセージの送信、受信、応答のために、SNMP Agent ソフトウェアを搭載しています。SNMP では管理情報ベース (MIB) を使用し、これは SNMP 管理可能な装置から入手できる情報を定義しています。



## ベースボード管理コントローラー

多くの xSeries サーバーは、システム・ボードにサービス・プロセッサが組み込まれています。使用されているサービス・プロセッサのタイプに応じて、異なるレベルのモニターおよびアラート機能が提供されます。この章では、各種の内蔵サービス・プロセッサについて、その通信方式、機構、機能、配線、および構成を説明します。ここでは、以下について説明します。

- ▶ IBM @server 325 および 326 で使用されるベースボード管理コントローラー (BMC)。9 ページの 2.2、『e325 および e326 内の BMC』を参照してください。
- ▶ xSeries および BladeCenter ベースのサーバーで使用される BMC。18 ページの 2.3、『xSeries サーバー内の BMC』を参照してください。
- ▶ 以前のサーバーに見られる内蔵システム管理プロセッサ (ISM プロセッサ)。47 ページの 2.4、『内蔵システム管理プロセッサ』を参照してください。

4 番目のタイプは、システム管理プロセッサ (ASM プロセッサ) で、これは営業活動が中止された古いサーバーにのみ見られます。この装置に関する情報は、IBM Redbook 「*Netfinity Server Management, SG24-5208*」を参照してください。

## 2.1 機能の比較

表 2-1 は、3 つのタイプの xSeries 内蔵サービス・プロセッサに標準装備されている主要な機能を示しています。

表 2-1 内蔵コントローラーの機能の比較

機能	BMC (e325 と e326)	BMC (xSeries サーバー)	ISM プロセッサ
RS-485 インターコネクト・ネットワーク	なし	なし	サポート
LAN/ シリアル経由のリモート・アクセス	サポート	サポート	サポート <sup>1</sup>
Serial-over-LAN	サポート	サポート	なし
リモート・システム電源制御	サポート	サポート	サポート <sup>2</sup>
テキスト・コンソール・リダイレクト	サポート	サポート	なし
リモート・アウト・オブ・バンド・アラート	サポート	サポート	サポート <sup>2</sup>
インバンド・アラート	サポート <sup>3</sup>	サポート <sup>3</sup>	サポート <sup>3</sup>
アウト・オブ・バンド環境モニター	サポート	サポート	サポート <sup>2</sup>
システム電圧モニター	サポート	サポート	サポート
バッテリー電圧モニター	サポート	サポート	なし
システム温度モニター	サポート	サポート	サポート
ファン速度制御	サポート	サポート	サポート
ファン・タコメーター・モニター	サポート	サポート	サポート
電源正常信号モニター	サポート	サポート	サポート
システム・リセット制御	サポート	サポート	サポート
NMI 検出	サポート	サポート	サポート
SMI 検出と生成	なし	サポート	
リマインド・ボタン検出	なし	サポート	サポート
オート・サーバー・リスタート・ウォッチドッグ・アラート	サポート	サポート	サポート
システム LED 制御 (電源、ディスク、アラート)	サポート	サポート	サポート

機能	BMC (e325 と e326)	BMC (xSeries サーバー)	ISM プロセッサ
Lightpath LED 制御	サポート	サポート	サポート
<p>注:</p> <ol style="list-style-type: none"> <li>この機能には、リモート管理アダプター II の追加が必要です。</li> <li>この機能は、ASM インターコネクト (RS-485) 経由、またはリモート管理アダプター II の追加により可能になります。</li> <li>インバンド・アラートは、IBM Director Agent V4 以降のインストールが必要です。</li> </ol>			

## 2.2 e325 および e326 内の BMC

BMC を介したシステム管理では、ユーザーはローカル側またはリモート側でサーバーを管理できます。BMC には、IPMI 準拠、テキスト・コンソール・リダイレクトまたはシリアル/共用 LAN、リモート・アウト・オブ・バンド・アラート、無人ファームウェア更新、PXE などの機能が組み込まれています。

BMC は、QLogic チップをベースとし、IPMI 仕様のバージョン 1.5 をインプリメントしています。仕様書は、次のサイトから入手できます。

[ftp://download.intel.com/design/servers/ipmi/IPMiv1\\_5rev1\\_1-012904markup.pdf](ftp://download.intel.com/design/servers/ipmi/IPMiv1_5rev1_1-012904markup.pdf)

### 2.2.1 外部接続

BMC は、システム Gigabit Ethernet のポート 1 を介して通信します。BMC と通信するには、標準イーサネット・ケーブルを接続します。正常な通信を確保するために、表 2-2 を参照して、BMC と共用できるイーサネット・ポートの詳細を確認してください。

**注:** xSeries サーバーの BMC とは異なり、ping を使用して接続が有効であるかどうかを確認できません。

表 2-2 BMC との共用イーサネット・ポート

サーバー	BMC と共用するシステム・イーサネット・ポート
eServer 325	イーサネット・ポート 1
eServer 326	イーサネット・ポート 1

正しいポートの位置は、10 ページの図 2-1 を参照してください。

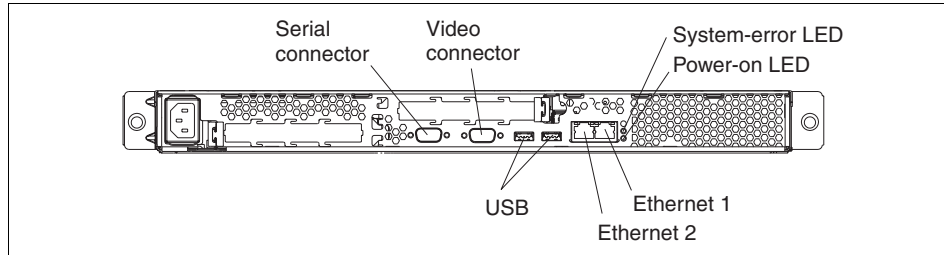


図 2-1 e325 および e326 サーバーの背面のコネクター

## 2.2.2 BMC ファームウェアのアップグレード

このセクションでは、e325 および 326 サーバー上の BMC のファームウェアをアップグレードするプロセスを説明します。

ファームウェアは、ISO イメージとしてダウンロードするか（この場合、CD を作成するための CD バーナーが必要です）、または EXE ファイルとしてダウンロードできます（これは、ブート可能ディスクを作成します）。次の手順に従って、最新の BMC ファームウェア更新をダウンロードしてください。

1. IBM 技術情報「*IBM @server xSeries BMC - Firmware and Drivers Cheatsheet, TIPS0532*」を参照して、該当するサーバー用のファームウェアのリンクをクリックします。

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

代わりに、次のサイトから該当するダウンロード・ページにナビゲートすることもできます。

<http://www.pc.ibm.com/support>

2. ディスクレット・イメージを作成する場合は、EXE ファイルを選択します。CD に焼き付ける場合は、ISO ファイルを選択します。

**注：**e325 と e326 は、ディスクレット・ドライブが標準装備されていません。EXE を使用してディスクレットを作成する予定の場合は、USB 接続の外付けディスクレット・ドライブを用意して、サーバーに接続する必要があります。

3. CD またはディスクレットを作成した後、メディアを挿入し（必要な場合は、外付けの USB 接続ディスクレット・ドライブを接続）、サーバーを再始動します。
4. ディスクレットからブートする場合、BIOS Configuration/Setup ユーティリティ・プログラムに入り（サーバーの始動中に F1 を押す）、外付け USB



ディスク・ドライブを始動装置として構成することが必要な場合があります。

5. 更新が完了すると、BMC の構成を行う準備ができています。11 ページの 2.2.3、『BMC の構成』を参照してください。
6. すでに BMC を構成済みの場合は、ディスクをドライブから取り出して、サーバーを再始動してください。

## 2.2.3 BMC の構成

lancfg 構成ユーティリティーが、この BMC を構成するために使用できる方法です。ネットワーク設定を構成した後は、IBM Director を使用して、ユーザー ID、パスワード、およびアラート転送プロファイルを構成できます。この両方の方法について、以下で説明します。

### lancfg を使用した BMC の構成

lancfg 構成ユーティリティーを使用して、必要な構成設定をすべて行うことができます。このユーティリティーは、前に BMC ファームウェアのアップグレードで作成した BMC ファームウェア・ディスクまたは CD に入っています。

**注：**LAN 構成ユーティリティー (lancfg.exe) は、始動可能な BMC 管理コントローラー用のファームウェア更新ディスク /CD からサーバーを始動した後、DOS セッションを立ち上げて実行する必要があります。Windows 内の DOS ウィンドウからこのユーティリティーを実行してはなりません。

1. BMC ファームウェアの更新が完了した後、コマンド・プロンプトが表示されます。lancfg と入力して、Enter を押してください。LAN 構成ユーティリティーが開始し、「BMC Information」画面が表示されます。表示されるデフォルト値は、読み取り専用です。この画面では変更できません。
2. LAN 構成ユーティリティーを使用するには、F10 を押し、矢印キーを使ってウィンドウ上部のメニュー項目を選択します。
3. 「LanCfg」を選択します。「LAN Configuration」画面が表示されます。12 ページの図 2-2 を参照してください。

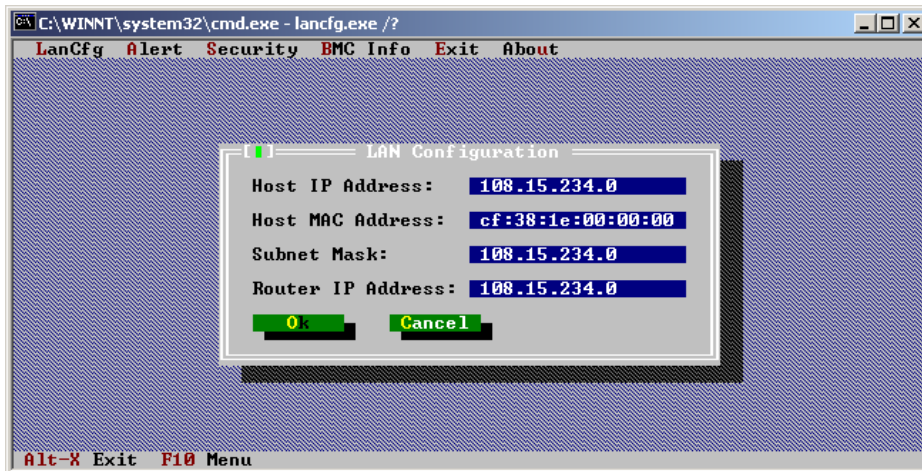


図2-2 LAN 構成画面

4. フィールドを編集するにはタブを押して、以下のフィールドに BMC の必要な情報を入力し、「OK」を選択します。
  - ホスト IP アドレス
  - サブネット・マスク
  - ルーター IP アドレス

注：「Host MAC Address」フィールドは読み取り専用で、LAN 構成ユーティリティーからは変更できません。

5. 「OK」を選択して、情報メッセージを閉じます。
6. F10 を押してメニューに入り、「Alert」を選択して、イベント宛先アドレスを入力します。「Alert Setting」画面が表示されます。13 ページの図 2-3 を参照してください。

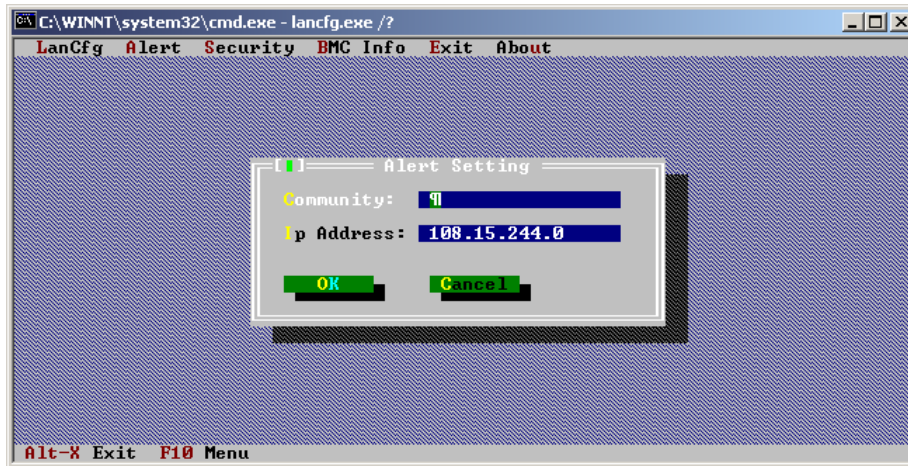


図 2-3 「Alert Settings」 ウィンドウ

- アラートの送信先の宛先 IP アドレスを入力し、該当するコミュニティ名もフィールドに入力します。入力する IP アドレスは、IBM Director のようなプラットフォーム・イベント・トラップ (PET) リスナーの IP アドレスです。「OK」を選択して保管した後、「OK」を選択して情報画面をクローズします。LAN アラートは、SNMP トラップとして PET フォーマットで、指定されたアラート宛先に送信されます。
- F10 を押してメニューに入り、「Security」を選択して、ログイン設定を表示または変更します。「Security Setting」画面が表示されます。14 ページの図 2-4 を参照してください。

**注：**デフォルトのユーザー ID とパスワードは、USERID と PASSWORD です (0 はゼロで、文字の O ではありません)。これは、すべての IBM サービス・プロセッサのデフォルトのユーザー ID とパスワードです。ユーザー ID とパスワードの変更方法は、後続のセクションで説明します。

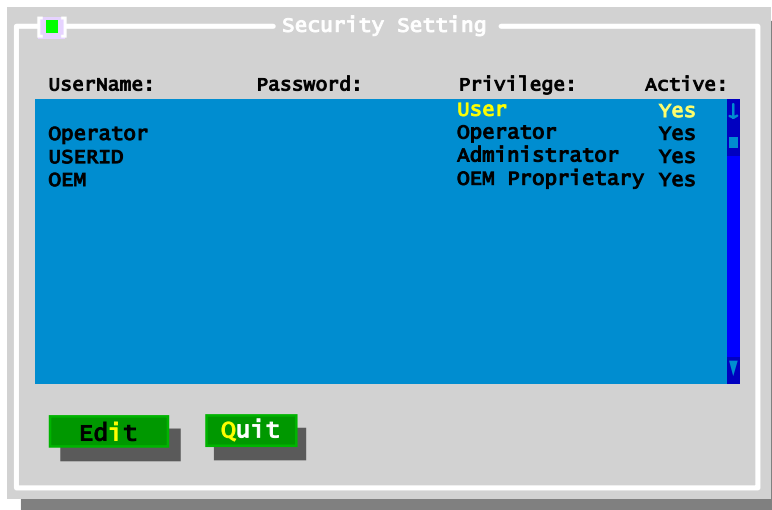


図 2-4 「Security Settings」画面

- この画面で、BMC ユーザー・アカウントを保守できます。この画面で変更を行うには、「Edit」を選択し、「Edit」画面に変更内容を入力して、「OK」を選択します。
- 必要な変更をすべて行った後、LAN 構成ユーティリティを終了する前に、ファームウェア更新ディスクレットをディスクレット・ドライブから取り出します。
- 「Exit」を選択します。サーバーの再始動を求めるプロンプトが出たら、「Reboot」を選択します。

## IBM Director を使用した BMC の構成

ご使用の環境に IBM Director サーバーがインストールされており、BMC のネットワーク設定が正しく構成されている場合は、この方法を使用して BMC に関する設定を構成できます。これにより、BMC OOB の管理も可能になります。このセクションでは、ユーザー ID、パスワード、およびアラート転送設定の構成方法について説明します。

- Director コンソールから、ブランク域の中央ペインで右クリックします。「New」→「Physical Platform」を選択します。
- 15 ページの図 2-5 のようなウィンドウが表示されます。追加する BMC の適切な名前と IP アドレスの詳細を入力して、「OK」を選択します。

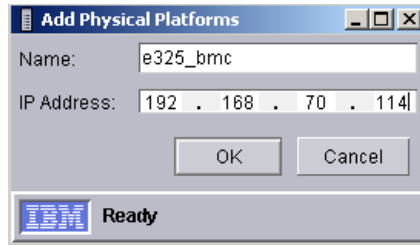


図 2-5 「Add Management Processors」 ウィンドウ

3. BMC が検出されると、IBM Director コンソール上に、アウト・オブ・バンド物理プラットフォーム・オブジェクトとして表示されます。
4. 図 2-6 に示すように、IBM Director コンソールの「Group Contents」に BMC が表示されます。



図 2-6 BMC が追加された IBM Director コンソールの「Group Contents」 ペイン

5. IBM Director は、デフォルトの USERID/PASSWORD 組み合わせを使用して、BMC へのアクセスを試みます。  
 デフォルトの USERID/PASSWORD 組み合わせを削除または変更した場合、小さいパッドロック・アイコンが装置の横に表示されます。装置を右クリックして、「Request Access」をクリックし、有効なユーザー ID とパスワードを入力します。
6. これで、「MPA Task」を使用して、ユーザー ID、パスワード、アラート転送プロファイルなどの設定値を構成できるようになりました。
7. BMC オブジェクトを右クリックして、「Management Processor Assistant」→「Configuration」を選択するか、または右側のペインの「Management Processor Assistant Task」を展開して「Configuration」を強調表示し、構成タスクを BMC オブジェクトにドラッグ・アンド・ドロップします。
8. 「Management Processor Assistant」ウィンドウが開いたら、変更する設定を選択します。ユーザー ID とパスワードを変更するには、左側のメニューから「Login profiles」を選択します。
9. 新規ユーザーを追加するには、任意のログイン・プロファイルをクリックします。これにより、項目が強調表示されます。「Add an Entry」を選択します。これは新規のログイン・プロファイルを追加します。フィールドをダブ

ルをクリックすることにより、既存のユーザーを変更することもできます。  
16 ページの図 2-7 を参照してください。

Server	Entry number	User ID	Password	Confirm password	Authority
E325_bmc	1		*****	*****	Read only ▼
E325_bmc	2	Operator	*****	*****	Operator ▼
E325_bmc	3	USERID	*****	*****	Supervisor ▼
E325_bmc	4	OEM	*****	*****	Custom ▼

図2-7 ログイン・プロファイルの設定

10. 「User ID」 フィールドをダブルクリックして、ユーザー名を入力します。
11. 次に、「Password」 フィールドをダブルクリックして、適切なパスワードを入力します。
12. 「Confirm Password」 フィールドをダブルクリックして、再度、パスワードを入力します。
13. 必要な許可レベルを指定します。選択項目は、次のとおりです。
  - 「*Supervisor*」 は、次の特権を示します。
    - ユーザー・アカウント管理
    - リモート・コンソール・アクセス
    - リモート・コンソールおよび仮想メディア・アクセス
    - リモート・サーバーおよび電源 / 再始動アクセス
    - イベント・ログ消去の権限
    - 基本アダプター構成
    - アダプター構成（ネットワーキングとセキュリティー）
    - 拡張アダプター構成
  - 「*Read only*」 は、データはすべて表示のみ可能であることを示します。更新は許可されません。
  - 「*Operator*」 は、次の特権を示します。
    - リモート・サーバーおよび電源 / 再始動アクセス
    - イベント・ログ消去の権限
  - 「*Custom*」 は、ユーザーの希望する内容を指定できることを示します。
14. 設定を構成した後、「Apply」 をクリックして変更を確定します。
15. アラート転送プロファイルを変更するには、左側のメニューから「Alert-forwarding profile」を選択します。右側に、次のようなペイン（図 2-8）が表示されます。

Server	Entry number	Status	Description	Connection type	IP address or host name
E325_bmc	4	Enabled	Not supported	IBM Director Comprehensive	192.168.70.107

図 2-8 アラート転送プロファイル

16. 4 つのプロファイルを設定できます。
17. 新規のプロファイルを追加するには、既存のプロファイルの 1 つをクリックして、「**Add an entry**」をクリックします。詳細を入力し、「**Apply**」をクリックして変更を確定します。

**注：**表示される設定をすべて変更できるわけではありません。表示される設定の一部のものは、BMC には適用されません。そのようなフィールドには、「not supported」と表示されています。

## 2.2.4 OSA IPMI デバイス・ドライバーのインストール

デバイス・ドライバーは、オペレーティング・システムをサポートするために必要であり、また IBM Director とのインバンド通信を使用可能にするためにも必要です。

使用可能なデバイス・ドライバーをダウンロードするには、IBM 技術情報「*IBM @server xSeries BMC - Firmware and Drivers Cheatsheet, TIPS0532*」を参照して、該当するサーバー用のドライバーのリンクをクリックします。

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

代わりに、次のサイトから該当するダウンロード・ページにナビゲートすることもできます。

<http://www.pc.ibm.com/support>

**注：**本書の作成日現在では、入手できるドライバーは、Windows 用のみ (Linux や NetWare 用はありません)、しかも eServer 325 上の BMC 用のみ (eServer 326 用はありません) でした。

必要なデバイス・ドライバーの明細は、表 2-3 を参照してください。

表2-3 IPMI に必要なデバイス・ドライバー

デバイス・ドライバー	補足説明
IPMI デバイス・ドライバー	<ul style="list-style-type: none"> <li>▶ IPMI ライブラリー・ファイルをサポートするために必要</li> <li>▶ IBM Director とのインバンド通信に必要</li> </ul>
IPMI ライブラリー (sp6lib)—OSA BMC マッピング・レイヤー (ライブラリー) ファイル	<ul style="list-style-type: none"> <li>▶ BMC マッピング・レイヤー (ドット・コマンドを IPMI コマンドにマップ)</li> <li>▶ IBM Director とのインバンド通信に必要</li> </ul>
ASR サーバー再始動ソフトウェア	<ul style="list-style-type: none"> <li>▶ ASR 機能に必要</li> </ul>

デバイス・ドライバーは特定の順序でインストールする必要があるため、順序を守らないとインストールに失敗します。順序は、次のとおりです。

1. IPMI デバイス・ドライバー
2. IPMI マッピング・レイヤー・ファイル (ライブラリー)
3. IPMI ASR サービス

これらのドライバーは、前述の Web サイトから EXE をダウンロードし、EXE を実行して、画面の指示に従います。プロンプトで指示された場合は、システムをリブートしてください。無人インストール手順も使用できます。インストール方法は、README.TXT ファイルを参照してください。

## 2.2.5 イベント・ログ

BMC システム・イベント・ログ (SEL) は、BIOS からアクセスするか、または IBM Director のようなツールからアクセスできます。

**注:** システム・イベント・ログは、128 個の項目を記録できます。ログが満杯の 75 パーセントと 90 パーセントに達した時点で、アラートを受け取ります。ただし、ログが満杯になった後は、新規の入力は保管されません。この時点で、ログを消去する必要があります。

## 2.3 xSeries サーバー内の BMC

xSeries サーバー内のベースボード管理コントローラー (BMC) は、サーバーの環境モニター機能を備えています。環境条件がしきい値を超えたり、システム・コンポーネントに障害が起きた場合、ベースボード管理コントローラーは、LED を点灯して、ユーザーの問題診断を援助し、BMC システム・イベント/エラー・ログにもエラーを記録します。



BMC は、Hitachi 2166 チップをベースとし、IPMI 仕様のバージョン 1.5 をインプリメントしています。仕様書は、次のサイトから入手できます。

[ftp://download.intel.com/design/servers/ipmi/IPMIV1\\_5rev1\\_1-012904markup.pdf](ftp://download.intel.com/design/servers/ipmi/IPMIV1_5rev1_1-012904markup.pdf)

ここでは、以下のトピックについて説明します。

- ▶ 19 ページの 2.3.1、『機能』
- ▶ 19 ページの 2.3.2、『外部接続』
- ▶ 22 ページの 2.3.3、『BMC ファームウェアの更新』
- ▶ 23 ページの 2.3.4、『BMC\_CFG を使用した BMC の構成』
- ▶ 35 ページの 2.3.5、『BIOS 内での BMC の構成』
- ▶ 38 ページの 2.3.7、『IBM Director による BMC の構成』
- ▶ 42 ページの 2.3.9、『BMC デバイス・ドライバーのインストール』

## 2.3.1 機能

この内蔵 BMC は、次の機能を備えています。

- ▶ システム電圧モニター
- ▶ バッテリー電圧モニター
- ▶ システム温度モニター
- ▶ ファン速度制御
- ▶ ファン・タコメーター・モニター
- ▶ 電源正常シグナル・モニター
- ▶ システム ID およびプレーナー・バージョン検出
- ▶ システム電源制御
- ▶ システム・リセット制御
- ▶ NMI 検出
- ▶ SMI 検出および生成
- ▶ シリアル・ポート・テキスト・リダイレクト
- ▶ リマインド・ボタン検出
- ▶ システム LED 制御（電源、HDD、アクティビティ、アラートなど）
- ▶ Lightpath LED 制御

全機能の明細は、8 ページの表 2-1 を参照してください。

## 2.3.2 外部接続

BMC は、サーバーの内蔵イーサネット・アダプターのいずれかを介して通信します。BMC と通信するには、標準イーサネット・ケーブルを接続します。正常な通信を確保するために、表 2-4 を参照して、BMC と共用できるイーサネット・ポートの詳細を確認してください。

**注：** ping コマンドを使用して、この接続が有効であることを確認できます。

表2-4 BMC との共用イーサネット・ポート

サーバー	BMC と共用するシステム・イーサネット・ポート
xSeries 236	イーサネット・ポート 1
xSeries 336	イーサネット・ポート 1
xSeries 346	イーサネット・ポート 1
xSeries 366	イーサネット・ポート 1
HS20 (8843)	なし。BMC 機能は管理モジュールを通して提供されます。
HS40 (8839)	なし。BMC 機能は管理モジュールを通して提供されます。

以下に、上記の xSeries サーバーのコネクタの位置を示します。

- ▶ x346: 20 ページの図 2-9
- ▶ x336: 21 ページの図 2-10
- ▶ x236: 21 ページの図 2-11
- ▶ x366: 22 ページの図 2-12

ヒント：サーバーに RSA II SlimLine を搭載した場合も、システム・イーサネット・ポートが BMC へのアクセスに使用するポートとなります。ただし、セキュリティ上の目的で、IP アドレスを無効な値（例えば、0.0.0.0）に設定して、BMC への接続を使用不可にすることもできます。

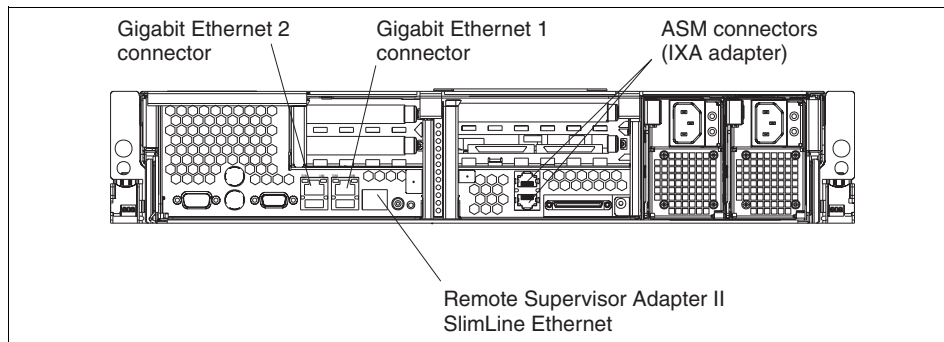


図 2-9 xSeries 346 の背面のポート

x346 や x366 のようなサーバーのリモート管理アダプター II SlimLine イーサネット・コネクタは、システム管理情報制御のためにサーバーをネットワークに接続するためのものです。このコネクタは、リモート管理アダプター II SlimLine を搭載した場合にのみアクティブになります。

x236、x346、および x366 の ASM コネクタは、サーバーを統合 xSeries アダプター (IXA) に接続するのに使用します (IXA がサーバーに搭載されている場合)。このコネクタは、ASM インターコネクト・ネットワークの形成には使用されません (ASM インターコネクト・ネットワークはサポートされません)。

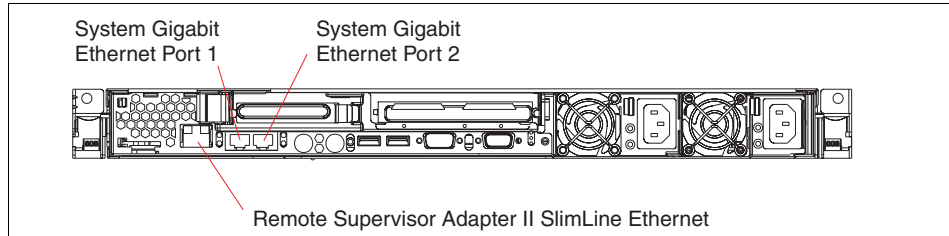


図 2-10 xSeries 336 の背面のポート

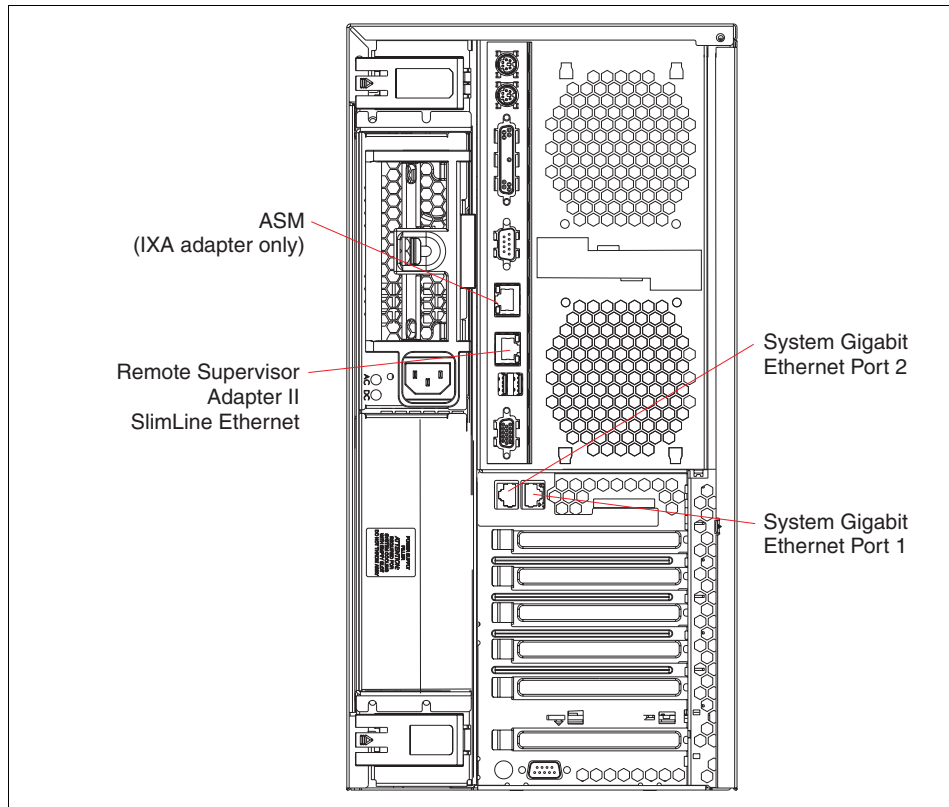


図 2-11 xSeries 236 の背面のポート

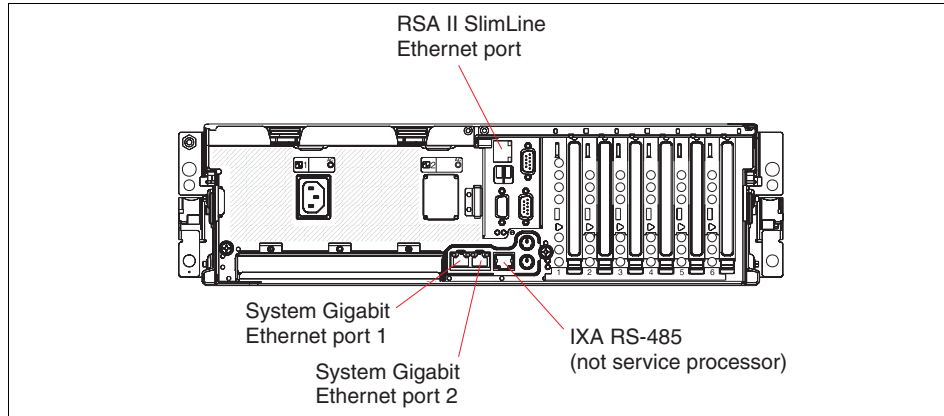


図2-12 x366 の背面のポート

### 2.3.3 BMC ファームウェアの更新

このセクションでは、xSeries サーバーの BMC をアップグレードするプロセスについて説明します。問題の発生を回避するには、BMC ファームウェアを最新レベルに保つのが最良の方法です。

**注:** BMC のファームウェアを更新しても、ユーザー設定は変更されません。

手順は、次のとおりです。

1. ご使用のサーバー用の適切なファームウェアをダウンロードします。IBM 技術情報「*IBM @server xSeries BMC - Firmware and Drivers Cheatsheet, TIPS0532*」を参照して、該当するサーバー用のファームウェアのリンクをクリックします。

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

代わりに、次のサイトから該当するダウンロード・ページにナビゲートすることもできます。

<http://www.pc.ibm.com/support>

2. BMC ファームウェア更新は、通常はブート可能ディスク形式 (EXE ファイル) で入手できますが、CD 作成用の ISO イメージ・ファイルとして入手できる場合もあります。x336 のようなサーバーの場合、サーバーにディスク・ドライブが標準装備されていないため、ISO ファイルが必要になります。ディスクまたは CD を作成します。
3. メディアをサーバーに挿入して、サーバーをブートします。場合によっては、POST/BIOS setup ユーティリティを使用して、正しいブート・デバイスを構成することが必要になります。

4. システムが始動すると、RAM ドライブが作成され、該当するファイルがこの RAM ドライブにコピーされて、BMC ファームウェアの更新が自動的に実行されます。
5. BMC ファームウェアの更新が終了したら、引き続きファームウェア更新ディスクまたは CD-ROM を使用して、サーバーを構成することができます。詳しくは、23 ページの 2.3.4、『BMC\_CFG を使用した BMC の構成』を参照してください。
6. すでに BMC を構成済みの場合は、メディアを取り出して、システムを再起動してください。

### 2.3.4 BMC\_CFG を使用した BMC の構成

初期 BMC ネットワーク設定 (IP アドレス、サブネット・マスク、ゲートウェイ) の構成には、2つの方法を使用できます。

- ▶ BIOS の「System Setup」を使用して (ブート時に F1 を押す)、「Advanced Options」メニューから BMC 設定にアクセスする。これについては、35 ページの 2.3.5、『BIOS 内での BMC の構成』で説明します。

BIOS の「Setup」を使用するのが、推奨される方法です。ネットワーク設定を構成した後、IBM Director の管理プロセッサ (MPA) を使用して、他の必要な設定 (ユーザー ID、パスワード、およびアラート宛先) を構成できます。

- ▶ ファームウェア更新ディスクから `bmc_cfg.exe` 構成ユーティリティーを使用する。このセクションでは、この方法について説明します。

`Bmc_cfg` は、主にデバッグ・ツールと考えられますが、これを使用して BMC 構成設定を表示または変更することもできます。`bmc_cfg.exe` 構成ユーティリティーを使用して、すべての必要な構成設定を行うことができます。22 ページの 2.3.3、『BMC ファームウェアの更新』で説明したように、このユーティリティーは BMC ファームウェア更新ディスクまたは CD に含まれています。独立したツールとして入手することはできません。

**注:** `bmc_cfg` は、ブート可能 BMC 管理ファームウェア更新ディスク / CD からサーバーをブートした後、DOS に出ることによってのみ実行できます。Windows のコマンド・プロンプトからこのユーティリティーを実行してはなりません。

BMC のアウト・オブ・バンド通信を使用可能にする計画の場合は、次の設定を構成する必要があります。

- ▶ IP アドレス。『IP アドレスの設定』（25 ページ）を参照してください。
- ▶ サブネット・マスク。『サブネット・マスクの設定』（26 ページ）を参照してください。
- ▶ デフォルト・ゲートウェイ。『デフォルト・ゲートウェイの設定』（26 ページ）を参照してください。
- ▶ アラート通知およびアラート宛先の設定。『BMC アラートを送信する宛先の設定』（26 ページ）を参照してください。

ユーザー ID とパスワードをデフォルトの USERID と PASSWORD から変更することもお勧めします。セキュリティ設定を変更するには、以下の変更が必要です。

- ▶ ユーザー ID とパスワード。『ユーザーの追加または変更』（28 ページ）を参照してください。
- ▶ ユーザー特権。『ユーザーに与えられるアクセス権限の設定』（31 ページ）を参照してください。

次の手順を実行して、bmc\_cfg を開始します。

1. いま BMC のファームウェアを更新したところであれば、更新ユーティリティを終了して、DOS プロンプトに戻ります。そうでない場合は、ファームウェア更新ディスク/CD からブートし、ファームウェアを更新するかどうかを尋ねるプロンプトが出たら「No」を選択します。
2. DOS プロンプトで、bmc\_cfg と入力します。メインメニュー画面が表示されます（24 ページの図 2-13）。

```
BMC Config Utility V1.12.0.15, (C)2004 OSA Technologies, Inc.

1.  Get Device ID
2.  IPM Device "Global" Commands Group
3.  BMC Device and Messaging Commands Group
4.  Chassis Device Commands Group
5.  SDR Device Commands Group
6.  SEL Device Commands Group
7.  LAN Device Commands Group
8.  Serial/Modem Device Commands Group
9.  Manual Command Configuration

(h)Help (e)Exit
=> Enter your choice:
```

図 2-13 BMC\_cfg メインメニュー

## IP アドレスの設定

次の手順に従って、サービス・プロセッサの IP アドレスを固定アドレスに設定します。

1. メインメニューから「7」を入力して、「Set LAN Device Commands Group」を選択します。図 2-14 が表示されます。

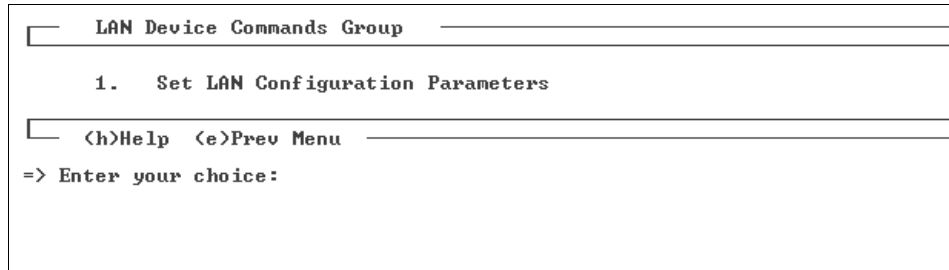


図 2-14 LAN デバイス・コマンド・グループ

2. 「1」を入力して、「Set LAN Configuration Parameters」を選択します。25 ページの図 2-15 が表示されます。

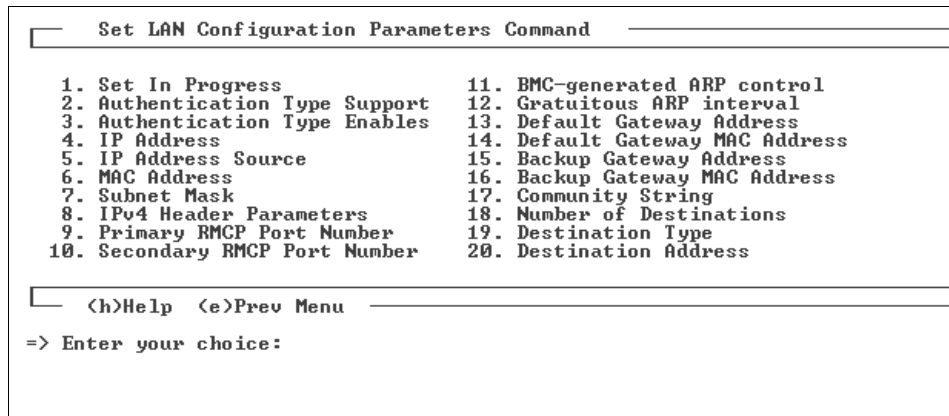


図 2-15 LAN 構成パラメーター・コマンド・メニュー

3. 「4」を入力して、IP アドレスを選択します。
4. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
  - 1 = LAN
  - 2 = シリアル
5. 「1」を入力して、IP アドレスを更新します。
6. BMC の IP アドレスを入力して、Enter を押します。

7. 「C」を入力して、変更を確定します。
8. 「E」を入力して、図 2-15 に戻ります。

**注:** オプション 5 の「IP Address Source」は DHCP を使用可能にしますが、テストの結果、これは機能しないことが示されました。したがって、上述の固定 IP アドレスを使用する必要があります。

### サブネット・マスクの設定

次の手順に従って、サービス・プロセッサのサブネット・マスクを設定します。

1. 図 2-15 から、「7」を入力して、サブネット・マスクを選択します。
2. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
  - 1 = LAN
  - 2 = シリアル
3. 「1」を入力して、サブネット・マスク値を更新します。
4. BMC のサブネット・マスクを入力して、Enter を押します。
5. 「C」を入力して、変更を確定します。
6. 「E」を入力して、図 2-15 に戻ります。

### デフォルト・ゲートウェイの設定

次の手順に従って、サービス・プロセッサのゲートウェイを設定します。

1. 25 ページの図 2-15 から、「13」を入力して、デフォルト・ゲートウェイ・アドレスを選択します。
2. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
  - 1 = LAN
  - 2 = シリアル
3. 「1」を入力して、ゲートウェイ値を更新します。
4. デフォルト・ゲートウェイのアドレスを入力して、Enter を押します。
5. 「C」を入力して、変更を確定します。
6. 「E」を入力して、25 ページの図 2-15 に戻ります。

### BMC アラートを送信する宛先の設定

BMC は、アラートの送信先として最大 4 つの宛先をサポートします。指定するアラート受信装置は、PET トラップ (プラットフォーム・イベント・トラップ)



を受信できなければなりません。IBM Director サーバーを稼働しているシステムは、PET トラップを受信できます。

次の手順に従って、BMC のアラート送信先を指定します。

1. 25 ページの図 2-15 から、「20」を入力して、デフォルト宛先を選択します。
2. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
  - 1 = LAN
  - 2 = シリアル
3. 変更する宛先の番号として、1、2、3、または 4 を入力します。
4. BMC アラートの送信先 IP アドレスを入力して、Enter を押します。例えば、この送信先を IBM Director 管理サーバーにすることができます。
5. 「C」を入力して、変更を確定します。
6. 「E」を入力して、25 ページの図 2-15 に戻ります。

## 宛先タイプの設定

宛先タイプは、BMC からのアラートを受信するシステムのタイプを指定します。現在サポートされているのは、PET 1.0（プラットフォーム・イベント・トラップ、IPMI 標準）だけです。構成するそれぞれの宛先ごとに、宛先タイプを設定する必要があります（最大 4 つ）。

PET は、特定の形式の SNMP で、トラップ・ハンドラーが実際にアラートを受け取ったことを確認するための確認通知を含んでいます。IPMI V1.5 は、アラートの送信を再試行する時期と、応答がない場合の再試行の頻度も指定します。IBM Director サーバーは、PET 1.0 タイプのアラートを受信できます。

次の手順に従って、サービス・プロセッサの宛先タイプを設定します。

1. 「19」を入力して、宛先タイプを選択します。
  2. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
    - 1 = LAN
    - 2 = シリアル
  3. 変更する宛先の番号として、1、2、3、または 4 を入力します。
  4. 変更するオプションを選択します。
    - 1 = 宛先タイプ
    - 2 = アラート確認応答のタイムアウト / 再試行間隔（秒数）
    - 3 = 再試行回数
- 「1」を入力して、宛先タイプの設定を変更します。

5. 「00」を入力して、PET トラップ宛先を選択します。これがサポートされる唯一の選択項目です。
6. 「E」を入力して、前のメニューに戻ります。
7. 「C」を入力して、変更を確定します。
8. 「E」を入力して、25 ページの図 2-15 に戻ります。

### SNMP コミュニティー名の設定

SNMP コミュニティー名を設定するには、次のようにします。

1. 「17」を入力して、コミュニティ名を選択します。
2. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
  - 1 = LAN
  - 2 = シリアル
3. 「1」を入力して、コミュニティ名を変更します。
4. 必要なコミュニティ名を入力して、Enter を押します。
5. 「C」を入力して、変更を確定します。
6. 「E」を入力して、25 ページの図 2-15 に戻ります。

### ユーザーの追加または変更

BMC へのリモート・アクセスは、ユーザー ID とパスワードによって制御されます。4 つのユーザー ID がありますが、変更できるのは、ID 2、3、4 だけです。ユーザー ID 1 は、ヌル・ユーザーであり、IPMI 仕様により、変更できません。

**注:** デフォルトでは、ユーザー ID 2 は USERID、パスワードは PASSWORD (数字の 0、文字の O ではない) です。

ユーザーを追加または変更するには (ID 2、3、または 4 のみ)、次のようにします。

1. BMC\_CFG メインメニューに戻ります。必要な場合は、「E」(前のメニュー)を選択して、メインメニューに戻ってください。
2. 「3」を入力して「BMC Device and Messaging Commands Group」を選択します。

BMC Device and Messaging Commands Group

1. Set BMC Global Enables Command
2. Get User Access Command
3. Set User Access Command
4. Set User Name Command
5. Set User Password Command

(h)Help (e)Prev Menu

=> Enter your choice:

図2-16 デバイスおよびメッセージ・コマンド・グループ

3. 「4」を入力して、「Set User Name Command」コマンドを選択します。
4. 変更するユーザー番号を選択します。2、3、または4（ユーザー1は変更できません）。
5. 「1」を入力して、ユーザー名を入力します。最大16文字を使用できます。
6. 「C」を入力して、BMC に対する変更を確定します。
7. 「E」を入力して、前のメニューに戻ります。

BMC ユーザーのパスワードを設定するには、変更するユーザーを選択し、パスワードを2回入力した後、ユーザーを有効にする必要があります。手順は、次のとおりです。

1. 「BMC Device and Messaging Commands Group」メニュー（図 2-16）から、「5」を入力して、「Set User Password Command」を選択します。29 ページの図 2-17 を参照してください。

Set User Password Command

#	Set	Description
1.	00h	User ID
2.	00h	Operation
3.		Password data:

(c)Commit (h)Help (s)Save Config (e)Prev Menu

=> Enter your choice:

図2-17 「Set User Password command」ウィンドウ

2. 「1」を入力して、ユーザー ID フィールドを選択します。
3. 変更するユーザーを入力します。2、3、または4。図 2-17 は、選択されたユーザーを反映して更新されます。
4. 「2」を入力して、実行する操作を選択します。

```

Byte 2, Set User Password command

Current Byte Value= 00h

#_Mod/Set_ _Description_____
      00h operation
                00. disable user   | 01. enable user
                02. set password  | 03. test password

(v)Modify (+)Enable (-)Disable

(h)Help (d)Discard (e)Prev Menu

=> Enter your choice:

```

図 2-18 ユーザー・パスワードに対して実行する操作の選択

オプション（図 2-18 に表示）は、次のとおりです。

- 00 = ユーザーを無効にする
- 01 = ユーザーを有効にする
- 02 = パスワードを設定する
- 03 = パスワードをテストする

5. 「02」を入力して、パスワードを設定する操作を選択します。
6. 「E」を入力して、前のメニューに戻ります。
7. 「3」を入力して、新しいパスワードを入力します。
8. ユーザーのパスワードを入力して（最大 16 文字まで）、Enter を押します。
9. 「C」を入力して、BMC に対する変更を確定します。
10. 「2」を入力して、別の操作を選択します。30 ページの図 2-18 が再度表示されます。
11. 「01」を入力して、ユーザーを有効にする操作を選択します。
12. 「E」を入力して、前のメニューに戻ります。
13. 「C」を入力して、BMC に対する変更を確定します。
14. 「E」を入力して、前のメニューに戻ります。

## ユーザーに与えられるアクセス権限の設定

BMC では、ユーザーに与えられるアクセス権限のタイプ（アクセス権限なしから全アクセス権限まで）を指定できます。

1. 「BMC Device and Messaging Command Group」メニュー（29 ページの図 2-16）で、「3」を入力して、「Set User Access Command」を選択します。図 2-19 が表示されます。

```
Set User Access Command

#_Set_ Description_____
1. 00h Options
2. 00h User ID
3. 00h User Limits

(c)Commit (h)Help (s)Save Config (e)Prev Menu

=> Enter your choice:
```

図 2-19 「Set User Access Command」メニュー

2. 最初のステップは、「Options」メニューからチャンネルを選択することです。「1」を入力して、オプションを変更します。

```
Byte 1, Options

Current Byte Value= 00h

#_Mod/Set_ Description_____
7.      -   Enable changing the following bits in the byte
6.      -   User Restricted to Callback
5.      -   User Link authentication enable
4.      -   User IPMI Messaging enable
3.      00h  Channel Number

(v)Modify (+)Enable (-)Disable

(h)Help (d)Discard (e)Prev Menu

=> Enter your choice:
```

図 2-20 「Set User Access Command」メニュー

3. 「3」を入力して、チャンネル番号を変更します。

4. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
  - 1 = LAN
  - 2 = シリアル
 図 2-20 は、選択されたチャンネル番号を反映して変更されます。
5. 「E」を入力して、前のメニューに戻ります。
6. 「2」を入力して、ユーザーを選択します。
7. 変更するユーザーを入力します。2、3、または4。29 ページの図 2-17 は、選択されたユーザーを反映して更新されます。

```

Set User Access Command

#_Set_ Description_____
1. 01h Options
2. 02h User ID
3. 00h User Limits

(c)Commit (h)Help (s)Save Config (e)Prev Menu

=> Enter your choice:

```

図2-21 「Set User Access Command」メニュー

8. 「3」を入力して、このユーザーのアクセス権を変更します。

```

Byte 3, User Limits

Current Byte Value= 00h

#_Mod/Set_ Description_____
      00h  User Privilege
              01. Callback      | 02. User
              03. Operator      | 04. Administrator
              05. OEM Proprietary | 0f. NO ACCESS

(v)Modify (+)Enable (-)Disable

(h)Help (d)Discard (e)Prev Menu

=> Enter your choice:

```

図2-22 ユーザー・アクセスの指定

選択できるオプションは、表 2-5 を参照してください。

表2-5 BMC ユーザー権限レベル

ユーザー・アクセス	説明
01 - コールバック	これは最低の特権レベルです。コールバックの開始をサポートするために必要なコマンドのみが許可されます。
02 - ユーザー	データの読み取りと状況の表示ができるコマンドのみが許可されます。構成を更新したり、状況を変更するコマンドは許可されません。
03 - オペレーター	電源制御やイベント・ログの消去などのコマンドはすべて許可されます。許可されないコマンドは、イーサネットおよびシリアル・インターフェースを変更するコマンドと、ユーザー・アクセス権を変更するコマンドです。
04 - 管理者	すべての BMC コマンドが許可されます。
05 - OEM 所有	予約済み
0f - アクセス権限なし	ユーザーはどのようなアクションも実行できません。

9. いずれかを入力して、必要な特権レベルを指定します。
10. 「E」を入力して、前のメニューに戻ります。
11. 「C」を入力して、BMC に対する変更を確定します。

### ユーザーが持つアクセス権限の確認

ユーザーが持つアクセス権限を確認するには、次のようにします。

1. 「BMC Device and Messaging Commands Group」メニュー（29 ページの図 2-16）から、「2」を入力して、「Get User Access Command」を選択します。
  2. チャンネル番号として、「1」を入力します。チャンネル番号は、次のとおりです。
    - 1 = LAN
    - 2 = シリアル
- 12 ページの図 2-2 が表示されます。

```
Get User Access Command

#_Set_ Description_____
1. 01h Channel Number
2. 01h User ID

      ---Inquired Data-----
      4 Maximum number of user IDs
      3 Count of currently enabled user IDs
      1 Count of user IDs with fixed names
3. 1fh Channel Access

(i)Inquire data (h)Help (s)Save Config (e)Prev Menu

=> Enter your choice:
```

図 2-23 既存のユーザーのアクセス権限の要求

3. 「2」を入力して、ユーザーを選択します。1、2、3、または4を入力します。
4. 「I」を入力して、照会要求を BMC に送信します。
5. 「3」を入力して、アクセス権限をテキスト形式で表示します。35 ページの図 2-24 のような画面が表示されます。

この例では、ユーザー特権は「04h」で、これは「管理者 (Administrator)」に対応します。



```

Byte 4, Channel Access

Current Byte Value= 14h

#_Set_ Description
-      "- "user access available during call-in/callback
      "+ "user access availalbe only during callback

-      user enabled for link authentication
+      user enabled for IPMI Messaging
04h    User Privilege Limit for given channel
        01. Callback          | 02. User
        03. Operator          | 04. Administrator
        05. OEM Proprietary   | 0f. NO ACCESS

(v)Modify (+)Enable (-)Disable

(h)Help (e)Prev Menu

=> Enter your choice:

```

図2-24 ユーザー・アクセスの表示

6. 「E」を入力して、このメニューを終了します。

### 2.3.5 BIOS 内での BMC の構成

システム BIOS 内で、次の設定を構成できます。

- ▶ IP アドレス
- ▶ サブネット・マスク
- ▶ デフォルト・ゲートウェイ

デフォルトのユーザー ID とパスワードを変更する場合は、bmc\_cfg (23 ページの 2.3.4、『BMC\_CFG を使用した BMC の構成』を参照) または IBM Director (38 ページの 2.3.7、『IBM Director による BMC の構成』を参照) を使用する必要があります。

BIOS を使用して BMC を構成するには、次の手順で行います。

1. サーバーが現在実行中の場合、サーバーをリブートします。POST 中に F1 を押して、「Configuration and Setup」ユーティリティーに入ります。
2. 「Advanced Setup」を選択します。

3. 「**Baseboard Management Controller (BMC) Settings**」を選択します。36 ページの図 2-25 のようなメニューが表示されます。

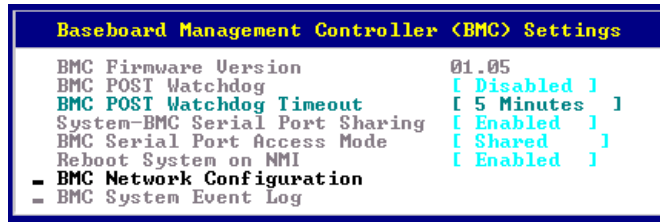


図2-25 BIOS 内の「BMC 設定」パネル

4. 「**BMC Network Configuration**」を選択します。

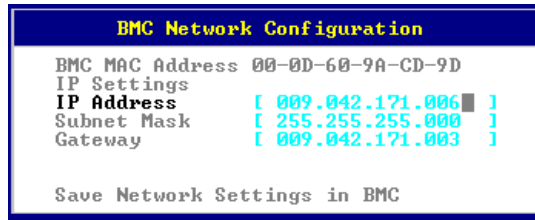


図2-26 BIOS 内のBMC ネットワーク設定

5. 該当する IP アドレス、サブネット・マスク、およびゲートウェイ・アドレスを入力して、「**Save Network Settings in BMC**」を選択します。

コンソール・リダイレクトおよび Serial over LAN を使用する予定の場合は、さらにパラメーターを調整する必要があります。この調整は、OSA SMBridgeなどのツールを使用して行います。204 ページの 6.4、『OSA SMBridge ユーティリティー』を参照してください。

## 2.3.6 イベント・ログ

BMC システム・イベント・ログ (SEL) には、図 2-25 に示したメニューを介してアクセスするか、OSA SMBridge のようなツールを使用してアクセスできます。このイベント・ログは、サーバーのハードウェア・アラートをすべて記録します。イベント・ログは、各画面に 1 つのイベントを表示します。「Get Next Entry」および「Get Previous Entry」リンクを使用して、イベントのページを移動します。

一部のイベントは 2070 のタイム・スタンプを持っていることに気付くことがあります。サーバーから電源が除去され、後に復元されると、BMC クロックは 1970 にリセットされます (これを BIOS は 2070 として表示します)。POST が

完了して、オペレーティング・システムに制御が渡されると、直ちに BMC クロックは BIOS からの正しい時刻を使用して更新されます。

**注：**誤った時刻は、IBM Director が受信するイベントのタイム・スタンプには影響を与えません。IBM Director 管理サーバーが正しい時刻であるかぎり、IBM Director イベント・ログに表示されるイベントは正しい時刻（イベントを受信した時刻）を表示します。

```
*****
*                               BMC System Event Log                               *
*****
*   Get Next Entry               **
*   Get Previous Entry           **
*   Clear BMC SEL                *
*                               *
*   Entry Number*   00001 / 00031   *
*   Record ID*     0001             *
*   Record Type*   02              *
*   Timestamp*    2070/01/01 00:00:14 *
*   Entry Details: Generator ID* 0020 *
*                   Sensor Type* 08   *
*                   Assertion Event  *
*                   Power Supply      *
*                   Sensor Specific Type *
*                   Presence detected  *
*                               *
*                               *
*                   Sensor Number* 70  ?*
*****
*                               *
*                   <F1> Help          <<?> MMove
*                   <Esc> Exit         <Enter> Select
```

図 2-27 BMC システム・イベント・ログ

**注：**システム・イベント・ログは、512 個の項目を記録できます。ログが満杯の 75 パーセントまたは 90 パーセントに達すると警報が出されます。ただし、RSA II や BladeCenter 管理モジュールとは異なり、ログが満杯になると、新しい項目は保管されません。この時点で、SMBridge のようなツールを使用して、ログを消去する必要があります。

サーバーに RSA II SlimLine が搭載されている場合、BMC システム・イベント・ログ内のイベントは、すべて RSA II にも提供されます。RSA II は、これとは別のログも維持しており、RSA II にアクセスして表示すると、RSA II のイベントと BMC ベースのイベントの両方を見ることができます。ただし、その逆は真ではありません。BIOS 内のイベント・ログを表示しても、RSA II のイベントを見ることができません。BIOS イベント・ログは、BMC ベースのイベントのみを表示します。

### 2.3.7 IBM Director による BMC の構成

ご使用の環境に IBM Director サーバーがインストールされており、BMC のネットワーク設定が正しく構成されている場合は、この方法を使用して BMC に関する設定を構成できます。これは IBM 推奨の BMC 構成方法で、BMC のアウト・オブ・バンド管理も可能になります。

このセクションでは、ユーザー ID、パスワード、およびアラート転送設定の構成方法について説明します。

#### IBM Director コンソールへの BMC の追加

BMC を管理オブジェクトとして Director に追加するには、次のようにします。

1. Director コンソールから、ブランク域の中央ペインで右クリックします。
2. 「New」→「Physical Platform」をクリックします。

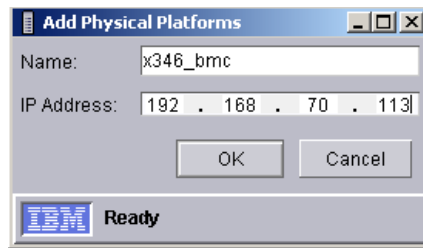


図 2-28 「Add Physical Platforms」 ウィンドウ

3. 追加する BMC の詳細を入力して、「OK」を選択します。
4. BMC が検出されると、Director コンソール上に、アウト・オブ・バンド (OOB) 物理プラットフォーム・オブジェクトとして表示され、図 2-29 のような画面が表示されます。

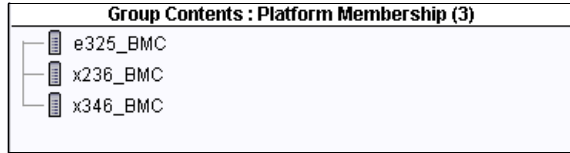


図 2-29 BMC が追加された IBM Director コンソールの「Group Contents」 ペイン

5. IBM Director は、デフォルトの USERID/PASSWORD 組み合わせを使用して、BMC へのアクセスを試みます。

デフォルトの USERID/PASSWORD 組み合わせを削除または変更した場合、小さいパッドロック・アイコンが装置の横に表示されます。装置を右クリックし、「Request Access」をクリックして、有効なユーザー ID とパスワードを入力します。

## ユーザーの追加

これで、MPA タスクを使用して、ユーザー ID とパスワードを構成できるようになりました。次の手順で行います。

**注：**ログイン・プロファイルの最大数は 4 つです。

1. BMC オブジェクトを右クリックして、「**Management Processor Assistant**」→「**Configuration**」を選択するか、または右側のペインの「Management Processor Assistant Task」を展開し、「Configuration」サブタスクを BMC オブジェクトにドラッグ・アンド・ドロップします。
2. MPA が開始したら、左側のメニューから「**Login profiles**」をクリックします (図 2-30)。

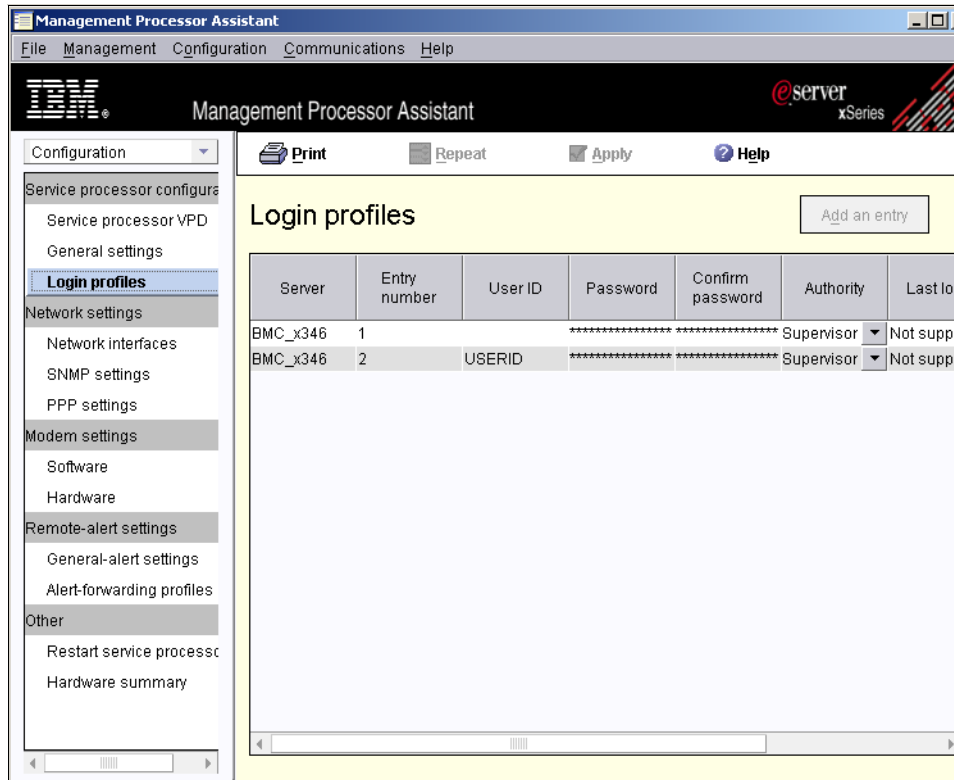


図 2-30 「Management Processor Assistant Configuration」 ウィンドウ

- 新規ユーザーを追加するには、最初のログイン・プロファイルを強調表示して、「Add an Entry」をクリックします。これにより、表示テーブルに新しい行が追加されます（40 ページの図 2-31）。

Server	Entry number	User ID	Password	Confirm password	Authority	Last login	Dial-back	
							Dial-back number	Dial-back enabled
BMC_x346	1		*****	*****	Supervisor	Not supported	Not supported	Not supported
BMC_x346	2	USERID	*****	*****	Supervisor	Not supported	Not supported	Not supported
BMC_x346	3	USER1	*****	*****	Supervisor	Not supported	Not supported	Not supported

図 2-31 BMC への新規セキュリティ項目の追加

- 「User ID」セルをダブルクリックして、新規ユーザーの詳細を入力します。
- 「Password」セルをダブルクリックして、該当するパスワードを入力します。
- 「Confirm Password」セルをダブルクリックして、確認のために再度パスワードを入力します。

7. 次に、必要な許可レベルを指定します。レベルは、次のとおりです。

「*Supervisor*」は、次の特権を持ちます。

- ユーザー・アカウント管理
- リモート・コンソール・アクセス
- リモート・コンソールおよび仮想メディア・アクセス (\*該当する場合)
- リモート・サーバーおよび電源 / 再始動アクセス
- イベント・ログ消去の権限
- 基本アダプター構成
- アダプター構成 (ネットワークとセキュリティー)
- 拡張アダプター構成

「*Read only*」は、表示特権のみを持ちます。変更はできません。

「*Operator*」は、次の特権を持ちます。

- リモート・サーバーおよび電源 / 再始動アクセス
- イベント・ログ消去の権限

「*No Access*」は、このユーザーに対しては BMC へのアクセスが使用不可にされます。

8. すべての詳細を正しく入力した後、「**Apply**」をクリックして変更を保管します。

## アラート転送の構成

左側のメニューから「**Alert-forwarding profile**」を選択することにより、アラート転送プロファイルも変更できます。アラート転送設定が、右側に図 2-32 のように表示されます。

Server	Entry number	Status	Description	Connection type	IP address or host name
BMC_x346	4	Enabled	Not supported	IBM Director Comprehensive	192.168.70.107

図 2-32 BMC のアラート通知設定

9. 新規プロファイルを追加するには、最初のプロファイルを強調表示して、「**Add an entry**」をクリックします。
10. IBM Director 管理サーバーの IP アドレスを入力して、接続タイプが「**IBM Director Comprehensive**」であることを確認します。
11. 「**Apply**」をクリックして、BMC に対する変更を確定します。

**注：**表示される設定をすべて変更できるわけではありません。表示される設定の一部のものは、BMC には適用されません。そのようなフィールドには、「**Not Supported**」と表示されています。

## 2.3.8 リモート制御

BMC は、OSA SMBridge ユーティリティと Serial over LAN を使用したリモート制御をサポートします。これは、BIOS 画面と特定のオペレーティング・システム・コンソールを制御できる、テキスト専用コンソール・インターフェースを提供します。Linux と Windows は両方とも、そうしたテキスト専用コンソールを備えています。204 ページの 6.4、『OSA SMBridge ユーティリティ』を参照してください。

## 2.3.9 BMC デバイス・ドライバーのインストール

デバイス・ドライバーは、オペレーティング・システムのサポートと、IBM Director とのインバンド通信のために必要です。このセクションでは、Windows および Linux プラットフォームの IPMI デバイス・ドライバーのインストール方法について説明します。必要なデバイス・ドライバーが表 2-6 にリストされています。

表 2-6 IPMI に必要なデバイス・ドライバー

デバイス・ドライバー	補足説明
IPMI デバイス・ドライバー	▶ IBM Director とのインバンド通信に必要
IPMI ライブラリー (sp6lib)。 これは OSA BMC IPMI マッピング・レイヤーです。	▶ BMC マッピング・レイヤー (ドット・コマンドを IPMI コマンドにマップします) ▶ IBM Director とのインバンド通信に必要
ASR サーバー再始動ソフトウェア	▶ ASR 機能に必要

デバイス・ドライバーは特定の順序でインストールする必要があるため、順序を守らないとインストールに失敗します。順序は、次のとおりです。

1. IPMI デバイス・ドライバー
2. IPMI マッピング・レイヤー・(ライブラリー) ファイル
3. IPMI ASR サービス

ご使用のサーバーに適切なドライバーをダウンロードするには、IBM 技術情報「*IBM @server xSeries BMC — Firmware and Drivers Cheatsheet, TIPS0532*」を参照して、該当するサーバー用のファームウェアのリンクをクリックします。

<http://www.redbooks.ibm.com/abstracts/tips0532.html>

代わりに、次のサイトから該当するダウンロード・ページにナビゲートすることもできます。

<http://www.pc.ibm.com/support>



## Windows 上のデバイス・ドライバーのインストール

このセクションでは、Windows 環境でのドライバーのインストール方法を説明します。

### IPMI デバイス・ドライバー

OSA IPMI デバイス・ドライバーをインストールするには、次の手順で行います。

1. Setup.exe を実行します。通常の初期ウィンドウが表示された後、ドライバー・パラメーターの選択を促すプロンプトが表示されます (図 2-33)。

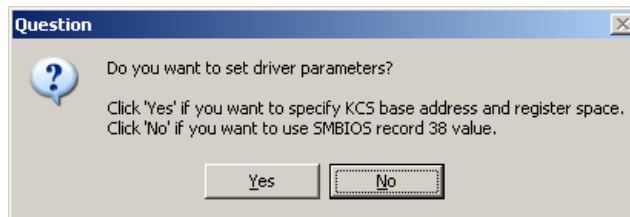


図 2-33 ドライバー・パラメーター

2. 「No」をクリックします。

「No」をクリックすることは、ドライバーが SMBIOS レコード 38 を照会して必要なデバイス・ドライバー・パラメーターを見つけることを意味します。「Yes」をクリックすることは、ユーザーが手動でパラメーターを設定することを意味します。「Yes」を選択するのは、IBM サポートに指示されるなど特殊な事情がある場合に限ってください。手動で個々のパラメーターを設定した場合、Windows がブルー・スクリーンになったり、リブートが必要になることがあります。

3. 「Next」をクリックして、インストールを開始します。インストールが完了すると、サーバーをリブートするように指示するプロンプトが出ますが、インストーラーは自動的にリブートしません。

### IPMI マッピング・レイヤー (ライブラリー) ファイル

IPMI マッピング・レイヤー (ライブラリー) ファイルをインストールするには、次のようにします。

1. このソフトウェアをインストールする前に、IPMI デバイス・ドライバーがインストール済みであることを確認してください。
2. 上記の Web サイトから EXE をダウンロードして、それを実行します。
3. 画面の指示に従います。
4. インストール手順でサーバーのリブートが指示された場合は、サーバーをリブートします。

## IPMI ASR サービス

ASR サービスをインストールするには、次のようにします。

1. このソフトウェアをインストールする前に、IPMI デバイス・ドライバーと IPMI ライブラリー・ファイルがインストール済みであることを確認してください。
2. 上記の Web サイトから EXE をダウンロードして、それを実行します。
3. 画面の指示に従います。
4. インストール手順でサーバーのリブートが指示された場合は、サーバーをリブートします。

## Linux 上のデバイス・ドライバーのインストール

このセクションでは、Linux 環境でのドライバーのインストール方法を説明します。

### IPMI デバイス・ドライバー

OSA IPMI デバイス・ドライバーをインストールするには、UNIX シェルを立ち上げて、ドライバー・モジュールを作成してシステムにインストールするために、次のコマンドを入力します。

```
rpm -i osa_ipmi-x.x.x-x.i386.rpm
```

Linux カーネルをアップグレードする場合は、OSA IPMI デバイス・ドライバーをアンインストールしたうえで、再コンパイル/再インストールする必要があります。ドライバーを再作成するには、ディレクトリー /usr/osa/osa\_ipmi-x.x.x-x に移動して、次のように入力します。

```
sh build_osadv
```

注：

- ▶ ご使用のシステムに必要なソース・コード・パッケージをインストールする必要があります。これは、/usr/src にインストールすることをお勧めします。
- ▶ gcc 3.2 が使用可能であることを確認してください。binutils パッケージのアップグレードが必要になることもあります。
- ▶ 32 ビット SUSE LINUX 8.2 (gcc Version 3.3 20030226 (プレリリース) がインストール済み) 上にインストールする場合、**insmod** は、-f オプションを付けないと機能しません。強制ロードのために、/sbin/ipmi\_load スクリプトの **insmod** コマンドに手動で -f オプションを追加する必要があります。ただし、

カーネルが損なわれたという警告を受け取る場合があります。他の gcc バージョンでも、同様の問題が起きることがあります。

OSA IPMI デバイス・ドライバーをアンインストールするには、次のいずれかを入力します。

```
rpm -e osa_ipmi-x.x.x-x  
rpm -e osa_ipmi
```

詳しくは、ドライバーに付属の README.TXT ファイルを参照してください。

### **IPMI マッピング・レイヤー (ライブラリー) ファイル**

IBM マッピング・レイヤー・ソフトウェアのインストールと除去は、Linux<sup>®</sup> RPMpackage 管理ツールを使用して行います。最初に IPMI ドライバーをインストールしたことを確認してください。

既存のソフトウェア・パッケージをアップグレードする場合は、最初に次のコマンドを使用して古いバージョンを除去します。

```
rpm -e ibmsp6a
```

システムの構成によっては、欠落ファイルについてのメッセージが表示されることがあります。これは無視して構いません。

IPMI マッピング・レイヤー (ライブラリー) ファイルをインストールするには、次のコマンドを発行します。

**EM64T と AMD64 の注:** x86\_64 カーネルでは、この RPM は、64 ビット共有オブジェクトと 32 ビット互換性共有オブジェクトを作成します。RPM を x86\_64 カーネルにインストールする前に、32 ビット互換性開発パッケージがインストール済みであることを確認してください。

```
rpmbuild --rebuild ibmsp6a-x.xx-y.src.rpm
```

続いて、次のように入力します。

```
cd /usr/src/package-dir/RPMS/architecture  
rpm -ivh ibmsp6a-x.xx-y.architecture.rpm
```

ここで、

- ▶ *package-dir* は、RPM ビルド・ディレクトリーのディストリビューション固有の名前（通常は、「redhat」または「packages」）です。
- ▶ *architecture* は、使用中のカーネルのアーキテクチャー（i386、i586、または x86\_64）です。

例えば、RPM を x86\_64 SUSE LINUX にインストールする場合、コマンドは次のようになります。

```
rpmbuild --rebuild ibmsp6a-x.xx-y.src.rpm
cd /usr/src/packages/RPMS/x86_64
rpm -ivh ibmsp6a-x.xx-y.x86_64.rpm
```

### **IPMI ASR サービス**

このセクションでは、ASR (ibmipmiasr) RPM のインストール方法を説明します。

インストールを開始する前に、ご使用のサーバーに IPMI デバイス・ドライバーと IBM マッピング・レイヤー・ソフトウェアの両方がインストール済みであることを確認してください。

ソース rpm ファイルを実行するシステムは、Linux 開発 / ビルド機能を備えていなければなりません。

既存のソフトウェア・パッケージをアップグレードする場合は、最初に次のコマンドを使用して古いバージョンを除去します。

```
rpm -e ibmipmiasr
```

システムの構成によっては、欠落ファイルについてのメッセージが表示されることがありますが、これは無視して構いません。

ソース rpm をインストールするには、次のコマンドを実行します。

```
rpm -ivh ibmipmiasr-x.xx-y.i386.rpm
```

インストールが完了した後、ログ・ファイル /var/log/message をチェックしてください。正常にインストールされると、次のメッセージがログに書き込まれます。

```
IBM IPMI ASR application loaded
```

バイナリー rpm をアンインストールするには、次のコマンドを実行します。

```
rpm -e ibmipmiasr
```

RPM は、ASR アプリケーションをアンロードし、すべての ibmipmiasr 関連ファイルをシステムから除去します。

## 2.3.10 BMC によって使用されるポート

BMC は、通信用にいくつかの TCP/UDP ポートを使用します。BMC との通信がファイアウォールを通過する場合、通信を正常に実行するために、ファイアウォール上で使用可能にする必要があるポートを知ることが重要です。

表 2-7 BMC によって使用される TCP/IP ポート

ポート番号	説明
623	SMBridge および Director への IPMI 通信
664	IPMI 通信 (2 次)
161	SNMP get/set コマンド
162	Director への SNMP トラップおよび PET アラート

## 2.4 内蔵システム管理プロセッサ

内蔵 ISM プロセッサを標準搭載しているサーバーについての詳細は、2 ページの表 1-1 を参照してください。

### 2.4.1 機能

ISM プロセッサは、次の機能を備えています。

- ▶ 侵入アラート
- ▶ システム温度 / CPU 温度のモニター
- ▶ ファン、メモリー、電源装置、電圧のモニター
- ▶ オート・サーバー・リスタート・ウォッチドッグ障害アラート
- ▶ RS-485 インターコネクト機能
- ▶ リモート・ファームウェア更新
- ▶ RS-485 インターコネクト・ネットワーク経由のアラート転送
- ▶ light path 診断の制御
- ▶ Alert Standard Format (ASF) 互換性

xSeries 345 は、標準的な ISM プロセッサ・ベースのサーバーです。48 ページの図 2-34 は、主要なコネクタの位置を示しています。

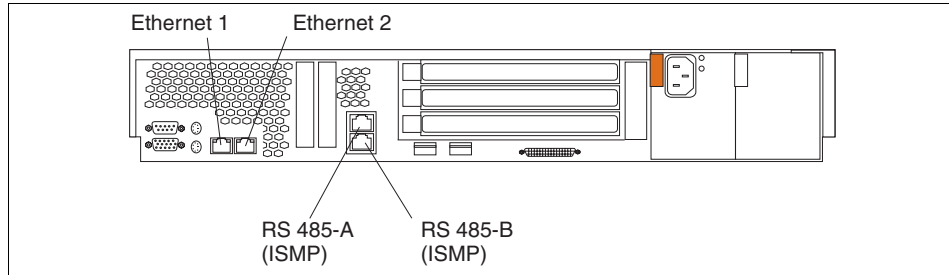


図 2-34 xSeries 345 上の接続

RS-485 コネクタは、サーバーを ASM インターコネクト・ネットワークに接続するのに使用されます。

## 2.4.2 制限

ISM プロセッサ・ベースのサーバーは、ASM ネットワークを介して RSA I、RSA II、または RSA II-EXA サービス・プロセッサに相互接続されて、そのサービス・プロセッサがゲートウェイとして構成されていない限り、サーバー・プロセッサからアウト・オブ・バンドでアラートを転送する機能を備えていません。57 ページの 3.3、『システム管理ネットワーク』を参照してください。

IBM Director エージェントをサーバーにインストールすることにより、ISM プロセッサからインバンドでアラートを転送することもできます。

IBM Director によるインバンド通信について詳しくは、「*Implementing Systems Management Solutions using IBM Director, SG24-6188*」、または以下の文書を参照してください。

- ▶ *IBM Director Installation and Configuration Guide:*  
<http://www.ibm.com/pc/support/site.wss/MIGR-50460.html>
- ▶ *IBM Director Systems Management Guide:*  
<http://www.ibm.com/pc/support/site.wss/MIGR-50461.html>

## 2.4.3 構成

ISM プロセッサに対しては、BIOS レベルで必要とされる構成はありません。

ISM プロセスからアラートを受信する必要がある場合は、ご使用の ASM インターコネクト・ネットワーク内に RSA または RSA II をゲートウェイとして構成し、その RSA または RSA II 上でアラートを構成することが必要です。61 ページの 3.3.1、『ASM ゲートウェイの指定』を参照してください。



## リモート管理アダプター II

Remote Supervisor Adapter II (RSA II) は、xSeries 用の最上位機種 of システム管理アダプターです。xSeries サーバーのアラート、モニター、およびリモート管理用のさまざまなオプションを備えています。

この章では、Remote Supervisor Adapter II の各種モデル、その機能、および共通の使用法について説明します。本書では、使用可能なすべての機能について詳しく説明するのではなく、IBM @server xSeries サーバーのハードウェア・ベースでのシステム管理を実装するために必要な機能のみを説明します。詳細については、製品の資料「*Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide*」を参照してください。

RSA II は、旧 Remote Supervisor Adapter (これを RSA I と呼びます) およびシステム管理 PCI アダプター (ASMA) に置き換わるものです。機能はそれぞれ異なりますが、これらはすべてシステム管理ネットワークに接続できます。この章の内容は、次のとおりです。

- ▶ 50 ページの 3.1、『機能および機構』
- ▶ 51 ページの 3.2、『Remote Supervisor Adapter ・ ファミリーの概要』
- ▶ 57 ページの 3.3、『システム管理ネットワーク』
- ▶ 63 ページの 3.4、『Remote Supervisor Adapter II の基本構成』
- ▶ 72 ページの 3.5、『リモート・コンソールとリモート・メディア』
- ▶ 91 ページの 3.6、『リモート管理アダプター II によって使用されるポート』

## 3.1 機能および機構

RSA II の最も役立つ機能を、以下にリストします。

- ▶ 自動通知およびアラート

RSA II は、自動的に種々のタイプのアラートおよび通知を、IBM Director のような別のサーバーや SNMP 宛先に送信し、また SMTP を使用して E メールで直接ユーザーに送ります。

- ▶ 継続的なヘルス・モニターおよび制御

RSA II は、温度や電圧など重要なシステム・パラメーターを継続的にモニターします。例えば、ファンが故障した場合、RSA II は強制的に残りのファンの速度を上げて、故障したファンを補います。

- ▶ イベント・ログ

サーバーの稼働中に、サーバーのイベント・ログおよびパワーオン・セルフテスト (POST) ログにアクセスし、それをエクスポートできます。

- ▶ LAN およびシステム管理 (ASM) インターコネクト経由のリモート・アクセス

RSA II は LAN インターフェースを備えており、これを使用して内蔵システム管理プロセッサ (ISMP) を ASM インターコネクト・ネットワークに接続できます。RSA II は、ASM ネットワークのフォーカル・ポイントとして機能し、接続された ISMP のすべてのアラートを転送して、イーサネット経由でアクセスを提供します。

- ▶ オペレーティング・システム障害画面のキャプチャー

例えば、オペレーティング・システムが停止してブルー・スクリーンになった場合、サポートの目的で、画面をキャプチャーすることができます。さらに、RSA II は最後の障害画面をメモリーに保管するため、後でそれを参照できます。

- ▶ リモート・メディア

「Remote Control」機能の一部として、リモート・メディア機能は、リモート PC 上で RSA II の Web インターフェースが実行されている場合、システムのディスクレット・ドライブ、ディスクレット・イメージ、光ディスク・ドライブ (DVD や CD-ROM など)、または光ディスク・ドライブ・イメージを使用して、それらをサーバー上のローカル・ドライブのように見せることができます。

**注:** 本書の作成日現在では、光ディスク・イメージ (ISO ファイル) に対するサポートは、Windows 用の RSA II をサポートするサーバーにのみ提供開始されていました。Linux に対するサポートは、後日実施されます。



▶ リモート電源制御

RSA II は、LAN または WAN 接続を介して、リモート電源制御によるサーバーの電源オン、電源オフ、または再始動をサポートします。これは、オペレーティング・システムをシャットダウンしても、しなくても実行できます。

▶ サーバー・コンソール・リダイレクト

サーバー・コンソールは、RSA II Web インターフェースでリモート管理用に使用できます。

## 3.2 Remote Supervisor Adapter ・ ファミリーの概要

xSeries サーバー用として、3 つの異なるタイプの RSA II アダプターがあります。

- ▶ Remote Supervisor Adapter II (53 ページを参照)
- ▶ Remote Supervisor Adapter II-EXA (54 ページを参照)
- ▶ Remote Supervisor Adapter II SlimLine (55 ページを参照)

表 3-1 は、各 xSeries サーバーでサポートされるアダプターを示しています。ここに記載されているサーバーは、本書の作成日現在でサポートされていたサーバーです。これより古いサーバーはサポートされません。これより新しいサーバーについては、サポートされるサーバーの最新リストで確認してください。次のサイトにある技術情報「*Service Processors Supported in IBM Netfinity and IBM @server xSeries Servers, TIPS0146*」を参照してください。

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

RSA II の場合、アダプターを取り付ける PCI スロットが示されています (RSA II SlimLine は、スロットを使用しません)。表にはシステム・ボード接続もリストされ、そのサーバーは提供されたミニ USB ケーブルを取り付ける必要があるかどうかを示されています。

ヒント : RSA II-EXA は、x445 サーバーでのみ使用されます。

表 3-1 RSA II とサポートされるサーバー

サーバー	RSA II	RSA II SlimLine	PCI スロット	システム・ボード・コネクタ	ミニ USB ケーブル接続
xSeries 205	オプション	なし	1	CN20	必要
xSeries 206	オプション	なし	2	CONN2	必要

サーバー	RSA II	RSA II SlimLine	PCI スロット	システム・ボード・コネクタ	ミニ USB ケーブル接続
xSeries 225 (8649)	オプション	なし	1	JMGT1 <sup>a</sup>	不要
xSeries 226	オプション	なし	2	JMGT1 <sup>a</sup>	不要
xSeries 235	オプション	なし	1	J27	必要
xSeries 236	なし	オプション	-	-	不要
xSeries 255	オプション	なし	1	J16	必要
xSeries 305	オプション	なし	1	CN12	必要
xSeries 306	オプション	なし	2	CN18	必要
xSeries 335	オプション <sup>b</sup>	なし	1	J2	必要
xSeries 336	なし	オプション	-	-	不要
xSeries 345	オプション	なし	5	J2	必要
xSeries 346	なし	オプション	-	-	不要
xSeries 365	標準	なし	-	標準	不要
xSeries 366	なし	オプション		入出力ボード	不要
xSeries 445	標準 <sup>c</sup>	なし	-	標準	必要 <sup>d</sup>
xSeries 460	なし	オプション		入出力ボード	不要
eServer 326	オプション	なし	2	JMGT1 <sup>a</sup>	不要

- a. USB 信号用の 26 ピン・ケーブルを使用。
- b. xSeries 335 は、リモート管理アダプター II をサポートしますが、アダプターのビデオがオンボード・ビデオを使用不可にするため、x335 の C2T 機能は RSA II とは連動しません。RSA II のリモート・ビデオ機能を使用する場合は、お客様がそれぞれの x335 に RSA II をインストールする必要があります。詳しくは、<http://www.pc.ibm.com/support?page=MIGR-54747> を参照してください。
- c. RSA II-EXA は、x445 の一部のモデルに標準搭載されています。その他のモデルは RSA I が標準ですが、RSA II-EXA (部品番号 13N0382) に置き換えることができます。RSA II (部品番号 59P2984) は、x445 ではサポートされません。
- d. RSA II-EXA が搭載されている場合、ブレークアウト・ケーブルに USB コネクタが付いています。

### 3.2.1 リモート管理アダプター II

リモート管理アダプター II (部品番号 59P2984) は、IBM xSeries サーバー用の第 3 世代システム管理アダプターです。これは、200 MHz で稼働する IBM PowerPC® 405 32 ビット RISC プロセッサをベースにしています。66 MHz/32 ビットの速度で動作するハーフ・サイズの PCI アダプターです。

x365 には標準機構として搭載され、PCI スロット 1 にプリインストールされています。その他の多くのサーバーでは、オプション機構として入手できます。

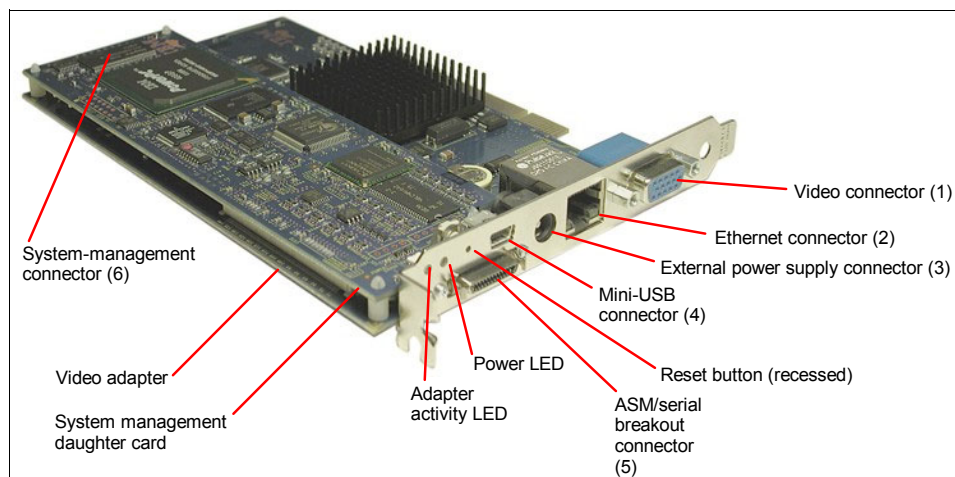


図 3-1 RSA II の外部コネクタとインディケータ

RSA II には、以下のコネクタが装備されています (番号は、図 3-1 を参照してください)。

- ▶ ビデオ・コネクタ (図 3-1 の 1)。RSA II は、アダプター上にもう 1 つ別のビデオ・サブシステムを搭載しています。サーバーに RSA II をインストールすると、自動的にオンボード・ビデオが使用不可になります。ユーザーがサーバーのモニターを RSA II ビデオ・コネクタに接続する必要があります。
- ▶ 10/100 イーサネット・コネクタ (2)。10 Mbps または 100 Mbps イーサネット・ベースのクライアント LAN または管理 LAN への接続用です。
- ▶ 電源コネクタ (3)。外部パワー・サプライ (アダプターをオプションとして購入した場合に提供されます) を使用すると、サーバーの電源が遮断された場合でも、RSA II にアクセスできます。パワー・サプライは、サーバーとは異なる給電部 (例えば、別の UPS) に接続してください。

**ヒント:** 外部パワー・サプライは、RSA II が標準搭載されているサーバー (x365 など) ではサポートされません。

- ▶ ミニ USB コネクタ (4)。このポートは、リモート制御機能を使用している場合、リモート・キーボードおよびマウス用の機能を提供します。このポートをサーバーの USB ポートに接続します。ただし、以下のサーバーは除きます。これらのサーバーにはケーブルを接続してはなりません (USB 信号はサーバー内部で伝送されます)。
  - x225
  - x226
  - x365
  - eServer 326
- ▶ ブレークアウト・コネクタ (5)。RSA II を ASM ネットワークのフォーカル・ポイントとして使用するか、またはモデムの接続に使用する場合、ブレークアウト・ケーブルが提供されます。このケーブルは、図 3-2 に示すように、ASM 接続とシリアル接続の両方を備えています。ブレークアウト・ケーブルには、シリアル・コネクタが 1 個または 2 個 (以前の RSA II アダプターはシリアル・ポートが 1 個だけでした) と ASM RS-485 インターコネクタ・ネットワークのデジター・チェーン用の RJ45 コネクタが 2 個付いています。

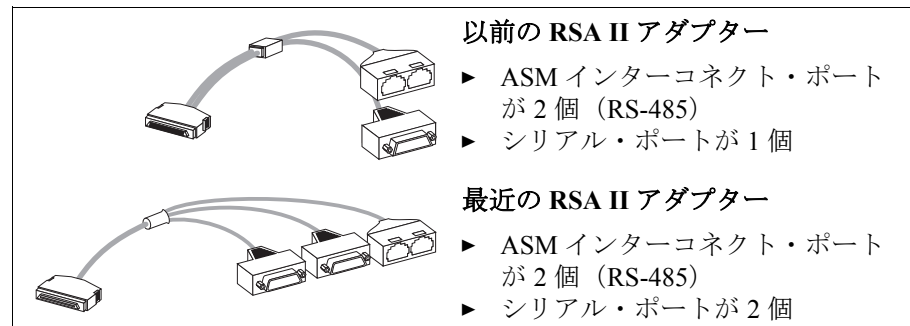


図3-2 RSA II のブレークアウト・ケーブル

- ▶ サーバーのマザーボードへの接続用の 20 ピン・コネクタ (6)。51 ページの表 3-1 は、提供されたケーブルを接続するプレーナー上のコネクタを示しています。

### 3.2.2 リモート管理アダプター II-EXA

RSA II-EXA (部品番号 13N0382) は、x445 だけのオプション機構で、現行モデルにはプリインストールされています。機能は RSA II と同じです。このアダプターは x445 にだけインストールでき、インストール作業はサービス技術員が行う必要があります (数多くのサーバー・コンポーネントを一時的に取り外す必要があるため)。

RSA II-EXA は、PCI スロットを使用しません。6 個の PCI スロットの下部に水平に取り付けられます。

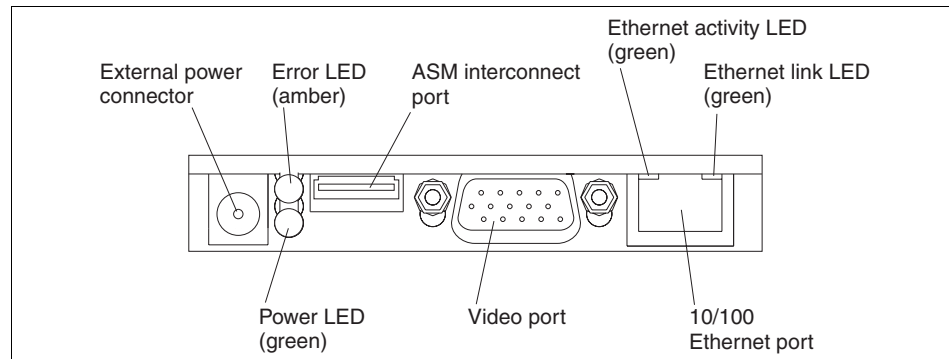


図 3-3 RSA II-EXA のコネクタ

**ヒント:** ご使用の x445 にどの Remote Supervisor Adapter が搭載されているか不確実な場合は、アダプター上のビデオ・コネクタを検査してください。ビデオ・コネクタがあれば RSA II-EXA であり、なければ RSA I です。

RSA II と RSA II-EXA は、コネクタは異なりますが、機能は同じです。RSA II-EXA のブレークアウト・ケーブルには、図 3-4 に示すように、USB コネクタ（サーバーの USB ポートに接続）と 2 番目のシリアル・ポートが含まれています。

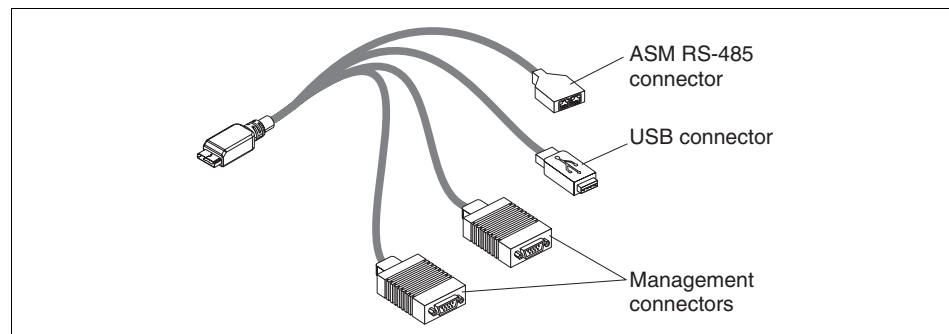


図 3-4 RSA II EXA ブレークアウト・ケーブル

### 3.2.3 Remote Supervisor Adapter II SlimLine

現行の xSeries サーバーの一部のもの、将来の xSeries サーバーでは、RSA II SlimLine アダプター（部品番号 73P9341）がオプションとして使用されます。

(51 ページの表 3-1 を参照)。ServerProven<sup>®</sup> Web サイトに、サポートされる全ラインのサーバーのリストがあります。

<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>

RSA II ファミリーのこの新規メンバーは、PCI スロットを使用しません。これは、Remote Supervisor Adapter II PCI アダプターのシステム管理ドーター・カードに似た小型の回路ボードです。

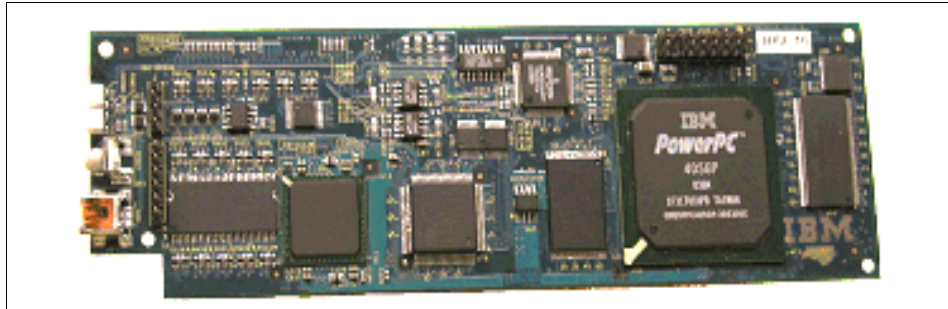


図 3-5 RSA II SlimLine アダプター

RSA II SlimLine は、PCI バージョンの RSA II とは異なり、外部コネクタもビデオ・カードもありません (56 ページの図 3-5 の左側に見えるコネクタは使用されません)。SlimLine をサポートするサーバーには、RSA II SlimLine 専用のイーサネット・コネクタが装備されています。

現行の xSeries サーバーの RSA II SlimLine には、次のような制限があります。

- ▶ 英数字または数字ページャー・アラートがサポートされません。
- ▶ サーバーのシリアル・ポートから出力される文字ベースのコンソール・リダイレクトがサポートされません。グラフィカル・コンソール・リダイレクトはサポートされ、文字ベース Serial Over LAN リダイレクトは、OSA SMBridge を使用して BMC によってサポートされます。

現行の制限については、ご使用のサーバーの「*Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide*」または「インストール・ガイド」を参照してください。

RSA II SlimLine は、サーバーの内蔵 Baseboard Management Controller (BMC) と共存します。BMC について詳しくは、7 ページの第 2 章、『ベースボード管理コントローラー』を参照してください。

RSA II SlimLine アダプターが BMC ベースのサーバーにインストールされた場合、BMC は使用可能のままです。したがって、すでに BMC に IP アドレスを構成した場合、そのアクセスは BMC のユーザー・アクセス・リストに定義されたユーザーが引き続き使用できます。そのうえ、BMC を介したアウト・オブ・

バンド通信は、RSA II のように暗号化を使用してセキュアにすることはできません。

一貫性のあるセキュアな管理を実現するために、BMC を再構成して、IP アドレスを 0.0.0.0 に変更することをお勧めします。これにより、すべてのアウト・オブ・バンド通信は RSA II SlimLine アダプター経由となり、これは、137 ページの第 5 章、『セキュリティおよび認証』で説明している方法で、セキュアな通信にすることができます。

**注:** RSA II や RSA II-EXA とは異なり、RSA II SlimLine は ASM インターコネクト・ネットワークをサポートしません。代わりに、サービス・プロセッサは、別の管理ネットワークを経由せずに、お客様のイーサネット・ネットワークに直接接続されます。

### 3.3 システム管理ネットワーク

システム管理ネットワークは、従来型サービス・プロセッサと Remote Supervisor Adapter II の相互接続用です。この ASM ネットワークを形成できるサービス・プロセッサには、次のものがあります。

- ▶ Remote Supervisor Adapter II
- ▶ Remote Supervisor Adapter
- ▶ 内蔵システム管理プロセッサ
- ▶ システム管理 PCI アダプター
- ▶ システム管理プロセッサ

最後の 2 つの装置は、本書では取り上げません。詳細については、IBM Redbook「*Implementing Systems Management Solutions using IBM Director, SG24-6188*」のセクション 6.1.5 を参照してください。

この ASM ネットワークを使用して、サービス・プロセッサはアラートおよび管理機能を送信することができ、またイーサネットおよびモデム接続を共有できます。

**重要:** ASM ネットワークは、従来型サービス・プロセッサの接続用です。現行および将来の xSeries サーバー（BMC または RSA II SlimLine コントローラーを使用）の多くは、ASM ネットワークをサポートしなくなるか、または必要としなくなります。代わりに、アラートや管理機能は、サーバーの Gigabit Ethernet ポートの 1 つを介して、サービス・プロセッサによって直接実行されます。

ASM ネットワーク（ASM インターコネクト・ネットワークとも言う）をサポートするサーバーの一覧表は、次のサイトを参照してください。

<http://www.redbooks.ibm.com/abstracts/tips0146.html>

<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>

RSA II は、ASM ネットワークのゲートウェイとして機能します。これは、LAN から接続管理プロセッサ（イーサネット接続を持たない）へのアクセスを提供し、管理プロセッサから LAN へのゲートウェイの役目を果たします。



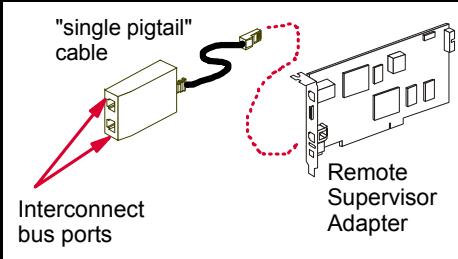
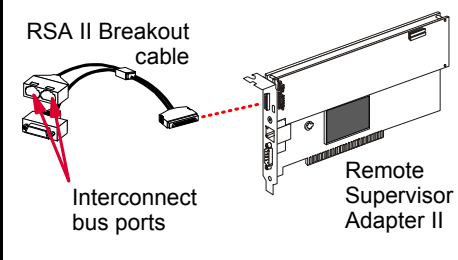
ASM ネットワークを構築するには、次のコンポーネントが必要です。

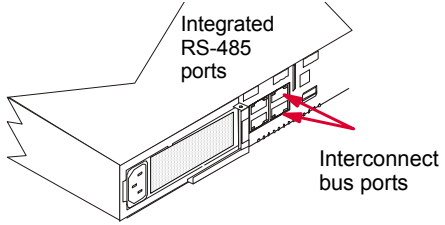
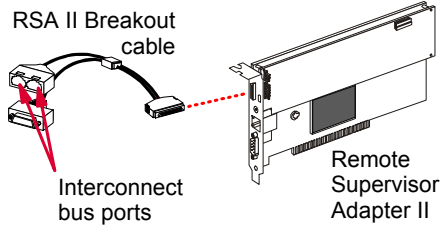
- ▶ ゲートウェイ装置 (RSA II) が最小 1 台
- ▶ メンバー装置 (例えば、ISMP、RSA I、RSA II)
- ▶ カテゴリー 5 のイーサネット・ケーブル (クロスオーバー・ケーブルではなく)
- ▶ ASM インターコネクト / シリアル・ポート・ブレイクアウト・ケーブル、RSA II 用 (54 ページの図 3-2) または RSA II-EXA 用 (55 ページの図 3-4)。
- ▶ ターミネーター (ネットワークの各端に 1 個ずつ)

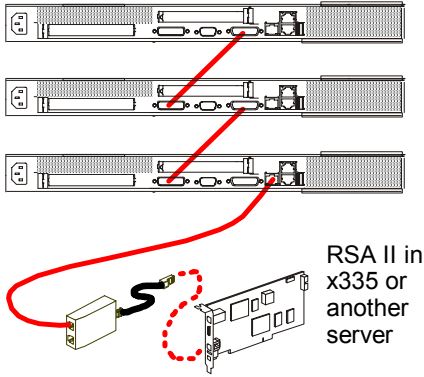
各サーバーをインターコネクト・バスに結合するには、サーバーをデジリー・チェーン内の他の 2 つのパートナーに接続するために、2 個の RS-485 ポートが必要です。この要件を満たすには、次の 2 つの方法のいずれかを使用できます。

- ▶ Remote Supervisor Adapter II 用の ASM インターコネクト / シリアル・ポート・ブレイクアウト・ケーブルを使用する。
- ▶ サーバーのシャーシの背面に 2 個の RS-485 ポートがある場合、直接接続する。

表 3-2 ASM インターコネクト・ネットワークを形成するために必要なハードウェア

構成	モデル	インターコネクト・ポートの位置
<p>サーバーにオンボード・サービス・プロセッサがなく、Remote Supervisor Adapter が追加されているか、または Remote Supervisor Adapter がサーバーに標準搭載されている場合。</p> <p>▶ アダプターに同梱されているシングル・ピッグテール・ケーブルを使用します。</p>	<p>x205 x225 x220 x305 x360 x440 x445 x450 x455</p>	 <p>"single pigtail" cable</p> <p>Interconnect bus ports</p> <p>Remote Supervisor Adapter</p>
<p>サーバーにオンボード・サービス・プロセッサがなく、Remote Supervisor Adapter II が追加されているか、リモート管理アダプター II がサーバーに標準搭載されている場合。</p> <p>▶ アダプターに同梱されているブレイクアウト・ケーブルを使用します。</p>	<p>x205 x206 x225 x226 x305 x306 x365 x445 e326</p>	 <p>RSA II Breakout cable</p> <p>Interconnect bus ports</p> <p>Remote Supervisor Adapter II</p>

構成	モデル	インターコネクト・ポートの位置
<p>サーバーが内蔵 ISM プロセッサを搭載し、サーバーのシャーシの背面に RS-485 ポートがある場合。</p> <p>▶ 追加ケーブルは必要ありません。</p> <p>注：サービス・プロセッサの最新のファームウェアがロードされていることを確認してください。</p>	<p>x232 x235 x255 x342 x345</p>	 <p>Integrated RS-485 ports</p> <p>Interconnect bus ports</p>
<p>サーバーが ISM プロセッサを搭載し、オプションの Remote Supervisor Adapter II が取り付けられている場合。</p> <p>▶ アダプターに同梱されているブレイクアウトケーブルを使用します。</p> <p>注：この状態では、Remote Supervisor Adapter II がサービス・プロセッサとしての役割を引き継ぎます。ISM プロセッサは、使用不可にされます。</p>	<p>x235 x255 x335 x345</p>	 <p>RSA II Breakout cable</p> <p>Interconnect bus ports</p> <p>Remote Supervisor Adapter II</p>

構成	モデル	インターコネクト・ポートの位置
<p>ケーブル・チェーン・テクノロジー (C2T) を使用しているサーバーの場合。</p> <ul style="list-style-type: none"> <li>▶ サーバーがオンボード ISM プロセッサのみを装備している場合、ASM インターコネクトは C2T 配線のみを使用して作成します。他のサーバーへの接続は、最後の x335 上の ISM ポートを介して行います。</li> <li>▶ サーバーに RSA II も搭載されている場合、または x335 が RSA II を使用して別のサーバーに接続されている場合、ISM ポートを RSA ブレークアウト・ケーブルの ASM ポートに接続します (図を参照)。</li> </ul> <p>IBM と特別なサポート契約を締結していないかぎり、C2T チェーン内の x335 で RSA II を使用してはなりません。IBM 担当員に連絡してください。より良いソリューションは、x335 以外のサーバーに RSA II を搭載することです。ただし、C2T 上ではリモート・ビデオはサポートされません。この表の脚注 52 ページの ステップ b を参照してください。</p> <p>注：C2T は、最大 42 台までのサーバーを接続できますが、1 つの ASM インターコネクト・ネットワークを形成できるのは 24 台に限られます。この場合の配線については、「Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide」を参照してください。</p>	<p>x335</p>	 <p>RSA II in x335 or another server</p>

古いサーバー、システム管理アダプター、およびプロセッサについての詳細は、IBM Redbook 「Implementing Systems Management Solutions using IBM Director, SG24-6188」の第 6 章を参照してください。

### 3.3.1 ASM ゲートウェイの指定

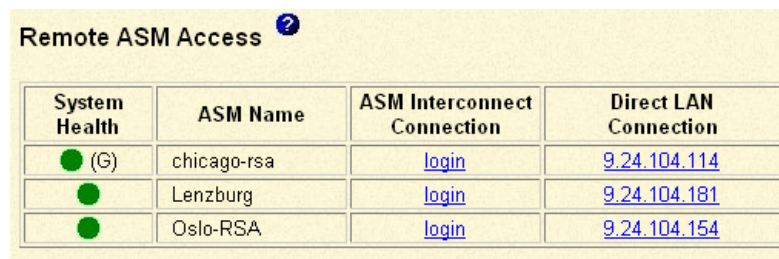
ASM インターコネクト・ゲートウェイの概念は、ISM プロセッサにのみ関係があります。

ISM プロセッサ以外のサービス・プロセッサは、ASM インターコネクト・バス上の他のすべてのサービス・プロセッサと通信でき、それぞれの装置のタイプやその装置が持つリソース (モデムおよびイーサネット接続) を判別できます。

一方、ISM プロセッサは、他のサービス・プロセッサのタイプやそれに接続されているリソースを判別できません。

そのため、ISM プロセッサにアラートの送信先を「通知して」、意図した受信側にアラートを転送できるようにする必要があります。ISM プロセッサがアラートを送信する先の装置を *ASM ゲートウェイ* と呼んでいます。

任意の RSA または RSA II (RSA II SlimLine は不可) をゲートウェイとして使用できます。どの装置が現行のゲートウェイであるかは、RSA Web インターフェースを介して (「Access Remote ASM」メニューを選択して) 示すことができます。図 3-6 に示されているように、ゲートウェイには (G) という文字が表示されます。



The screenshot shows a web interface titled "Remote ASM Access" with a help icon. Below the title is a table with four columns: "System Health", "ASM Name", "ASM Interconnect Connection", and "Direct LAN Connection". The first row shows a green circle with "(G)" next to it, indicating it is the gateway, for the "chicago-rsa" device with a "login" connection and IP "9.24.104.114". The other two rows show green circles without "(G)", for "Lenzburg" and "Oslo-RSA", both with "login" connections and IP "9.24.104.181" and "9.24.104.154" respectively.

System Health	ASM Name	ASM Interconnect Connection	Direct LAN Connection
● (G)	chicago-rsa	<a href="#">login</a>	<a href="#">9.24.104.114</a>
●	Lenzburg	<a href="#">login</a>	<a href="#">9.24.104.181</a>
●	Oslo-RSA	<a href="#">login</a>	<a href="#">9.24.104.154</a>

図 3-6 ゲートウェイは、「System Health」列に (G) が表示されます。

イベントが発生した場合、報告する ISMP は、ゲートウェイにのみアラートを送信します。ゲートウェイは、そのアラートを送信出力するか、または別の RSA に転送して意図した受信側に送達できるようにします。

**重要:** ゲートウェイの RSA または RSA II では、アラートの受信側を構成しておく必要があります。そうしないと、ISM プロセッサからアラートを受信したときに、アラートを受信側に送信せず、別の RSA にも転送しません。

ゲートウェイのサービス・プロセッサにはアラートの受信側が構成されている必要があるため、特定の RSA を強制的にゲートウェイにすると便利な場合があります。この指定は、サービス・プロセッサ構成 Web ページの「Alerts」セクションで「**Make this ASM the Gateway**」ボタンをクリックすることによって行えます。

RSA または RSA II をゲートウェイにした後は、オフラインになるまでゲートウェイとして働きます。オフラインになった時点で、残りの RSA および RSA II 装置が折衝して、ゲートウェイになる装置を決めます。元のゲートウェイがオンラインに戻ると、再度それがゲートウェイになります。

**重要:** ゲートウェイのサービス・プロセッサがオフラインになり、新しく選択されたゲートウェイにリモート・アラートの受信側が構成されていない場合、ISM プロセッサからのアラートは送信されません。この理由から、ゲートウェイ装置になる可能性があるすべての装置（つまり、すべての RSA および RSA II サービス・プロセッサ）でアラートを構成する必要があります。また、ゲートウェイ装置になる可能性があるすべての装置で、アラート受信側の定義が整合していることも確認する必要があります。

ISM プロセッサと他のサービス・プロセッサ（Remote Supervisor Adapter、ASM プロセッサ、ASM PCI アダプターなど）を比較してみましょう。他のサービス・プロセッサは、アラートを送信するためのゲートウェイは必要ありません。RSA が自分でアラートを送信できない場合、RS-485 ネットワーク上でアラートを送信できる別の RSA を見つけて、その RSA にアラートを転送します。

どのサービス・プロセッサも ASM インターコネクト・ネットワークを「所有」していません。すべてのサービス・プロセッサ（ISM プロセッサ以外の）が、自分でアラートを送信するか、または自分で送信できない場合には、送信できる別の装置が分かっています。ネットワーク上の他のサービス・プロセッサの機能についての情報が、45 秒程度の間隔で相互に送信されるハートビート・メッセージに含まれています。

ISM プロセッサは、他のサービス・プロセッサからのこの情報を無視し、常に単純にゲートウェイ装置にアラートを送ります。ゲートウェイは、どのリソースがネットワーク上のどこにあるかを知っており、自分自身でアラートを送信するか、または適切なサービス・プロセッサに転送し、それが宛先への送信を行います。

## 3.4 Remote Supervisor Adapter II の基本構成

RSA の機能を使用するには、最初にアダプターを構成する必要があります。このセクションでは、基本構成の手順を説明します。詳細な構成オプションについては、「*Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide*」、および本書の 247 ページの第 7 章、『シナリオおよびベスト・プラクティス』を参照してください。

### 3.4.1 RSA II の取り付け

RSA II は、51 ページの表 3-1 に示したように、特定のスロットに取り付けます。RSA II SlimLine を使用する場合は、サーバーのシステム・プレーナー上の専用に設計されたコネクタに取り付けてください。コネクタの位置は、サーバーに付属の資料を参照してください。

**重要** : RSA II を取り付ける *前*に、サーバーの BIOS および BMC ファームウェアを最新レベルに更新してください。

RSA II アダプターを取り付けるには、次の手順で行います。

1. 20 ピン (x225/x226 の場合は 26 ピン) リボン・ケーブルを、RSA II とオンボードまたはライザー・カード・コネクターに接続します。このコネクターの位置は、サーバーの資料を参照してください。
2. ミニ USB ケーブルを RSA II とサーバーの USB ポートの 1 つに接続します。ただし、サーバーが x225、x226、または x365 の場合を除きます。これらのサーバーの場合、リボン・ケーブルに USB 信号接続が含まれています。x445 の場合は、ブレイクアウト・ケーブルを取り付けます。これに USB ケーブルが組み込まれています。

**注** : ローカル接続された PS/2<sup>®</sup> マウスを使用して、x235 または x345 に Red Hat Linux を新規インストールする計画の場合は、オペレーティング・システムをインストールした *後*で、ミニ USB ケーブルを接続してください。インストール・プロセス中、Red Hat は 1 つのタイプのマウスしか使用できず、USB が存在すれば、それを使用します。次のサイトの RETAIN<sup>®</sup> tipH177279 を参照してください。

<http://www.pc.ibm.com/support?page=MIGR-50413>

3. オンボード・ビデオ・カードのビデオ・コネクターからビデオ・ケーブルを抜き取って、それを RSA II に接続します。
4. イーサネット・ケーブルを RSA II のイーサネット・ポートに接続します。
5. ASM インターコネクト・ネットワークを作成する場合、またはモデムを RSA II に接続する計画の場合は、ASM ブレイクアウト・ケーブルを接続します。x445 の場合は、ブレイクアウト・ケーブルを接続する必要があります。このケーブルに、サーバーの USB ポート用の USB コネクターが付いています。
6. RSA II SlimLine をイーサネット・ネットワークに接続するには、イーサネット・ケーブルのプラグをサーバーの専用イーサネット・ポートに差し込みます。このポートの位置は、サーバーの資料を参照してください。

### 3.4.2 ネットワーク設定

ご使用のサーバーにアダプターを取り付けた後、Web インターフェースまたは telnet を使用して RSA II に接続するためのネットワーク設定を構成する必要があります。

あります。アダプターを最新のファームウェアに更新済みであること、それがこの特定サーバー用のファームウェアであることを確認してください。

ネットワーク設定を構成するには、次のようにします。

1. サーバーをブートし、F1 を押して BIOS 設定に入ります。
2. 「Advanced Setup」 → 「RSA II Settings」 を選択します。

RSA II Settings	
RSA II MAC Address	00-09-6B-9E-08-5C
DHCP IP Address	000.000.000.000
DHCP Control	[ Use Static IP ]
Static IP Settings	
Static IP Address	[ 009.042.171.238 ]
Subnet Mask	[ 255.255.255.000 ]
Gateway	[ 009.042.171.003 ]
OS USB Selection	[ Other OS ]
Save Values and Reboot RSA II	

図 3-7 サーバー BIOS 内の RSA II 設定

3. 左右の矢印キーを使用して、「DHCP Control」を「Use Static IP」に変更します。DHCP に問題が起きてもアクセスを確保できるようにするために、RSA II に対しては固定 IP アドレスを使用することをお勧めします。
4. RSA II に割り当てる IP アドレス、ネットワークのサブネット・マスク、および標準ゲートウェイを入力します。詳細については、ネットワーク管理者にお尋ねください。
5. 「OS USB Selection」として、「Other OS」（Windows オペレーティング・システムの場合）または「Linux OS」を選択します。選択には左右の矢印キーを使用します。

この選択の目的は、Linux とその汎用 human interface device (HID) ドライバーに伴う既知の問題を防止するためです。Linux は、汎用 HID (Windows で使用) を使って RSA II と USB 通信を確立することができません。ここで「Linux OS」を選択することにより、RSA II が汎用 HID ではなく OEM HID に見えるようになり、これで正常に機能します。

次に、矢印キーを使用して「Save the Values and Reboot RSA II」を選択し、Enter を押します。ユーティリティを終了します。

**ヒント:** RSA II のネットワーク接続を検査するには、ネットワークに接続された別のシステムから ping コマンドを使用します。

### 3.4.3 ファームウェアの更新

次のステップは、RSAII のファームウェアを最新バージョンに更新することです。

ヒント：リモート側でファームウェアを更新する他の方法は、273 ページの 7.8、『リモート側での BIOS とファームウェアの更新』で説明しています。

RSA II のファームウェアは、アダプターが搭載されているサーバーに特定のものであるため、正しいバージョンをダウンロードしたことを確認してください。「*Remote Supervisor Adapter II Family — Firmware and Drivers Cheatsheet, TIPS0532*」の該当するリンクから、ファームウェアをダウンロードします。

<http://www.redbooks.ibm.com/abstracts/tips0534.html>

代わりに、<http://www.pc.ibm.com/support> にアクセスし、ご使用のサーバーまでナビゲートして、サーバーの「**Advanced Systems Management**」のもとでリンクを見つけることもできます。

Cheatsheet からも分かるように、RSA II のファームウェアを更新するには、3 つの方法があります。

- ▶ Windows を実行しているサーバー上でローカルで更新する
- ▶ Linux を実行しているサーバー上でローカルで更新する
- ▶ RSA II Web ブラウザー・インターフェースからパケット (PKT) ファイルを使用して更新する

ここでは、PKT ファイルを使用してファームウェアを更新します。

注：RSA II を別のサーバーに移動する計画の場合

- ▶ Windows または Linux ベースのファームウェア更新ユーティリティーを使用する計画の場合、最初にアダプターを新規サーバーに取り付けてから、RSA II のファームウェアを更新してください。POST 中にいくつかのエラー・メッセージが出ることがありますが、これは無視して構いません。ファームウェアが更新されると、すぐに消えます。
- ▶ Web ブラウザー・インターフェースを使用してアダプターをフラッシュする計画の場合、最初に「**Advanced Options**」リンクを使用してファームウェアを更新してから、アダプターを移動してください。
- ▶ 一部のサーバーでは、ファームウェアを更新した後も、古いサーバーからの VPD データが残っている場合があります。例えば、「RSA II Vital Product Data」ページの「Diagnostics VPD」セクションに、古いサーバーからの値が表示されることがありますが、RSA II は正常に機能します。



1. 上記の Cheetsheet URL から、ご使用のサーバー用の「Packet files」リンクをクリックします。
2. EXE ファイルをダウンロードして、ローカル・ディレクトリーに保管します。
3. EXE を実行して、ファイルを解凍します。ファイルを解凍した後、少し時間をとって `readme.txt` をお読みください。ご使用のディレクトリーに、以下のファイルを入れる必要があります。2つの PKT ファイルがあることに注意してください。ファームウェアの更新手順を2回（各ファイルごとに1回）実行する必要があります。

Name	Size	Type
26r0562.zip	1,327 KB	PKZIP File
RAETBRUS.PKT	65 KB	PKT File
RAETMNIUS.PKT	1,286 KB	PKT File
readme.txt	13 KB	Text Document
RTALERT.MIB	34 KB	MIB File
RTRSAAG.MIB	268 KB	MIB File

図 3-8 RSA II ファームウェア更新パッケージのファイル

ヒント : Web ブラウザーを介した更新に適しているファームウェア・パッケージは、ZIP ファイルとして配布され、ZIP ファイルには2つの PKT ファイルのみが入っています。

次に、ブラウザーを使用して RSA II に接続します。標準ユーザー `USERID` と `PASSWORD`（ゼロ、文字の `O` ではなく）をパスワードとして使用して（変更されていない場合）、RSA II にログオンします。セキュリティ上の理由から、最初にログオンした後で、標準パスワードを変更する必要があります。

以前に別のサーバーにインストールしてフラッシュした RSA II をインストールする計画の場合、実行は可能ですが、以下 68 ページのステップ 4 で「**Advanced Options**」をクリックする必要があります。アダプターを新しいサーバーに移動する前に、新規ファームウェアを使用してアダプターをフラッシュすることをお勧めします。そうしないと、POST 中にいくつかのエラー・メッセージを受け取ることがあります。

1. ナビゲーション・フレームで、「**Tasks**」 → 「**Firmware Update**」をクリックします。

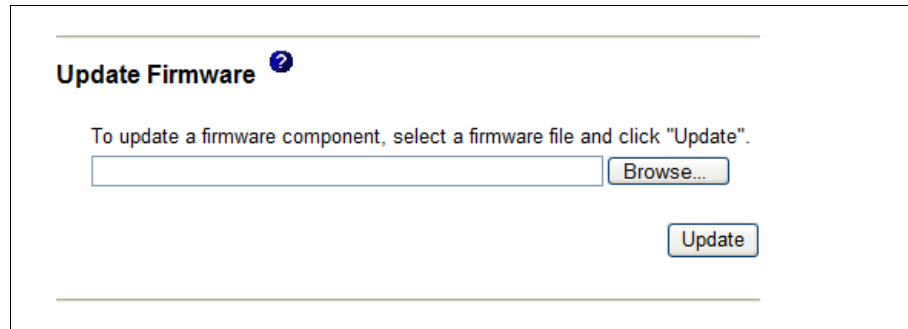


図3-9 RSA II ファームウェア更新

2. 「**Browse**」をクリックして、ファームウェア更新用の2つのファイルのうち最初のファイルを選択します。

ファームウェアを更新するには、正しい順序でファイルを選択する必要があります。最初に RAETBRUS.PKT (RSA ブート ROM) を選択し、次に RAETMNUM.PKT (RSA メイン・アプリケーション) を選択します。両方のファイルを適用した後で、RSA を再始動します。
3. 更新するために、「**Update**」をクリックします。これで、ファイルは RSA II に転送されました。
4. 「**Continue**」をクリックして RSA II をフラッシュします。あるいは、別のサーバー用のファームウェアを使用してアダプターをフラッシュする場合は、次のようにします。
  - a. 「**Advanced Options**」をクリックします。

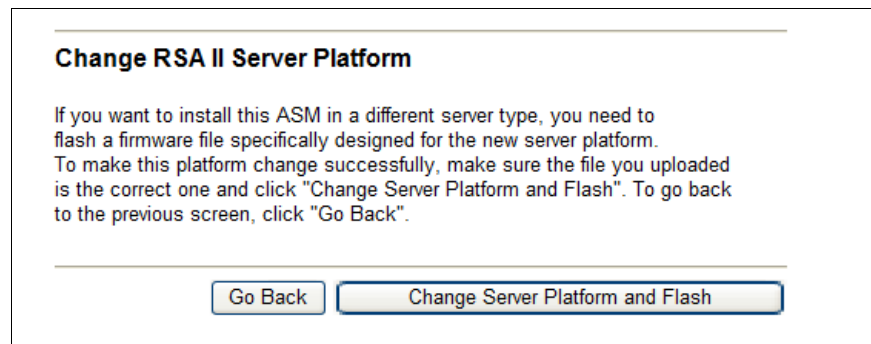


図3-10 「Advanced Options」ウィンドウ

- b. 「**Change Server Platform and Flash**」をクリックします。
  - c. 「**OK**」をクリックして、処置を確認します。
5. 2番目の PKT ファイルについて、ステップ1から4を繰り返します。

6. 「ASM Control」 → 「ASM Restart」 をクリックして、アダプターを再始動します。

ヒント : x205、x235、x255、または x345 内の RSA II を更新し、ディスプレイにストライプが表示される場合は、RSA II のビデオ BIOS も更新する必要があります。これはファームウェアと同じ場所からダウンロードできますが、カテゴリ・フィルターで「**BIOS (adapter)**」を選択してください。ファイルを解凍してディスクに保管し、そのディスクを使用してサーバーをブートします。画面の指示に従ってください。

これで、この章の残りの部分で説明する RSA II の他のオプションを構成できるようになりました。

### 3.4.4 デバイス・ドライバーのインストール

ご使用のサーバーで実行されているオペレーティング・システムは、RSA II アダプター用のドライバーを必要とします。

ヒント : Web からダウンロードするこの RSA II ドライバーは、古いサービス・プロセッサ用のドライバーとは異なるものです。RSA II ドライバーは、Windows サービスまたは Linux デーモンとしてインストールします。

「*Remote Supervisor Adapter II Family — Firmware and Drivers Cheatsheet, TIPS0532*」の該当するリンクから、ドライバーをダウンロードします。

<http://www.redbooks.ibm.com/abstracts/tips0534.html>

代わりに、<http://www.pc.ibm.com/support> にアクセスし、ご使用のサーバーまでナビゲートして、サーバーの「**Advanced Systems Management**」のもとでリンクを見つけることもできます。

#### Windows サービスのインストール

RSA II サーバー・ソフトウェア・パッケージのインストールは、古いシステム管理アダプターのドライバーのインストールとは異なります。ダウンロードした実行可能ファイルを実行することにより、インストールが行われます。

注意 : RSA II ソフトウェアをインストールする前に、USB ケーブルが必要な場合 (51 ページの表 3-1 を参照) は、ケーブルが RSA II とサーバーの USB ポート間に接続されていることを確認してください。また、Windows の場合、システム BIOS で RSA II が「*Other OS*」に構成されていることも確認してください (65 ページの図 3-7)。

インストールは、次の手順で行います。

1. RSA II が搭載されたサーバー上で、ダウンロードした EXE ファイルを実行します。
2. オプションで、「**Change**」をクリックして、インストール・ファイルの一時フォルダーを指定できます。
3. ファイルがコピーされた後、インストール・プロセスが自動的に開始されます。
4. 画面の指示に従います。
5. インストールが終了したら、一時フォルダー内のファイルを削除して構いません。

インストールが正常に行われたかどうかを調べるには、「IBM Remote Supervisor Adapter II」のサービスを検査します。

1. タスクバーで「スタート」ボタンをクリックします。
2. 「すべてのプログラム」→「管理ツール」→「サービス」をクリックします。

サービス「IBM Remote Supervisor Adapter II」までスクロールダウンして、状況が「started」であることを確認します。

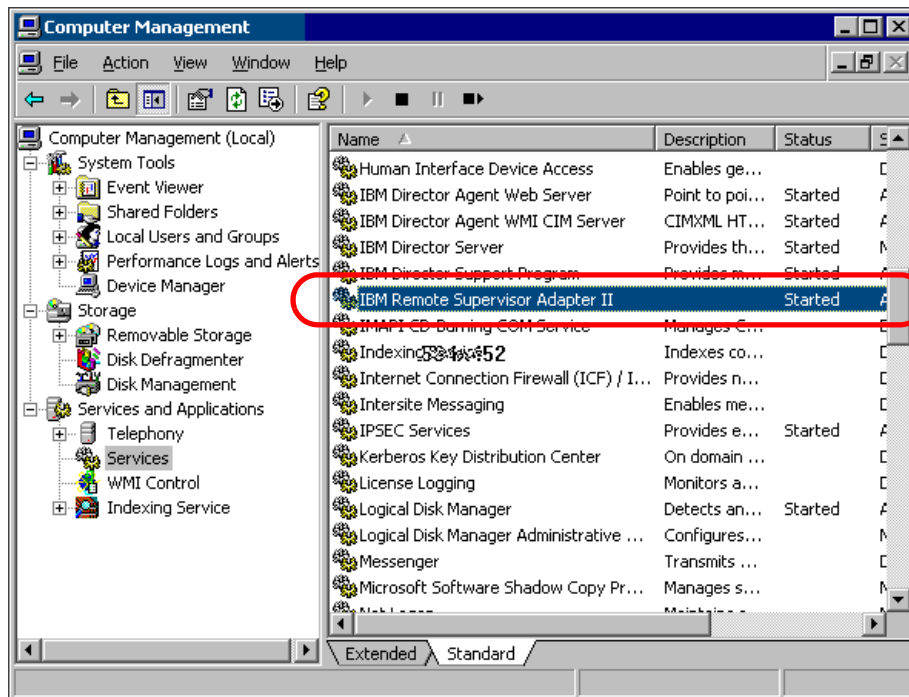


図 3-11 Windows 2003 の RSA II サービス

## Linux デーモンのインストール

RSA II 用の Linux デーモンをインストールするには、最初に、これを IBM Support Web サイトからダウンロードします。69 ページの 3.4.4、『デバイス・ドライバのインストール』の手順を使用してください。

1. ご使用の Linux ディストリビューション用の正しい rpm パッケージ (Red Hat または SUSE LINUX) を選択します。
2. rpm パッケージの `readme` ファイルを読み、前提条件とインストール手順を確認します。

**注意:** RSA II ソフトウェアをインストールする前に、USB ケーブルが必要な場合 (51 ページの表 3-1 を参照) は、ケーブルが RSA II とサーバーの USB ポートの間に接続されていることを確認してください。また、サーバーの BIOS で RSA II が「Linux OS」に構成されていることも確認してください (65 ページの図 3-7)。

3. ダウンロードしたファイルを Linux サーバーのフォルダー (例えば、`/tmp/inst`) にコピーします。
4. デーモンをインストールします (例えば、SUSE。ここで、`xx` はバージョン)。

```
rpm -ivh ibmusbasm-1.xx.i386.rpm
```

ここで、デーモンが実行されているかどうかを検査できます。例 3-1 に示すような `ps` コマンドを使用してください。

例 3-1 RSA デーモンの実行を検査するコマンド

---

```
linux:~ # ps -ef | grep ibmasm
root      11056      1  0 10:47 pts/1    00:00:00 /sbin/ibmasm
root      11060 11056   0 10:47 pts/1    00:00:00 /sbin/ibmasm
root      11062 10996   0 10:48 pts/1    00:00:00 grep ibmasm
linux:~ #
```

---

リストに `/sbin/ibmasm` が表示された場合、デーモンは実行中です。ibmusbasm デーモンは、オペレーティング・システムのブート・プロセス中に自動的に開始します。

手動でデーモンを開始するには、コマンド `ibmspup` を使用します。デーモンを停止するには、`ibmspdwn` を入力します。

### 3.4.5 MIB ファイル

RSA II は、IBM Director を含めて、さまざまな管理ツールからの SNMP をサポートします。MIB ファイルが必要な場合、ご使用のサーバーの RSA II ファームウェア更新時に、ZIP ファイル内で（この中に、PKT ファイルも含まれています）見つけることができます。ZIP ファイルをダウンロードするには、xSeries ソフトウェア・マトリックスを参照してください。

<http://www.ibm.com/pc/support/site.wss/MIGR-4JTS2T.html>

## 3.5 リモート・コンソールとリモート・メディア

リモート・ロケーションからサーバーを管理するには、キーボード、ビデオ、マウス（KVM）リダイレクトだけでは十分ではありません。例えば、オペレーティング・システムやパッチをインストールするには、CD-ROM またはディスクをサーバーに接続するためにリモート・メディアが必要です。

**ヒント:** 複数のリモート・ドライブを同時にマウントすることも可能です。例えば、CD-ROM とディスクまたはディスク・イメージをマウントできます。

リモート・メディアを使用するには、OS の稼働中または OS のインストール中に、オペレーティング・システムからの USB サポートが必要です。リモート・メディアは、次のオペレーティング・システムで機能します。

- ▶ Windows Server 2003
- ▶ Windows 2000 Server（Service Pack 4 以降を搭載）
- ▶ Red Hat Enterprise Linux AS 3（ただし、OS のインストールには使用できない）
- ▶ SUSE LINUX Enterprise Server 8（ただし、OS のインストールには使用できない）

Java™ ランタイムが必要です。これは、次のサイトからインストールできます。

<http://www.java.com/en/download/manual.jsp>

**制約事項:** リモート・メディアは、Red Hat および SUSE LINUX のインストール時にはサポートされません。インストーラーによるリモート CD-ROM の認識またはマウント/アンマウントに問題があるためです。これは、Linux ディストリビューションの将来のバージョンで訂正される予定です。

RSA II と xSeries の特定の組み合わせについての最新情報は、IBM ServerProven Web サイトで、テーブル内の関連のチェック・マークをクリックしてください。

<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>

ご使用のブラウザで初めてリモート・コンソールを立ち上げると、セキュリティー警告ウィンドウがポップアップ表示されます。この警告は、Remote Control が使用する Java アプレットから出されるものです。この警告はごく一般的に見られるもので、IBM からの証明を信用して「Yes」または「Always」をクリックできます。



図 3-12 セキュリティー警告

「More Details」をクリックして、この警告の詳細を見るか、または「Yes」をクリックして続行します。

**ヒント:** 「Always」をクリックしない限り、「Remote Control」に入るたびに、このウィンドウがポップアップ表示されます。

「Remote Control」 ウィンドウには、図 3-13 に示すように、特定のキー・ストロークおよびビデオ速度セクターをシミュレートした一連のボタンがあります。スライダーを使用して、ご使用のコンピューターのリモート・コンソール・ディスプレイに割り当てる帯域幅を制限します。

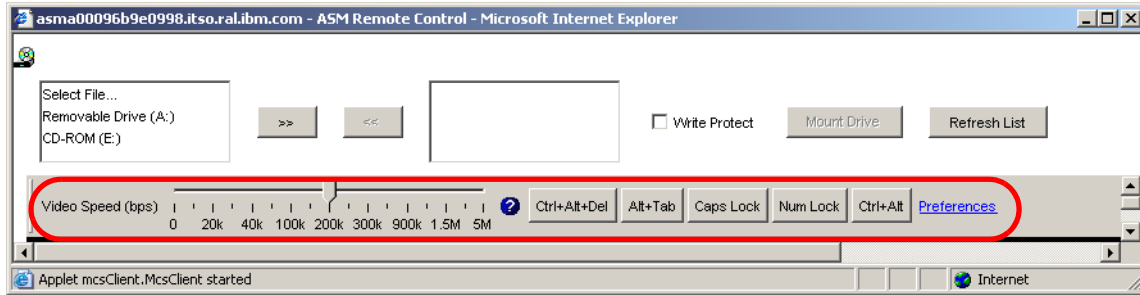


図 3-13 RSA II - 「Remote Control」 のボタン

ビデオ速度を下げると、表示する必要があるビデオ・データが制限されて、リモート・コンソール・ディスプレイを最新表示する速度が改善されます。必要な場合は、ビデオ・データを削減（あるいは、停止）して、リモート・ディスクにより多くの帯域幅を割り当てることができます。最良の結果が得られる帯域幅が見つかるまで、スライダーを左右に移動して調整してください。

各ボタンは、キーまたはキーの組み合わせを表します。ボタンを押すと、対応するキー・ストローク・シーケンスがサーバーに送信されます。追加ボタンが必要な場合は、「**Preferences**」をクリックすると、新規のキー・ボタンを変更または作成できます。

**ヒント** : BladeCenter 管理モジュールのリモート・コンソール用 Web インターフェイスも非常によく似ていますが、「Remote Control」のユーザー定義ボタンを変更したり、作成したりする機能は備えていません。

ボタン・バーは、グレーの背景の任意の場所をクリックしてドラッグすることにより、切り離すことができます。ボタン・バーをドロップすると、別のウィンドウが作成されます。



図 3-14 切り離されたボタン・バー

「Preferences」リンクでは、キーボードを指定したり、マウスの同期を使用可能にすることもできます（これにより、リモート・システム上のマウス・ポイン



ターが、ローカル・マウス・ポインターに正確に追従するようになります)。次のキーボード・タイプがサポートされています。

- ▶ 米国英語 104 キー・キーボード
- ▶ ベルギー語 105 キー・キーボード
- ▶ フランス語 105 キー・キーボード
- ▶ ドイツ語 105 キー・キーボード
- ▶ イタリア語 105 キー・キーボード
- ▶ 日本語 109 キー・キーボード
- ▶ スペイン語 105 キー・キーボード
- ▶ 英国英語 105 キー・キーボード

### 3.5.1 Linux の Remote Control サポート

Linux ディストリビューションで Remote Control 機能を使用する場合、リモート・マウスおよびキーボードを機能させるために、オペレーティング・システム内で追加の構成ステップが必要です。この追加のステップは、ローカル・キーボードとマウスが通常は PS/2 コネクタ付きの装置であるために必要になります。Remote Control は USB 装置を使用するため、マウスとキーボードを手動で追加する必要があります。

次のステップを実行して、Linux で USB マウスとキーボードを構成します。

1. テキスト画面にログインします (GUI モードにある場合は、Ctrl+Alt+F1 を押します)。
2. ビデオ・ドライバーを VESA ドライバーに変更します。

`/etc/X11/XF86Config` (Red Hat の場合は、`/etc/X11/XF86Config-4`) ファイルで、「`radeon`」というワードを見つけて、それを「`vesa`」に置き換えます。

3. カラー階調とウィンドウ・サイズ

ファイル `/etc/X11/XF86Config` を編集して、次のように変更します。

```
Section "Screen"
    DefaultDepth 16
    SubSection "Display"
        Depth 16
        Modes "1024x768"
    EndSubSection
...
```

「Depth」値が 16 で (必要な場合は、上記の Depth 行を追加してください)、「Modes」値が 1024x768 のみであることを確認します。他のモード値は削除してください。

Red Hat の場合、「Monitor」セクションの「`dmps`」を「`off`」に変更します。

4. PS/2 および USB マウス・サポートを使用可能にします。

mousedev モジュールと usb-storage モジュール (USB ストレージ・サポート) を始動時にロードするように構成するために、/etc/init.d/boot.local ファイルを編集して、ファイルの最後に次の行を追加します。

```
/sbin/modprobe mousedev
/sbin/modprobe usb-storage
```

リブートせずにこのサポートをアクティブにするために、コマンド・プロンプトで両方のコマンドを入力することもできます。

5. 新規の入力装置を X Window システム構成ファイルに追加します。

-SUSE LINUX の場合、次の行をファイル /etc/X11/XF86Config に追加します。

```
Section "InputDevice"
    Driver "mouse"
    Identifier "USB Mouse"
    Option "Device" "/dev/input/mice"
    Option "Name" "AutoDetected"
    Option "Protocol" "IMPS/2"
    Option "Vendor" "AutoDetected"
EndSection
```

2 番目のマウスを追加し、それがコア・イベントを送信することを指定します。

```
Section "ServerLayout"
    Identifier "Layout[all]"
    InputDevice "Keyboard[0]" "CoreKeyboard"
    InputDevice "Mouse[1]" "SendCoreEvents"
    InputDevice "USB Mouse" "CorePointer"
    Screen "Screen[0]"
EndSection
```

"CorePointer" を "SendCoreEvents" に変更します

この新しい行を追加します

- Red Hat Linux の場合、次の行をファイル /etc/X11/XF86Config-4 に追加します。

```
Section "InputDevice"
    Identifier "USB_Mouse"
    Driver "mouse"
    Option "Protocol" "IMPS/2"
    Option "Device" "/dev/input/mice"
EndSection
```

2 番目のマウスを追加し、それがコア・イベントを送信することを指定します。

```
Section "ServerLayout"
    Identifier "Anaconda Configured"
    Screen 0 "Screen0" 0 0
    InputDevice "USB Mouse" "CorePointer"
    InputDevice "Mouse0" "SendCoreEvents"
EndSection
```

この新しい行を追加します

"CorePointer" を "SendCoreEvents" に変更します

6. これらの変更を行った後、Ctrl+Alt+Backspace を押して、X Windows システムを再始動します。
7. 解像度が 1024 x 768 でない場合、正しい解像度情報をマウス・ハンドラーに提供するために、次のようにします。
  - a. Linux コマンド・プロンプトで、init 3 と入力します。
  - b. マウス・ドライバー・モジュールをアンロードします。これを行うには、`rmmod mousedev` と入力します。
  - c. 次のステートメントをファイル `/etc/modules.conf` に追加します。  
`options mousedev xres=X, yres=Y`  
ここで、*X* と *Y* は、ビデオ解像度を指定します。
  - d. コマンド `insmod mousedev` を使用して、マウス・ドライバー・モジュールを再ロードします。
  - e. `init 5` と入力して、`runlevel 5` に戻します。
8. Remote Control セッション中にローカル・マウスとリモート・マウスを同期化するには（その結果、2つのマウス・ポインターの動きが一致します）、グラフィカル・ログイン画面（XDM）とユーザーの優先 GUI（KDE や GNOME など）を変更する必要があります。

ヒント：ここでは、KDE と GNOME についてのみ説明します。WindowMaker、MWM、または TWM を使用している場合は、RSA II に同梱されている「*IBM Remote Supervisor Adapter II Technical Update for Linux, 2nd Edition (November 2003) - 88P9248*」を参照してください。この資料は、<http://www.pc.ibm.com/support> からダウンロードできます。文書番号を検索してください。

- XDM の場合は、次のようにします。
  - i. `init 3` と入力して、`runmode 3` に変更します。

- ii. SUSE LINUX の場合、ファイル /etc/X11/xdm/Xsetup の exit 0 行の直前に、次の行を追加します。

```
$xset m 1 1
```

- iii. Red Hat の場合、ファイル /etc/X11/xdm/Xsetup\_0 の exit 0 行の直前に、次の行を追加します。

```
xset m 1 1
```

- iv. ファイルを保管し、init 5 と入力して、runmode 5 に変更します。

- KDE の場合、次のステップを実行して、マウスの加速値としきい値を設定します。

- i. キーボードを使用して、Alt+F1 または Ctrl+Esc を押して、デスクトップにメニューを開きます。
- ii. メニューから、「**Preferences**」 → 「**Peripherals**」 → 「**Mouse**」 をクリックします。
- iii. 「**Advanced**」 タブを選択して、「**Pointer Acceleration**」 値と 「**Threshold**」 値を 1 に変更します。
- iv. このセッションからログアウトし、必ず 「**Log out**」 ウィンドウで 「**Save current setup**」 チェック・ボックスにチェック・マークを付けてください。

次回にログインすると、リモート・マウスとローカル・マウスは同期化されています。

- GNOME の場合、次のステップを実行して、マウスの加速値としきい値を設定します。

- i. キーボードを使用して Alt+F1 または Ctrl+Esc を押し、デスクトップにメニューを開きます。
- ii. メニューから、「**Programs**」 → 「**Settings**」 → 「**Session**」 → 「**Session Properties & Startup Programs**」 または 「**Extras**」 → 「**Preferences**」 → 「**Sessions**」 を選択します (Linux のバージョンに応じて)。
- iii. 「**Startup Programs**」 タブを選択し、次に 「**Add**」 を選択して、別のウィンドウを開きます。
- iv. コマンド・ラインで、xset m 1 1 と入力し、「**OK**」 をクリックして、このコマンドを保管します。
- v. 「**Apply**」 をクリックし、次に 「**OK**」 をクリックして、このウィンドウを終了します。このセッションからログアウトし、必ず 「**Log out**」 ウィンドウの 「**Save current setup**」 チェック・ボックスにチェック・マークを付けてください。

次回にログインすると、リモート・マウスとローカル・マウスは同期化されています。

**ヒント:** 初めてローカルとリモートのマウス・ポインターを同期化する (ローカルとリモートのマウス矢印を相互に重ねる) には、ポインターをディスプレイの 4 隅の 1 つに移動して、ローカルとリモートのマウス・ポインターを同じ位置に置きます。

オペレーティング・システムの次回の再始動時に、新規ハードウェアが検出されます。

**注意:** システムの次回のリブート時に、Linux のハードウェア検出プログラムが新規ハードウェアを検出します。以下の指示を注意してお読みください。

▶ SUSE LINUX の場合

サーバーの次回の再始動時に、SUSE LINUX オペレーティング・システムのハードウェア検出サービス・プログラム (YaST2) は、ハードウェアの変更を検出します。YaST2 では構成変更を行わないでください。ユーザーが手で追加した装置 (例えば、USB マウス) は、リモート・コンソールがサーバーに接続されているときにのみ、オペレーティング・システムによって認識されるためです。プロンプトが表示されたら、「**Cancel**」をクリックしてください。

▶ Red Hat の場合

サーバーの次回の再始動時に、Red Hat LINUX オペレーティング・システムのハードウェア検出プログラム (Kudzu) は、ハードウェアの変更を検出します。次の表は、Kudzu の照会と推奨ユーザー処置を示しています。

表 3-3 Kudzu メッセージと推奨ユーザー処置

Kudzu 照会	ユーザー応答
ATI Rage XL が除去された	「 <b>Keep Configuration</b> 」を選択
汎用 USB マウスが追加された	「 <b>Ignore</b> 」を選択
ATI RADEON が追加された	「 <b>Ignore</b> 」を選択
汎用 USB キーボードが追加された	「 <b>Ignore</b> 」を選択

### 3.5.2 リモート・メディアの使用

リモート・メディア・サポートを使用する前に、使用可能なネットワーク接続の帯域幅を確認してください。この機能は、100 Mbps LAN 環境で正常に機能します。低帯域幅の WAN 接続の場合、満足できるパフォーマンスが得られないことがあります。

リモート・メディアは、ブート・プロセス中またはオペレーティング・システムの稼働中に使用できません (72 ページの 3.5、『リモート・コンソールとリモート・メディア』で説明している制約事項を参照してください)。RSA II のこの機能を使用して、リモート・ロケーションからサーバーの完全なインストール (オペレーティング・システムおよびパッチを含む) を実行できます。これには、次のものが含まれます。

- ▶ サーバーの BIOS 更新 (ディスクレット・ベース)
- ▶ 診断プログラムの更新 (ディスクレット 2 個と、ブート用の BIOS 更新ディスクレット 1 個)
- ▶ ServeRAID™ アダプターのファームウェア・アップグレードと RAID 構成 (ServeRAID CD をブートする場合)

**ヒント :** Red Hat Enterprise Linux AS 3 または SUSE LINUX Enterprise Server 8 でリモート・ディスクレットまたは CD-ROM を使用している場合、システムがハングしたり、リモート・デバイスを認識しなかったりする場合があります。この問題は、将来の Linux バージョンで訂正されます。次のサイトの「RETAIN tip H181968」を参照してください。

<http://www.ibm.com/pc/support/site.wss/MIGR-55671.html>

上記の制約への対処方法は、リモート・コンソールでリモート・メディアを使用している間、デーモンを停止し、完了したらデーモンを再始動することです。手順は、次のとおりです。

1. Linux コマンド・プロンプトから、次のコマンドを使用して、ibmasm デーモンをアンロードします。

```
ibmspdwn
```

2. 手動でリモート・デバイスをマウントします。詳しくは、以下を参照してください。

- 83 ページの 3.5.3、『リモート・ディスクレット』
- 86 ページの 3.5.4、『リモート CD-ROM および DVD』
- 88 ページの 3.5.5、『リモート・ファイル』

3. リモート・コンソールと一緒にリモート・メディアを使用して、管理タスク (以下で説明) を実行します。
4. 管理タスクが終了したら、次のコマンドを使用して、ibmasm デーモンを再始動します。

```
ibmspup
```

リモート・メディアを使用するには、次のようにします。

1. ブラウザーのウィンドウを開いて、RSA II Web インターフェースにアクセスします。

2. 「**Tasks**」 → 「**Remote Control**」 をクリックします。
3. シングル・ユーザーまたはマルチ・ユーザー・モードを選択します。リモート・コンソールを開始するには、2つのオプションがあります。
  - シングル・ユーザー・モード。ユーザーがセッションを終了するまでは、他の人はこの RSA II 上で **Remote Control** を使用できません。通常は、このモードを使用します。「**Start Remote Control in Single User Mode**」をクリックします。
  - マルチ・ユーザー・モード。ユーザーのセッション中、他のユーザーがリモート・コンソールにアクセスできます。このモードは通常、2人の管理者に同時にマウス、キーボード、およびディスプレイの制御権を与える場合にのみ使用します。この場合、「競争条件」を作成し、各ユーザーが「競う」ことによりマウスとキーボードに対する制御権を取得するように設定できます。「**Start Remote Control in Multi User Mode**」をクリックします。
4. リモート・コンソール・ウィンドウで、デバイス（ファイル、ディスクレット、または CD-ROM）を選択し、「>>」をクリックして、リモート・メディアをサーバーにマウントします。
5. 複数のデバイスが必要な場合は、他のデバイスを選択します。
6. オプションで、「**Write Protect**」をクリックして、デバイスへの書き込みを防止できます。
7. 「**Mount Drive**」をクリックします。
8. ご使用のサーバーで **Windows** を実行している場合は、これで、そのメディアにドライブ名としてアクセスできるようになったはずですが。Linux の場合は、以下の説明に従って、ドライブをマウントする必要があります。
  - 83 ページの 3.5.3、『リモート・ディスクレット』
  - 86 ページの 3.5.4、『リモート CD-ROM および DVD』
  - 88 ページの 3.5.5、『リモート・ファイル』

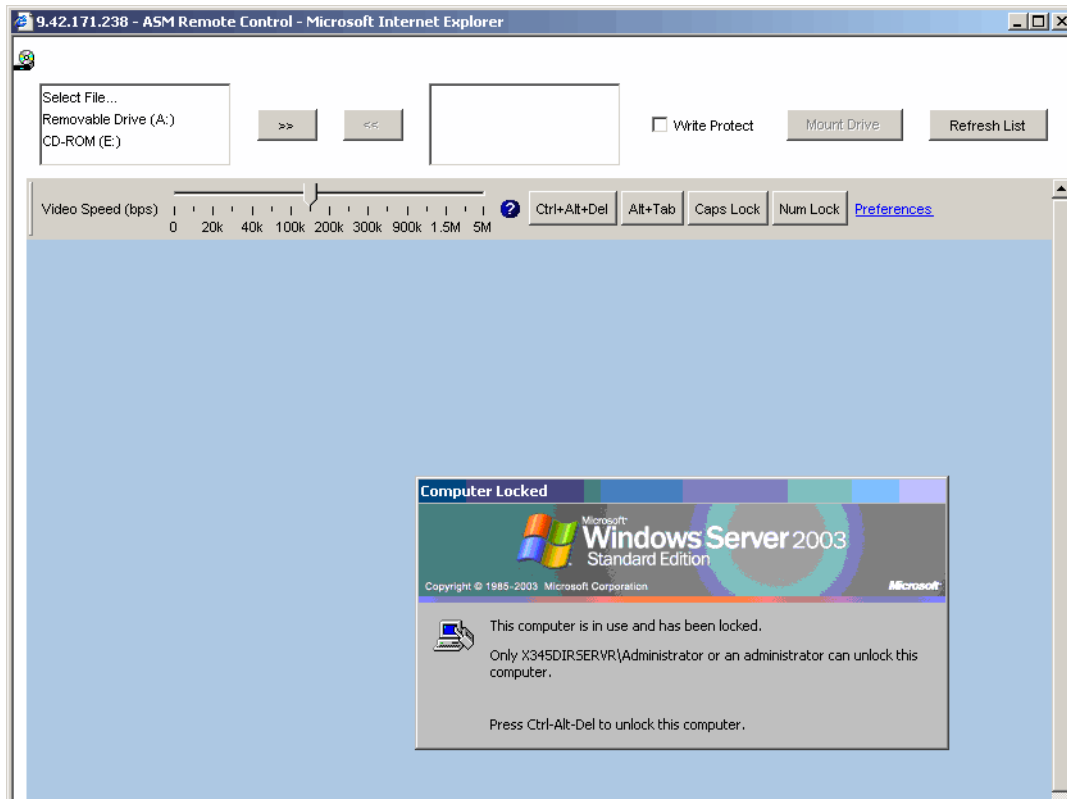


図3-15 リモート・コンソールとリモート・メディア

9. リモート・メディアをアンマウントするには、次のようにします。

Windows の場合

- a. リモート・コンソールのタスクバーの「Safely Remove Hardware」アイコンをダブルクリックします。



図3-16 Windows のタスクバーを使用したハードウェアの安全な取り外し

- b. 開いたウィンドウで、「**USB Mass Storage Device**」をクリックして、「**Stop**」をクリックします。
- c. 「**IBM Remote Disk USB device**」をクリックして、「**OK**」をクリックします。ハードウェアを安全に取り外せるようになったことを告げるメッセージが表示されます。
- d. 「**Close**」をクリックして、ウィンドウを閉じます。



Linux の場合は、オペレーティング・システム・レベルで **umount** コマンドを使用して、リモート・ドライブをアンマウントします。例えば、ご使用のマウント・コマンドが **mount /dev/sdb /media/floppy** であった場合は、**umount /media/floppy** を使用します。通常は、マウント・コマンドの 2 番目のパラメーター（マウント・ポイントを表す）をアンマウントで使用します。

10. 「**Unmount Drive**」をクリックし（ボタン「**Mount Drive**」は、マウント・プロセス中に「**Unmount Drive**」に変更されています）、次に「<<」をクリックして、ドライブ・リストから除去します。

### 3.5.3 リモート・ディスケット

リモート・ディスクを使用する場合、接続されている RSA II を使用して、ローカル・ディスケット・ドライブをサーバーにマウントできます。リモート・ディスケットを使用するには、次の手順を実行します。

1. 「**Removable Drive (A:)**」を選択して、「>>」をクリックします。
2. ディスケット・ドライブの内容をイメージとして RSA II にアップロードするかどうかを尋ねる際に、図 3-17 のようなダイアログが表示され、2 つのオプションが提供されます。

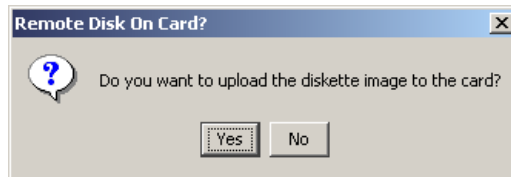


図3-17 RSA II - リモート・ディスケットのアップロード

「**Yes**」をクリックすると、RSA II はディスケットをメモリーにロードします。進行状況が表示されます。マウントは自動的に行われるため、「**Mount Drive**」をクリックする必要はありません。完了すると、オペレーティング・システム内で追加のドライブまたはデバイスとして使用可能になります。



図3-18 RSA II - カード上のリモート・ディスク

ディスケット・イメージ・ファイルをアップロードしない場合は、「**No**」をクリックします。オペレーティング・システム内でそれを使用できるようにするには、「**Mount Drive**」をクリックします。

サーバーをブートする際に、RSA II にディスク・イメージまたはディスクが含まれている場合、またはリモート・メディア Web インターフェースがまだオープンしている間にディスクまたはディスク・イメージがマウントされている場合、サーバーはそこからブートを試みます。メディアがブート可能であるのに機能しない場合は、BIOS 内のブート・シーケンスを検査してください。

**ヒント:** アップロード・オプションを使用した場合、不要になったらドライブをアンマウントしてください。次のリブート時に、ドライブがまだ存在すると、サーバーは RSA II のメモリー内のディスク・イメージからブートするためです。ディスク・イメージは、ユーザーが「**Unmount Drive**」をクリックするか、RSA II が再始動されるか、またはファームウェアが更新されるまで、そこに存在します。

## Windows 固有のステップ

Windows では、リモート・メディアは通常、B ドライブとして表示されます。

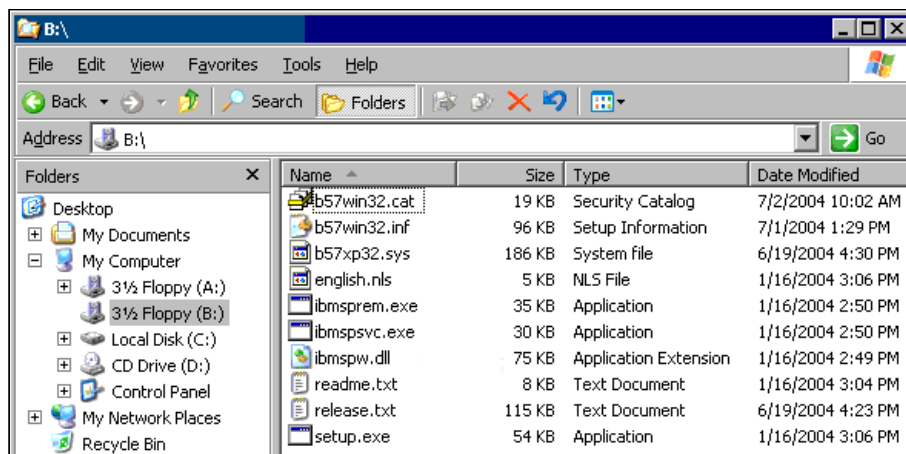


図 3-19 RSA II - リモート Windows 上のリモート・ディスク

アンマウントするには、リモート・メディア Web インターフェースを立ち上げて、82 ページの ステップ 9 に従います。

## Linux 固有のステップ

ユーザーが「**Mount Drive**」ボタンをクリックした後、Linux オペレーティング・システムはドライブを認識しますが、Linux のディストリビューションによっては、手動でドライブをマウントして、アクセスできるようにすることが必要な場合があります。マウントするデバイスの名前は、サーバーによって異なり、または以前にリモート・ファイルを使用したかどうかによっても異なります。デバイス名は、/dev/sda であったり、/dev/sdb であったりします。

## SUSE LINUX

SUSE LINUX の場合、「Mount Drive」ボタンをクリックした後で、ファイル `/etc/fstab` で、マウントするデバイスの名前を確認してください。85 ページの図 3-20 では、デバイス名は `/dev/sda` です。

<code>/dev/hda2</code>	<code>/</code>	<code>reiserfs</code>	<code>defaults 1 1</code>
<code>/dev/hda1</code>	<code>/data1</code>	<code>auto</code>	<code>noauto,user 0 0</code>
<code>/dev/hdc1</code>	<code>/data2</code>	<code>auto</code>	<code>noauto,user 0 0</code>
<code>/dev/hdc2</code>	<code>/data3</code>	<code>auto</code>	<code>noauto,user 0 0</code>
<code>/dev/hdc5</code>	<code>/data4</code>	<code>auto</code>	<code>noauto,user 0 0</code>
<code>/dev/hdc6</code>	<code>/data5</code>	<code>auto</code>	<code>noauto,user 0 0</code>
<code>/dev/hdc7</code>	<code>/data6</code>	<code>auto</code>	<code>noauto,user 0 0</code>
<code>/dev/hda3</code>	<code>swap</code>	<code>swap</code>	<code>pri=42 0 0</code>
<code>/dev/hdc3</code>	<code>swap</code>	<code>swap</code>	<code>pri=42 0 0</code>
<code>devpts</code>	<code>/dev/pts</code>	<code>devpts</code>	<code>mode=0620,gid=5 0 0</code>
<code>proc</code>	<code>/proc</code>	<code>proc</code>	<code>defaults 0 0</code>
<code>usbdevfs</code>	<code>/proc/bus/usb</code>	<code>usbdevfs</code>	<code>noauto 0 0</code>
<code>/dev/cdrom</code>	<code>/media/cdrom</code>	<code>auto</code>	<code>ro,noauto,user,exec 0 0</code>
<code>/dev/sda</code>	<code>/media/sda</code>	<code>auto</code>	<code>noauto,user,exec 0 0 #HOTPLUG B3Fu.NTFFBnoEy7</code>

図 3-20 SUSE LINUX - ファイル `/etc/fstab` とリモート・ドライブ

最後の行（丸で囲まれた）に、ホット・プラグ接続のリモート・メディア `/dev/sda` が示されています。

**重要：** SUSE LINUX Enterprise Server 8 のリモート・メディアは、SUSE Service Pack 3 がインストールされている場合にのみ機能します。

これで、次のコマンドを使用して、リモート・ディスクをマウントできるようになりました。

```
mount /media/sda
```

あるいは、追加のマウント・ポイント名も指定する必要がある場合は、`mount /dev/sda /media/floppy` を使用できます。

リモート・ディスクを使用した後、リモート・メディアをアンマウントしてください。これを行うには、リモート・メディア Web インターフェースを立ち上げて、82 ページの ステップ 9 に従います。

## Red Hat

Red Hat Linux を使用している場合、リモート・ディスクはファイル /etc/fstab に記述されません。そのため、ユーザーはリモート・デバイスへの接続に成功するまで、sda、sdb、sdcなどを試みる必要があります。

86 ページの図 3-21 では、**mount** コマンドを使用して、最初に /dev/sda、2 番目に /dev/sdb を試しています。

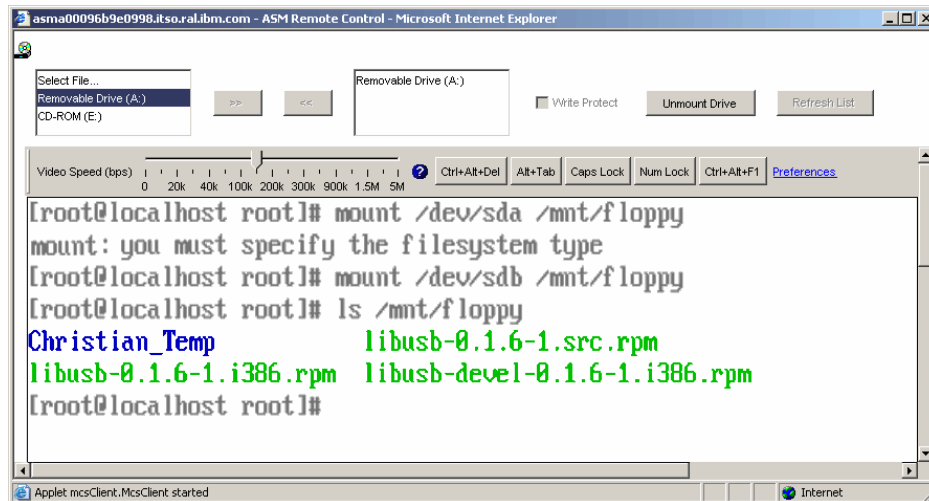


図 3-21 RSA II - Red Hat Linux でのリモート・ディスクの使用

デバイスをアンマウントするには、リモート・メディア Web インターフェースを立ち上げ、82 ページの ステップ 9 以降のステップを実行します。

### 3.5.4 リモート CD-ROM および DVD

リモート CD-ROM の機能は、リモート・ディスクに非常によく似ています。唯一の相違点は、RSA II は CD-ROM の内容をメモリーにロードしないことです。リモート CD-ROM からブートすることができ、またオペレーティング・システム内でそれをドライブ名として使用できます。リモート CD-ROM は、DVD ドライブおよびメディアと一緒に使用することもできます。

マウントは、リモート・メディア Web インターフェースがオープンしている間のみアクティブです。インターフェースをクローズすると、メディアは自動的にアンマウントされます。

リモート CD-ROM を使用するには、次の手順を実行します。

1. 「CD-ROM({driveletter}:)」を選択して、「>>」をクリックします。

2. 「Mount Drive」をクリックすると、CD-ROMをリモート・サーバーにマウントするプロセスが開始します。しばらくすると、ご使用のオペレーティング・システム内でリモートCD-ROMを使用できるようになります。

## Windows 固有のステップ

Windows オペレーティング・システムでは、ユーザーが「Mount Drive」ボタンを押した後しばらくして、オペレーティング・システム内にリモートCD-ROMがドライブ名として表示されます。次の図では、ドライブ E: として表示されています。

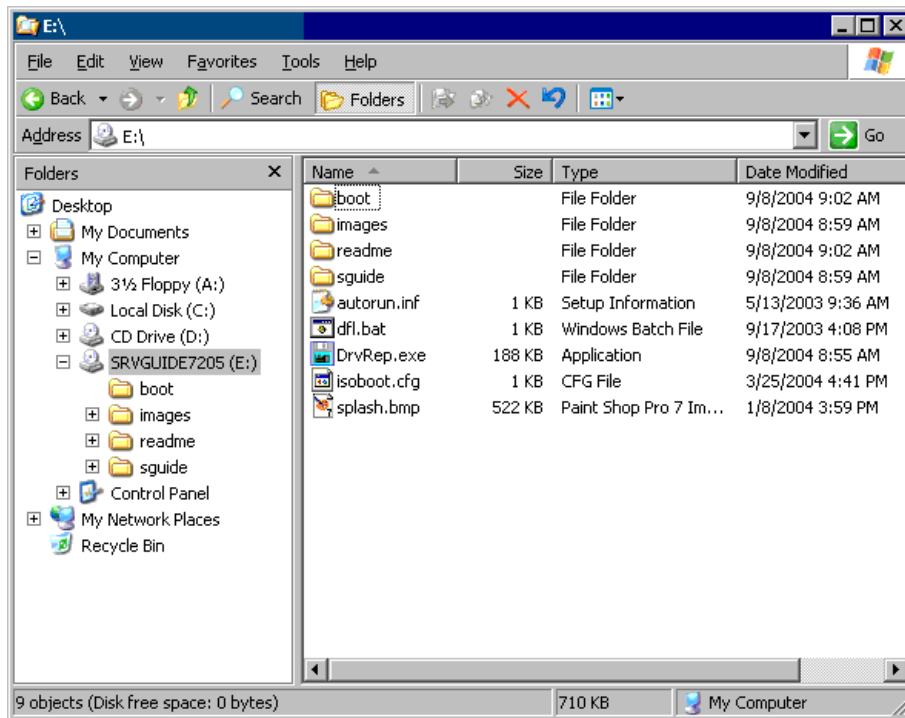


図 3-22 RSA II - リモート Windows 上のリモート CD-ROM

アンマウントするには、82 ページの ステップ 9 以降のステップに従います。

## Linux 固有のステップ

Linux オペレーティング・システムでは、リモート・メディアは自動的にマウントされません。ユーザーがマウントする必要があります。リモートCD-ROMは、SUSE および Red Hat のファイル /etc/fstab に表示されます。

## SUSE

オペレーティング・システムの `/etc/fstab` を検査します。デバイス `/dev/sr0` が見つかります。それをマウントするには、次のコマンドを入力します。

```
mount /dev/sr0 /media/cdrom
```

リモート・ディスクットを使用した後、リモート・メディアをアンマウントしてください。これを行うには、リモート・メディア Web インターフェースを立ち上げて、82 ページの ステップ 9 に従います。

## Red Hat

次の図は、Red Hat Linux のファイル `/etc/fstab` の例を示しています。

<code>LABEL=/</code>	<code>/</code>	<code>ext3</code>	<code>defaults</code>	<code>1 1</code>
<code>LABEL=/boot</code>	<code>/boot</code>	<code>ext3</code>	<code>defaults</code>	<code>1 2</code>
<code>none</code>	<code>/dev/pts</code>	<code>devpts</code>	<code>gid=5,mode=620</code>	<code>0 0</code>
<code>none</code>	<code>/proc</code>	<code>proc</code>	<code>defaults</code>	<code>0 0</code>
<code>none</code>	<code>/dev/shm</code>	<code>tmpfs</code>	<code>defaults</code>	<code>0 0</code>
<code>/dev/sda3</code>	<code>swap</code>	<code>swap</code>	<code>defaults</code>	<code>0 0</code>
<code>/dev/cdrom</code>	<code>/mnt/cdrom</code>	<code>udf,iso9660</code>	<code>noauto,owner,kudzu,ro</code>	<code>0 0</code>
<code>/dev/fd0</code>	<code>/mnt/floppy</code>	<code>auto</code>	<code>noauto,owner,kudzu</code>	<code>0 0</code>
<code>/dev/cdrom1</code>	<code>/mnt/cdrom1</code>	<code>udf,iso9660</code>	<code>noauto,owner,kudzu,ro</code>	<code>0 0</code>

図 3-23 Red Hat Linux - ファイル `/etc/fstab` とリモート・ドライブ

最後の行に、リモート・メディア `/dev/cdrom1` が示されています。ご使用のオペレーティング・システムにドライブをマウントします。

```
mount /mnt/cdrom1
```

アンマウントするには、82 ページの ステップ 9 以降のステップに従います。

### 3.5.5 リモート・ファイル

リモート・ファイル機能を使用すると、ディスクットおよび CD-ROM イメージを、マウントするドライブとして使用できます。リモート・ファイルは、リモート・ディスクット / CD-ROM と同様に機能します。ドライブ・イメージ・ファイルは、標準 IMG または BIN ファイルや ISO ファイルのような、ディスクットの非圧縮バイト単位コピーでなければなりません。

**制約事項:** 次のような制約があります。

- ▶ ISO イメージ・サポートには、2005 年 3 月以降の日付の RSA II ファームウェアが必要です。
- ▶ ISO ファイルは、ISO9660 フォーマットであることが必要です。

ファイルをマウントするには、次のようにします。

1. 「**Select File...**」をクリックして、「>>」ボタンをクリックします。

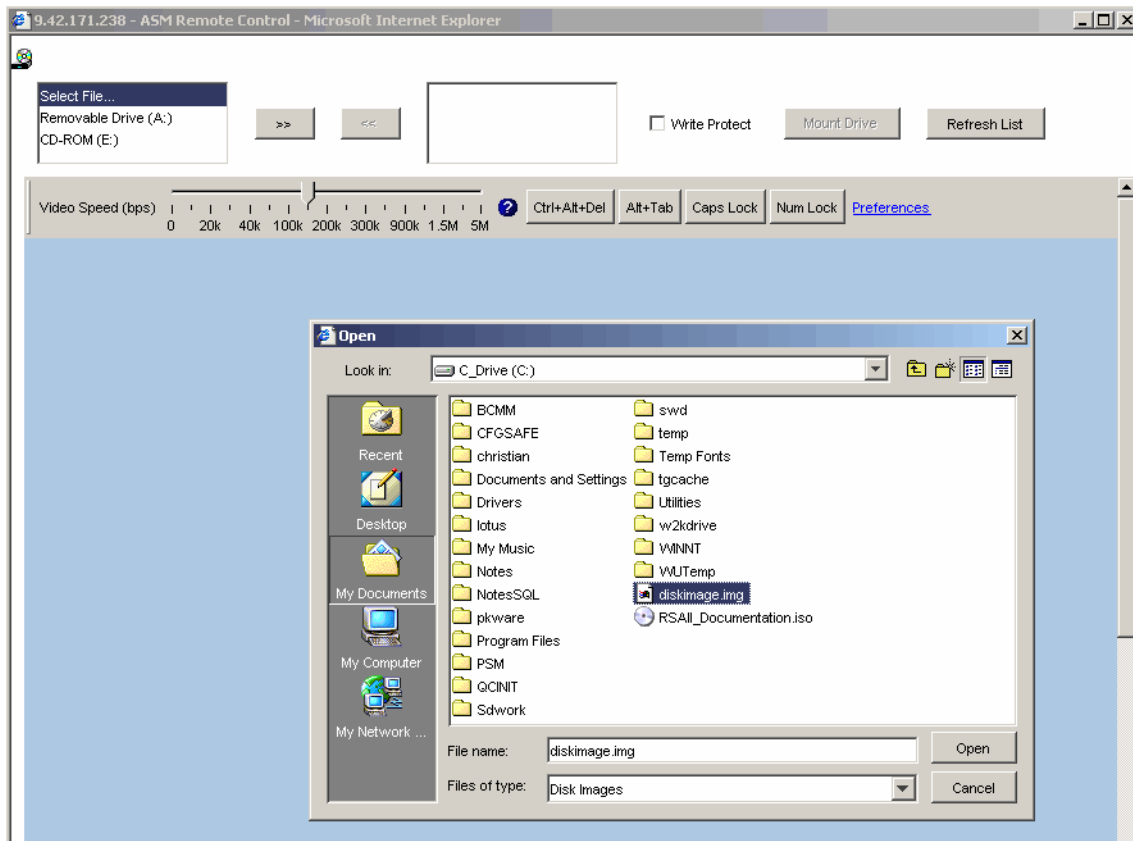


図 3-24 RSA II リモート・メディア-ファイル

2. 使用するディスク・イメージを選択した後、「**Open**」をクリックします。次のようなプロンプトが表示されます。

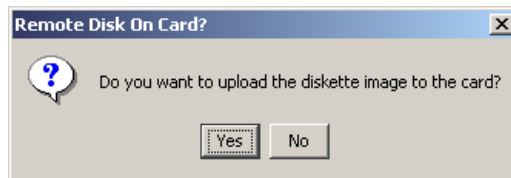


図 3-25 RSA II- リモート・ファイルのアップロード

「**Yes**」をクリックすると、ファイルはサーバー上の RSA II アダプターの RAM にアップロードされます。イメージをアップロードするには、イメー

ジの大きさが 1.44 MB を超えないことが必要です。ネットワーク接続によっては、アップロードに少し時間がかかることがあります。進行状況が表示され、アップロード・プロセスにかかる時間が示されます。



図3-26 RSA II - カード上のリモート・ディスク

**ヒント:** ユーザーが「**Unmount**」ボタンを使用してアンマウントするか、RSA II が再始動されるか、またはファームウェアが更新されるまで、イメージはサーバーにアクセス可能のままです。

「**No**」をクリックした場合は、さらに「**Mount Drive**」をクリックして、リモート・サーバーにドライブをマウントする必要があります。ファイルはアップロードされておらず、ご使用のローカル PC からネットワーク経由でリモート・アクセスします。このリモート・ファイルからの後続のファイル・アクセスは、ネットワーク速度になります。リモート・コンソール・ウィンドウをクローズすると、リモート・ファイルは自動的にアンマウントされます。

## Windows 固有のステップ

サーバーが Windows を実行している場合、ディスク・イメージ・ファイルは、オペレーティング・システムでドライブ名として使用可能になっています。Windows Explorer で新規ドライブを確認してください。

アンマウントするには、リモート・メディア Web インターフェースを立ち上げ、82 ページの ステップ 9 以降のステップを実行します。

## Linux 固有のステップ

サーバーが Linux を実行している場合、次に、オペレーティング・システムにドライブをマウントする必要があります。

### SUSE

「**Mount Drive**」ボタンを押す前と後に、ファイル /etc/fstab で新規デバイスを検査します。



/dev/sda2	/	reiserfs	defaults	1 1
/dev/sda1	swap	swap	pri=42	0 0
devpts	/dev/pts	devpts	mode=0620,gid=5	0 0
proc	/proc	proc	defaults	0 0
usbdevfs	/proc/bus/usb	usbdevfs	noauto	0 0
/dev/cdrom	/media/cdrom	auto	ro,noauto,user,exec	0 0
/dev/fd0	/media/floppy	auto	noauto,user,exec	0 0
/dev/sdb	/media/sdb	auto	noauto,user,exec	0 0 #HOTPLUG
B3Fu.c+j0WmpZdK6				

図 3-27 ファイル/etc/fstab とリモート・ファイル

最後の行に、リモート・ファイルのデバイスが表示されています。次のコマンドを使用して、それをマウントします。

```
mount /dev/sdb /media/usbfloppy
```

アンマウントするには、82 ページの ステップ 9 以降のステップに従います。

### Red Hat

Red Hat Linux を使用している場合、リモート・ディスクはファイル /etc/fstab にリストされません。そのため、ユーザーはリモート・デバイスへの接続に成功するまで、sda、sdb、sdc などを試みる必要があります。

86 ページの図 3-21 では、**mount** コマンドを使用して、最初に /dev/sda、2 番目に /dev/sdb を試しています。

始めに、次のコマンドを使用して、リモート・ディスクをマウントします。

```
mount /dev/sda /mnt/floppy
```

これは機能せず、エラー・メッセージ「mount: you must specify the file system」を受け取る場合、デバイス名は /dev/sdb です。今度は、mount /dev/sdb /mnt/floppy と入力して、ドライブをマウントします。

アンマウントするには、リモート・メディア Web インターフェースを立ち上げ、82 ページの ステップ 9 以降のステップを実行します。

## 3.6 リモート管理アダプター II によって使用されるポート

RSA II は、通信用にいくつかの tcp/udp ポートを使用します。RSA II との通信がファイアウォールを通過する場合、RSA との通信のためにファイアウォール上のどのポートを使用可能にする必要があるかを知ることが重要です。以下に、デフォルト・ポートを示した表を掲載します。RSA 内でポートを変更し

た場合は、ファイアウォールでも変更する必要があることを覚えておいてください。

表 3-4 RSA II によって使用されるユーザー構成可能な TCP/IP ポート

ポート名	ポート番号	説明
http	80 (デフォルト)	Web サーバー HTTP 接続 - TCP
https	443 (デフォルト)	SSL 接続 - TCP
telnet	23 (デフォルト)	Telnet コマンド・ライン・インターフェース接続 - TCP
SSH	22 (デフォルト)	Secure Shell (SSH) コマンド・ライン・インターフェース - TCP
SNMP エージェント	161 (デフォルト)	SNMP get/set コマンド - UDP
SNMP トラップ	162 (デフォルト)	SNMP トラップ - UDP

いくつかの他のポートは固定で、変更できません。

表 3-5 RSA II によって使用される固定 TCP/IP ポート

ポート番号	説明
427	SLP 接続 - UDP
1044	リモート・ディスク機能 - TCP
1045	永続リモート・ディスク (カード上のディスク) - TCP
2000	リモート・コンソール・ビデオ・リダイレクト - TCP
6090	IBM Director コマンド - TCP
7070-7074	パーティション管理 - TCP



## BladeCenter 管理モジュール

BladeCenter 管理モジュールは、49 ページの第 3 章、『リモート管理アダプター II』で説明した RSA II によく似た機能を備えています。その他に、統合 KVM スイッチなど、BladeCenter に固有の機能がいくつかあります。

BladeCenter 管理モジュールは、シャーシに搭載されたすべてのブレード・サーバーに対するグローバル RSA II のような働きをします。この章では、BladeCenter 管理モジュールと RSA II の相違点と類似点、および管理モジュールに固有のいくつかの問題について説明します。

この章の内容は、次のとおりです。

- ▶ 94 ページの 4.1、『機構および機能』
- ▶ 97 ページの 4.2、『管理モジュールの基本構成』
- ▶ 103 ページの 4.3、『リダンダント管理モジュール』
- ▶ 106 ページの 4.4、『リモート・コンソールとリモート・メディア』
- ▶ 127 ページの 4.5、『ブレード固有の機能の基本構成』
- ▶ 134 ページの 4.6、『管理モジュールによって使用されるポート』
- ▶ 136 ページの 4.7、『管理モジュールの出荷時のデフォルト値へのリセット』

## 4.1 機構および機能

管理モジュールは、シャーシにすべてのネットワーク・モジュール（例えば、Gigabit Ethernet または SAN）とすべてのブレード・サーバーを搭載した状態で、BladeCenter シャーシ自体を管理します。

管理モジュールは、ブレード・サーバーを管理するために、統合 KVM スイッチと、すべてのモジュール（イーサネット・スイッチ・モジュール（ESM）、ファイバー・チャンネル・スイッチ・モジュールなど）への内部 IP 接続用の内蔵ネットワーク・スイッチを装備しています。それに加えて、搭載された個々のブレード・サーバーに対して RSA II と同様の役目も果たします。

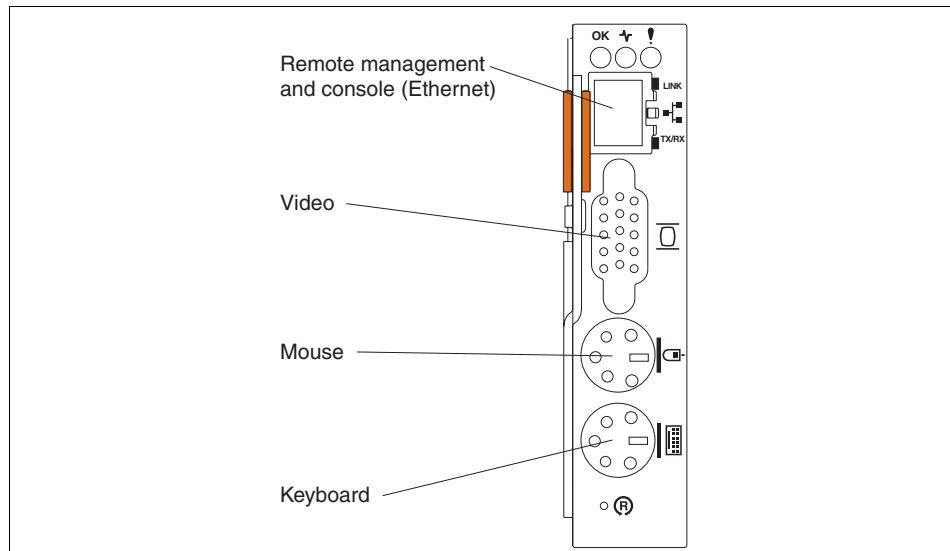


図 4-1 BladeCenter 管理モジュールのコネクター

RSA II と同様に、管理モジュールは、各ブレード・サーバーに内蔵されたサービス・プロセッサと通信します。

**注：** BladeCenter 管理モジュールは、ASM インターコネクト・ネットワークをサポートしません。

BladeCenter 管理モジュールは、BladeCenter または BladeCenter T でサポートされます。BladeCenter T は、特に通信業界に適した、Network Equipment Building Standard (NEBS) 準拠の特殊シャーシで、標準サーバー・ラックより奥行きが浅いラックに収容できます。ブレード・サーバーと BladeCenter のオプションの

ほとんどは、両方タイプの BladeCenter シャーシでサポートされます。詳細については、IBM ServerProven Web サイトでご確認ください。

<http://www.pc.ibm.com/us/compat/>

表 4-1 は、管理モジュールの機能の概要を示し、副見出しにより、モニター、ブレード・サーバー・タスク、入出力モジュール・タスク、および管理モジュール制御に分けて表示しています。この表は、それぞれの機能を実行するために必要なユーザー権限を示しています。

表 4-1 BladeCenter 管理モジュールの機能と必要な権限

ウィンドウ	情報の変更またはタスクの実行に必要な権限								
	Supervisor	Blade server Remote Console Access	Blade server remote console and remote media access	Blade and I/O module Power/Restart Access	Ability to clear event logs	Basic configuration (MM, I/O modules, blades)	Network and security configuration	Advanced configuration (MM, I/O modules, blades)	User account management
<b>モニター</b>									
System Status	✓	✓	✓	✓	✓	✓	✓	✓	✓
Event Log (表示)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Event Log (クリア)	✓				✓				
LEDs	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hardware VPD	✓	✓	✓	✓	✓	✓	✓	✓	✓
Firmware VPD	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>ブレード・タスク</b>									
Power/restart	✓			✓					
On demand	✓			✓					
Remote control (リモート・コンソール)	✓	✓	✓						
Remote control (リモート・メディア)	✓		✓						

ウィンドウ	情報の変更またはタスクの実行に必要な権限								
	Supervisor	Blade server Remote Console Access	Blade server remote console and remote media access	Blade and I/O module Power/Restart Access	Ability to clear event logs	Basic configuration (MM, I/O modules, blades)	Network and security configuration	Advanced configuration (MM, I/O modules, blades)	User account management
Firmware update	✓							✓	
Configuration	✓					✓		✓	
Serial over LAN	✓						✓	✓	
入出力モジュール・タスク									
Power/restart	✓			✓					
Management	✓						✓	✓	
Firmware update	✓							✓	
管理モジュール・タスク									
General settings	✓					✓		✓	
Login profiles	✓							✓	✓
Alerts	✓					✓		✓	
Port assignments	✓						✓	✓	
Network interfaces	✓						✓	✓	
Network protocols	✓						✓	✓	
Security	✓						✓	✓	
Configuration file	✓							✓	
Firmware update	✓							✓	
Restore defaults	✓							✓	
Restart MM	✓							✓	

## 4.2 管理モジュールの基本構成

管理モジュールの機能を使用するには、最初に管理モジュールを構成する必要があります。このセクションでは、基本構成の手順を説明します。詳細については、255 ページの 7.3、『すべての BladeCenter モジュールへのリモート・アクセスの提供』、および製品資料「BladeCenter 管理モジュール ユーザーズ・ガイド」を参照してください。

### 4.2.1 BladeCenter への取り付け

BladeCenter をインストールする場合、管理モジュールが 1 個、上部管理モジュール・ベイ（ベイ 1）にプリインストールされた状態で出荷されます。BladeCenter は、2 台目のリダンダント管理モジュールもサポートし、図 4-2 に示すように、これをベイ 2 に取り付けることができます。

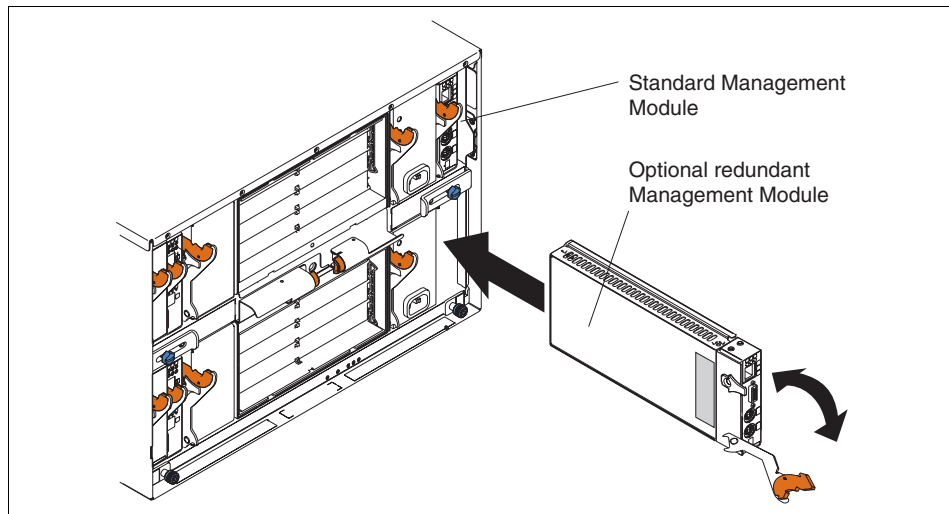


図 4-2 リダンダント管理モジュールの取り付け

リダンダント管理モジュールの使用については、103 ページの 4.3、『リダンダント管理モジュール』で説明します。

**注：**オレンジ色のリリース・ラッチが付いたモジュールは、すべてホット・スワップ可能です。BladeCenter の電源を遮断する必要はありません。ただし、モジュールを交換する前に、実行中のサーバーやアプリケーションにアクティブ接続する可能性があるため十分な注意が必要です。

## 4.2.2 ネットワーク設定

管理モジュールは、自動的に IP アドレスの設定を試みます。これは、次の方法で行います。

1. 管理モジュールは、アクティブ DHCP サーバーを検索して、IP アドレスとサブネット・マスクおよびデフォルト・ゲートウェイの取得を試みます。
2. DHCP サーバーから 2 分以内に応答がない場合、管理モジュールは、デフォルトの IP アドレス 192.168.70.125 とサブネット・マスク 255.255.255.0 を使用します。ホスト名は MMxxxxxx になります。ここで、xxxxxx は、管理モジュールの MAC アドレスです。MAC アドレスは、図 4-3 に示すように、最下部のラベルに記載されています。

BladeCenter のサブネットにアクティブの DHCP サーバーまたは DHCP リレー・エージェントがある場合、DHCP サーバーの専用線を検査して、管理モジュールの MAC アドレスを確認してください。

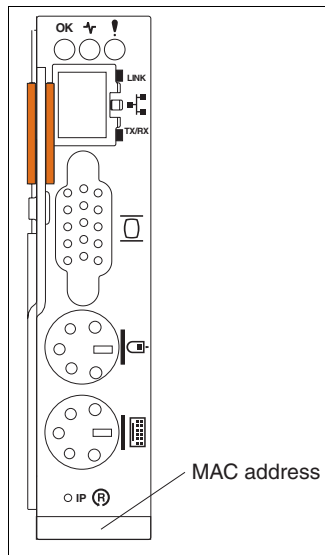


図 4-3 BladeCenter 管理モジュールの MAC アドレス

**ヒント：** DHCP サーバーに問題があっても装置にアクセスできるようにするために、xSeries システム管理ハードウェアはすべて固定 IP アドレスを使用することをお勧めします。



固定アドレスの使用をお勧めしますが、動的アドレスから固定アドレスに変更するには、管理モジュールに接続して、設定を変更する必要があります。動的に割り当てられたアドレスを入手するには、2つの方法があります。

▶ DHCP サーバーからアドレスを取得

管理モジュールの MAC アドレスを使用して DHCP サーバーを検査し、それに割り当てられた動的 IP アドレスを入手します。管理モジュールと同じ LAN へのイーサネット接続をもつ PC を使用して、管理モジュールの IP アドレスを使って Web ブラウザーを立ち上げます。

▶ DHCP を使用しない

DHCP サーバーがないか、最初の方法は利用できない場合、管理モジュールをイーサネット・ネットワークから切断し、BladeCenter の電源をオンにします。これにより、管理モジュールは、強制的にデフォルト・アドレスの 192.168.70.125 を取ります。イーサネット・クロスケーブルを使用して、管理モジュールをスタンドアロン PC またはノートブックに接続します。この PC は、192.168.70.0/24 サブネット内に IP アドレスを持っている必要があります。

PC には、サポートされるブラウザと Java 1.4 がインストールされていることが必要です。詳細な仕様は、232 ページの 6.5、『Web インターフェース』を参照してください。

**ヒント:** イーサネット・クロスケーブルを使用して PC またはノートブックを管理モジュールに接続する際に、以下の IP アドレスを使用してはなりません。以下のアドレスは、BladeCenter の事前定義 IP アドレスです。

- ▶ 192.168.70.125 - 管理モジュール外部ポート
- ▶ 192.168.70.126 - 管理モジュール内部ポート
- ▶ 192.168.70.127 - モジュール・ベイ 1 内部ポート
- ▶ 192.168.70.128 - モジュール・ベイ 2 内部ポート
- ▶ 192.168.70.129 - モジュール・ベイ 3 内部ポート
- ▶ 192.168.70.130 - モジュール・ベイ 4 内部ポート

接続された PC のブラウザを使用して、管理モジュールの Web インターフェースを立ち上げ、基本ネットワーク構成を行います。

1. 標準ユーザー USERID と PASSWORD (ゼロ、文字の O ではない) をパスワードとして使用して、ログオンします。

**ヒント:** セキュリティ上の理由から、標準パスワードはできるだけ早く変更するように計画する必要があります。

2. Web インターフェースが始動したら、「**Continue**」をクリックします。ここでは、タイムアウト値を変更する必要はありませんが、必要であれば変更できます。
3. 左側のナビゲーション・フレームで、「**MM Control**」をクリックしてサブメニューを展開し、「**Network Interfaces**」をクリックします。
4. 「**External Network Interface (eth0)**」セクションの DHCP プルダウンから「**Disabled - Use static IP configuration**」を選択します。
5. 管理モジュールのホスト名を入力します。
6. 管理モジュールに割り当てる IP アドレス、ネットワークのサブネット・マスク、および標準ゲートウェイを入力します。詳細については、ネットワーク管理者にお尋ねください。
7. スクロールダウンして、「**Save**」をクリックします。
8. 変更は管理モジュールを再始動したときに有効になることを説明するダイアログに対して、「**OK**」をクリックします。
9. ナビゲーション・フレームの「**MM Control**」メニューで、「**Restart MM**」をクリックします。
10. 「**Restart MM**」セクションで、「**Restart**」をクリックします。
11. 「**OK**」をクリックして、管理モジュールを再始動します。
12. 管理モジュールのリセットを告げるメッセージを表示したブラウザー・ウィンドウがポップアップ表示されます。表示された後しばらくしてから、ウィンドウ内の「**Yes**」をクリックして、ブラウザーを閉じます。

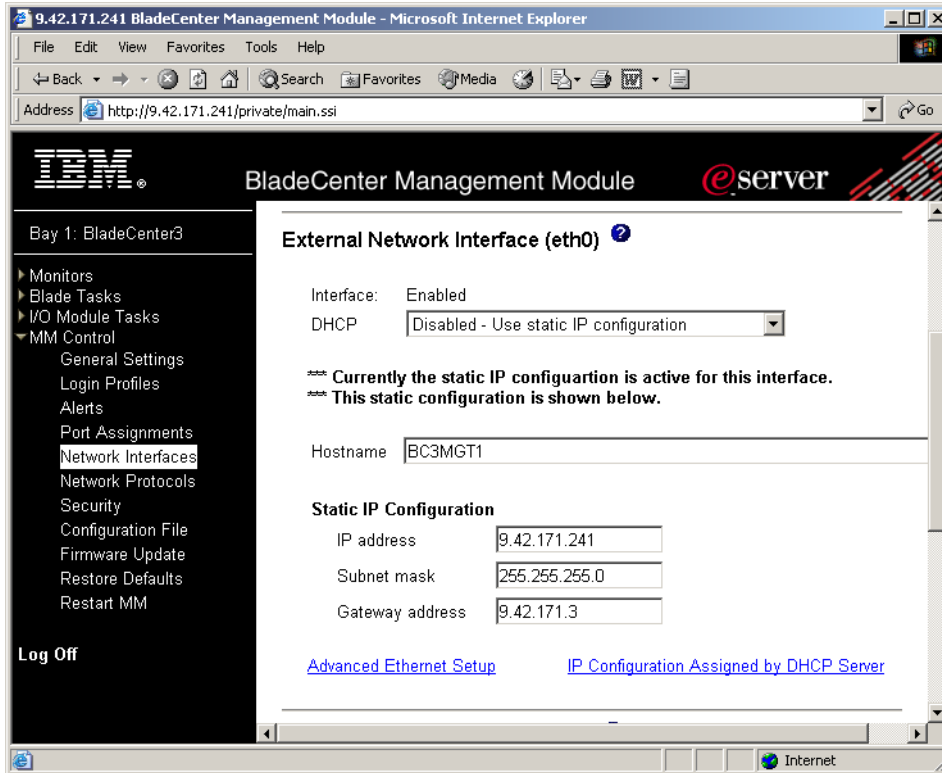


図 4-4 ネットワーク・インターフェース

管理モジュールの再始動には 1 分かかります。イーサネット・クロスケーブルを使用してスタンドアロン PC に接続している場合、これは、管理モジュールをご使用のイーサネット・ネットワークに接続するのにかかる適正な時間です。

ヒント: 管理モジュールのネットワーク接続を検査するには、ネットワークに接続された別のシステムから **ping** コマンドを使用します。

### 4.2.3 ファームウェアの更新

次のステップは、管理モジュールのファームウェアを最新バージョンに更新することです。最新バージョンは、次の URL からダウンロードできます。

- ▶ BladeCenter: <http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>
- ▶ BladeCenter T: <http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>

ファイルを解凍した後、少し時間をとって **readme.txt** をお読みください。次のファイルをご使用のディレクトリーに入れる必要があります。

Name ▲	Size	Type	Modified
26r0697.zip	1,796 KB	PKZIP File	10/28/2004 6:35 PM
cnetbrus.pkt	65 KB	PKT File	9/30/2004 12:27 PM
cnetmnus.pkt	1,678 KB	PKT File	9/30/2004 12:50 PM
cnetrgus.pkt	68 KB	PKT File	9/30/2004 12:27 PM
mmalert.mib	37 KB	MIB File	9/30/2004 12:20 PM
mmblade.mib	488 KB	MIB File	9/30/2004 12:22 PM
readme.txt	12 KB	Text Document	9/30/2004 1:25 PM

図 4-5 ファームウェア更新パッケージのファイル

**注：**BladeCenter 管理モジュールのファームウェアの更新には、管理プロセッサ・コマンド・ライン・インターフェース (MPCLI) も使用できます。詳しくは、273 ページの 7.8.1、『MPCLI を使用したファームウェアの更新』を参照してください。

以下のステップを実行して、ファームウェアを更新し、Web インターフェースを使用して管理モジュールを再始動します。

1. ナビゲーション・フレームで、「**Tasks**」 → 「**Firmware Update**」をクリックします。

### Update MM Firmware ?

To update a firmware component on the MM, select a firmware file and click "Update". If there is a redundant MM installed, the firmware on the redundant MM will be automatically updated to the same level.

**Note:** To ensure proper operation of the management module, make sure you update all MM firmware components to the same level.

図 4-6 BladeCenter 管理モジュールのファームウェア更新

2. 「**Browse**」をクリックして、ファームウェア更新用の 3 つのファイルのうち最初のファイルを選択します。
3. 更新するために、「**Update**」をクリックします。これで、ファイルは管理モジュールに転送されました。
4. ファイルの転送が終了したら、「**Continue**」をクリックして、フラッシュ・プロセスを開始します。

5. 残りの2つのファイルについて、上記のステップを繰り返します。
6. 終了したら、「**MM Control**」 → 「**Restart MM**」をクリックして、アダプターを再始動します。

これで、管理モジュールの他のオプションを使用または構成できるようになりました。その他のオプションの一部のものについて、この章の残りの部分で説明します。

**ヒント:** 管理モジュールの基本構成を行った後、インストールされたスイッチ・モジュールに対しても同じ作業を行う必要があります。詳しくは、132 ページの 4.5.3、『入出力モジュール・タスク』を参照してください。

## 4.2.4 MIB ファイル

管理モジュールは、IBM Director を含めて、さまざまな管理ツールからの SNMP をサポートします。MIB ファイルが必要な場合、管理モジュールのファームウェア更新用の ZIP ファイルに含まれています。

- ▶ BladeCenter の管理モジュール・ファームウェア  
<http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>
- ▶ BladeCenter T の管理モジュール・ファームウェア  
<http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>

## 4.3 リダンダント管理モジュール

BladeCenter 全体の概念の基本は、完全な冗長性です。管理モジュール自体も、リダンダントにできます。1 次のアクティブ・モジュールに障害が起きた場合、またはユーザーが切り替えを開始した場合、リダンダント管理モジュールがアクティブ・モジュールに取って代わり、前のアクティブ・モジュールは障害モジュールまたはリダンダント・モジュールになります。

### 4.3.1 取り付けと配線

BladeCenter に取り付けした後、1 次モジュールのすべての構成データが、自動的にリダンダント・モジュールに転送されます。ユーザーが構成データを変更した場合、1 次モジュールは自動的にリダンダント・モジュールに変更を転送します。

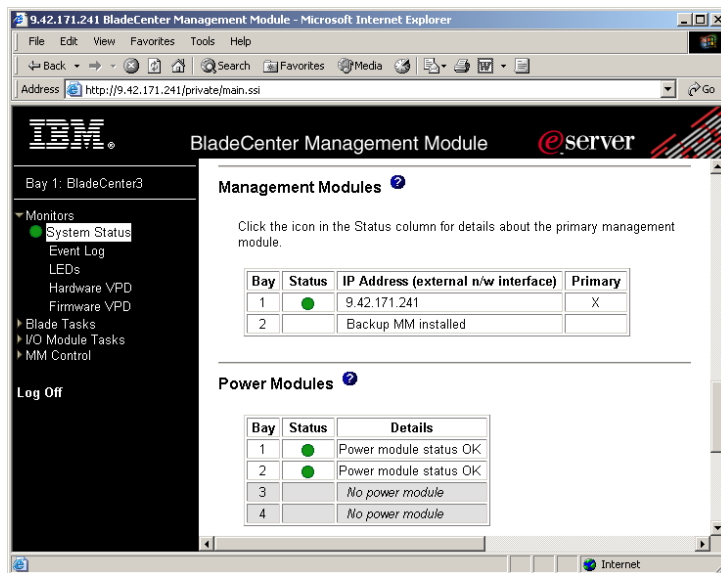


図4-7 リダンダント管理モジュール

## ファームウェアの更新

1次管理モジュールのファームウェアを更新すると、更新されたファイルが自動的にリダンダント管理モジュールに転送されます。リダンダント・モジュール上の新規ファームウェアをアクティブにするには、リダンダント・モジュールを再始動する必要があります。

リダンダント・モジュールの再始動は、手動切り替えで行うことができます。105ページの4.3.2、『手動切り替え』を参照してください。この機能は、ファームウェア・バージョン 1.15 (BRET73E) で追加されたものです。

**注:** リダンダント管理モジュールのファームウェアが1次モジュールのファームウェアよりかなり古い場合、更新の転送が正常に行われず、次のようなメッセージが出る場合があります。

Transfer of MM main application image from MM1 to MM2 failed: Could not write new firmware image to the device to be updated.

この場合の対処方法は、手動でフェイルオーバーを実行し、その後でファームウェアを更新することです。

## イーサネット・インターフェース

リダンダント管理モジュールのイーサネット・ポートを、ご使用のLANに接続します。1次モジュールのIP設定が使用可能ですが、イーサネット・ポートは

切り替えが行われるまで使用不可にされます。切り替えの後しばらくすると、同じ IP アドレスを使用して、アクティブ管理モジュールの Web インターフェースに接続できるようになります。

### **KVM 接続**

マウス、キーボード、およびモニターをリダンダント管理モジュールに接続することが必要です。KVM ポートは、コンソール・スイッチに接続するか、または専用のキーボード、モニター、およびマウスに接続します。リダンダント・モジュールが 1 次モジュールになった場合、その KVM 接続を使用する必要があります。

## **4.3.2 手動切り替え**

フェイルオーバー・ソリューションをインプリメントした場合、それをテストして、障害が発生したときに正常に機能することを確認しておく必要があります。BladeCenter の管理モジュールの切り替えをテストするには、Web インターフェースを立ち上げて、ログオンします。

1. ナビゲーター・バーで、「**MM Control**」をクリックします。
2. 「**Restart MM**」をクリックします。
3. 「**Switch Over**」をクリックします。
4. 「**OK**」をクリックします。

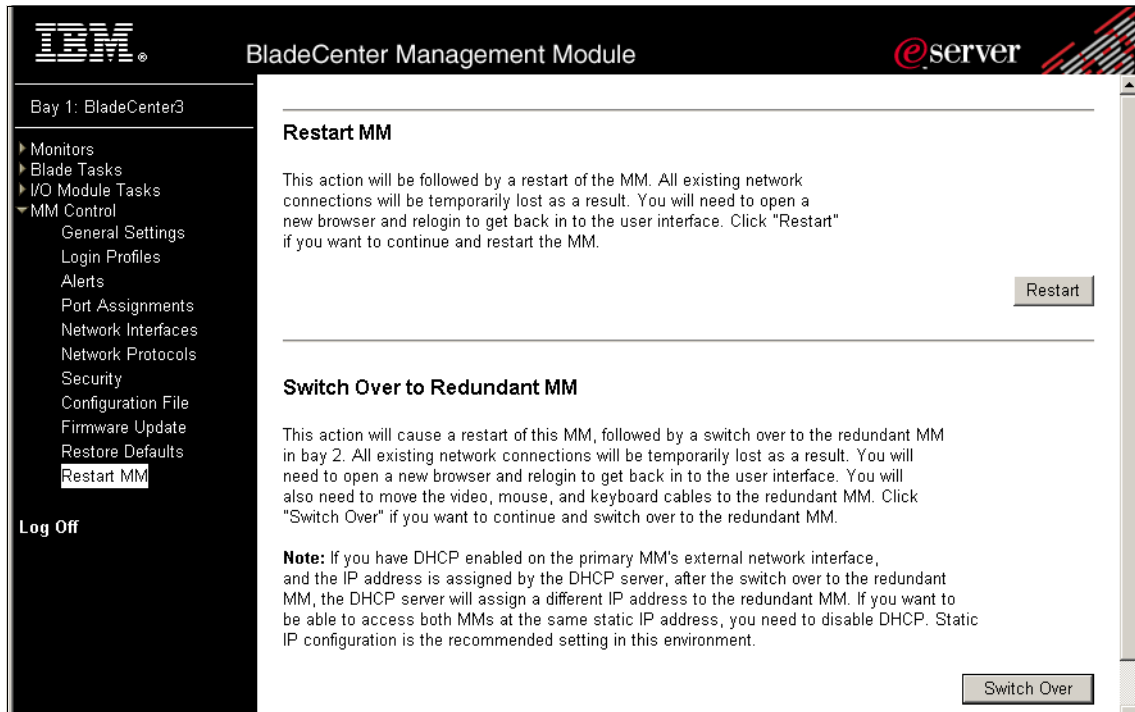


図 4-8 リダンダント管理モジュールへの切り替え

リダンダント管理モジュールが 1 次管理モジュールになります。前のアクティブ・モジュールがリポートして、それがリダンダント・モジュールになります。リダンダント・モジュールがアクティブになるまでは、BladeCenter を管理するための管理モジュールが存在しません。そのため、ファンは両方とも 100 パーセントで作動し、オレンジ色のエラー LED が点灯します。切り替えプロセスが完了し、管理モジュールが役割の交代を終了した後は、BladeCenter の状況は再び正常に戻ります。

## 4.4 リモート・コンソールとリモート・メディア

リモート・コンソールおよびリモート・メディア機能は、RSA II と非常によく似ています。その他に、ブレード・サーバーと BladeCenter のメディア・トレイに関連した追加機能を備えています。

リモート・メディアを使用するには、OS の稼働中または OS のインストール中に、オペレーティング・システムからの USB サポートが必要です。リモート・メディアは、次のオペレーティング・システムで機能します。

- ▶ Windows Server 2003



- ▶ Windows 2000 Server (Service Pack 4 以降を搭載)
- ▶ Red Hat Enterprise Linux AS 3 (ただし、OS のインストールには使用できない)
- ▶ SUSE LINUX Enterprise Server 8 (ただし、OS のインストールには使用できない)

Java ランタイムが必要です。これは、次のサイトからインストールできます。

<http://www.java.com/en/download/manual.jsp>

**制約事項:** リモート・メディアは、Red Hat および SUSE LINUX のインストール時にはサポートされません。インストーラーによるリモート CD-ROM の認識またはマウント/アンマウントに問題があるためです。これは、Linux ディストリビューションの将来のバージョンで訂正される予定です。

リモート・コンソールを立ち上げるには、Web インターフェースをオープンしてログオンし、ナビゲーション・フレームで「**Blade Tasks**」→「**Remote Control**」をクリックします。

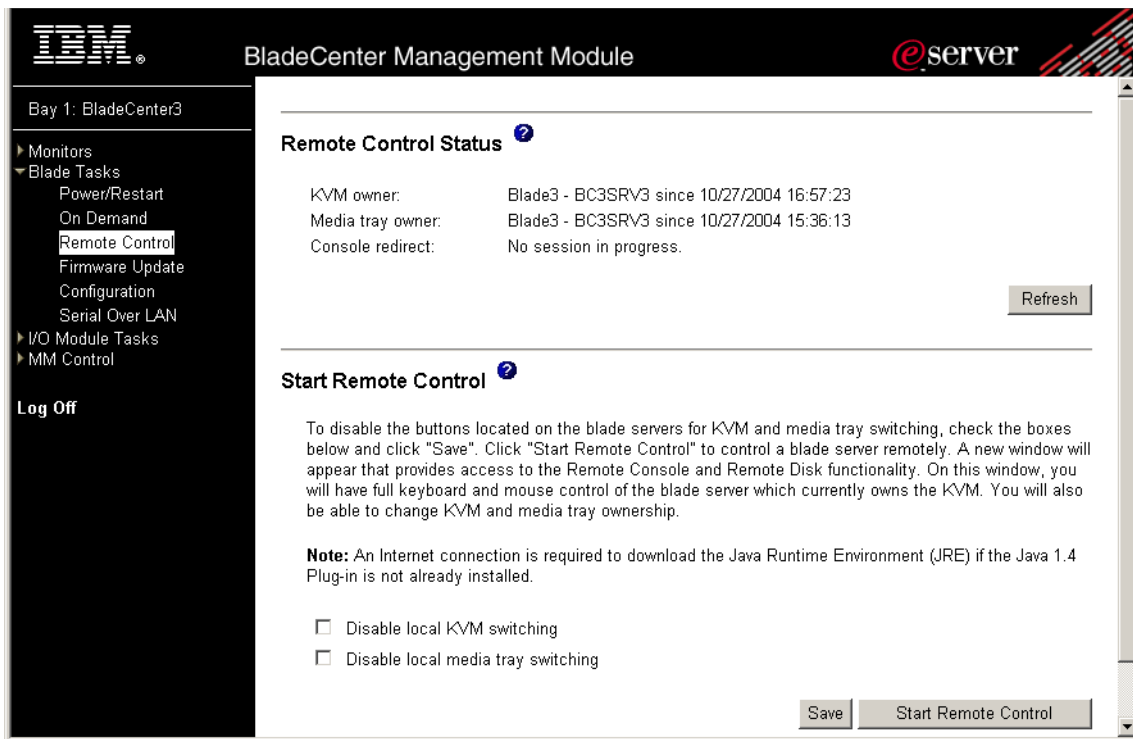


図 4-9 Remote Control の立ち上げ

「Remote Console Status」セクションを見ると、どのブレード・サーバーが KVM の所有者で、どれがメディア・トレイ (CD/DVD-ROM およびディスクレット・ドライブ) の所有者であるかが分かります。「Start Remote Control」セクションでは、ブレード・サーバーでの KVM およびメディア・トレイのローカル手動切り替えを使用不可にすることを選択できます。

**ヒント:** 上記のオプションを使用して KVM とメディア・トレイのローカル切り替えを使用不可にしない場合、製品のインストール中に誰かが BladeCenter で KVM またはメディア・トレイを別のブレード・サーバーに切り替える危険性があります。これが起きた場合、インストールは失敗します。

「Start Remote Control」をクリックして、「Remote Control」ウィンドウを立ち上げます。セキュリティー警告のウィンドウがポップアップ表示されることがあります。この警告は、Remote Control が使用する Java アプレットから出されるものです。この警告は正常なもので、IBM からの証明を信用して「Yes」をクリックして構いません。

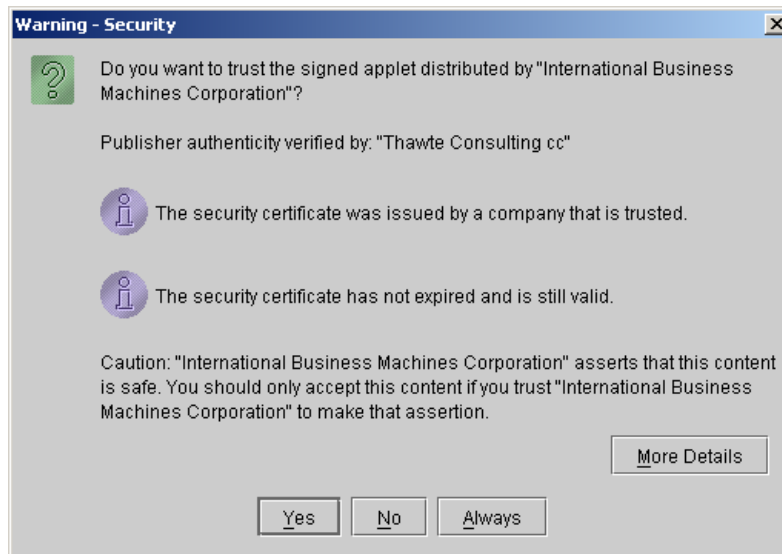


図 4-10 セキュリティー警告

「More Details」をクリックして、この警告の詳細を見るか、または「Yes」をクリックして続行します。

**ヒント:** 「Always」をクリックしない限り、「Remote Control」に入るたびに、このウィンドウがポップアップ表示されます。

ロードされると、現在 KVM を所有しているブレード・サーバーのコンソールが表示されます。

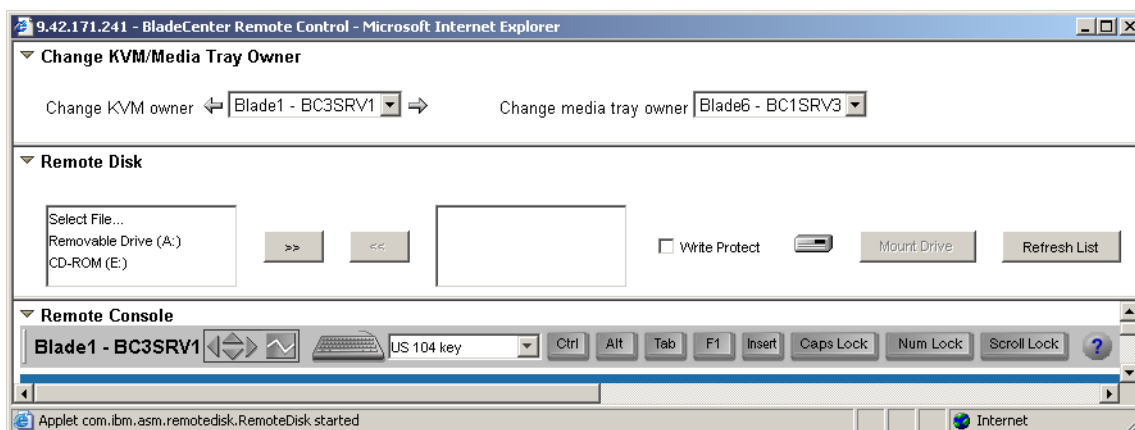








図 4-11 BladeCenter の Remote control

「Remote Control」ウィンドウ（109 ページの図 4-11）には、リモート・コンソールの上に 3 つのコントロール・パネルがあります。

- ▶ 「Change KVM/Media Tray Owner」パネルでは、リモート側で制御するブレード・サーバーを選択できます。KVM を所有するブレード・サーバーが、リモート側で制御できるブレード・サーバーです。メディア・トレイ（ディスク・ドライブと CD/DVD-ROM ドライブの両方）を所有するブレード・サーバーも、ここで指定できます。
- ▶ 「Remote Disk」パネルは、ブレード・サーバーに対して、ご使用のローカル PC またはノートブック上のディスクをリモート側で使用できるように設定する場所です。
- ▶ 「Remote Console」パネルは、次の機能を備えています。
  - 画面調整コントロール  は、アプレット・ウィンドウ内のビデオの表示位置を指定します。ビデオ・ディスプレイの相違により、各ブレード・サーバーのビデオの位置合わせが多少異なることがあります。画面調整コントロールを使用して、ビデオの左上隅をアプレットのビデオ表示域の左上隅に位置合わせします。正確なマウス操作のためには、正しいビデオの位置合わせが必要です。
  - 位相調整ボタン  は、リモート・サーバー上のアナログ・ビデオを強制的に自動調整します。ビデオの映像がぼやけたり、破損したりしていることに気付いた場合、このボタンを押す必要があります。位相調整の実行中は、リモート更新は送信されません。リモート・ユーザーは、位相調整がアクティブの間、サーバーの表示が静止していることを確認する必要があります。

- キーボード・セレクター   では、エミュレートするキーボード・タイプを指定できます。

キー・アイコンは、キー・ストロークを直接リモート・サーバーに送信するのに使用します。Alt または Ctrl キーの組み合わせを送信するには、別のキーを押す前に、Alt および / または Ctrl キー・アイコンをクリックします。たとえば、Ctrl-Alt-Del キーの組み合わせを送信するには、 をクリックし、 をクリックした後で、ご使用のキーボード上で Delete キーを押します。Delete を押した時点で、3つのキー・ストロークのすべてがサーバーに送信されます。Alt または Ctrl アイコンをクリックして、それをアクティブにした場合、キーボード・キーを押すか、そのアイコンを再度クリックするまで、アクティブのままです。表示されているその他のキーを送信するときも、キーボード・キーの代わりにアイコンを使用してください。ご使用のコンピューター上の Lock キーではなく、Caps Lock、Num Lock、および Scroll Lock アイコンを使用してください。

**ヒント:** リモート・サーバーのリモート・コンソールの表示部分を大きくするために、各見出しの前にある小さい三角をクリックして、この3つのパネルを縮小できます。

#### 4.4.1 Linux の Remote Control サポート

Linux ディストリビューションで Remote Control 機能を使用する場合、リモート・マウスおよびキーボードを機能させるために、オペレーティング・システム内で追加の構成ステップが必要です。

1. 解像度が 1024 x 768 でない場合、正しい解像度情報をマウス・ハンドラーに提供するために、次のようにします。
  - a. Linux コマンド・プロンプトで、`init 3` と入力します。
  - b. マウス・ドライバー・モジュールをアンロードします。これを行うには、`rmmmod mousedev` と入力します。
  - c. 次のステートメントをファイル `/etc/modules.conf` に追加します。

```
options mousedev xres=X, yres=Y
```

ここで、*X* と *Y* は、ビデオ解像度を指定します。
  - d. コマンド `insmod mousedev` を使用して、マウス・ドライバー・モジュールを再ロードします。
  - e. `init 5` と入力して、runlevel 5 に戻します。

2. Remote Control セッション中にローカル・マウスとリモート・マウスを同期化する（動きを一致させる）には、グラフィカル・ログイン画面（XDM）とユーザーの優先 GUI（KDE や GNOME など）を変更する必要があります。
  - XDM の場合は、次のようにします。
    - i. `init 3` と入力して、`runmode 3` に変更します。
    - ii. SUSE LINUX の場合、ファイル `/etc/X11/xdm/Xsetup` の `exit 0` 行の直前に、次の行を追加します。

```
$xset m 1 1
```
    - iii. Red Hat の場合、ファイル `/etc/X11/xdm/Xsetup_0` の `exit 0` 行の直前に、次の行を追加します。

```
xset m 1 1
```
    - iv. ファイルを保管し、`init 5` と入力して、`runmode 5` に変更します。
  - KDE の場合、次のステップを実行して、マウスの加速値としきい値を設定します。
    - i. キーボードを使用して `Alt+F1` または `Ctrl+Esc` を押し、デスクトップにメニューを開きます。
    - ii. メニューから、「**Preferences**」→「**Peripherals**」→「**Mouse**」をクリックします。
    - iii. 「**Advanced**」タブを選択して、「**Pointer Acceleration**」値と「**Threshold**」値を 1 に変更します。
    - iv. このセッションからログアウトし、必ず「**Log out**」ウィンドウで「**Save current setup**」チェック・ボックスにチェック・マークを付けてください。次回にログインすると、リモート・マウスとローカル・マウスは同期化されています。
  - GNOME の場合、次のステップを実行して、マウスの加速値としきい値を設定します。
    - i. キーボードを使用して `Alt+F1` または `Ctrl+Esc` を押し、デスクトップにメニューを開きます。
    - ii. メニューから、「**Programs**」→「**Settings**」→「**Session**」→「**Session Properties & Startup Programs**」または「**Extras**」→「**Preferences**」→「**Sessions**」を選択します（Linux のバージョンに応じて）。
    - iii. 「**Startup Programs**」タブを選択し、次に「**Add**」を選択して、別のウィンドウを開きます。
    - iv. コマンド・ラインで、`xset m 1 1` と入力し、「**OK**」をクリックして、このコマンドを保管します。

- v. 「**Apply**」をクリックし、次に「**OK**」をクリックして、このウィンドウを終了します。このセッションからログアウトし、必ず「**Log out**」ウィンドウで「**Save current setup**」チェック・ボックスにチェック・マークを付けてください。

次回にログインすると、リモート・マウスとローカル・マウスは同期化されています。

**ヒント:** 初めてローカルとリモートのマウス・ポインターを同期化する（ローカルとリモートのマウス矢印を相互に重ねる）には、ポインターを 4 隅の 1 つに移動して、ローカルとリモートのマウス・ポインターを同じ位置に置きます。

## 4.4.2 リモート・メディアの使用

リモート・メディア・サポートを使用する前に、使用可能なネットワーク接続の帯域幅を確認してください。この機能は、100 Mbps LAN 環境で正常に機能します。低帯域幅の WAN 接続の場合、満足できるパフォーマンスが得られないことがあります。

リモート・メディアは、ブート・プロセス中またはオペレーティング・システムの稼働中に使用できます（106 ページの 4.4、『リモート・コンソールとリモート・メディア』で説明している制約事項を参照してください）。この機能を使用して、リモート・ロケーションからサーバーの完全なインストール（オペレーティング・システムおよびパッチを含む）を実行できます。

**ヒント:** Linux で両方のディスクレット・ドライブ（ローカルとリモート。両方とも USB デバイスであるため）を使用する場合、1 つのマウント・ポイントを両方に使用して混乱しないようにするために、リモート・ディスクレット用に新規のマウント・ポイントを作成する必要があります。SUSE Linux コマンド・ラインに `mkdir /media/usbfloppy` と入力します（Red Hat の場合は、`mkdir /mnt/usbfloppy`）。

メディア・トレイ内のローカル・デバイス（ディスクレットまたは CD-ROM）が、SUSE LINUX および Red Hat Linux のファイル `/etc/fstab` に項目を作成します。

リモート・メディアをマウントするプロセスは、少し時間がかかります。Web インターフェースのリモート・メディア・セクションのメディア・シンボルが点滅を停止するまで待つから、Windows Explorer または Linux の `/etc/fstab` で確認してください。

**重要** : SUSE LINUX Enterprise Server 8 のリモート・メディアは、SUSE Service Pack 3 がインストールされている場合にのみ機能します。

リモート・メディアを使用するには、次のようにします。

1. ブラウザーのウィンドウを開いて、**Web** インターフェースにアクセスします。
2. 「**Blade Tasks**」 → 「**Remote Control**」 をクリックします。
3. 「**Start Remote Control**」 をクリックします。
4. リモート・コンソール・ウィンドウで、タイプ（ファイル、ディスク、または CD-ROM）を選択して、「>>」 をクリックし、次に 「**Mount Drive**」 をクリックして、リモート・メディアをサーバーにマウントします。オプションで、書き込み保護を選択できます。
5. ご使用のサーバーで **Windows** を実行している場合は、これで、そのメディアにドライブ名としてアクセスできるはずですが、**Linux** の場合は、以下の説明に従って、ドライブをマウントする必要があります。
  - 115 ページの 4.4.3、『リモート・ディスク』
  - 120 ページの 4.4.4、『リモート CD-ROM および DVD』
  - 123 ページの 4.4.5、『リモート・ファイル』

**ヒント** : 現時点では、リモート・メディア・イメージ・ファイルに書き込みアクセスすることはできません。

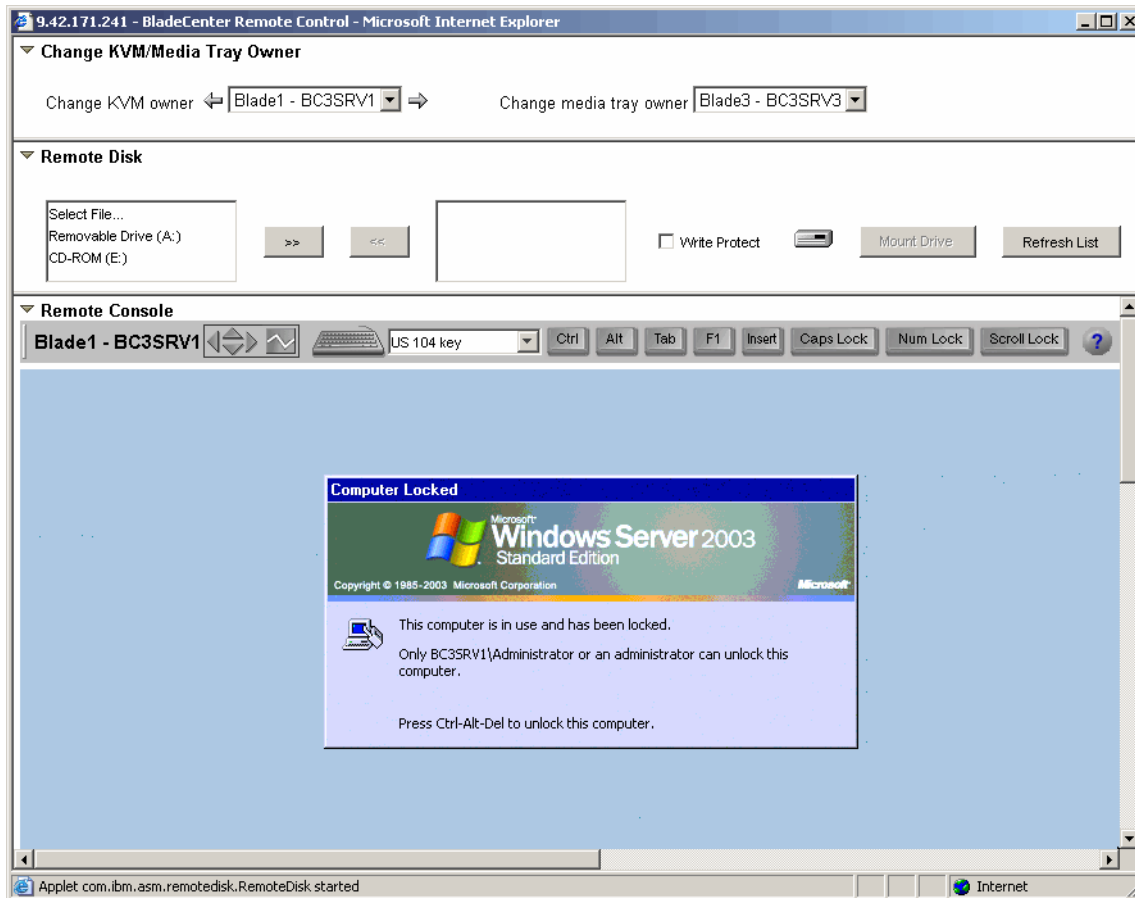


図 4-12 リモート・コンソールとリモート・メディア

6. リモート・メディアをアンマウントするには、次のようにします。

Windows の場合

- a. リモート・コンソールのタスクバーの「Safely Remove Hardware」アイコンをダブルクリックします。



図 4-13 Windows のタスクバーの「ハードウェアの安全な取り外し」アイコン

- vi. 開いたウィンドウで、「USB Mass Storage Device」をクリックして、「Stop」をクリックします。



b. 「**IBM Remote Disk USB device**」をクリックして、「**OK**」をクリックします。ハードウェアを安全に取り外せるようになったことを告げるメッセージが表示されます。

c. 「**Close**」をクリックして、ウィンドウを閉じます。

Linux の場合は、オペレーティング・システム・レベルで **umount** コマンドを使用して、リモート・ドライブをアンマウントします。例えば、ご使用のマウント・コマンドが **mount /dev/sdb /media/floppy** であった場合は、**umount /media/floppy** を使用します。通常は、マウント・コマンドの 2 番目のパラメーター（マウント・ポイントを表す）をアンマウントで使用します。

7. 「**Unmount Drive**」をクリックし（ボタン「**Mount Drive**」は、マウント・プロセス中に「**Unmount Drive**」に変更されています）、次に「**<<**」をクリックして、ドライブ・リストから除去します。

### 4.4.3 リモート・ディスク

リモート・ディスクを使用する場合、接続されているブレード・サーバーにローカル・ディスク・ドライブをマウントできます。

1. 「**Removable Drive (A:)**」を選択して、「**>>**」をクリックします。
2. ディスケット・ドライブの内容をイメージとして管理モジュールにアップロードするかどうかを尋ねられた場合、2つのオプションがあります。

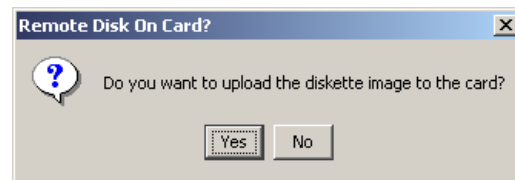


図4-14 リモート・ディスクのアップロード

「**Yes**」をクリックすると、管理モジュールはディスク・イメージをメモリにロードします。進行状況が表示されます。ディスク・イメージを管理モジュールのメモリにロードする際にマウントが自動的に行われるため、「**Mount Drive**」をクリックする必要はありません。完了すると、オペレーティング・システム内で追加のドライブとして使用可能になります。



図4-15 カード上のリモート・ディスク

ディスク・イメージ・ファイルをアップロードしない場合は、「**No**」をクリックします。オペレーティング・システム内でそれを使用できるようにするには、「**Mount Drive**」をクリックします。

サーバーをブートする際に、管理モジュールにディスク・イメージまたはディスクが含まれている場合、またはリモート・メディア Web インターフェイスがまだオープンしている間にディスクまたはディスク・イメージがマウントされている場合、サーバーはそこからブートを試みます。メディアがブート可能であるのに機能しない場合は、BIOS 内のブート・シーケンスを検査してください。

**ヒント:** アップロード・オプションを使用した場合、不要になったらドライブをアンマウントしてください。次のリブート時に、ドライブがまだ存在すると、サーバーは管理モジュールのメモリー内のディスク・イメージからブートするためです。

## Windows 固有のステップ

Windows オペレーティング・システムでは、おそらく新規の B ドライブとして検出されます。

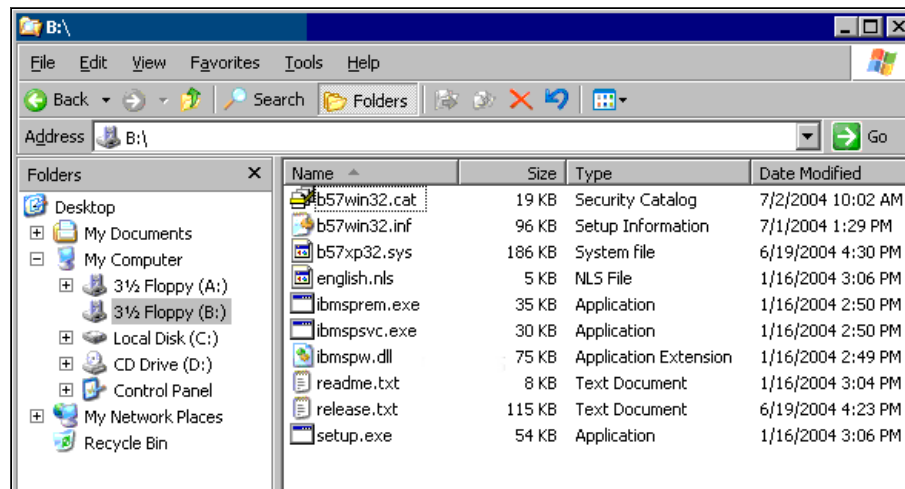


図 4-16 RSA II - リモート Windows 上のリモート・ディスク

アンマウントするには、リモート・メディア Web インターフェイスを立ち上げて、114 ページの ステップ 6 に従います。

## Linux 固有のステップ

Windows ではオペレーティング・システムが自動的にリモート・ドライブをドライブ名にマウントしますが、Windows とは異なり、Linux でのリモート・メ

ディアは、手動による追加作業が必要になります。「Mount Drive」ボタンをクリックした後、Linux オペレーティング・システムはデバイスを認識しますが、それにアクセスするには、ユーザーが手動でドライブをマウントする必要があります。

## SUSE LINUX

SUSE LINUX では、リモート・メディアおよびローカル・メディア・トレイ（ディスクおよび CD-ROM）は、接続されると、ファイル /etc/fstab に「HOTPLUG」項目を作成します。それをマウントするには、/etc/fstab で正しいデバイス名を確認してください。デバイス /dev/cdrom は、BladeCenter の SUSE LINUX 内では使用されません。

**ヒント：** Web インターフェースで「Mount Drive」ボタンをクリックする前と後に、ファイル /etc/fstab を検査して、どのデバイスがリモート・メディア・デバイスであるかを確認してください。

図 4-17 は、「Mount Drive」ボタンをクリックする前のファイル /etc/fstab を示しています。メディア・トレイのデバイスは、/dev/sda（ディスク）と /dev/sr0（CD-ROM）です。

**注：** デバイス /dev/cdrom は、SUSE LINUX およびブレード・サーバーでは使用されません。

/dev/hda2	/	reiserfs	defaults	1 1
/dev/hda1	/data1	auto	noauto,user	0 0
/dev/hdc1	/data2	auto	noauto,user	0 0
/dev/hdc2	/data3	auto	noauto,user	0 0
/dev/hdc5	/data4	auto	noauto,user	0 0
/dev/hdc6	/data5	auto	noauto,user	0 0
/dev/hdc7	/data6	auto	noauto,user	0 0
/dev/hda3	swap	swap	pri=42	0 0
/dev/hdc3	swap	swap	pri=42	0 0
devpts	/dev/pts	devpts	mode=0620,gid=5	0 0
proc	/proc	proc	defaults	0 0
usbdevfs	/proc/bus/usb	usbdevfs	noauto	0 0
/dev/cdrom	/media/cdrom	auto	ro,noauto,user,exec	0 0
/dev/sr0	/media/sr0	auto	ro,noauto,user,exec	0 0 #HOTPLUG B3Fu.dJIEZns+fE6
/dev/sda	/media/sda	auto	noauto,user,exec	0 0 #HOTPLUG B3Fu.oDWa+wJIPbZ

図 4-17 SUSE LINUX - リモート・ドライブの前のファイル /etc/fstab

118 ページの図 4-18 では、リモート・ディスクが新規デバイス /dev/sdb として認識されていることが分かります。下の図に示されたマウント・コマンドを使用するか、または次の例のように、マウント・ポイントの分かりやすい名前を使用します。

```
mount /dev/sdb /media/usbfloppy
```

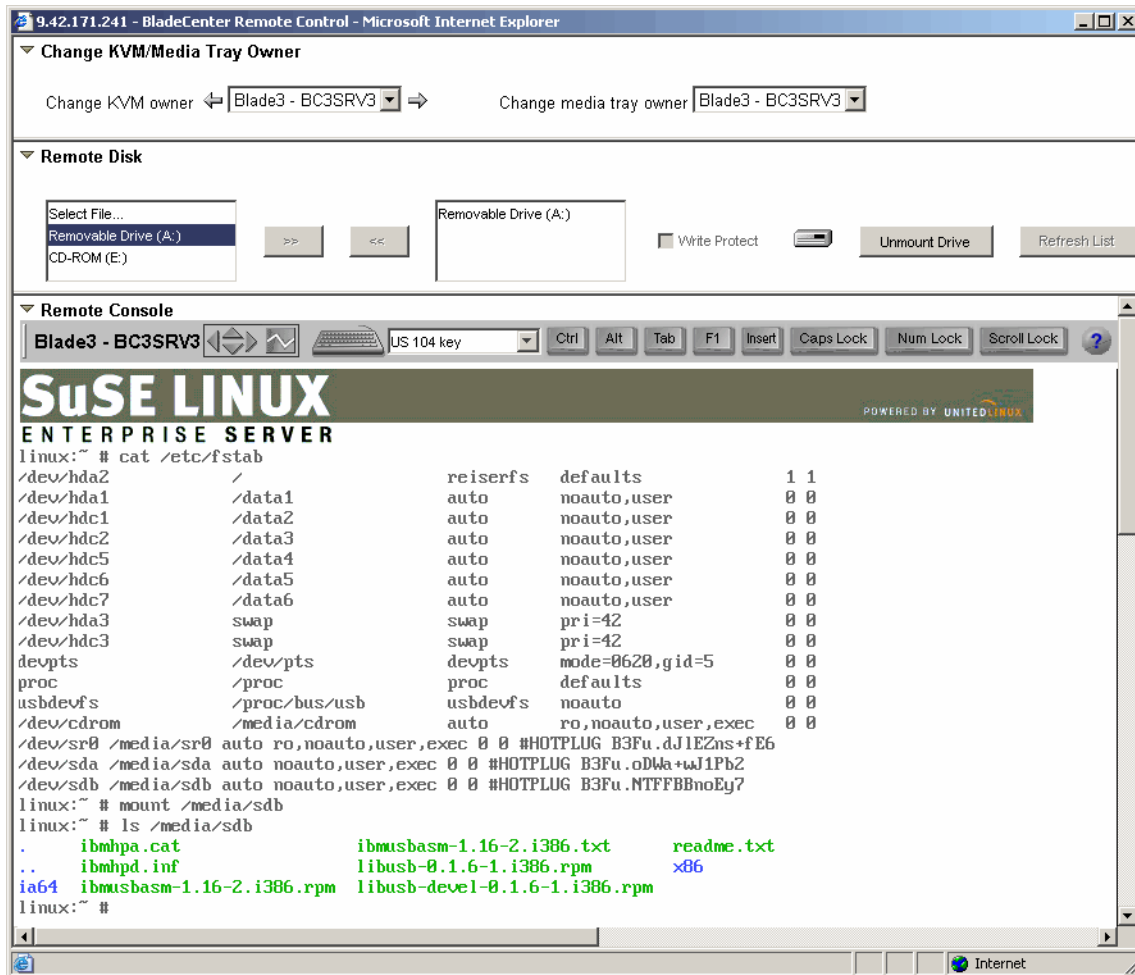


図 4-18 BladeCenter 管理モジュール - Linux でのリモート・ディスク

このドライブは、不要になったらアンマウントしてください。114 ページのステップ 6 以降のステップを実行します。

## Red Hat Linux

Red Hat Linux を使用している場合、`/etc/fstab` にはリモート・ディスク用の新規項目はありません。リモート・ディスクのデバイス名は、メディア・ベイの所有権と、サーバーのブート後に最初に使用されたデバイス（リモート・ディスク、リモート・ファイル、またはメディア・ベイ）によって決まります。

最初にリモート・ディスクまたはリモート・ファイルを使用した場合、デバイス名は `/dev/sda` になります。最初にサーバーがメディア・トレイの所有権を持っていた場合、リモート・ディスクのデバイス名は `/dev/sdb` になります。

そのため、ユーザーはリモート・デバイスへの接続に成功するまで、`sda`、`sdb`、`sdc` などを試みる必要があります。

図 4-19 では、最初に `mount /dev/sda /mnt/usbfloppy` を試み、次に `mount /dev/sdb /mnt/usbfloppy` を試みて、これが成功しました。

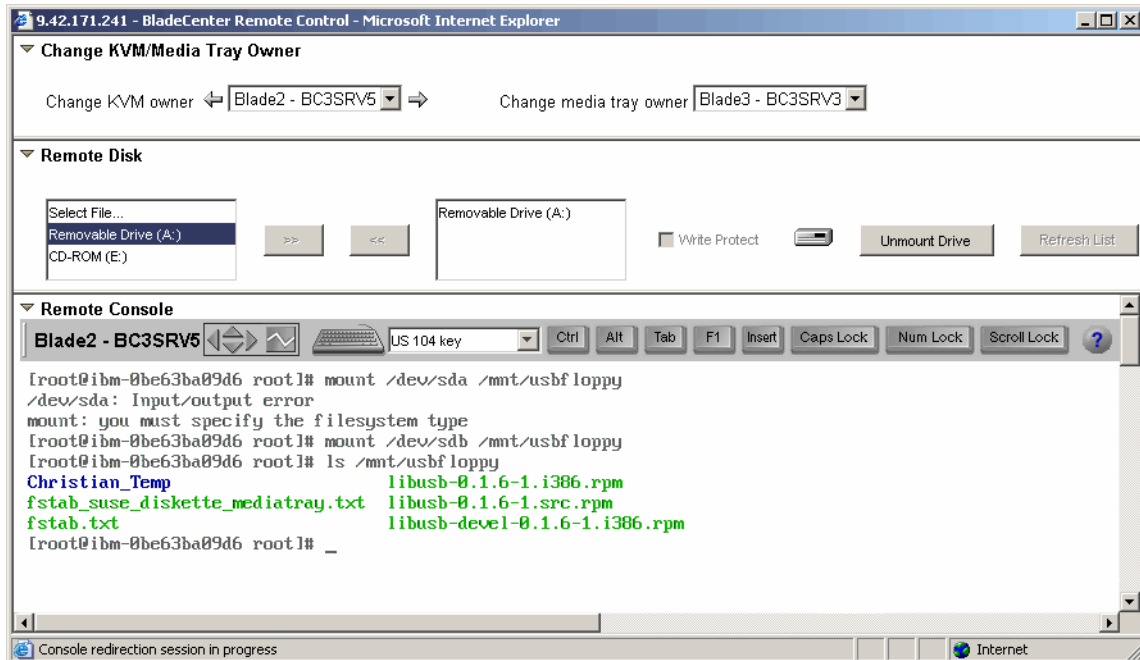


図 4-19 Red Hat Linux でのリモート・ディスクの使用

デバイスをアンマウントするには、リモート・メディア Web インターフェースを立ち上げ、114 ページの ステップ 6 以降のステップを実行します。

#### 4.4.4 リモート CD-ROM および DVD

リモート CD-ROM の機能は、リモート・ディスクに非常によく似ています。唯一の相違点は、管理モジュールは CD-ROM の内容をメモリーにロードしないことです。リモート CD-ROM からブート可能であり、オペレーティング・システムでそれをドライブ名として使用できます。マウントは、リモート・メディア Web インターフェイスがオープンしている間のみアクティブです。インターフェイスをクローズすると、メディアは自動的にアンマウントされます。リモート CD-ROM は、DVD ドライブおよびメディアと一緒に使用することもできます。

リモート CD-ROM を使用するには、次の手順を実行します。

1. 「**CD-ROM({driveletter}:)**」を選択して、「>>」をクリックします。
2. 「Mount Drive」をクリックすると、CD-ROM をリモート・サーバーにマウントするプロセスが開始します。しばらくすると、リモート CD-ROM がオペレーティング・システムで使用可能になります。

#### Windows 固有のステップ

Windows では、リモート CD-ROM は、オペレーティング・システム内にドライブ名として表示されます。次の図では、ドライブ E: として表示されています。

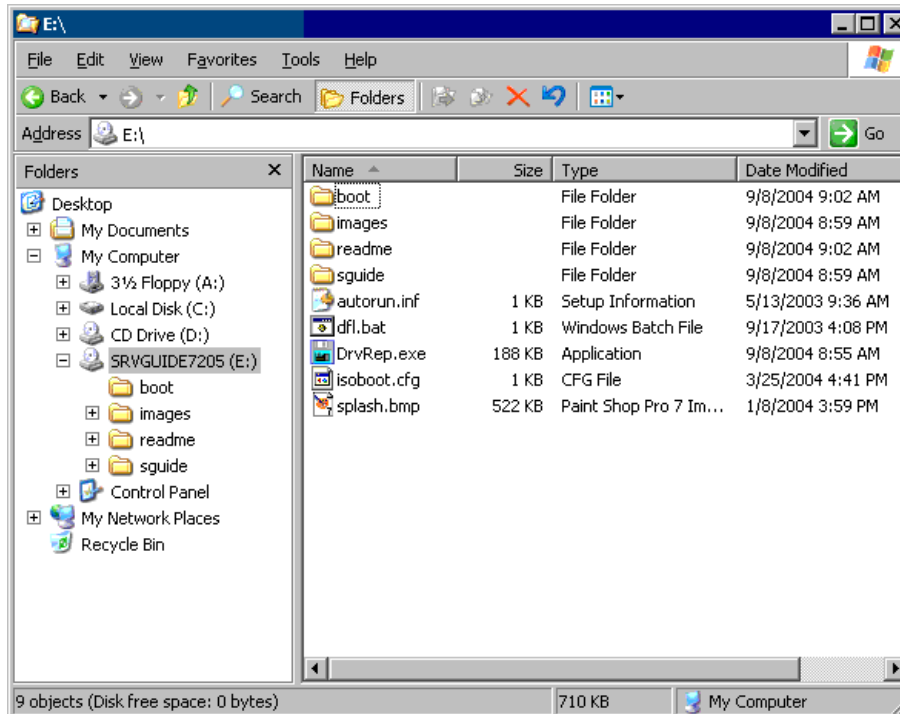


図 4-20 BladeCenter - リモート Windows 上のリモート CD-ROM

アンマウントするには、リモート・メディア Web インターフェースを立ち上げて、114 ページの ステップ 6 に従います。

## Linux 固有のステップ

Linux オペレーティング・システムでは、リモート・メディアは自動的にマウントされません。ユーザーがマウントする必要があります。リモート CD-ROM は、SUSE および Red Hat のファイル `/etc/fstab` に表示されます。

### SUSE LINUX

「Mount Drive」 ボタンをクリックする前と後に、オペレーティング・システムの `/etc/fstab` を検査して、`/etc/fstab` に新規に追加されたデバイスを調べます。新規の「HOTPLUG」デバイスが見つかります。

図 4-21 には、デバイス `/dev/sr2` が表示されており、この場合、これがリモート CD-ROM です。下の図に示されているマウント・コマンドを例として使用してください。

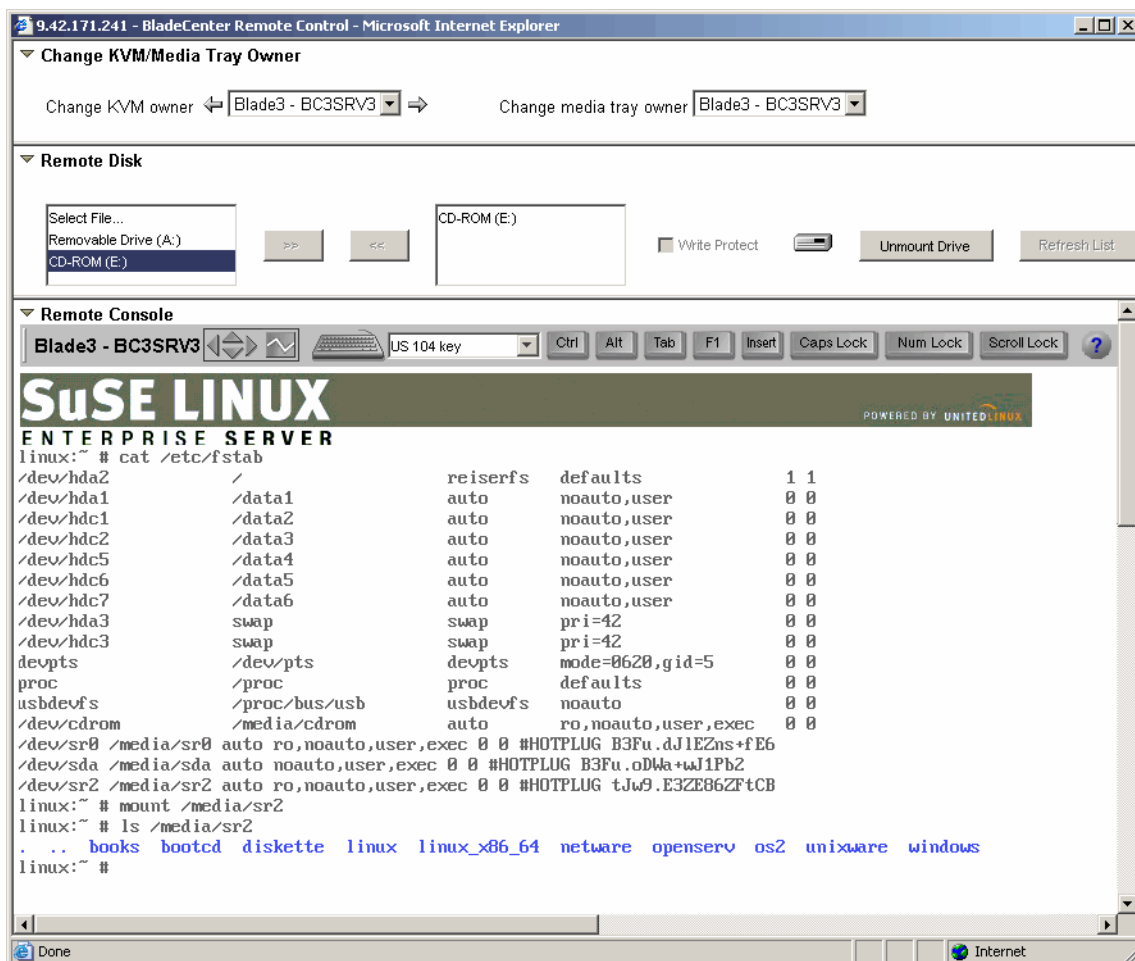


図 4-21 SUSE LINUX でのリモート CD-ROM

リモート・ディスクの使用後に、リモート・メディアをアンマウントしてください。これを行うには、リモート・メディア Web インターフェースを立ち上げて、114 ページの ステップ 6 に従います。

### Red Hat

Red Hat Linux でも、リモート CD-ROM はファイル /etc/fstab に表示されます。「Mount Drive」ボタンをクリックする前と後に、ファイルを検査します。見つかった新しいデバイスが、リモート CD-ROM です。以下は、/etc/fstab の例です。



LABEL=/	/	ext3	defaults	1 1
LABEL=/boot	/boot	ext3	defaults	1 2
none	/dev/pts	devpts	gid=5,mode=620	0 0
none	/proc	proc	defaults	0 0
none	/dev/shm	tmpfs	defaults	0 0
/dev/hda3	swap	swap	defaults	0 0
<b>/dev/cdrom</b>	<b>/mnt/cdrom</b>	udf,iso9660	noauto,owner,kudzu,ro	0 0
/dev/cdrom1	/mnt/cdrom1	udf,iso9660	noauto,owner,kudzu,ro	0 0
/dev/sda	/mnt/floppy	auto	noauto,owner,kudzu	0 0

図 4-22 Red Hat Linux - ファイル/etc/fstab とリモート・ドライブ

ブレード・サーバーは、「Mount Drive」ボタンをクリックした後にメディア・トレイの所有者になりました。この理由から、リモート CD-ROM はデバイス /dev/cdrom であって、/dev/cdrom1 ではないこととなります。

ご使用のオペレーティング・システムにドライブをマウントします。

```
mount /mnt/cdrom
```

アンマウントするには、114 ページの ステップ 6 以降のステップに従います。

#### 4.4.5 リモート・ファイル

リモート・ファイル機能を使用すると、ディスクおよび CD-ROM イメージを、マウントするドライブとして使用できます。

ISO イメージをインターネットからダウンロードした場合、CD-ROM を作成する必要はありません。直接それをリモート・メディアとして使用できます。

ヒント: IsoBuster (<http://www.smart-projects.net/isobuster/>) や Magic ISO maker (<http://www.magiciso.com/>) などのツールを使用して、ISO イメージを作成できます。1.44 MB を超えないファイル・セットがある場合は、どちらかのツールを使用して、代わりにディスク・ディスク・イメージを作成することもできます。

ファイルをマウントするには、次のようにします。

1. 「Select File」を選択して、
2. 「>>」をクリックします。

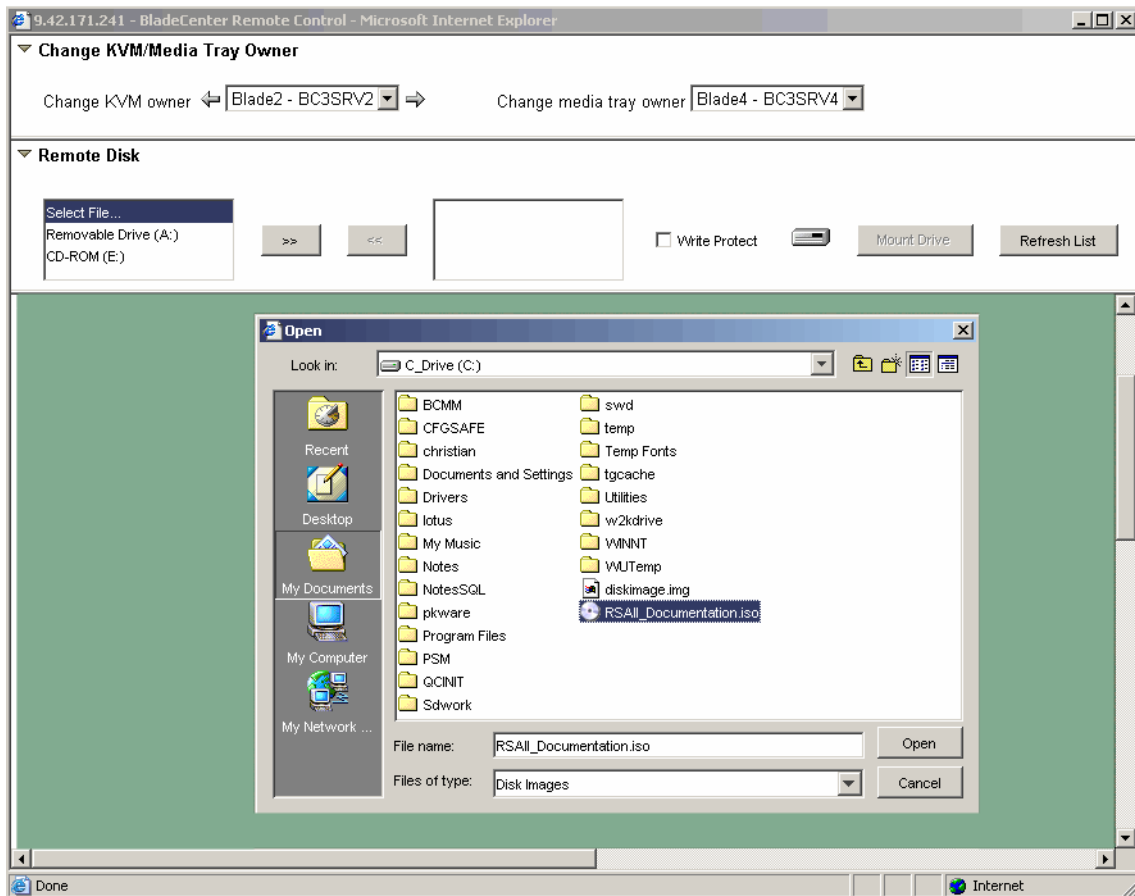


図 4-23 BladeCenter 管理モジュール - リモート・ファイル

3. 使用するディスク・イメージ・ファイルを選択して、「**Open**」をクリックします。
4. ディスケット・イメージの場合（つまり、ISO ファイルでない場合）、図 4-24 のようなプロンプトが表示されます。

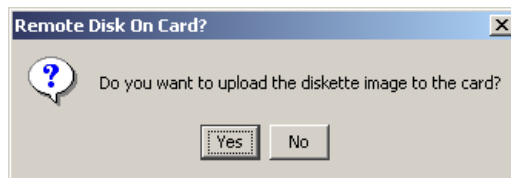


図 4-24 BladeCenter - リモート・ファイルのアップロード

「Yes」をクリックすると、ファイルは BladeCenter 管理モジュールの RAM にアップロードされます。イメージをアップロードするには、イメージの大きさが 1.44 MB を超えないことが必要です。ネットワーク接続によっては、アップロードに少し時間がかかることがあります。進行状況表示バーが表示されます。

**ヒント:** ユーザーが「Unmount」ボタンを使用してアンマウントするか、管理モジュールが再始動されるか、またはファームウェアが更新されるまで、イメージは RAM に残り、KVM の所有者であるブレード・サーバーに対してアクセス可能のままです。KVM の所有者を変更した場合、新規の所有者もリモート・ディスク・イメージを使用できます。

「No」をクリックした場合は、さらに「Mount Drive」をクリックして、リモート・サーバーにドライブをマウントする必要があります。ファイルはアップロードされておらず、ご使用のローカル PC からネットワーク経由でリモート・アクセスします。このリモート・ファイルからの後続のファイル・アクセスは、ネットワーク速度になります。リモート・コンソール・ウィンドウをクローズすると、リモート・ファイルは自動的にアンマウントされます。

5. ISO イメージを持っている場合は、「Mount Drive」ボタンをクリックします。

## Windows 固有のステップ

これで、イメージ・ファイルは Windows オペレーティング・システム内でドライブとして使用可能です。Windows Explorer で新規ドライブを確認してください。

アンマウントするには、リモート・メディア Web インターフェースを立ち上げ、114 ページの ステップ 6 以降のステップを実行します。

## Linux 固有のステップ

ISO イメージ・ファイルも使用できる点を除いて、リモート・ファイル機能はリモート・ディスク機能と同様の働きをします。

### SUSE LINUX

「Mount Drive」ボタンをクリックする前と後に /etc/fstab ファイルを検査して、どれが新しいデバイスであるかを調べます。126 ページの図 4-25 では、ISO イメージはデバイス /dev/sr1 です。

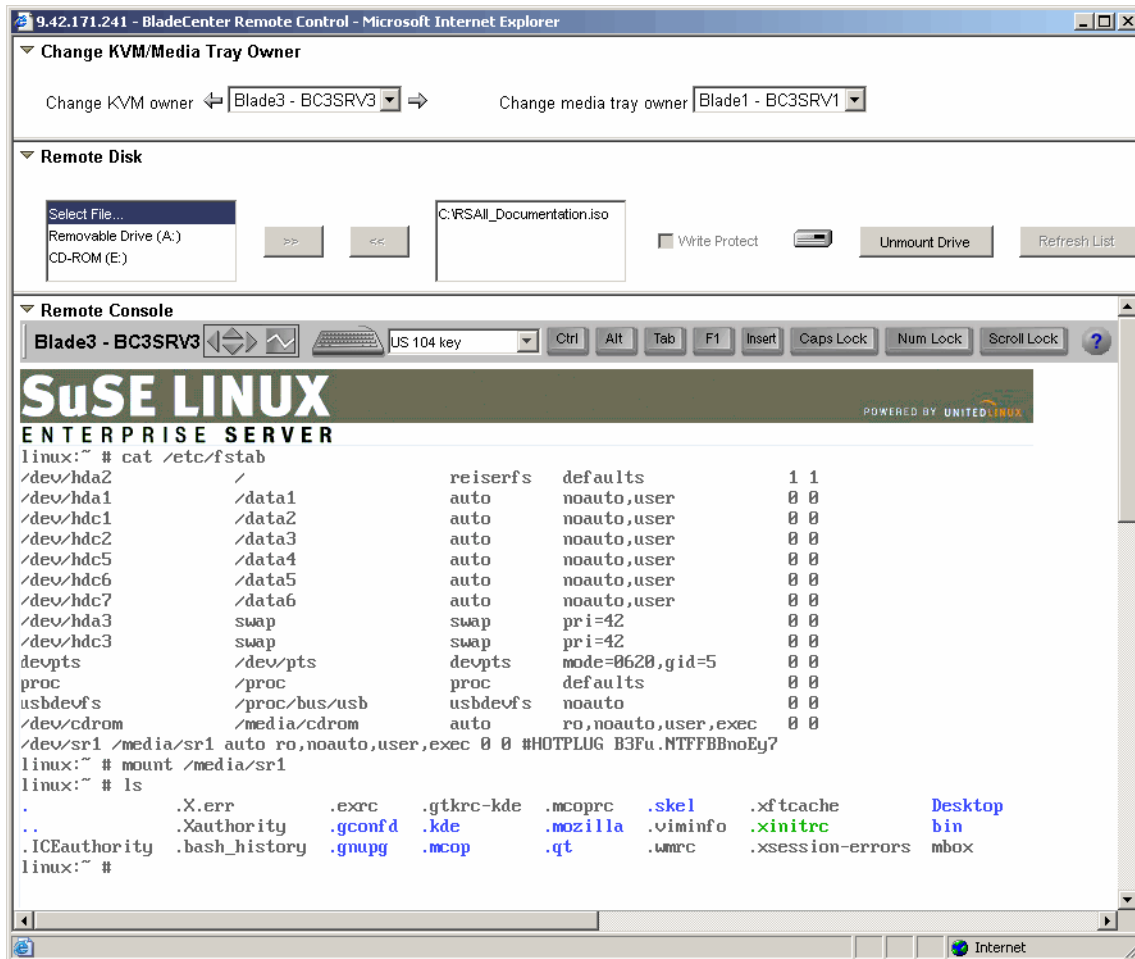


図 4-25 SUSE LINUX でのリモート・ファイル

アンマウントするには、114 ページの ステップ 6 以降のステップに従います。

### Red Hat

Red Hat Linux を使用している場合、リモート・ファイルはファイル /etc/fstab に記述されません。そのため、ユーザーはリモート・デバイスへの接続に成功するまで、sda、sdb、sdc などを試みる必要があります。

127 ページの図 4-26 では、ISO イメージ・ファイルをマウントするための 2 番目の試みが成功しました。

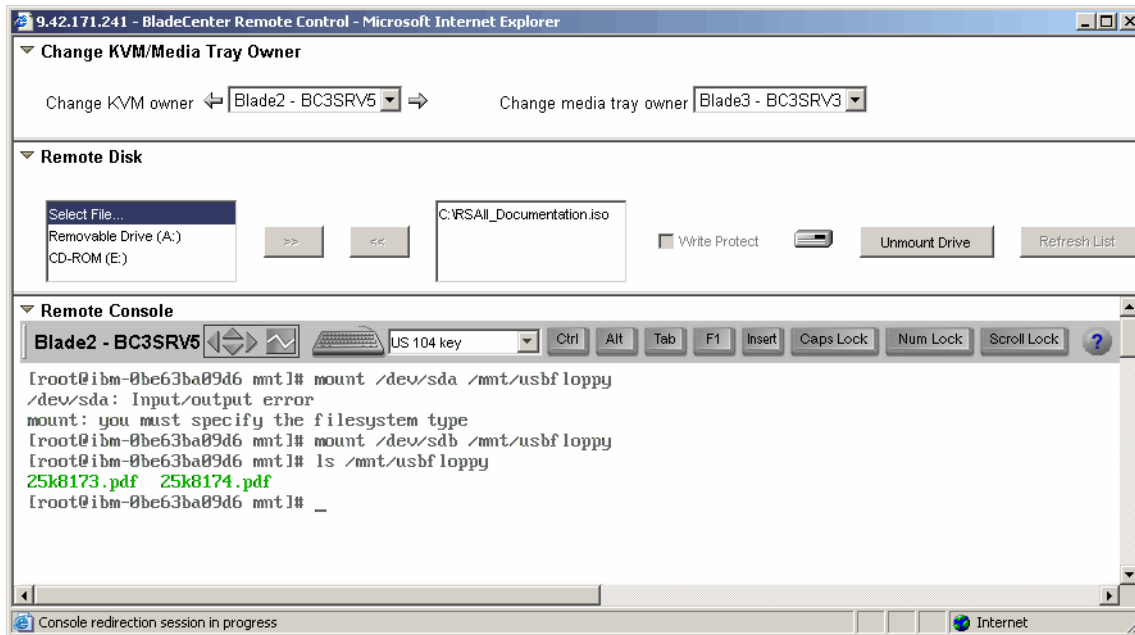


図 4-26 Red Hat でのリモート・ファイル (ISO イメージ)

アンマウントするには、リモート・メディア Web インターフェースを立ち上げ、114 ページの ステップ 6 以降のステップを実行します。

## 4.5 ブレード固有の機能の基本構成

以下では、最も一般的なブレード・サーバー固有の機能について簡単に説明します。構成の詳細な説明は、次の製品資料を参照してください (<http://www.pc.ibm.com/support> から入手できます)。

- ▶ *BladeCenter 管理モジュール インストール・ガイド*
- ▶ *BladeCenter 管理モジュール ユーザーズ・ガイド*

### 4.5.1 デバイス・ドライバー

BMC サービス・プロセッサ (HS20 8843 など) を搭載したブレード・サーバーは、IPMI ドライバーが必要です。

- ▶ IPMI デバイス・ドライバー
- ▶ IPMI マッピング・レイヤー・(ライブラリー) ファイル
- ▶ IPMI ASR サービス

詳しくは、42 ページの 2.3.9、『BMC デバイス・ドライバーのインストール』を参照してください。

## 4.5.2 ブレード・タスク

このセクションの各見出しは、ナビゲーション・フレームの「Blade Tasks」メニューのサブメニューです。「**Blade Tasks**」をクリックしてメニューを展開し、実行するタスクをクリックします。

### On Demand

このパネルでは、インストール済みのスタンバイ・ブレード・サーバーを使用可能にできます。スタンバイ・サーバーは、「スタンバイ・キャパシティー・オンデマンド」オファリングの一部です。説明は、次のサイトを参照してください。

[http://www.ibm.com/servers/eserver/bladecenter/scod/more\\_info.html](http://www.ibm.com/servers/eserver/bladecenter/scod/more_info.html)

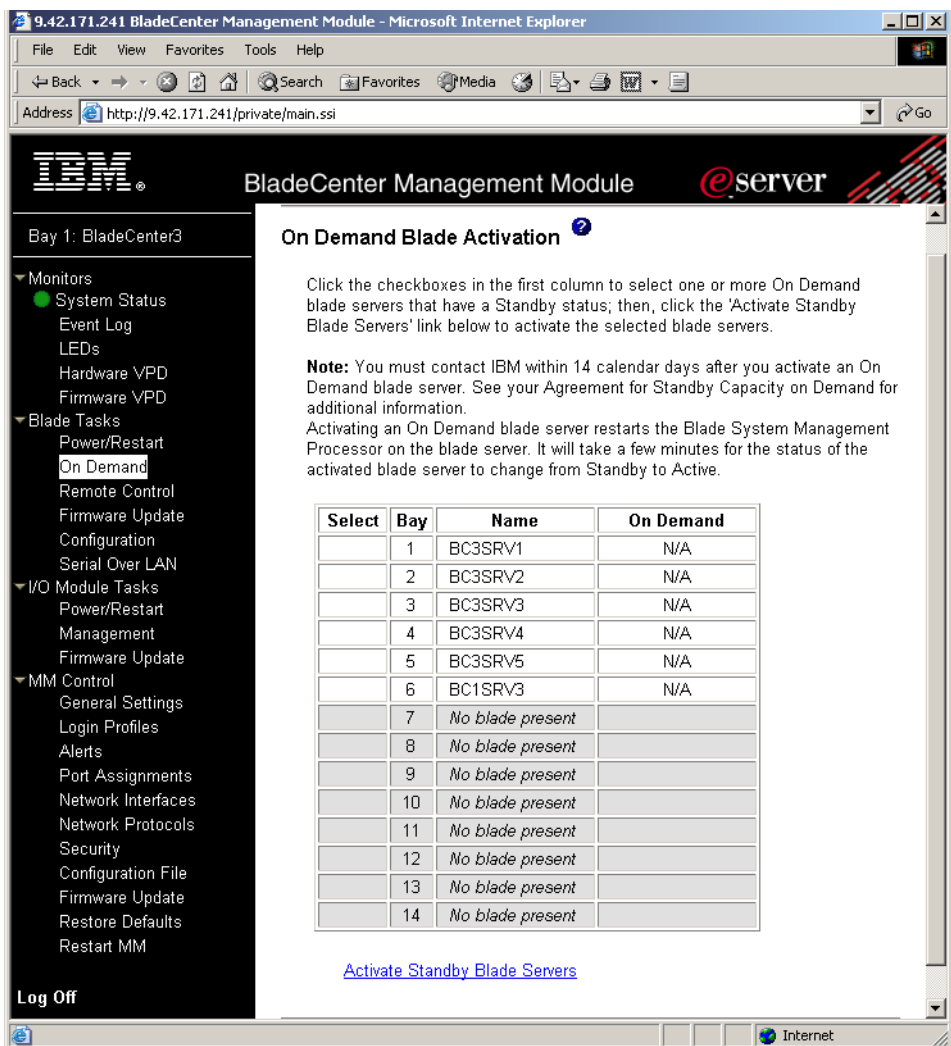


図 4-27 オンデマンド・ブレード・サーバー

本書の例では、活動化するオンデマンド・ブレードはありません。

このページの表は、各ブレード・サーバーに関する情報を表示し、オンデマンド・ブレード・サーバーの状況（アクティブまたはスタンバイ）を示しています。すべてのスタンバイ・サーバーの横にチェック・ボックスが表示され、それにチェック・マークを付けてアクティブにします。

## Firmware update

このパネルは、特定のブレードのファームウェア・コンポーネントを更新するために使用します。現在のところ、このページでファームウェアを更新できる唯一のコンポーネントは、ブレード・サーバーのオンボード・システム管理プロセッサです。最初に、IBM Support Web サイト <http://www.pc.ibm.com/support> から、最新のファームウェア・ファイルをダウンロードする必要があります。次に、「Target」プルダウンを使用してターゲット・ブレードを選択し、次のステップを実行します。

1. 「**Browse**」をクリックします。ご使用のコンピューターのファイル・システム内で、ファームウェア・ファイルを見つけます。
2. 必要なファイルをクリックして、「**Open**」をクリックします。ファイル（絶対パスを含む）が「Browse」ボタンの横のボックスに表示されるはずですが。
3. 更新プロセスを開始するために、「**Update**」をクリックします。ファイルが管理モジュールの一時ストレージに転送されている間、進行標識が表示されます。転送が完了するまで、このページのままです。ファイルの転送が完了すると、確認ページが表示されます。
4. 「Confirm Firmware Update」ページに表示されたファイルのタイプが、更新する予定のファイルであることを確認します。そうでない場合は、「**Cancel**」をクリックします。
5. 更新プロセスを完了させるために、「**Continue**」をクリックします。ファームウェア更新の進行中、進行標識が表示されます。プロセスが完了するまで、このページのままです。完了した時点で、状況ページが表示され、更新が成功したかどうかを示します。必要な場合は、追加の指示がこのページに表示されます。

## Configuration

このページでは、ブレード・サーバーの一部の構成パラメーターを表示または変更できます。

### Blade information

「Blade information」ペインには、シャーシ内のすべてのブレードについて、ユーザーが構成した名前をリストした表が表示されます。表は、ブレード・ベイごとに 1 行を表示します。空のベイは、空としてのマークが付けられます。ブレードが複数のベイを占める場合も、そのことが表示されます。

ブレード名は、この画面で変更できます。ブレードの名前を設定するには、対応するテキスト・ボックスに希望の名前を入力します。最大 15 文字の英数字を入力できます。「**Save**」をクリックして、変更を保管します。



**ヒント:** ブレード名の更新は、有効になるまでに少し時間がかかることがあります。名前の変更がすぐに画面に反映されない場合は、しばらく待ってから、画面を最新表示してください。

### **Blade policy settings**

このセクションでは、ローカル制御および Wake on LAN のグローバル・ポリシー設定を構成できます。ローカル電源制御、ローカル KVM 制御、ローカル・メディア制御、および Wake on LAN (WOL) の設定が、空のベイも含めて、すべてのブレード・ベイに適用されます。

**ヒント:** 個別のブレード・サーバーのポリシー設定値を設定するには、管理モジュールのコマンド・ライン・インターフェースを使用します。詳しくは、「*BladeCenter and BladeCenter T Management Module Command-Line Interface Reference Guide*」を参照してください。

ローカル電源制御が「Enabled」に設定されている場合、すべてのベイの電源ボタンが使用可能です。「Disabled」に設定されている場合、すべてのベイの電源ボタンが使用不可です。「Not set」の値は、グローバル・ポリシーが設定されていないことを示します（一部のベイの電源ボタンは使用可能であり、他のベイでは使用不可ということがあります）。

**ヒント:** ローカル電源制御を使用不可に設定するのは、インストール・プロセス中、または BladeCenter が安全な区域に設置されていない場合に限る必要があります。ローカル電源制御を永続的に使用不可に設定した場合、ブレード・サーバーの電源オン/オフを行う唯一の方法は、管理モジュールの Web インターフェースまたはコマンド・ライン・インターフェースを使用する方法だけになります。

ローカル KVM 制御は、ローカル電源制御と同様の働きをします。「Enabled」に設定されている場合、すべてのベイの「KVM Select」ボタンが使用可能です。「Disabled」に設定されている場合、すべてのベイの「KVM Select」ボタンが使用不可です。「Not set」の値は、グローバル・ポリシーが設定されていないことを示します（一部のベイの「KVM Select」ボタンは使用可能であり、他のベイでは使用不可ということがあります）。

「local media tray control」セクションでは、ブレード・サーバーのメディア・トレイ（ディスク、CD-ROM/DVD-ROM、USB）へのアクセスを制御できます。

このフィールドは、すべてのブレード・ベイのローカル・メディア・トレイ切り替えのグローバル・ポリシー設定を表示します。「Enabled」に設定されている場合、すべてのベイの「Media Tray Select」ボタンが使用可能です。

「Disabled」に設定されている場合、すべてのベイの「Media Tray Select」ボタンが使用不可です。「Not set」の値は、グローバル・ポリシーが設定されていないことを示します（一部のベイの「Media Tray Select」ボタンは使用可能であり、他のベイでは使用不可ということがあります）。

Wake on LAN (WOL) が「Enabled」に設定されている場合、すべてのベイの WOL が使用可能です。「Disabled」に設定されている場合、すべてのベイの WOL が使用不可です。「Not set」の値は、グローバル・ポリシーが設定されていないことを示します（一部のベイの Wake on LAN<sup>®</sup> は使用可能であり、他のベイでは使用不可ということがあります）。Wake on LAN のデフォルト BIOS 設定は、すべてのブレードで使用可能であることに注意してください。

### **Boot sequence**

このセクションでは、シャーシ内のすべてのブレードのブート・シーケンス設定を表示または変更できます。表は、ブレード・ベイごとに 1 行を表示します。空のベイは、空としてのマークが付けられます。複数のベイを使用するブレードも、複数使用することが示されます。ブレードのブート・シーケンス設定を変更するには、ブレード名のリンクをクリックします。これにより、別の画面に進み、そこで設定を変更して保管することができます。

### **Serial over LAN (SOL)**

SOL は、ブレード・サーバーのテキスト・コンソール・プロンプトを提供します。この機能は特に、ビデオ・アダプターを装備していないブレード・サーバー JS20 で使用されます。SOL は、BladeCenter 管理モジュールのコマンド・ライン・インターフェースの内部で開始されます。

詳しい情報、サポートされるハードウェア、および SOL に関する詳細は、次の資料を参照してください。

- ▶ *BladeCenter and BladeCenter T Management Module Command-Line Interface Reference Guide*
- ▶ *BladeCenter and BladeCenter T Serial over LAN Setup Guide*

## **4.5.3 入出力モジュール・タスク**

入出力モジュール・タスクにアクセスするには、ナビゲーション・フレームで「I/O Module Tasks」をクリックしてメニューを展開し、サブメニューの 1 つをクリックします。

### **Power/restart**

ここでは、モジュール・ベイ 1 から 4 に取り付けられたモジュールの電源オン/オフを行うことができます。2 番目の機能は、モジュールを再始動して、標準診断、拡張診断、または完全診断を実行します。

**注意:** モジュールの電源オフまたは再始動を行う前に、モジュール上でデータ転送が行われていないことを確認してください。リダンダント・モジュールがある場合は、リダンダント・モジュールが作動していることを確認してください。

スイッチ・モジュール・ベイ 1 から 4 の位置は、133 ページの図 4-28 を参照してください。

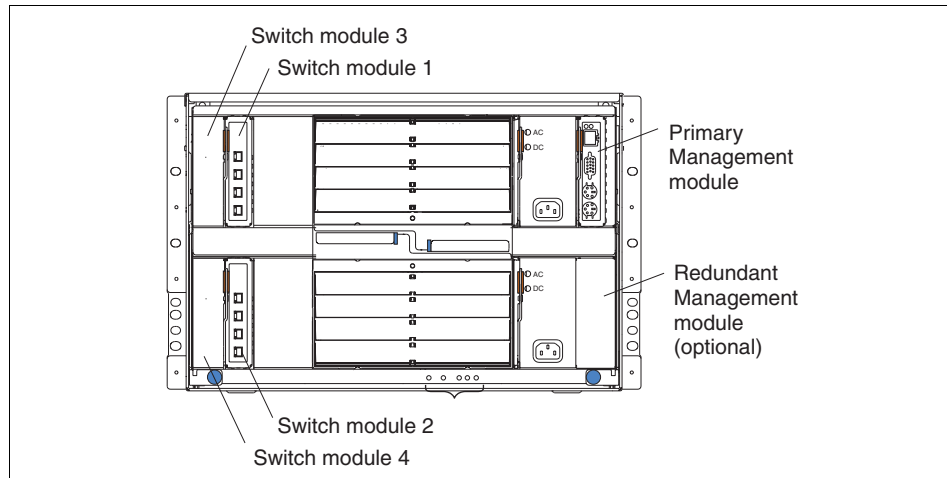


図 4-28 BladeCenter モジュール・ベイ

モジュールの電源オン、電源オフ、または再始動を行うには、対応するモジュールの下のボックスにチェック・マークを付けて（複数のボックスにチェック・マークを付けることができます）、開始するアクション（例えば、「Restart Module (s)」や「Run Standard Diagnostics」）をクリックします。

## Management

このページでは、シャーシ内のスイッチ・モジュールの基本 IP 構成パラメータを表示および変更できます。各スイッチ・モジュールの拡張構成の場合は、該当するモジュール・ベイ・ペインで「**Advanced Management**」をクリックします。

### Advanced Management

「Advanced Management」では、拡張パラメータの構成、最後の POST 結果の表示、モジュールの ping、あるいは telnet または Web ブラウザー・セッションの開始などのタスクを実行できます。モジュールが IP によってアクセス可能かどうかを検査するには、「**Ping Switch Module**」をクリックします。問題がある

場合は、ネットワーク管理者に連絡し、255 ページの 7.3、『すべての BladeCenter モジュールへのリモート・アクセスの提供』を参照してください。

スイッチ・モジュールがアクセス可能な場合は、「**Start Telnet Session**」または「**Start Web Session**」をクリックして、アクセスできます。

Web インターフェースを立ち上げた場合は、標準ログインを使用してログインします。これで、スイッチ・モジュールの構成と管理ができるようになります。最初のステップとして、スイッチ・モジュールのファームウェアを最新バージョンに更新します。

詳細については、スイッチ・モジュールに同梱されている資料を参照してください。

**ヒント:** イーサネット・スイッチ・モジュール (ESM) を取り付けた場合は、ESM の外部イーサネット・ポートを使用可能にしたことを確認してください。このポートは、初期時には使用不可になっています。「**Configuration**」→「**Port settings**」→「**Configure Ports**」をクリックして、ポートを使用可能にし、「**Apply**」をクリックします。

## Firmware update

このパネルは、特定の入出力モジュールのファームウェア・コンポーネントを更新するために使用します。最初に、IBM Support Web サイトから、最新のファームウェア・ファイルをダウンロードする必要があります。次に、「**Target**」プルダウンを使用してターゲット・モジュールを選択し、プロンプトで指示された手順を実行します。

**ヒント:** 「**Target**」プルダウンには、管理モジュール Web GUI 経由でのフラッシュをサポートする入出力モジュールのみがリストされる点に注意してください。「**Target**」プルダウンでは選択できないモジュールを更新する場合は、『**Management**』（133 ページ）を参照して、該当するモジュール自体の Web インターフェースにアクセスしてファームウェアを更新する方法について確認してください。

## 4.6 管理モジュールによって使用されるポート

管理モジュールは、通信用にいくつかの TCP/UDP ポートを使用します。管理モジュールとの通信がファイアウォールを通過する場合、管理モジュールとの通信のためにファイアウォール上のどのポートを使用可能にする必要があるかを知っていることが重要です。

表 4-2 は、ユーザーが構成できる管理モジュールのポートをリストしています。管理モジュールのポートを変更する場合は、ファイアウォール内のポートも変更する必要があることを覚えておいてください。

表4-2 ユーザーが構成できる管理モジュールのポート

ポート名	デフォルトのポート番号	説明
http	80	Web サーバー HTTP 接続 - TCP
https	443	SSL 接続 - TCP
telnet	23	Telnet コマンド・ライン・インターフェース接続 - TCP
SSH	22	セキュア・シェル (SSH) コマンド・ライン・インターフェース - TCP
SNMP エージェント	161	SNMP get/set コマンド - UDP
SNMP トラップ	162	SNMP トラップ - UDP

以下のポートは固定で、変更できません。

表4-3 固定の管理モジュールのポート

固定ポート番号	説明
25	E メール・アラート - TCP
53	UDP ドメイン・ネーム・サーバー (DNS) リゾルバー - UDP
68	DHCP クライアント接続 - UDP
427	Service Location Protocol (SLP) 接続 - UDP
1044	リモート・ディスク機能 - TCP
1045	永続リモート・ディスク (カード上のディスク) - TCP
5900	リモート・コンソール - TCP
6090	IBM Director コマンド - TCP
13991	IBM Director アラート - UDP

## 4.7 管理モジュールの出荷時のデフォルト値へのリセット

BladeCenter 管理モジュールにはリセット・ボタンが装備されており、これを使用してモジュールを出荷時のデフォルト値にリセットできます。このリセット・ボタンは、管理モジュールのコネクターの下の MAC アドレスの近くにありません。

真っすぐに伸ばした用紙クリップまたは類似の物を使用して、操作します。リセット・ボタンには、2つの用途があります。


- ▶ ネットワーク構成をリセットする。リセット・ボタンを押して、3秒以下の時間押し続けます。
- ▶ 管理モジュール全体（ユーザー ID とパスワードを含む）を出荷時のデフォルト値にリセットする。これは、押して放す一連の操作が必要です。
  - a. リセット・ボタンを押して、5秒間押し続けます。
  - b. ボタンを放して5秒間待ちます。
  - c. ボタンを押して、さらに10秒間押し続けます。

正常に操作するためには、この手順をできるだけ正確に行う必要があることに注意してください。5秒間押し、5秒間放し、10秒間押しします。この方法で完全に出荷時のデフォルト値にリセットした後は、デフォルトのユーザー ID とパスワードが有効になります。つまり、USERID（すべて大文字）と PASSWORD（ゼロ、文字の O ではなく）です。

ネットワーク構成をリセットした後で、Web インターフェースにアクセスして、再構成することができます。再構成するには、管理モジュールの IP アドレスを知っている必要があります。これは、次の方法で見つけることができます。

- ▶ 管理モジュールは、デフォルトで DHCP を使用します。ホスト名は MMxxxxxx です。ここで、xxxxxx は、管理モジュールの MAC アドレスです。この番号は、リセット・ボタンの下に記載されています。
- ▶ DHCP サーバーが見つからない場合、管理モジュールはデフォルトの IP アドレス 192.168.70.125 とサブネット・マスク 255.255.255.0 を使用します。ホスト名は MMxxxxxx です。

**注：**リセット・ボタンを使用してパスワードをリセットすることが可能であるため、BladeCenter シャーシを物理的に保護して、許可された人だけがリセット・ボタンに物理的にアクセスできるようにする必要があります。



## セキュリティーおよび認証

RSA II および BladeCenter 管理モジュールへのアクセスは、初期時にはデフォルト・ユーザー ID とパスワードの使用により保護されます。このパスワードを変更すると（または、デフォルトを使用不可にして、新規ユーザーを追加すると）、サービス・プロセッサは無許可アクセスから保護されます。

デフォルトでは、ユーザー ID とパスワードはデータ暗号化規格（DES）アルゴリズムを使用して暗号化され、プライベート・セッション・キーを使用して管理セッション全体のセキュリティーを維持します。ご使用のシステム管理環境の保護をさらに強化するための追加手段として、SSL 暗号化と LDAP を使用した認証があります。

この章では、以下の内容を説明します。

- ▶ 138 ページの 5.1、『SSL を使用したセキュリティー』では、SSL および SSH を使用するようにサービス・プロセッサを構成する方法について説明します。
- ▶ 148 ページの 5.2、『LDAP を使用した認証』では、LDAP をインプリメントして、すべてのサービス・プロセッサのユーザー ID とパスワードを集中管理する方法について説明します。

こうしたセキュリティー機能および認証機能は、Remote Supervisor Adapter II (EXA および SlimLine ファミリー・メンバーを含む) と BladeCenter 管理モジュールで使用可能です。Baseboard Management Controller (BMC) では利用できません。

## 5.1 SSL を使用したセキュリティー

RSA II または BladeCenter 管理モジュールとのセキュア通信に（特に、WAN 接続を使用する場合）、Secure Sockets Layer（SSL）または Secure Shell Server（SSH）を使用できます。

### 5.1.1 Secure Sockets Layer (SSL)

RSA II または BladeCenter 管理モジュールは、セキュア Web サーバー（HTTPS）の SSL サーバーとして機能することも、LDAP サーバー（Windows Active Directory Service（ADS）や Linux OpenLDAP など）のセキュア LDAP クライアント（LDAPS）として機能することもできます。

SSL 接続を提供するためには、SSL 証明書が必要です。自己署名証明書を使用するか、または第三者認証局によって署名された証明書を使用できます。

SSL を使用する最も簡単な方法は、自己署名証明書を使用することですが、セキュリティー上のリスクが多少伴います。リスクが生じる原因は、クライアントとサーバーの間で最初に接続を試みる際に、SSL クライアントには SSL サーバーの ID を確認する手段がないことにあります。第三者がサーバーの偽名を使用して、RSA II または管理モジュールと Web ブラウザー間で伝送されるデータを傍受する可能性があります。ブラウザーと RSA II または管理モジュール間の初回接続時に、自己署名証明書がブラウザーの証明書ストアにインポートされると、そのブラウザーでは将来の通信はすべてセキュアになります（初回接続時に攻撃による暗号漏えいがなかったことを前提として）。

より完全なセキュリティーを実現するには、認証局が署名する証明書を使用できます。署名された証明書を入手するには、「SSL Certificate Management」ページを使用して、証明書署名要求を生成します。次に、その証明書署名要求を認証局に送信して、証明書の購入の手配をする必要があります。

#### セキュア Web サーバーの構成

次のような汎用タスク・リストを使用して、RSA II または BladeCenter 管理モジュールのセキュア Web サーバーを構成します。

1. ブラウザーのウィンドウを開いて、RSA II Web インターフェースにアクセスします。
2. 「ASM Control」または「MM Control」→「Security」をクリックします。  
139 ページの図 5-1 が表示されます。



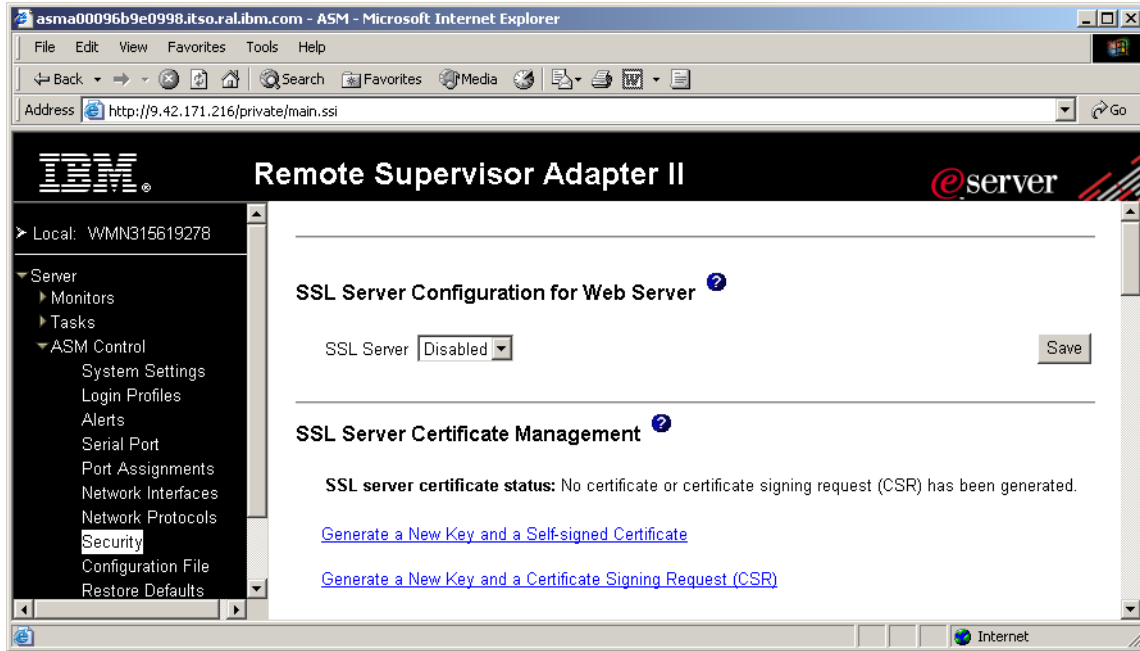


図 5-1 セキュア Web サーバーの構成

3. 「SSL server configuration for the Web server」に対して「**Disabled**」を選択します。
4. 「**Save**」をクリックします。
5. 証明書を生成またはインポートします。自己署名証明書を使用する場合は「**Generate a new key and a self-signed certificate**」をクリックし、第三者認証局の証明書を使用する場合は「**Generate a New Key and a Certificate Signing Request (CSR)**」をクリックします。

**注：**残りのステップでは、自己署名証明書のプロセスを説明します。第三者認証局によって署名された証明書の詳細については、「*Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide*」または「*BladeCenter Management Module User's Guide*」の第3章の『Secure Web server and secure LDAP』を参照してください。

6. 自己署名証明書のデータを入力します。

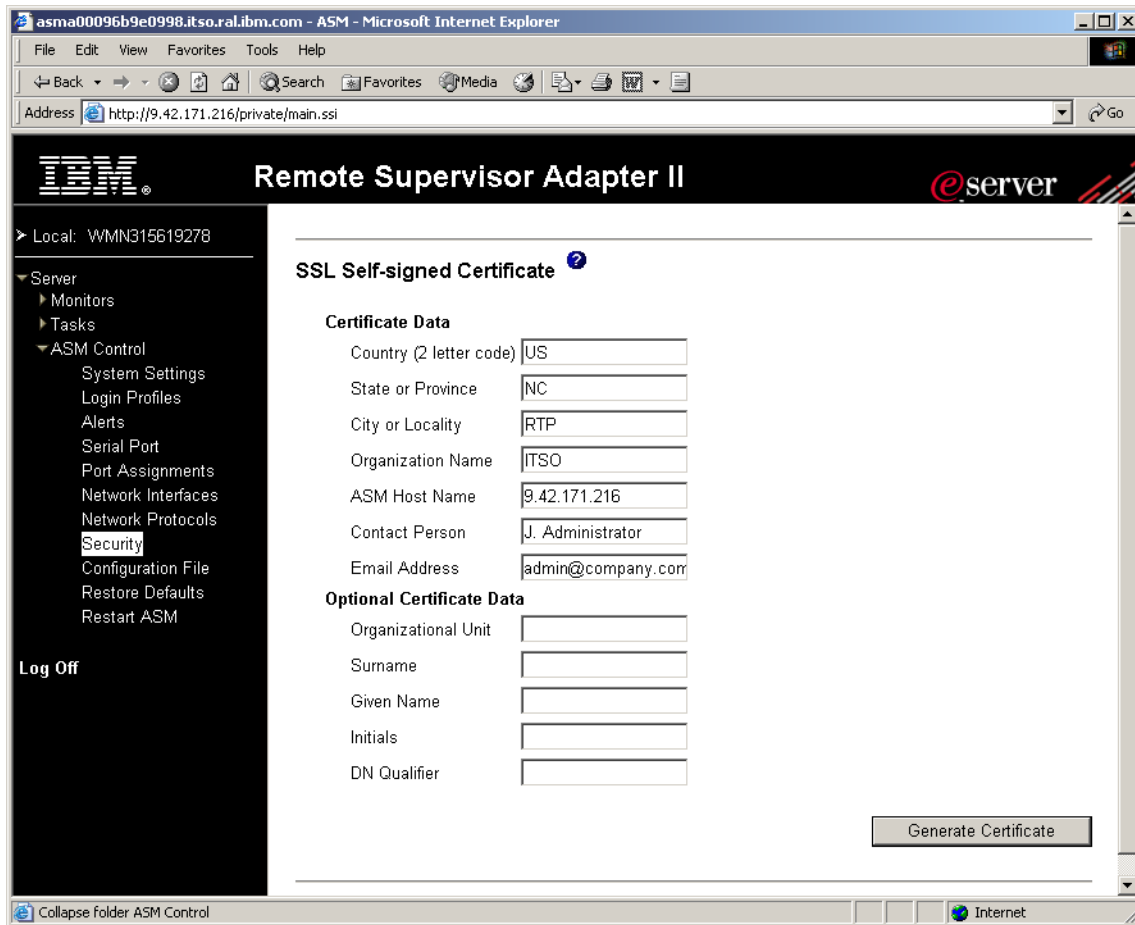


図 5-2 自己署名証明書

ASM または MM ホスト名フィールドに入力する値は、Web ブラウザーに認知されているホスト名と正確に一致させるように注意してください。ブラウザーは、解決された URL 内のホスト名と証明書に表示されている名前を比較します。

ブラウザーから証明書に関する警告が出されるのを防止するために、このフィールドに使用する値は、ブラウザーが ASM または管理モジュールに接続するのに使用するホスト名と一致している必要があります。

例えば、ブラウザーの URL アドレス・バーに現在 `http://mm11.example.com/private/main.ssi` と表示される場合、ASM または MM ホスト名のフィールドに使用する値は `mm11.example.com` となります。URL が `http://192.168.70.2/private/main.ssi` であれば、使用する値は `192.168.70.2` となります。

7. 「**Generate Certificate**」をクリックして、生成プロセスを開始します。
8. 生成プロセスが終了するまで待ちます。終了すると、SSL サーバー証明書の状況は、次のように変更されます。

A self-signed certificate is installed

9. 「SSL server configuration for the Web server」に対して「**Enabled**」を選択します。
10. 「**Save**」をクリックします。
11. RSA II を再始動するために、「**Restart ASM**」をクリックします。

RSA II Web インターフェースに再接続すると、セキュア接続が使用されます。最初にセキュリティー・アラートがポップアップ表示され、セキュア接続を使用することを通知します。「**OK**」をクリックした後、別のセキュリティー・アラートが表示されます (図 5-3)。



図 5-3 セキュリティー・アラート

このメッセージは、ユーザーは現在、証明書を信用していないことを示します。証明書を信用するには、ご使用のコンピューターに証明書をインストールする必要があります。コンピューターに証明書をインストールしない場合、RSA II の Web インターフェースを立ち上げるたびに、セキュリティー・アラートが表示されます。

コンピューターに証明書をインストールするには、次のようにします。

1. 「**View Certificate**」をクリックします。
2. 「**General**」タブで、「**Install Certificate**」をクリックします。
3. 「**Certificate Import Wizard**」が表示されます。

4. 「Next」 をクリックします。
5. 証明書を特定の場所に保管する場合は、「Place all certificates in the following store」を選択して、場所を指定します。そうでない場合は、「Automatically select the certificate store based on type of certificate」を選択します。
6. 「Next」 をクリックし、次に「Finish」 をクリックします。
7. 警告を読んでから「Yes」 をクリックして、証明書をインストールします。
8. 証明書ウィンドウ内の情報は更新されませんでした。インストールを確認するために、「OK」 をクリックします。次に、「View Certificate」 をクリックして、再度ウィンドウを開き、証明書情報を検討します。

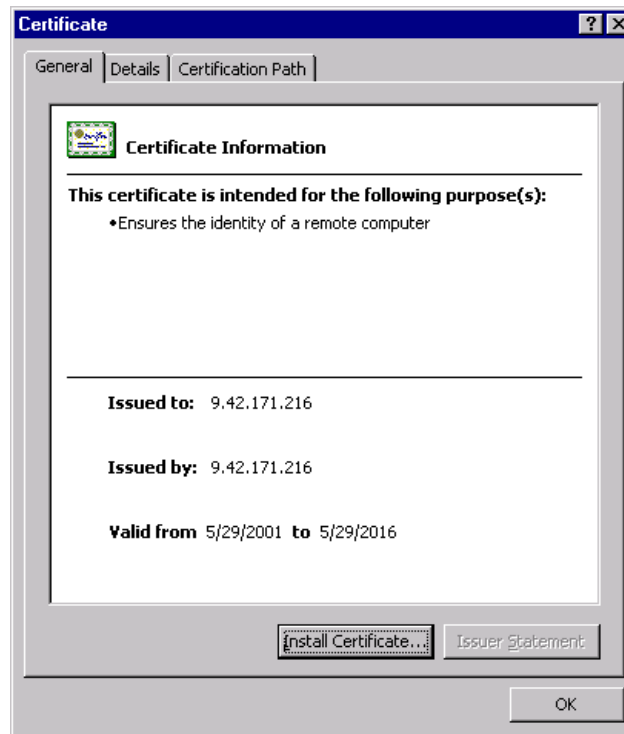


図 5-4 証明書情報

9. 「OK」 をクリックして、ウィンドウを閉じます。
10. 先に進むために、「Yes」 をクリックします。
11. ユーザーの証明書を使用してログオンします。
12. ブラウザーのアドレス・フィールドを検査してください。RSA II または管理モジュールとの通信は、HTTP ではなく HTTPS プロトコルを使用するようになっています。

次回に Web インターフェースを立ち上げたときには、証明書に関するセキュリティー・アラートは出なくなります。

## セキュア LDAP クライアントの構成

SSL 通信を使用して LDAP クライアントをセキュアにするには、最初に SSL クライアント証明書を取得する必要があります。生成プロセスは、立ち上げるリンクが異なるだけで、SSL サーバー証明書の場合と同じです。詳しくは、『セキュア Web サーバーの構成』（138 ページ）を参照してください。証明書を生成するには、次のようにします。

1. 「SSL client certificate management」セクションで、「**Generate a new key and a self-signed certificate**」をクリックします。
2. 自己署名証明書のデータを入力します。
3. 「**Generate Certificate**」をクリックして、生成プロセスを開始します。
4. 生成プロセスが終了するまで待ちます。終了すると、SSL クライアント証明書の状況は、次のように変更されます。

A self-signed certificate is installed

LDAP クライアントの構成について詳しくは、148 ページの 5.2、『LDAP を使用した認証』を参照してください。

### 5.1.2 セキュア・シェル (SSH)

セキュア・シェル (SSH) 機能は、コマンド・ライン・インターフェースと、RSA II および BladeCenter 管理モジュールのシリアル (テキスト・コンソール) リダイレクト機能へのセキュア・アクセスを提供します。

**注:** SSH は BladeCenter 管理モジュールでサポートされますが、RSA II を搭載したサーバーでは SSH 機能を利用できない場合があります。ご使用のサーバーの RSA II 用ファームウェア更新パッケージの README ファイルで確認してください。

セキュア・シェル (SSH) 機能は、コマンド・ライン・インターフェース、および管理モジュールのシリアル (テキスト・コンソール) リダイレクト機能へのセキュア・アクセスを提供します。

セキュア・シェルのユーザーは、ユーザー ID とパスワードを交換することにより認証されます。パスワードとユーザー ID は、暗号化チャネルが確立された後で送信されます。ユーザー ID とパスワードのペアは、ローカルに保管されている 12 個のユーザー ID とパスワードのいずれかを使用することもできますし、LDAP サーバーに保管することもできます。公開鍵認証はサポートされません。

セキュア・シェル・サーバー鍵は、クライアントに対してセキュア・シェル・サーバーの ID を認証するために使用されます。新規のセキュア・シェル・サーバー秘密鍵を作成する前は、セキュア・シェル・サーバーは使用不可にされている必要があります。サーバー鍵を作成した後で、セキュア・シェル・サーバーを使用可能にする必要があります。

新規のサーバー鍵を要求すると、Rivest、Shamir、および Adelman 鍵と DSA 鍵が作成されるため、SSH バージョン 1.5 または SSH バージョン 2 クライアントのいずれからでもリモート管理アダプター II にアクセスできます。セキュリティー上の理由から、セキュア・シェル・サーバー秘密鍵は、構成の保管および復元操作時にはバックアップされません。

SSH サーバーにアクセスするには SSH クライアントが必要です。SSH クライアントは、Linux に標準搭載されており、また以下で説明するように、サード・パーティー製品（PuTTY など）として入手することもできます。

新規のセキュア・シェル・サーバー鍵を作成するには、次のステップを実行します。

1. ブラウザーのウィンドウを開いて、サービス・プロセッサ Web インターフェイスにアクセスします。
2. 「ASM Control」または「MM Control」→「Security」をクリックします。  
図 5-5 が表示されます。

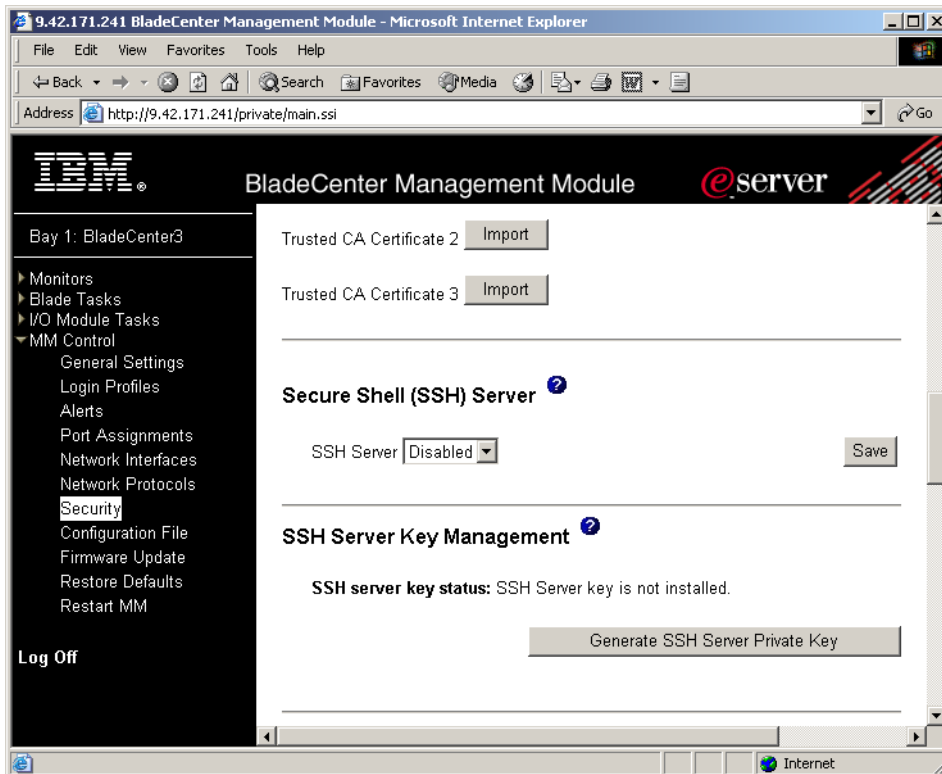


図 5-5 セキュア・シェル (SSH) サーバー - BladeCenter 管理モジュール

3. 「Secure Shell (SSH) Server」セクションまでスクロールして、セキュア・シェル・サーバーが使用不可になっていることを確認します。使用不可になっていない場合は、「SSH Server」フィールドで「**Disabled**」を選択して、「**Save**」をクリックします。
4. 「SSH Server Key Management」セクションまでスクロールします。「**Generate SSH Server Private Key**」をクリックします。
5. 次のウィンドウで「**OK**」をクリックして、続行します。
6. 進行状況を示すウィンドウが開きます。操作が完了するまでお待ちください。この操作は完了するまでに数分かかることがあります。

「Security」ページから、セキュア・シェル・サーバーを使用可能または使用不可にできます。行った選択は、管理モジュールを再始動した後で有効になります。画面に表示されている値 (Enabled または Disabled) は、最後に選択された値であり、サービス・プロセッサを再始動したときに使用される値です。

**ヒント:**セキュア・シェル・サーバーを使用可能にできるのは、有効なセキュア・シェル・サーバー・プライベート・キーがインストールされている場合に限られます。

次のステップを実行して、セキュア・シェル・サーバーを使用可能にします。

1. ナビゲーション・フレームで、「**Security**」をクリックします。
2. 「Secure Shell (SSH) Server」セクションまでスクロールします。
3. 「SSH Server」フィールドで「**Enabled**」をクリックして、「**Save**」をクリックします。
4. ナビゲーション・フレームで「**Restart ASM**」または「**Restart MM**」をクリックして、サービス・プロセッサを再始動します。

これで、SSH クライアントを使用して管理モジュールの CLI に接続できるようになりました。本書の例は、次のサイトから入手できるフリー・ツールの PuTTY を使用しました。

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

1. EXE ファイルを実行して、PuTTY を立ち上げます。
2. 初回には、セキュリティー・アラートがポップアップ表示されます。注意してお読みになり、続行する場合は「**Yes**」をクリックします。

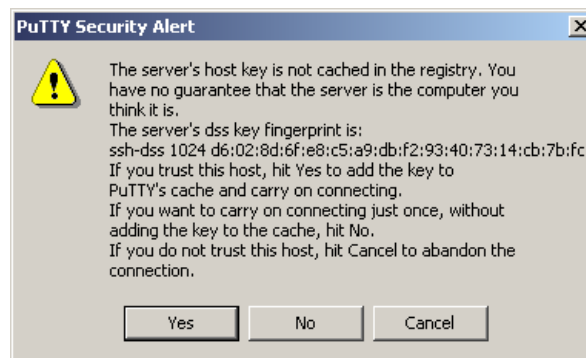


図 5-6 PuTTY セキュリティー・アラート

3. RSA II または管理モジュールにログオンします。

```
login as: USERID  
USERID@9.42.171.241's password:  
system>
```

これで、セキュア接続を通して CLI を使用できるようになりました。



RSA II を使用している場合、セキュア CLI のために SSH を使用可能にする場合には、非セキュアな Telnet インターフェースを使用不可にすることも必要です。

**制約事項：**本書の作成日現在では、Telnet プロトコルを使用不可にするオプションは、管理モジュールでは利用できませんでした。対処方法として、管理モジュールでは telnet を使用せず、Telnet プロトコルのポートを変更してください。

RSA II の Telnet インターフェースを使用不可にするには、次のステップを実行します。

1. ブラウザーのウィンドウを開いて、RSA II Web インターフェースにアクセスします。
2. 「ASM Control」 → 「Network Protocols」をクリックします。
3. 「Telnet Protocol」セクションまでスクロールし、「Telnet connection count」フィールドで「Disabled」を選択します。

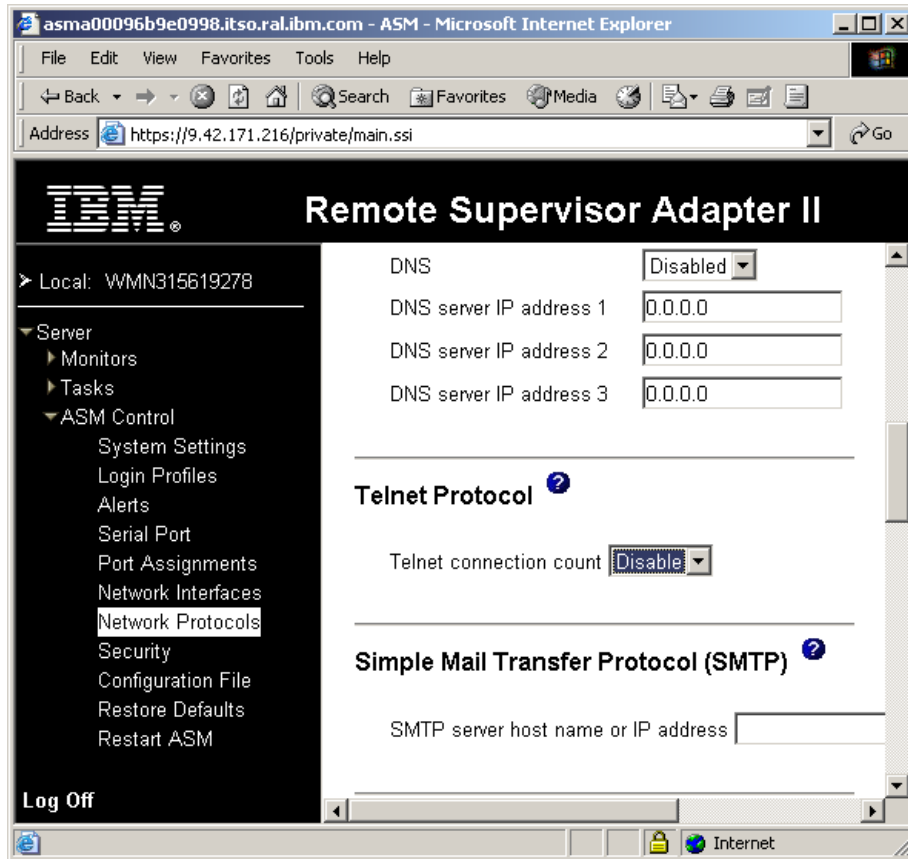


図 5-7 Telnet プロトコルの使用不可化

4. ページの下部までスクロールダウンして、「**Save**」をクリックします。
5. 注意書きを読み、「**OK**」をクリックします。
6. 「**ASM Control**」 → 「**Restart**」をクリックして、RSA II または管理モジュールを再始動します。
7. 「**Restart**」をクリックします。

## 5.2 LDAP を使用した認証

アカウント管理を最適化するために、各サービス・プロセッサ上のユーザーを別々に管理するのではなく、LDAP サーバーを使用して、すべての RSA II および管理モジュール・デバイスを一緒に認証することができます。

## 5.2.1 LDAP 認証属性

LDAP サーバーを使用した認証の場合、RSA II または管理モジュールを LDAP クライアントとして構成する必要があります。ユーザーの権限レベルを設定するために、LDAP サーバーで設定される属性が 1 つあります。この属性は、12 ビットで構成されます。ビットは、左から右に番号が付けられ、次のような意味を持っています。

▶ ビット 0 - Deny always

このビットが設定されると、ユーザーは常に認証に失敗します。この機能は、特定のユーザーまたは特定のグループに関連付けられたユーザーをブロックするために使用されます。

▶ ビット 1 - Supervisor access

このビットが設定されると、ユーザーに管理者特権が与えられます。ユーザーは、すべての機能に対して読み取りおよび書き込みアクセス権限を持ちます。このビットを設定した場合、他のビットを個別に設定する必要はありません。

▶ ビット 2 - Read only access

このビットが設定されると、ユーザーは読み取り専用アクセス権を持ちますが、保守手順（例えば、再始動、リモート操作、ファームウェア更新）は実行できず、変更操作（保管、消去、復元機能を使用）も行えません。読み取り専用のビットと他のすべてのビットは相互に排他的であり、読み取り専用は最下位の優先順位であることに注意してください。すなわち、他のいずれかのビットが設定されている場合、このビットは無視されます。

▶ ビット 3 - Networking and security

このビットが設定されると、ユーザーは Web インターフェースの「Security」、「Network Protocols」、「Network Interface」、「Port Assignments」、および「Serial Port」ページで構成を変更できます。

▶ ビット 4 - User account management

このビットが設定されると、ユーザーは Web インターフェースの「Login Profiles」ページで、ユーザーの追加、変更、削除を行うことができ、また「Global Login Settings」を変更できます。

▶ ビット 5 - Remote console access

このビットが設定されると、ユーザーはリモート・サーバーまたはリモート・ブレード・サーバー・コンソールにアクセスできます。

▶ ビット 6 - Remote console and remote media

このビットが設定されると、ユーザーはリモート・サーバー・コンソールおよびリモート（ブレード）サーバーのリモート・メディア機能にアクセスできます。

- ▶ ビット 7 - Remote power/Restart access  
このビットが設定されると、ユーザーはリモート・サーバーまたはブレード・サーバーおよび BladeCenter の入出力モジュールのパワーオンおよび再始動機能にアクセスできます。これらの機能は、Web インターフェースの「Power/Restart」ページで使用可能です。
- ▶ ビット 8 - Basic adapter configuration  
このビットが設定されると、ユーザーは Web インターフェースの「System Settings」および「Alerts」ページで、基本構成パラメーターを変更できます。
- ▶ ビット 9 - Ability to clear event logs  
このビットが設定されると、ユーザーはイベント・ログを消去できます。イベント・ログは誰でも表示できますが、ログを消去するにはこの許可が必要です。
- ▶ ビット 10 - Advanced adapter configuration  
このビットが設定されると、ユーザーはアダプターを構成する際の制限が何もありません。加えて、ユーザーはリモート管理アダプター II に対する管理アクセス権限を持ちます。これは、ユーザーが次のような拡張機能も実行できることを意味します。ファームウェア更新、PXE ネットワーク・ブート、アダプターの出荷時のデフォルト設定への復元、構成ファイルからのアダプター構成の変更と復元、およびアダプターの再始動とリセット。
- ▶ ビット 11 - 将来のために予約済み

以下に、この属性の表示例とその意味を示します。

010000000000 - Supervisor Access (ビット位置 1 が設定)  
 001000000000 - Read-Only Access (ビット位置 2 が設定)  
 100000000000 - No access (ビット位置 0 が設定)  
 000011111100 - Advanced Adapter Configuration を除くすべての権限  
 000011011110 - 仮想メディアへのアクセスを除くすべての権限

以下のセクションでは、属性を使用して、該当する権限をグループに割り当てます。

詳細については、「*Lightweight Directory Access Protocol User's Guide for IBM @server BladeCenter Management Module and IBM Remote Supervisor Adapters*」を参照してください。これは、次のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-55014.html>

## 5.2.2 LDAP サーバーの構成

本書の例では、Windows Server 2003 上の Active Directory を LDAP サーバーとして使用しました。3 つのグループを作成し、それに 4 名のユーザーを割り当てています。次の表に、詳細を示します。

表 5-1 例で使用したグループ、ユーザー、および権限

ドメイン	グループ	権限	ユーザー
ibm.com <sup>®</sup>	RSA_Supervisor	Supervisor access	Bain
			Leitenberger
	RSA_Basic	Network & Security	管理者
	RSA_ReadOnly	Read only access	Watts

ユーザーはドメインの管理権限を持っていること（例えば、「Domain Admins」または「Enterprise Admins」グループのメンバーであるか、または管理者がユーザーに適切な権限を委任したこと）を確認してください。

### グループの作成とユーザーの割り当て

最初のステップは、サービス・プロセッサの管理用のグループを作成することです。この例では、3 つのグループを作成しています。

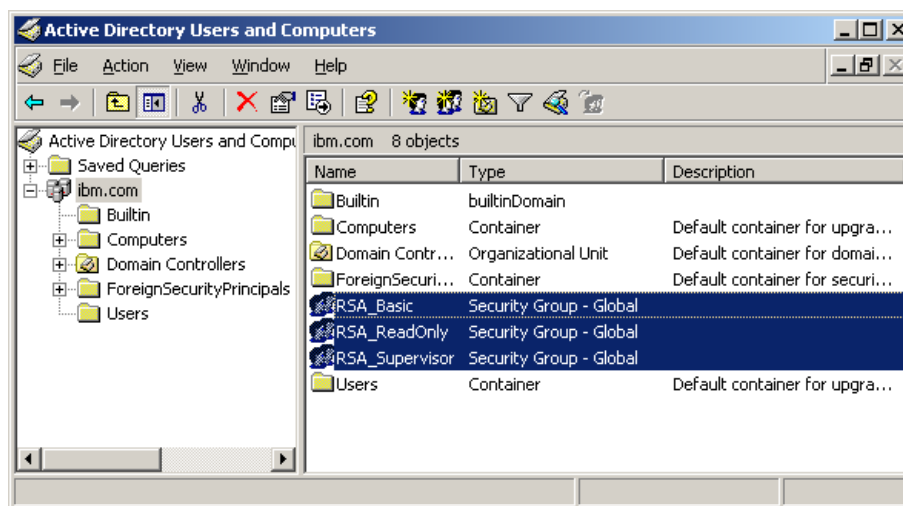


図 5-8 Active Directory 内のグループ

各グループを右クリックして、「Properties」をクリックします。「Add」をクリックして、グループにメンバーを追加します。すべてのグループとすべてのメンバーについて、この手順を繰り返します。

## 新規スキーマ属性の作成

149 ページの 5.2.1、『LDAP 認証属性』で説明した属性を作成して、それをグループに割り当てるには、「Active Directory Schema」で追加の属性を作成し、これをグループまたはユーザーに割り当てる必要があります。属性は追加フィールドとなり、特定値（12 ビット）を持ちます。

**ヒント:** 新規のスキーマ属性を作成するには、それにオブジェクト ID (OID) を割り当てる必要があります。この値は LDAP 管理者から入手できます。

代わりに、将来使用する予定のない既存の未使用の属性を使用することもできます。この方法を使用する場合は、新規の属性を作成する必要はなく、『スキーマ属性のユーザーまたはグループへの割り当て』（154 ページ）の手順に進むことができます。

スキーマの MMC スナップインは、デフォルトではアクティブになりません。Windows の「スタート」メニューの「管理ツール」で、「Active Directory Schema」項目があるか確認してください。そこにはない場合は、アクティブにするために、次のステップを実行します。

1. コマンド・プロンプトを開きます。
2. 次のコマンドを入力して、「Active Directory Schema Manager (schmmgmt.dll)」をご使用のコンピューターに登録します。  
`regsvr32 schmmgmt.dll`
3. 「スタート」をクリックし、「ファイル名を指定して実行」をクリックし、`mmc /a` と入力して、「OK」をクリックします。  
`/a` パラメーターは、Microsoft® Management Console を作成者モードで開始します。
4. 「File」メニューで、「Add/Remove Snap-in」をクリックします。
5. 「Add」をクリックします。
6. リスト内の「Active Directory Schema」をダブルクリックします。
7. 「local」を選択するか（LDAP サーバーから作業をしている場合）、または LDAP サーバーの名前を入力します。
8. 「Close」をクリックし、次に「OK」をクリックします。
9. このコンソールを保管するために、「File」メニューで「Save」をクリックします。
10. 「Save in」で、`systemroot\system32` ディレクトリーを指示します。
11. 「File name」に、`schmmgmt.msc` と入力して、「Save」をクリックします。

将来の使用のために、「スタート」メニュー上にショートカットを作成できます。

1. 「スタート」を右クリックして、「開く」をクリックし、「プログラム」フォルダーをダブルクリックして、次に「管理ツール」フォルダーをダブルクリックします。
2. 「ファイル」メニューで、「新規作成」をポイントして、「ショートカット」をクリックします。
3. 「Create Shortcut Wizard」で、その項目の場所を入力し、schmmgmt.msc と入力して、「Next」をクリックします。
4. 「Select a Title for the Program」 ページで、「Type a name for this shortcut」に Active Directory Schema と入力して、「Finish」をクリックします。

**注意：**スキーマの変更は、上級の操作であるため、経験を積んだプログラマーやシステム管理者が実行するのが最良です。スキーマの変更についての詳しい情報は、Microsoft Web サイトの「*Active Directory Programmer's Guide*」を参照してください。

「Active Directory Schema」スナップインを立ち上げて、「Action」→「Create Attribute」をクリックします。

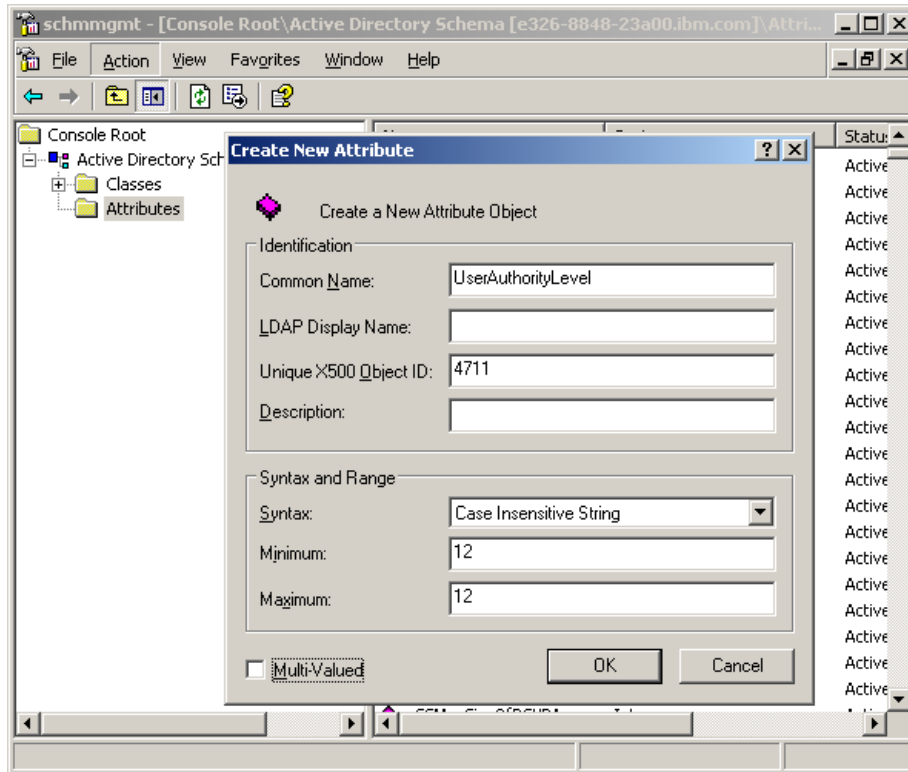


図 5-9 Active Directory schema での新規属性の作成

次の入力を行います。

1. 使用する共通名を入力します。この例では、UserAuthorityLevel を使用しています。名前は大文字小文字の区別をしません。
2. ご使用の X.500 オブジェクト ID を入力します。

**注：**新規の X.500 OID を割り当てる場合は、LDAP システム管理者に問い合わせてください。

3. 「Syntax」を **Case Insensitive String** に設定します。
4. 「Minimum」と「Maximum」を **12** に設定します。
5. 「**OK**」をクリックして、属性を保管します。

### スキーマ属性のユーザーまたはグループへの割り当て

次に、属性をグループまたはユーザーに割り当て、その属性の値を入力します。この値は 12 ビット値です。



**ヒント:** 多数のユーザーを管理するよりも、少数のグループを管理する方が容易であるため、属性は、ユーザーではなくグループに割り当てることをお勧めします。

属性をユーザーまたはグループに割り当てるには、次のようにします。

1. 「**Classes**」をクリックして、項目「user」または「groups」までスクロールします。
2. クラス「user」または「groups」をダブルクリックします。
3. 「Properties」ウィンドウがポップアップ表示されます。ここで、「Attributes」タブをクリックします。

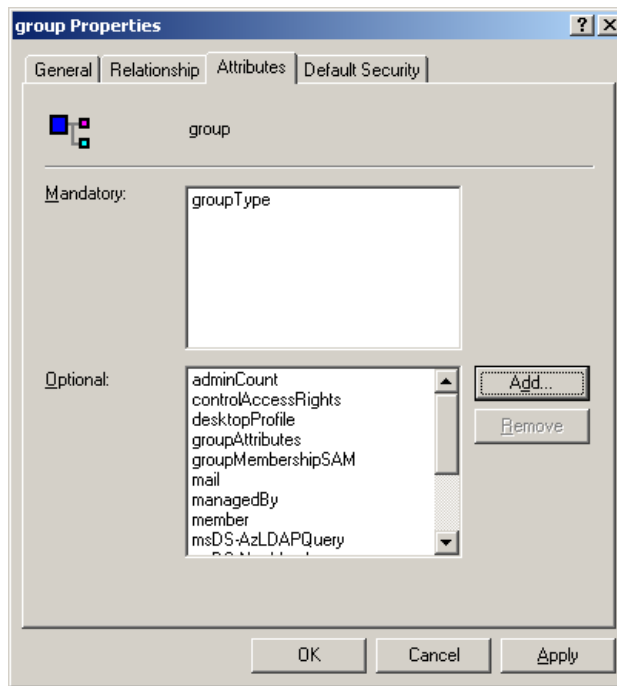


図 5-10 グループ・プロパティ

4. 「Add」をクリックして、グループに属性を追加します。

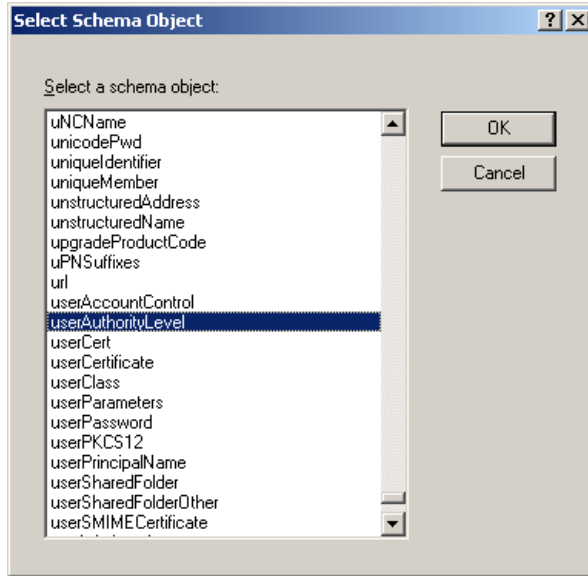


図 5-11 スキーマ・オブジェクトの選択

5. 前に作成した属性「**UserAuthorityLevel**」を選択して、「**OK**」をクリックします。
6. 「**Apply**」と「**OK**」をクリックします。

これで、新規の属性を作成し、それをクラス「**group**」に割り当てました。新規の属性は、グループの通常のプロパティ・ウィンドウには表示されないため、値を入力するには、特別なツールを使用する必要があります。

### 新規属性への値の割り当て

「Objects Properties」ウィンドウに表示されない属性に値を割り当てるためのツールは、Active Directory Service Interfaces (ADSI) Edit ツールと呼ばれ、Windows サポート・ツールに含まれています。インストールされていない場合は、Windows CD からサポート・ツールをインストールしてください。インストール・プログラムは ¥SUPPORT¥TOOLS で見つかります。インストーラーを実行して、指示に従ってください。

ツールがインストールされたら、インストール先のフォルダーに移動します。デフォルトのフォルダーは、¥Program Files¥Support Tools です。ファイル **adsiedit.msc** をダブルクリックします。

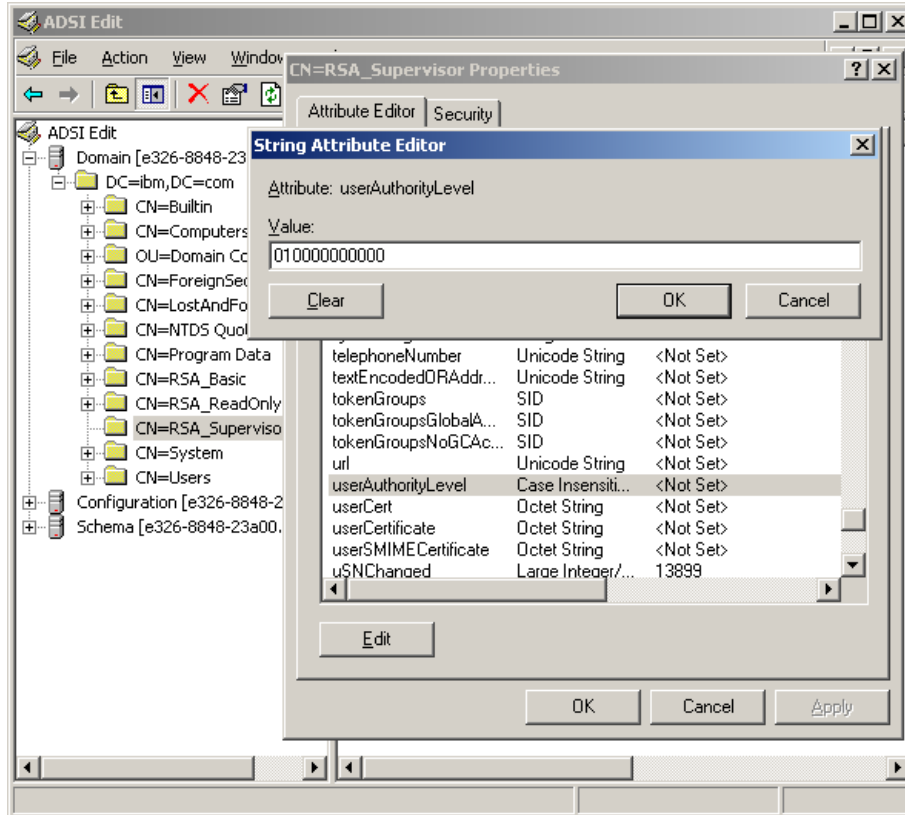


図 5-12 属性への値の割り当て

1. ツリー・ビューの「**Domain**」項目を展開します。
2. 値を入力するグループをダブルクリックし、userAuthorityLevel の値を入力して、「**Properties**」をクリックします。
3. 属性「**UserAuthorityLevel**」までスクロールして、「**Edit**」をクリックします。
4. 必要な値を入力して、「**OK**」をクリックします。値の説明は、149 ページの 5.2.1、『LDAP 認証属性』を参照してください。

UserAuthorizationLevel の値を入力する必要があるすべてのオブジェクト（グループまたはユーザー）について、この手順を繰り返します。

### 5.2.3 LDAP サーバー構成のテスト

サービス・プロセッサを構成する前に、LDAP ブラウザーを使用して、構成をテストする必要があります。LDAP ブラウザーは、サポート・ツール・ディレクトリー LDP.EXE にインストールされています。

1. メニュー・ペインで、「**Connection**」→「**Connect**」をクリックします。
2. LDAP サーバーとポートを入力します。「**OK**」をクリックします。
3. 次に、「**Connection**」→「**Bind**」をクリックします。
4. ユーザー、パスワード、およびドメインを入力します。「**OK**」をクリックします。結果は、次のようになります。

```
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, 1158); // v.3
      {NtAuthIdentity: User='administrator'; Pwd= <unavailable>; domain
      = 'IBM'.}
```

Authenticated as dn:'administrator'.

5. ブラウズを開始するために、「**Browse**」→「**Search**」をクリックします。次のウィンドウがポップアップ表示されます。

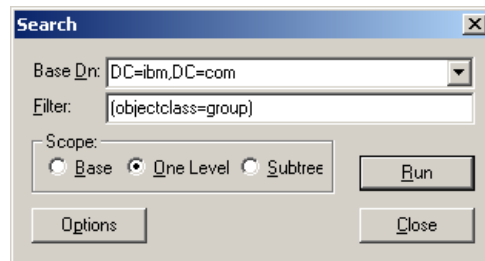


図 5-13 「Search」ウィンドウ

6. 該当する「Base Dn」を選択し、フィルターを (objectclass=group) に変更します。
7. 次に、「**Options**」をクリックします。
8. 「Attributes」を **member; userAuthorityLevel** に変更して、「**OK**」をクリックします。

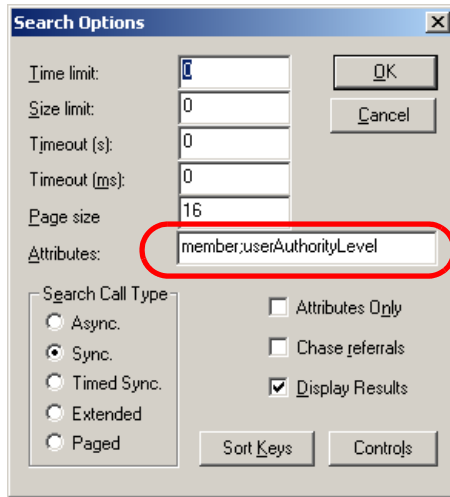


図 5-14 「Attributes」フィールドの設定

9. ここで「**Run**」をクリックします。

照会結果は、図 5-15 のようになります。

```

***Searching...
ldap_search_s(1d, "DC=ibm,DC=com", 1, "(objectclass=group)",
attrList, 0, &msg)
Result <0>: (null)
Matched DNs:
Getting 3 entries:
>> Dn: CN=RSA_Basic,DC=ibm,DC=com
    1> member: CN=Administrator,CN=Users,DC=ibm,DC=com;
    1> userAuthorityLevel: 000100000000;
>> Dn: CN=RSA_ReadOnly,DC=ibm,DC=com
    1> member: CN=Watts,CN=Users,DC=ibm,DC=com;
    1> userAuthorityLevel: 001000000000;
>> Dn: CN=RSA_Supervisor,DC=ibm,DC=com
    2> member: CN=Leitenberger,CN=Users,DC=ibm,DC=com;
CN=Bain,CN=Users,DC=ibm,DC=com;
    1> userAuthorityLevel: 010000000000;
-----

```

図 5-15 LDAP 照会の結果

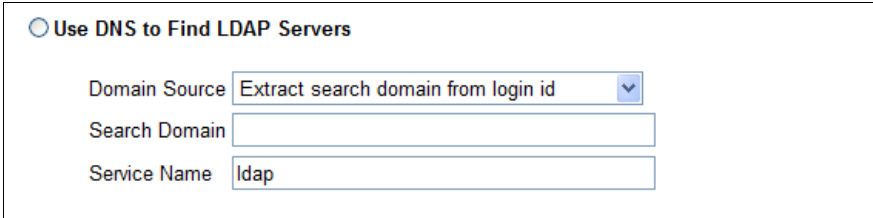
この例では、異なる権限レベルを持つ3つのグループに4名のユーザーがいます。LDAP ブラウザーは、ユーザーのグループ・メンバーシップとグループの権限レベルを表示します。

## 5.2.4 LDAP クライアントの構成

システム管理ハードウェアは、Version 2.0 LDAP クライアントとして機能します。認証要求が来ると（つまり、ユーザーがログインすると）、LDAP クライアントはユーザーの信用証明情報を LDAP サーバーに送信して検証します。ユーザーが認証されると、ユーザーは定義されたアクセス権限に応じて、RSA II または BladeCenter 管理モジュールにアクセスできるようになります。

一般 LDAP 設定を構成するために、Web インターフェースを立ち上げて、次のステップを実行します。

1. ナビゲーション・ペインの「ASM Control」（または、BladeCenter 管理モジュールを使用している場合は、「MM Control」）のもとで、「**Network Protocols**」をクリックします。
2. 「Lightweight Directory Access Protocol (LDAP) Client」セクションまでスクロールダウンします。
3. 「Use DNS to find LDAP servers」（DNS を通して自動的に検出する場合）または「Use pre-configured LDAP servers」（手動で LDAP サーバーのアドレスを構成する場合）を選択します。
  - DNS を使用して LDAP サーバーを検出する場合は、ドメイン・ネームを指定する方法を選択する必要があります。選択項目は、次のとおりです。
    - Extract search domain from login id
    - Use only configured search domain below
    - Try login id first, then configured value



○ Use DNS to Find LDAP Servers

Domain Source  ▼

Search Domain

Service Name

図5-16 DNS を使用する場合に指定するパラメーター

「Extract search domain from login id」では、LDAP クライアントは、ログイン ID のドメイン・ネームを使用します。例えば、ログイン ID が admin@example.com である場合、ドメイン・ネームは example.com になります。ドメイン・ネームを抽出できない場合、ユーザー認証は自動的に失敗します。

ドメイン・ネームを手動で構成する場合は、「**Use only configured search domain below**」を選択して、「Domain search」フィールドにドメイン・ネームを入力します。

3番目のオプションは「Try login id first, then configured value」です。このオプションでは、LDAP クライアントは、最初にログイン ID からドメイン・ネームの抽出を試みます。これが成功すると、このドメイン・ネームが DNS SRV 要求で使用されます。このログイン ID にドメイン・ネームが存在しない場合、代わりに LDAP クライアントは、構成された「Search Domain」パラメーターを DNS SRV 要求でドメイン・ネームとして使用します。何も構成されていない場合、ユーザー認証は即時に失敗します。

**ヒント：**「Domain Name System (DNS)」セクションには、必ず、少なくとも2つの DNS サーバーを構成してください。スクロールアップして、このセクションを見つけてください。

DNS サーバーに送信される DNS SRV 要求では、サービス名も指定する必要があります。構成された値が、この目的に使用されます。空白のままにした場合、使用されるデフォルト値は LDAP です。DNS SRV 要求ではプロトコル名も指定する必要があることに注意してください。これは、デフォルトで tcp になり、構成することはできません。

Use Pre-Configured LDAP Servers	
LDAP Server Host Name or IP Address	Port
1. <input type="text"/>	<input type="text"/>
2. <input type="text"/>	<input type="text"/>
3. <input type="text"/>	<input type="text"/>

図 5-17 DNS を使用する場合に指定するパラメーター

- 事前構成（ハードコーディング）された LDAP サーバーを指定する場合（図 5-17）、必ず、少なくとも2つの異なるサーバー・アドレスを提供して、LDAP サーバーに障害が起きた場合に冗長性を持たせます。

IP アドレスまたはホスト名を入力し（ホスト名を使用する場合は、ネーム・レゾリューション（例えば、DNS）が正常に機能していることを確認してください）、使用する LDAP ポートを入力します。LDAP サーバーのポートを変更しない場合は、このパラメーターは空白のまま構いません。

ヒント：「pre-configured LDAP servers」オプションを使用するのは、中堅規模ビジネス、および主として静的環境に限定してください。LDAP サーバーのアドレスが変更されるたびに、すべてのサービス・プロセッサの更新が必要になります。

- LDAP 通信用のその他のパラメーターを提供します。「Root DN」フィールドに、ドメインのルート・エントリーの識別名を入力します。この例の場合は、dc=ibm,dc=com です。

**Miscellaneous Parameters**

Root DN	<input type="text" value="dc=ibm,dc=com"/>
User Search Base DN	<input type="text"/>
ASM Group Filter	<input type="text" value="RSA*"/>
Binding Method	<input type="text" value="User Principal Name"/>

[Set DN and password only if Binding Method used is Client Authentication](#)

[Set attribute names for LDAP client search algorithm](#)

図5-18 LDAP の各種パラメーター

ヒント：Windows ADS 以外の LDAP サーバーを使用している場合、「Root DN」のフォーマットが異なることがあります。例えば、Novell eDirectory を使用している場合、このパラメーターは dc=ibm.com になります。

- 「User Search Base DN」フィールド。ユーザー認証プロセスの一部として、LDAP サーバーで、特定のユーザーまたはグループに関連付けられた 1 つ以上の属性を検索することが必要です。検索要求では、実際の検索のためのベース DN を指定する必要があります。

「User Search Base DN」フィールドでは、objectClass が user（ユーザー・レコードを検索する場合）または group（グループ・レコードを検索する場合）であるオブジェクトの検索に使用するベース DN を指定します。ユーザー検索またはグループ検索は、認証プロセスの一部です。これは、ユーザー（ログイン許可およびグループ・メンバーシップ）またはグループ（ログイン許可）に関する情報を検索するために実行されます。

このパラメーターは、ユーザー（objectClass=user）とグループ（objectClass=group）の両方の検索ベースである点に注意することが重要です。ユーザーとグループが異なるサブツリーにある場合、このパラメーターは両方のサブツリーが表示されるように設定されていることを確認してくだ



さい。このフィールドをブランクのままにすると、代わりに「Root DN」が検索ベースとして使用されます。

6. 「Group Filter」フィールドは、グループ認証に使用されます。これは、このサービス・プロセッサが所属するグループを指定します。ブランクのままにすると、グループ認証は使用不可にされます。それ以外の場合、グループ認証はこのフィルターを適用して実行されます。フィルターには、特定のグループ名（例えば、RSAWest）、すべてに一致するワイルドカード（\*）、または接頭部付きのワイルドカード（例えば、RSA\*）を指定できます。デフォルトのフィルターは RSA\* です。

ユーザー認証の後に、グループ認証が行われ、グループ（ユーザーが所属する）をここで定義されたグループ・フィルターに突き合わせます。一致しない場合、ユーザーは認証を通過せず、ブロックされます。一致した場合、一致したグループからユーザーのログイン許可が取得されます（すでに LDAP サーバーから取得されたユーザー・レコードから直接、ユーザーにログイン許可が割り当てられていない場合）。

7. 「Binding Method」フィールド。ユーザー認証での LDAP サーバーへの初回バインド時に、バインド方式として選択できる 4 つのオプションがあります。

- 「Anonymous authentication」。バインドの試行は、クライアント DN またはパスワードを使用せずに行われます。バインドが成功すると、ログインしようとしているユーザーのエントリを LDAP サーバーで見つけるために、検索が要求されます。エントリが見つかると、今度はユーザーの DN とパスワードを使用して、2 回目のバインドが試行されます。これが成功すると、ユーザーはユーザー認証フェーズを通過したと見なされます。次に、グループ認証が試行されます（使用可能に設定されている場合）。

**注意：**「anonymous authentication」は使用しないでください。初回バインド要求に対するパラメーターとしてヌル・ユーザー ID とヌル・パスワードが使用されている場合、後続の検索要求は失敗します。

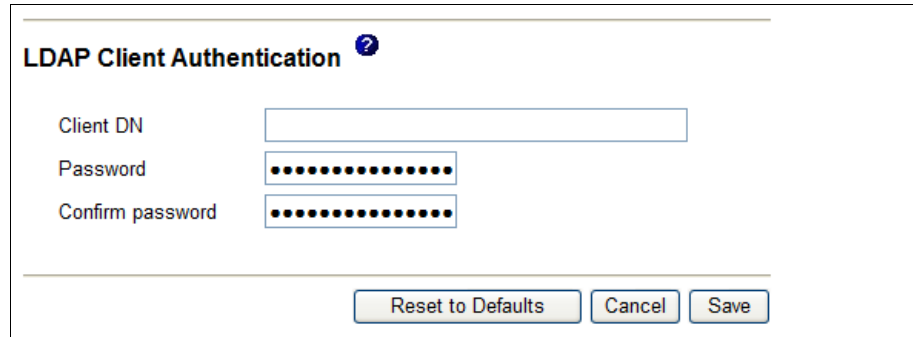
- 「Client authentication」。バインドの試行は、この構成パラメーターで指定されたクライアント DN とパスワードを使用して行われます。バインドに成功すると、ユーザー認証フェーズは上記の「Anonymous authentication」と同様に進行します。
- 「User Principal Name (UPN)」。これはデフォルトです。バインドの試行は、ログイン・プロセスで使用された信用証明情報を直接使用して行われます。これが成功すると、ユーザーはユーザー認証フェーズを通過し

たと見なされます。Active Directory サーバーの場合、ユーザー ID の形式は user@domain、または単に user です。

- 「Strict UPN」。これは、ユーザー ID の形式が someuser@domain でなければならない点を除いて、上記の UPN と同じです。ユーザーによって入力されたストリングは、@ 記号で構文解析されます。

**ヒント :** UPN 方式と strict UPN 方式は、どちらも Windows ADS でのみ機能します。

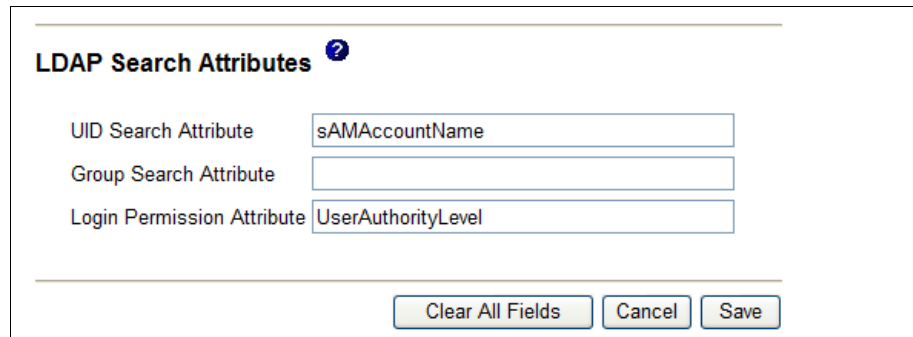
8. バインド方式としてクライアント認証を使用する場合、「**Set DN and password only if Binding Method used is Client Authentication**」をクリックします。164 ページの図 5-19 が表示されます。初回バインド要求時のユーザー ID とパスワードを提供します。パラメーターを入力した後、「**Save**」をクリックします。



The image shows a dialog box titled "LDAP Client Authentication" with a help icon. It contains three input fields: "Client DN" (empty), "Password" (masked with dots), and "Confirm password" (masked with dots). At the bottom, there are three buttons: "Reset to Defaults", "Cancel", and "Save".

図 5-19 初回バインド要求時の LDAP クライアント認証

9. LDAP Search 属性を設定するために、「**Set attribute names for LDAP client search algorithm**」をクリックします。図 5-20 が表示されます。「**Save**」をクリックして、行った変更を保管し、前のウィンドウに戻ります。



The image shows a dialog box titled "LDAP Search Attributes" with a help icon. It contains three input fields: "UID Search Attribute" (containing "sAMAccountName"), "Group Search Attribute" (empty), and "Login Permission Attribute" (containing "UserAuthorityLevel"). At the bottom, there are three buttons: "Clear All Fields", "Cancel", and "Save".

図 5-20 初回バインド要求時の LDAP クライアント認証

- LDAP サーバー上のユーザー ID を表すのに使用される属性名を指定します。デフォルトの UID 検索属性は uid です。Windows ADS の場合は、sAMAccountName と入力します。

選択されたバインド方式が UPN または Strict UPN の場合、入力されたユーザー ID の形式が user@domain であれば、ユーザー認証時にこのフィールドは自動的にデフォルトの userPrincipalName になります。

- どのユーザーがどのグループに属するかを検出するには、グループ検索属性を指定します。このフィールドを空白のままにした場合、フィルター内の属性名はデフォルトの memberOf になります。デフォルト値は、Windows ADS および Novell eDirectory で機能します。
- ASM に対して正しいユーザー権限を割り当てるために、LDAP サーバーで使用される属性名を指定します。『新規スキーマ属性の作成』(152 ページ) により、この例では属性 UserAuthorityLevel を使用しています。

10. スクロールダウンして「**Save**」をクリックし、すべての変更を保管します。

**ヒント** : LDAP 構成の変更時には、リブートする必要はありません。

最後のステップは、サービス・プロセッサが認証に LDAP サーバーを使用するように構成することです。これを行うには、ナビゲーション・フレームで「**ASM Control**」(または「**MM Control**」、BladeCenter 管理モジュールを使用している場合) → 「**Login Profiles**」をクリックします。「Global Login Settings」セクションの値を変更します。

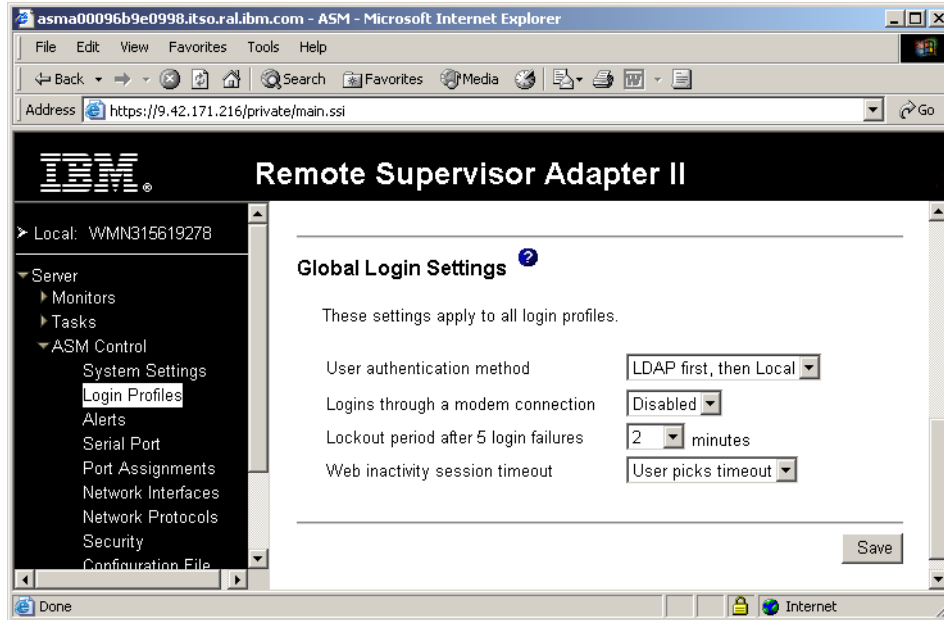


図 5-21 グローバル・ログイン設定

「User authentication method」フィールドには、4つの選択項目があります。


- ▶ Local only
- ▶ LDAP only
- ▶ Local first, then LDAP
- ▶ LDAP first, then local

「Local first, then LDAP」または「LDAP first, then local」のみを使用することをお勧めします。そうすれば、LDAP 認証に関する問題が起きた場合でも、ローカルで定義されたユーザーを通して、RSA II または BladeCenter 管理モジュールにアクセスすることが可能です。

ご使用のインストール環境に適していると思われる任意の他の設定に変更し、「Save」をクリックして、変更を保管します。

ここでログオフし、LDAP ユーザーとして再度ログインして、機能をテストします。

**ヒント :** Windows Active Directory を LDAP サーバーとして使用している場合、Windows セキュリティ・イベント・ログを検討することによって、LDAP 認証プロセスを検査できます。



## システム管理ユーティリティー

この章では、IBM @server 325/326、BladeCenter、および xSeries ファミリーのサーバーの管理に使用できるユーザー・インターフェースについて説明します。この章で説明するインターフェースは、次のとおりです。

- ▶ 170 ページの 6.2、『Advanced Settings ユーティリティー』
- ▶ 186 ページの 6.3、『管理プロセッサ・コマンド・ライン・インターフェース』
- ▶ 204 ページの 6.4、『OSA SMBridge ユーティリティー』
- ▶ 232 ページの 6.5、『Web インターフェース』
- ▶ 234 ページの 6.6、『Telnet インターフェース』
- ▶ 239 ページの 6.7、『IBM Director の統合』

この章では、ユーザー・インターフェースの入手先、インストール方法、システム管理用にユーザー・インターフェースを構成する方法、およびユーザー・インターフェースの使用法について詳しく説明します。

## 6.1 ツールの比較

この章では、xSeries サーバーでサポートされる入手可能なユーザー・インターフェースのすべてを説明します。ただし、それぞれのツールは、すべてのサーバー、すべてのサービス・プロセッサをサポートするわけではありません。

表 6-1 は、この章で取り上げるツールと、そのツールをサポートするサーバーをリストしています。詳細については、この章のそれぞれのツールのセクションを参照してください。

表 6-1 各 xSeries サーバーでサポートされるユーザー・インターフェース

サーバー	ASU	MPCLI <sup>1</sup>	SMBridge	SP Web	SP telnet	Director
xSeries 200	なし	なし	なし	なし	なし	サポート
xSeries 205	なし	なし	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 206	なし	なし	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 220	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 225	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 226	なし		なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 230	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 232	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 235	サポート	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 236	なし	なし	サポート	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 240	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 250	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 255	サポート	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 300	なし		なし	なし	なし	サポート
xSeries 305	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 306	なし	なし	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 330	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 335	サポート	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 336	なし	なし	サポート	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 340	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート

サーバー	ASU	MPCLI <sup>1</sup>	SMBridge	SP Web	SP telnet	Director
xSeries 342	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 343	なし		なし	なし	なし	サポート
xSeries 345	サポート	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 346	なし	なし	サポート	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 350	なし	サポート	なし	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 360	なし	サポート	なし	サポート	サポート	サポート
xSeries 365	なし		なし	サポート	サポート	サポート
xSeries 366	なし	なし	サポート	オプション <sup>2</sup>	オプション <sup>2</sup>	サポート
xSeries 370	なし		なし	サポート	サポート	サポート
xSeries 440	サポート	サポート	なし	サポート	サポート	サポート
xSeries 445	サポート	なし	なし	サポート	サポート	サポート
xSeries 450	なし	サポート	なし	サポート	サポート	サポート
xSeries 455	なし	サポート	なし	サポート	サポート	サポート
BladeCenter MM	なし	サポート	なし	サポート	サポート	サポート
Blade HS20	なし	サポート	なし	サポート	サポート	サポート
Blade HS40	なし	サポート	なし	サポート	サポート	サポート
eServer 325	なし	なし	なし	なし	なし	サポート
eServer 326	なし	なし	なし	なし	なし	サポート

**注：**

1. MPCLI サポートは、サポートされるサーバー上の特定のサービス・プロセッサに限定される場合があります。詳細については、175 ページの表 6-3 を参照してください。
2. サーバーのサービス・プロセッサに組み込まれた Web ベースおよび Telnet ベースのインターフェースをサポートするには、RSA II SlimLine、RSA II、RSA、または ASM PCI アダプターのいずれかを追加する必要があります。ANSI 端末インターフェース (COM ポートを使用する点を除いて Telnet と同じ) は、ハードウェアを追加しなくてもサーバー上でサポートされます。

この章で説明するように、ユーザー・インターフェースを使用して、さまざまな管理タスクを実行できます。170 ページの表 6-2 は、管理インターフェースを使用して実行することが予想されるタスクと、そのタスクを実行できるツールをリストしています。

表6-2 サポートされるタスク別のツールの比較

タスク	ASU	MPCLI	SMBridge	SP Web	SP telnet
サーバー・ヘルスの表示	なし	サポート	なし	サポート	サポート
SP 構成	サポート	サポート	なし	サポート	サポート
BIOS 構成	あり	なし	サポート <sup>1</sup>	サポート <sup>1</sup>	なし
電源制御	なし	サポート	サポート	サポート	サポート
グラフィカル Remote Control	なし	なし	なし	サポート <sup>2</sup>	なし
テキスト・ベース Remote Control	なし	なし	サポート	サポート	なし
バッチ/コマンド・ライン・モード	サポート	サポート	限定 <sup>3</sup>	なし	なし
イベント・ログの表示	なし	サポート	サポート	サポート	サポート
SP ファームウェアのフラッシュ	なし	サポート	なし	サポート	サポート <sup>5</sup>
システム BIOS のフラッシュ	なし	なし	なし	なし	なし
リモート側での使用	なし <sup>4</sup>	サポート	サポート	サポート	サポート

**注：**

1. Remote Control 機能を使用し、サーバーをリブートします。
2. 古いサービス・プロセッサ (ASM PCI アダプターなど) は、このタスクをサポートしません。
3. SMBridge コマンド・ライン・インターフェースは、電源制御と状況照会に限定されます。229 ページの 6.4.7、『コマンド・ライン・インターフェースを介した接続』を参照してください。
4. ASU は、リモート側で使用するようには設計されていませんが、IBM Director と一緒に使用すれば、リモート側での使用も可能です。269 ページの 7.7、『リモート側での ASU の使用法』を参照してください。
5. ファームウェア更新ファイルのホストとして、ネットワークに TFTP サーバーがインストールされていることが必要です。

## 6.2 Advanced Settings ユーティリティ

Advanced Settings ユーティリティ (ASU) を使用すると、複数のオペレーティング・システム・プラットフォーム上で、コマンド・ラインからファームウェア設定を変更できます。ユーティリティを使用して、BIOS およびサービス・プロセッサ・ファームウェアのユーザー設定と構成パラメーターを変更でき、サーバーを再始動して F1 キーを押し、BIOS Setup にアクセスする必要がありません。



さらに、Advanced Settings ユーティリティーは、そのバッチ処理モードを通してスクリプト環境もサポートします。

このユーティリティーは現在、次のファームウェア・タイプをサポートしています。

- ▶ xSeries システム BIOS コード
- ▶ リモート管理アダプター I ファームウェア
- ▶ リモート管理アダプター II ファームウェア

ユーティリティーは、コマンド・ライン・インターフェースを使用して、サポートされるファームウェア・タイプからユーザー設定を検索し、変更します。ユーティリティーは、ファームウェア・コードは更新しません。

### 6.2.1 ASU のサポート・リスト

ASU は現在、次の xSeries サーバーの Remote Supervisor Adapter および Remote Supervisor Adapter II をサポートしています。

- ▶ x235
- ▶ x255
- ▶ x335
- ▶ x345
- ▶ x440 (単一ノード構成のみ)
- ▶ x445 (単一ノード構成のみ)

ASU は、次のブレード・サーバーもサポートします。

- ▶ BladeCenter HS20 タイプ 8678
- ▶ BladeCenter HS20 タイプ 8832

注：x440 および x445 のマルチノード構成はサポートされません。

サポートされるサーバーの最新リストは、ASU のダウンロード・ページを参照してください。次の URL は、Windows 用のページです。

<http://www.ibm.com/pc/support/site.wss/MIGR-55019.html>

### 6.2.2 ASU のサポートされるプラットフォーム

ASU は、次のオペレーティング・システムをサポートします。

- ▶ Windows NT<sup>®</sup> 4.0、Windows 2000、Windows XP、および Windows Server 2003
- ▶ Red Hat Linux 7.x、8.x、および 9
- ▶ Red Hat Enterprise Linux AS 2.1、Red Hat Enterprise Linux 3.0

**注：**互換性 libstdc++ ライブラリーがインストールされていない Red Hat Enterprise Linux 3.0、Red Hat 9、およびその他の Linux ディストリビューションの場合、次のようなメッセージが表示されることがあります。

```
./asu: error while loading shared libraries:  
libstdc++-libc6.1-1.so.2: cannot open shared object file: No such  
file or directory.
```

このメッセージが表示された場合は、ディストリビューション・メディアに組み込まれている compat-libstdc++\*.rpm をインストールしてください。

- ▶ SUSE LINUX 7.x、8.x、および 9
- ▶ SUSE LINUX Enterprise Server 8
- ▶ PC-DOS: 7.0 以降

ASU は、表示および変更する設定を収容しているサーバー上で実行します。パラメーターを変更する場合は、root (Linux) または管理者 (Windows) としてアクセスする必要があります。

RSA または RSA II の設定を表示したり変更したりするには、RSA または RSA II のデバイス・ドライバーが使用されるため、デバイス・ドライバーがインストールされている必要があります。ご使用のシステム用の RSA および RSA II デバイス・ドライバーは、次のサイトからダウンロードできます。

<http://www.pc.ibm.com/support>

**注：**以下の注意事項をお読みください。

1. サポートされるデバイス・ドライバーのないオペレーティング・システムからは、ユーティリティーを使用して RSA または RSA II の設定を表示したり、構成したりすることはできません。サポートされるデバイス・ドライバーの詳細は、次の ServerProven サイトを参照してください。

<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>

2. PC-DOS 用の RSA または RSA II デバイス・ドライバーは提供されていないため、ユーティリティーを使用して PC-DOS から RSA や RSA II の設定を構成することはできません。
3. 設定の表示と変更は、ローカル・サーバー上でのみ実行できます。ただし、IBM Director と一緒に使用すれば、リモート側でも実行できます。269 ページの 7.7、『リモート側での ASU の使用法』を参照してください。

## 6.2.3 ASU と定義ファイルのダウンロード

基本 ASU ユーティリティーは、次のサイトからダウンロードできます。

Windows: <http://www.ibm.com/pc/support/site.wss/MIGR-55019.html>  
Linux: <http://www.ibm.com/pc/support/site.wss/MIGR-55020.html>  
PC-DOS: <http://www.ibm.com/pc/support/site.wss/MIGR-55021.html>

定義ファイルは、ASU ユーティリティーを拡張して、特定のサーバーと Remote Supervisor Adapter を構成できるようにする手段です。Remote Supervisor Adapter およびサポートされるサーバー用の定義ファイルは、次のリンクから入手できます。

RSA I / RSAII: <http://www.ibm.com/pc/support/site.wss/MIGR-55027.html>  
HS20 (8678): <http://www.ibm.com/pc/support/site.wss/MIGR-56860.html>  
HS20 (8832): <http://www.ibm.com/pc/support/site.wss/MIGR-56555.html>  
x235: <http://www.ibm.com/pc/support/site.wss/MIGR-55803.html>  
x255: <http://www.ibm.com/pc/support/site.wss/MIGR-56393.html>  
x335: <http://www.ibm.com/pc/support/site.wss/MIGR-55804.html>  
x345: <http://www.ibm.com/pc/support/site.wss/MIGR-55778.html>  
x440 (8-Way): <http://www.ibm.com/pc/support/site.wss/MIGR-56858.html>  
x445: <http://www.ibm.com/pc/support/site.wss/MIGR-55944.html>

## 6.2.4 ASU 定義ファイルの使用

ASU は、それぞれのファームウェア・タイプごとに定義ファイル（パッチ）を必要とします。定義ファイルを適用すると、ASU ユーティリティーが変更されて、特定のハードウェアと連動するようになります。そのファームウェア・タイプ用の定義ファイルを適用するまでは、ASU ユーティリティーを使用できません。単一の定義ファイルは、次のファームウェア設定のいずれかに対するサポートを追加します。

- ▶ サーバー上の単一 BIOS バージョン
- ▶ 任意のサーバー上の RSA または RSA II

ASU 定義ファイルは、単一 BIOS バージョンの設定、あるいは RSA または RSA II ファームウェアの設定が置かれている場所を ASU に知らせて、設定の適用方法が分かるようにするにすぎません。定義ファイルは、ユーティリティー実行可能プログラムの最後にデータを追加します。ASU に定義ファイルを追加したり除去したりすることができ、また定義ファイルはいくつでも追加できます。

174 ページの図 6-1 は、定義ファイルを ASU バイナリー・コードに追加する方法を示しています。ASU ユーティリティーに定義を追加するには、該当する定義をダウンロードして .def ファイルを解凍し（Linux では **unzip** を使用）、次のコマンドを実行して、定義を追加します。

Windows: **asu patchadd <definition file>.def**  
DOS: **asu patchadd <definition file>.def**

Linux: `./asu patchadd <definition file>.def`

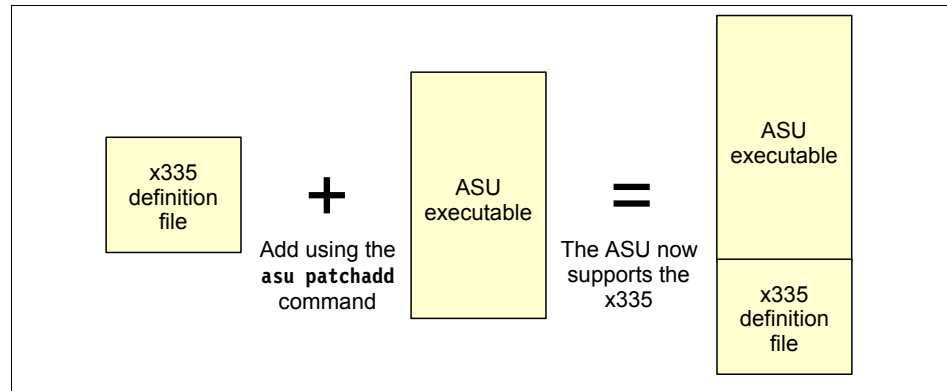


図 6-1 ASU 実行可能プログラムへの x335 定義の追加

ASU を実行すると、それに適用されたパッチを自動的にスキャンし、設定に適用できる定義ファイルが存在するかどうかを調べます。適用できる定義ファイルが存在する場合、ユーティリティーはその設定を適用します。定義ファイルが存在しない場合、ASU はエラーを戻します。

## 6.2.5 ASU コマンドの使用

**asu** コマンドを使用する前に、適用できる定義ファイルをインストールして ASU ファイルを更新する必要があります。ASU コマンドは、ユーティリティー・ファイルが置かれているディレクトリーから入力する必要があります。ASU コマンドの構文は、次のとおりです。

- ▶ Windows: **asu [command] [setting] [value]**
- ▶ Linux: **./asu [command] [setting] [value]**

以下のコマンド・リストでは、*setting* は、表示または変更するパラメーターを表し、*value* は、ユーザーがそのパラメーターに指定する値を表します。*value* にスペースが含まれる場合は、値ストリングを引用符で囲んでください。

ASU の使用可能なコマンドとその構文を、表 6-3 にリストします。

**ヒント** : `-v` オプションを付けると、詳細モードを指定でき、より詳細な出力が得られます。

表 6-3 使用可能な ASU コマンドとその構文

ASU コマンド	機能	構文
(コマンドなし)	すべての ASU コマンドとオプションを表示します。	パラメーターなし
<b>batch</b> <filename>	複数のコマンドを実行します。185 ページの 6.2.8、『ASU バッチ・コマンド』を参照してください。	batch <filename>  ここで、<filename> は、さまざまな ASU コマンドを含んでいるテキスト・ファイルです。
<b>comparedefault</b>	1 つの設定またはすべての設定の現行値とデフォルト値を比較します。	comparedefault [all   <CMOS setting>] [-v]
<b>dump</b>	RAW CMOS 設定を表示します。	dump
<b>help</b>	1 つの設定またはすべての設定のオンライン・ヘルプを表示します。BIOS 設定の場合、ヘルプ情報は、セットアップ中に F1 を押してアクセスするヘルプと同じです。	help [all   <CMOS setting>]
<b>loaddefault</b>	1 つの設定またはすべての設定のデフォルト値をロードします。	loaddefault [all   <CMOS setting>] [-v]
<b>patchadd</b>	特定のサーバーまたはデバイスのサポートを追加します。	patchadd <.def file> [<patched program>]  ここで、<.def file> は、BIOS ビルドから取られた CMOS 定義ファイル、<patched program> は、書き込む、パッチを当てたプログラムのファイル名です。
<b>patchextract</b>	ユーティリティーからパッチ・ファイルに定義ファイルを抽出します。抽出された定義ファイルをユーティリティーの別のバージョンにパッチとして適用できます。	patchextract <patch #> <.def file>  ここで、<patch #> は、 <b>patchlist</b> コマンドによって出力されたインデックス、<.def file> は、作成するファイルです。
<b>patchlist</b>	現在適用されている定義ファイルを表示します。	パラメーターなし

ASU コマンド	機能	構文
<b>patchremove</b>	定義ファイルを除去します。	patchremove <patch #> [<unpatched program>]  ここで、<patch #> は、 <b>patchlist</b> コマンドによって出力されたインデックス、<unpatched program> は、書き込む、パッチを当てていないプログラムのファイル名です。
<b>rebootrsa</b>	サービス・プロセッサを再始動します。このコマンドは、構成変更を有効にするために、Remote Supervisor Adapter を再始動する必要がある場合に便利です。	パラメーターなし
<b>resetsra</b>	RSAI/RSAIL をリセットして、デフォルト設定に戻します。	パラメーターなし
<b>replicate</b>	1 つ以上の <b>show</b> コマンドの出力を使用して、複数の設定値を同時に設定します。	replicate <filename>  ここで、<filename> は、 <b>show</b> コマンドからのパイピング出力によって作成されたファイルです。
<b>set</b>	設定の値を変更します。	set <CMOS setting> <value> [-v]  ここで、<value> は、showvalues から示されたストリングです。
<b>show</b>	1 つの設定またはすべての設定の現行値を表示します。	show [all   <CMOS setting>] [-v]
<b>showdefault</b>	1 つの設定またはすべての設定のデフォルト値を表示します。	showdefault [all   <CMOS setting>] [-v]
<b>showvalues</b>	1 つの設定またはすべての設定の可能な値をリストします。このコマンドは、 <b>set</b> コマンドで使用する値パラメーターを見つけるのに便利です。	showvalues [all   <CMOS setting>] [-v]
<b>version</b>	ユーティリティのバージョンと作成日を表示します。	パラメーターなし

## 6.2.6 ASU を使用したシステム設定の表示

特定のシステムの現行値を表示するには、次のコマンドを入力します。

```
asu show all
```

次のような出力が表示されます。この例では、RSA II アダプターを搭載した xSeries 345 を使用しました。この出力は、サーバー構成ごとに異なります。

**ヒント:** すべての詳細を表示する容易な方法として、コマンドをテキスト・ファイルにパイプ接続できます。例えば、次のように指定します。

```
asu show all > showall.txt
```

これにより、すべての使用可能な CMOS または RSA/RSA II 設定のクイック・リファレンスが得られます。例 6-1 は、この出力例を示しています。

**注:** この出力は、アルファベット順にソートされていません。

*例 6-1 RSA II を搭載した x345 で実行した ASU からの出力例*

---

```
CMOS_DisketteA=1.44 MB 3.5"
CMOS_CRTRequired=Enabled
CMOS_KbdRequired=Enabled
CMOS_UsbLegacy=Enabled
CMOS_HD_Auto1=Autoconfigure
CMOS_HD_Auto0=Autoconfigure
CMOS_PrimaryBootDevice4=Network
CMOS_PrimaryBootDevice3=Hard Disk 0
CMOS_PrimaryBootDevice2=Diskette Drive 0
CMOS_PrimaryBootDevice1=CD ROM
CMOS_AlternateBootDevice4=Hard Disk 0
CMOS_AlternateBootDevice3=CD ROM
CMOS_AlternateBootDevice2=Diskette Drive 0
CMOS_AlternateBootDevice1=Network
CMOS_NumLock=Off
CMOS_PS2Mouse=Installed
CMOS_UserPwdChange=No
CMOS_ServerMode=On
CMOS_FloppyRequired=Enabled
CMOS_PostBootFailRequired=Enabled
CMOS_MappingPref=Enabled
CMOS_PerfPref=Yes
CMOS_Remap=No
CMOS_MemoryRow0Disable=Row Is Enabled
CMOS_MemoryRow1Disable=Row Is Enabled
CMOS_MemoryRow2Disable=Row Is Enabled
CMOS_MemoryRow3Disable=Row Is Empty
CMOS_UserPrefInterleave=2 Way Interleaved
CMOS_DisketteController=Enabled
CMOS_Parallel=Disabled
```

CMOS\_ParallelMode=Standard  
CMOS\_ParallelIRQ=IRQ 7  
CMOS\_ParallelDMA=DMA 1  
CMOS\_StopOnError=Disabled  
CMOS\_ENET1\_PLANAR\_ENABLE=Enabled  
CMOS\_SCSI\_PLANAR\_ENABLE=Enabled  
CMOS\_Slot1\_ENABLE=Enabled  
CMOS\_Slot2\_ENABLE=Enabled  
CMOS\_Slot3\_ENABLE=Enabled  
CMOS\_Slot4\_ENABLE=Enabled  
CMOS\_Slot5\_ENABLE=Enabled  
CMOS\_SerialB=Disabled  
CMOS\_SPVD=Hidden  
CMOS\_RemoteConsoleEnable=Disabled  
CMOS\_RemoteConsoleComPort=COM 1  
CMOS\_RemoteConsoleBaud=9600  
CMOS\_RemoteConsoleDataBits=8  
CMOS\_RemoteConsoleParity=None  
CMOS\_RemoteConsoleStopBits=1  
CMOS\_RemoteConsoleEmulation=ANSI  
CMOS\_RemoteConsoleBootEnable=Disabled  
CMOS\_SerialA=Port 3F8, IRQ 4  
CMOS\_ENET\_PXE\_ENABLE=Planar Ethernet 1  
CMOS\_PciUsbIrqValue=Autoconfigure  
CMOS\_PciSCSIAIntAValue=Autoconfigure  
CMOS\_PciSCSIBIntAValue=Autoconfigure  
CMOS\_PciVideoIntAValue=Autoconfigure  
CMOS\_PciEnetIntAValue=Autoconfigure  
CMOS\_PciEnetBIntAValue=Autoconfigure  
CMOS\_PciSlot1IntACValue=Autoconfigure  
CMOS\_PciSlot1IntBDValue=Autoconfigure  
CM\_VIRUS\_DETECT=Disabled  
CMOS\_JacksonTechnology=Enabled  
CMOS\_INT\_19H=Enabled  
CMOS\_PciSlot2IntAValue=Autoconfigure  
CMOS\_PciSlot2IntBValue=Autoconfigure  
CMOS\_PciSlot2IntCValue=Autoconfigure  
CMOS\_PciSlot2IntDValue=Autoconfigure  
CMOS\_PciSlot3IntACValue=Autoconfigure  
CMOS\_PciSlot3IntBDValue=Autoconfigure  
CMOS\_PciSlot4IntACValue=Autoconfigure  
CMOS\_PciSlot4IntBDValue=Autoconfigure  
CMOS\_PciSlot5IntACValue=Autoconfigure  
CMOS\_PciSlot5IntBDValue=Autoconfigure  
CMOS\_PCIMLT1=40h



```
CMOS_PCIBootPriority=Planar SCSI
CMOS_PrefetchQueue=Enabled
CMOS_SystemCacheType=Write Back
CMOS_SPRebootOnNMI=Enabled
CMOS_ThresholdLockout=5
CMOS_WakeOnLAN=Enabled
CMOS_IDEControllerPrimary=Enabled
CMOS_DHCPControl=Use Static IP
CMOS_OSUSBControl=Other OS
CMOS_RemoteConsoleKybdEmul=ANSI
CMOS_RemoteConsoleFlowCtrl=Disabled
CMOS_ENET_PXE_PRIORITY=High
CMOS_LoopOnBootSequence=Disabled
CMOS_PeriodicSMI=Enabled
CMOS_HD_Mode1=PIO mode 0
CMOS_HD_Mode0=PIO mode 0
RSA_Network1=Enabled
RSA_LANDataRate1=Auto
RSA_Duplex1=Auto
RSA_DHCP1=Disabled
RSA_PPPOAuthProt1=PAP Only
RSA_Network2=Disabled
RSA_DHCP2=Disabled
RSA_ModemBaudRate1=57600
RSA_ModemParity1=None
RSA_ModemStopBits=1
RSA_SerialRedirectionPort1=Disabled
RSA_SerialRedirectionCLIMode1=CLI disabled
RSA_SerialRedirectionNoAuthentication1=Require authentication
RSA_SerialRedirectionPort2=Enabled
RSA_SerialRedirectionCLIMode2=CLI active / EMS compatible keystroke
sequences
RSA_SerialRedirectionNoAuthentication2=Require authentication
RSA_LinkSerialPort1And2=Disabled
RSA_LoginFlags1=Read/Write, Dial back disabled
RSA_LoginFlags2=Read/Write, Dial back disabled
RSA_LoginFlags3=Read Only, Dial back disabled
RSA_LoginFlags4=Read Only, Dial back disabled
RSA_LoginFlags5=Read Only, Dial back disabled
RSA_LoginFlags6=Read Only, Dial back disabled
RSA_LoginFlags7=Read Only, Dial back disabled
RSA_LoginFlags8=Read Only, Dial back disabled
RSA_LoginFlags9=Read Only, Dial back disabled
RSA_LoginFlags10=Read Only, Dial back disabled
RSA_LoginFlags11=Read Only, Dial back disabled
```

RSA\_LoginFlags12=Read Only, Dial back disabled  
RSA\_TemperatureAlert=Disabled  
RSA\_VoltageAlert=Disabled  
RSA\_TamperAlert=Disabled  
RSA\_MultipleFanFailureAlert=Disabled  
RSA\_PowerFailureAlert=Disabled  
RSA\_HardDriveAlert=Disabled  
RSA\_VRMFailureAlert=Disabled  
RSA\_RedundantPowerTriggeredAlert=Disabled  
RSA\_OneFanFailureAlert=Disabled  
RSA\_NonCriticalTemperatureAlert=Disabled  
RSA\_NonCriticalVoltageAlert=Disabled  
RSA\_POSTHangAlert=Disabled  
RSA\_OSHangAlert=Disabled  
RSA\_ApplicationLoggedErrorAlert=Disabled  
RSA\_SystemPowerOffAlert=Disabled  
RSA\_SystemPowerOnAlert=Disabled  
RSA\_SystemBootFailureAlert=Disabled  
RSA LoaderWatchdogFailureAlert=Disabled  
RSA\_PFAAlert=Disabled  
RSA\_PartitionNotificationAlert=Disabled  
RSA\_NetworkChangeNotificationAlert=Disabled  
RSA\_AlertRecipientStatus1=Invalid  
RSA\_AlertRecipientNotificationMethod1=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly1=Disabled  
RSA\_AlertRecipientStatus2=Invalid  
RSA\_AlertRecipientNotificationMethod2=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly2=Disabled  
RSA\_AlertRecipientStatus3=Invalid  
RSA\_AlertRecipientNotificationMethod3=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly3=Disabled  
RSA\_AlertRecipientStatus4=Invalid  
RSA\_AlertRecipientNotificationMethod4=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly4=Disabled  
RSA\_AlertRecipientStatus5=Invalid  
RSA\_AlertRecipientNotificationMethod5=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly5=Disabled  
RSA\_AlertRecipientStatus6=Invalid  
RSA\_AlertRecipientNotificationMethod6=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly6=Disabled  
RSA\_AlertRecipientStatus7=Invalid  
RSA\_AlertRecipientNotificationMethod7=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly7=Disabled  
RSA\_AlertRecipientStatus8=Invalid  
RSA\_AlertRecipientNotificationMethod8=Numeric pager

RSA\_AlertRecipientCriticalAlertsOnly8=Disabled  
RSA\_AlertRecipientStatus9=Invalid  
RSA\_AlertRecipientNotificationMethod9=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly9=Disabled  
RSA\_AlertRecipientStatus10=Invalid  
RSA\_AlertRecipientNotificationMethod10=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly10=Disabled  
RSA\_AlertRecipientStatus11=Invalid  
RSA\_AlertRecipientNotificationMethod11=Numeric pager  
RSA\_AlertRecipientCriticalAlertsOnly11=Disabled  
RSA\_AlertRecipientStatus12=Enabled  
RSA\_AlertRecipientCriticalAlertsOnly12=Disabled  
RSA\_POSTWatchdog=Disabled  
RSA\_OSWatchdog=Disabled  
RSA\_LoaderWatchdog=Disabled  
RSA\_LogFullNotification=75% Full Enabled, 100% Full Enabled  
RSA\_HostIPAddress1=9.42.171.238  
RSA\_GatewayIPAddress1=9.42.171.3  
RSA\_PPPIPAAddress1=0.0.0.0  
RSA\_HostIPSubnet1=255.255.255.0  
RSA\_DHCPAssignedHostIP1=0.0.0.0  
RSA\_DHCPAssignedGateway1=0.0.0.0  
RSA\_DHCPAssignedNetMask1=0.0.0.0  
RSA\_DHCPAssignedDHCPServer1=0.0.0.0  
RSA\_DHCPAssignedPrimaryDNS1=0.0.0.0  
RSA\_DHCPAssignedSecondaryDNS1=0.0.0.0  
RSA\_DHCPAssignedTertiaryDNS1=0.0.0.0  
RSA\_HostIPAddress2=192.96.1.1  
RSA\_GatewayIPAddress2=0.0.0.0  
RSA\_PPPIPAAddress2=255.255.255.255  
RSA\_HostIPSubnet2=255.255.255.255  
RSAString\_HostName1=ASMA00096B9E085C  
RSAString\_HostName2=  
RSAString\_LoginId1=USERID  
RSAString\_LoginId2=leitenberger  
RSAString\_LoginId3=  
RSAString\_LoginId4=  
RSAString\_LoginId5=  
RSAString\_LoginId6=  
RSAString\_LoginId7=  
RSAString\_LoginId8=  
RSAString\_LoginId9=  
RSAString\_LoginId10=  
RSAString\_LoginId11=  
RSAString\_LoginId12=

RSAStrIng\_Password1=  
RSAStrIng\_Password2=  
RSAStrIng\_Password3=  
RSAStrIng\_Password4=  
RSAStrIng\_Password5=  
RSAStrIng\_Password6=  
RSAStrIng\_Password7=  
RSAStrIng\_Password8=  
RSAStrIng\_Password9=  
RSAStrIng\_Password10=  
RSAStrIng\_Password11=  
RSAStrIng\_Password12=  
RSAStrIng\_AlertRecipientName1=  
RSAStrIng\_AlertRecipientNumber1=  
RSAStrIng\_AlertRecipientAlphanumericPagerPIN1=  
RSAStrIng\_AlertRecipientEmail Address1=  
RSAStrIng\_AlertRecipientPPPLogin1=  
RSAStrIng\_AlertRecipientPPPPassword1=  
RSAStrIng\_AlertRecipientName2=  
RSAStrIng\_AlertRecipientNumber2=  
RSAStrIng\_AlertRecipientAlphanumericPagerPIN2=  
RSAStrIng\_AlertRecipientEmail Address2=  
RSAStrIng\_AlertRecipientPPPLogin2=  
RSAStrIng\_AlertRecipientPPPPassword2=  
RSAStrIng\_AlertRecipientName3=  
RSAStrIng\_AlertRecipientNumber3=  
RSAStrIng\_AlertRecipientAlphanumericPagerPIN3=  
RSAStrIng\_AlertRecipientEmail Address3=  
RSAStrIng\_AlertRecipientPPPLogin3=  
RSAStrIng\_AlertRecipientPPPPassword3=  
RSAStrIng\_AlertRecipientName4=  
RSAStrIng\_AlertRecipientNumber4=  
RSAStrIng\_AlertRecipientAlphanumericPagerPIN4=  
RSAStrIng\_AlertRecipientEmail Address4=  
RSAStrIng\_AlertRecipientPPPLogin4=  
RSAStrIng\_AlertRecipientPPPPassword4=  
RSAStrIng\_AlertRecipientName5=  
RSAStrIng\_AlertRecipientNumber5=  
RSAStrIng\_AlertRecipientAlphanumericPagerPIN5=  
RSAStrIng\_AlertRecipientEmail Address5=  
RSAStrIng\_AlertRecipientPPPLogin5=  
RSAStrIng\_AlertRecipientPPPPassword5=  
RSAStrIng\_AlertRecipientName6=  
RSAStrIng\_AlertRecipientNumber6=  
RSAStrIng\_AlertRecipientAlphanumericPagerPIN6=

```
RSAStrng_AlertRecipientEmailAddress6=  
RSAStrng_AlertRecipientPPPLogin6=  
RSAStrng_AlertRecipientPPPPassword6=  
RSAStrng_AlertRecipientName7=  
RSAStrng_AlertRecipientNumber7=  
RSAStrng_AlertRecipientAlphanumericPagerPIN7=  
RSAStrng_AlertRecipientEmailAddress7=  
RSAStrng_AlertRecipientPPPLogin7=  
RSAStrng_AlertRecipientPPPPassword7=  
RSAStrng_AlertRecipientName8=  
RSAStrng_AlertRecipientNumber8=  
RSAStrng_AlertRecipientAlphanumericPagerPIN8=  
RSAStrng_AlertRecipientEmailAddress8=  
RSAStrng_AlertRecipientPPPLogin8=  
RSAStrng_AlertRecipientPPPPassword8=  
RSAStrng_AlertRecipientName9=  
RSAStrng_AlertRecipientNumber9=  
RSAStrng_AlertRecipientAlphanumericPagerPIN9=  
RSAStrng_AlertRecipientEmailAddress9=  
RSAStrng_AlertRecipientPPPLogin9=  
RSAStrng_AlertRecipientPPPPassword9=  
RSAStrng_AlertRecipientName10=  
RSAStrng_AlertRecipientNumber10=  
RSAStrng_AlertRecipientAlphanumericPagerPIN10=  
RSAStrng_AlertRecipientEmailAddress10=  
RSAStrng_AlertRecipientPPPLogin10=  
RSAStrng_AlertRecipientPPPPassword10=  
RSAStrng_AlertRecipientName11=  
RSAStrng_AlertRecipientNumber11=  
RSAStrng_AlertRecipientAlphanumericPagerPIN11=  
RSAStrng_AlertRecipientEmailAddress11=  
RSAStrng_AlertRecipientPPPLogin11=  
RSAStrng_AlertRecipientPPPPassword11=  
RSAStrng_AlertRecipientName12=X345DIRSERVER  
RSAStrng_AlertRecipientNumber12=9.42.171.237  
RSAStrng_AlertRecipientAlphanumericPagerPIN12=  
RSAStrng_AlertRecipientEmailAddress12=  
RSAStrng_AlertRecipientPPPLogin12=  
RSAStrng_AlertRecipientPPPPassword12=  
RSAKeystroke_EnterCLISequence='ESC' '('  
RSAKeystroke_ExitCLISequence='ESC' 'Q'
```

---

## 6.2.7 ASU を使用した RSA または RSA II 設定の構成

ASU を使用して、直接 RSA または RSA II を構成できます。ユーティリティーを使用する前に、必ず RSA/RSA II の定義ファイルとデバイス・ドライバーをインストールしてください。デバイス・ドライバーのインストールについては、69 ページの 3.4.4、『デバイス・ドライバーのインストール』を参照してください。

### 例：RSA II の IP アドレス設定の構成

RSA II は、アダプターのイーサネット・コネクタを通してアダプターにリモート・アクセスできるように構成することが必要です。この構成を ASU を使用してコマンド・ラインから実行する方法を示します。

**注：**Linux オペレーティング・システムを使用している場合は、必ず `asu` の前に `./` を入力してください。

サーバー上で、ASU ユーティリティーを解凍して該当する定義ファイルのパッチを当てたディレクトリーから、次のコマンドを入力します。

▶ **asu show RSA\_HostIPAddress1**

サービス・プロセッサの IP アドレスの値を表示します。このコマンドから受け取った出力は、次のとおりです。

```
RSA_HostIPAddress1=9.42.171.238
```

▶ **asu showvalues RSA\_HostIPAddress1**

すべての可能な値タイプを表示します。受け取った出力は、次のとおりです。

```
RSA_HostIPAddress1=x.x.x.x where (x is 0-255)
```

▶ **asu set RSA\_HostIPAddress1 xxx.xxx.xxx.xxx**

IP アドレスの値を、指定した値に変更します。

▶ **set RSA\_DHCP1 disabled**

DHCP を使用不可にして、固定アドレスを使用します。

他のパラメーターの設定については、177 ページの例 6-1 リストを参照してください。設定できるその他の関連パラメーターとして、次のものがあります。

```
RSA_Network1 enabled|disabled
RSA_HostIPsubnet1 xxx.xxx.xxx.xxx
RSA_GatewayIPAddress1 xxx.xxx.xxx.xxx
RSA_KLANSDataRate1 "100M Ethernet"
RSA_Duplex1 Half|Full|Auto
```

▶ **asu rebootrsa**

完了した後、RSA を再始動すると、構成の変更が有効になります。

▶ **exit**

ASU ユーティリティーを終了します。

## 6.2.8 ASU バッチ・コマンド

ASU **batch** コマンドを使用すると、ユーティリティーの操作のスク립トを記述できます。スク립ト・ファイルの構文は、オペレーティング・システムから独立しています。

バッチ・コマンドの構文は、**asu batch *commandfile*** です。ここで、*commandfile* は、**asu** コマンドのリストが入っているファイルの名前です。

**ヒント:** コマンド・ファイルの各行の先頭に **asu** を含めないでください。

バッチ・ファイルで **batch** コマンドを使用している場合、**stdout** と **stderr** に送られる出力は、バッチ・ファイル内のすべてのコマンドの出力の集合になります。バッチ・ファイル内のそれぞれのコマンドの出力は、大括弧で囲われた **asu** コマンドが先行して表示されます。185 ページの例 6-2 を参照してください。

例 6-2 *asu* バッチ・コマンドからの *stdout* のレイアウト

---

```
[command1]
command 1 の出力
[command 2]
command 2 の出力
.
[command n ]
command n の出力
```

---

例えば、この例で使用したコマンド・ファイル *showboot.txt* は、次の行が含まれます (例 6-3)。

例 6-3 コマンド・ファイル *showboot.txt*

---

```
show CMOS_PrimaryBootDevice1
show CMOS_PrimaryBootDevice2
show CMOS_PrimaryBootDevice3
show CMOS_PrimaryBootDevice4
```

---

次のコマンドを実行すると、例 6-4 にリストしたような出力が表示されます。

```
asu batch showboot.txt
```

```
[show CMOS_PrimaryBootDevice1]
CMOS_PrimaryBootDevice1=CD ROM
[show CMOS_PrimaryBootDevice2]
CMOS_PrimaryBootDevice2=Diskette Drive 0
[show CMOS_PrimaryBootDevice3]
CMOS_PrimaryBootDevice3=Hard Disk 0
[show CMOS_PrimaryBootDevice4]
CMOS_PrimaryBootDevice4=Network
```

---

ASU の使用例については、264 ページの 7.6、『RSA II の出荷時のデフォルト値へのリセット』、および 269 ページの 7.7、『リモート側での ASU の使用法』を参照してください。

## 6.3 管理プロセッサ・コマンド・ライン・インターフェース

IBM 管理プロセッサ・コマンド・ライン・インターフェース (MPCLI) は、Windows または Linux を実行する xSeries サーバーの管理ツールです。システム管理機能は、サーバー内のサービス・プロセッサに接続されるコマンド・ライン・インターフェース (CLI) から提供されます。

この CLI を使用して、システム・ヘルス、構成、通信、状態など、幅広い情報にアクセスし、設定できます。こうした機能は、CLI をインストールしてサービス・プロセッサに接続すると、すぐに利用できるようになります。

リモート・サービス・プロセッサの IP アドレスを知っており、有効なユーザー ID とパスワードを持っていれば、リモート・サーバー上でも MPCLI を使用できます。サービス・プロセッサとの通信に使用できる、3 つの方式がサポートされています。

- ▶ デバイス・ドライバを使用したインバンド通信
- ▶ IP 接続を使用したアウト・オブ・バンド通信
- ▶ RS-485 インターコネクトを使用したアウト・オブ・バンド通信

### 6.3.1 サポートされるサービス・プロセッサ構成

MPCLI は、次のサービス・プロセッサの少なくとも 1 つを備えているシステムでのみサポートされます。

- ▶ システム管理プロセッサ
- ▶ ASM PCI アダプター
- ▶ 内蔵システム管理プロセッサ



- ▶ BladeCenter 管理モジュール
- ▶ Remote Supervisor Adapter
- ▶ Remote Supervisor Adapter II

**制約事項** : Remote Supervisor Adapter II SlimLine と Remote Supervisor Adapter II-EXA は、現在は MPCLI によってサポートされていません。

サービス・プロセッサとサーバーの組み合わせがサポートされていることも確認する必要があります。この情報は、188 ページの表 6-4 にリストされています。

この表には、サービス・プロセッサの構成に応じて得られる種々のレベルのサポートもリストされています。表の項目の説明は、次のとおりです。


- ▶ **完全** : サーバーで使用可能な、システム管理ハードウェアに関連したすべての機能をサポートします。
- ▶ **互換性** : コマンド・ライン・インターフェースの現行機能をサポートします。サーバーまたはコマンド・ライン・インターフェースに追加される新機能をサポートする計画はありません。
- ▶ **SP 構成** : サービス・プロセッサ構成。サービス・プロセッサ構成のみをサポートします。サービス・プロセッサがシステム・ハードウェアにアクセスできないためです。
- ▶ **非サポート** : MPCLI はこの構成をサポートしません。
- ▶  (グレーの陰影付けのブランク・セル) : サーバーはこの特定サービス・プロセッサをサポートしないため、サポートの記述は適用外です。

表 6-4 は、サーバーとサービス・プロセッサのサポートされる構成をリストしています。

**注** : 表には ASM PCI アダプターに対するサポートはリストされていません。

Netfinity サーバーと新しい xSeries サーバーのサポートされる構成については、サポートされるサーバーのリストを参照してください。

<http://www.ibm.com/pc/support/site.wss/MIGR-54216.html>

サポートされるサーバーのリストは、次のサイトから入手できる最新版の「MPCLI User Guide」にも記載されています。

<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>

表 6-4 MPCLI のサポートされる構成

xSeries サーバー	ISMP	BMC	ASMP	RSA	RSA II	BCMM
xSeries 220				互換性		
xSeries 225				互換性	非サポート	
xSeries 230			互換性			
xSeries 232	互換性			互換性		
xSeries 235	互換性			非サポート	互換性	
xSeries 236		非サポート				
xSeries 240			互換性			
xSeries 250			互換性			
xSeries 255	互換性			互換性	互換性	
xSeries 305				SP 構成	非サポート	
xSeries 306					非サポート	
xSeries 330			互換性	互換性		
xSeries 335	互換性			非サポート	互換性	
xSeries 336		非サポート				
xSeries 340			互換性			
xSeries 342	互換性			互換性		
xSeries 345	互換性			完全	互換性	
xSeries 346		非サポート				
xSeries 350			互換性			
xSeries 360				完全		
xSeries 365					非サポート	
xSeries 366		非サポート				
xSeries 440				完全		
xSeries 445				完全		
xSeries 450				互換性		
xSeries 455				完全		

xSeries サーバー	ISMP	BMC	ASMP	RSA	RSA II	BCMM
BC MM						完全
HS20	非サポート					完全
HS40	非サポート					完全

## 6.3.2 機能

MPCLI は、以下の機能を備えています。

- ▶ システム・コンポーネントの重要プロダクト・データ (VPD) の照会
  - BladeCenter 格納装置 (スイッチ・モジュールを含む)
  - キャッシュの干渉性
  - シャーシ/格納装置
  - CPU および CPU EEPROM
  - 診断
  - ハード・ディスク・バックプレーンおよびシステム・ボード
  - DIMM
  - パワー・サブライおよびバックプレーン
  - サービス・プロセッサのデバイス・ドライバ、ファームウェア、およびハードウェアの更新
  - システム・スロット
  - POST/BIOS
- ▶ Light Path 診断を使用したコンポーネント LED の照会
  - BladeCenter 格納装置
  - CD-ROM ドライブとハード・ディスクのケーブル
  - センタープレーン、メモリー、およびアダプター
  - チップおよびチップ・セット VRM
  - CPU および CPU キャッシュ
  - 診断およびフロント・パネル
  - 拡張装置、ファン、拡張容易性ポート、システム・ボード、および VRM
  - メモリー、メモリー・ホット・プラグ可能、およびメモリー・サブシステム
  - PCI バスおよび PCI アダプター
  - サービス・プロセッサのアダプターとスロット
- ▶ サービス・プロセッサ構成の表示および変更
  - 再始動
  - ネットワーク・インターフェース : SNMP、PPP、および IP
  - シリアル・ポートのハードウェアとソフトウェア
  - 汎用 ID
  - VPD

- 内部クロック
- アラート・ダイヤルアウト設定
- ダイヤルイン入力
- ▶ イベント・ログの表示
  - BIOS
  - 診断
  - POST
  - サービス・プロセッサ
- ▶ システムのサーバー・タイムアウトの照会または設定
  - オペレーティング・システム・ローダー
  - オペレーティング・システム・ハートビート
  - POST
  - パワーオフ遅延
- ▶ システム・ヘルスおよび環境情報の表示
  - システム・ボードの電圧としきい値
  - VRM の電圧
  - パワー・サプライの電圧
  - コンポーネントの温度としきい値
- ▶ リモート側でのシステム電源オン/オフの機能
  - 即時電源オフとオペレーティング・システム・シャットダウン
  - 即時再始動とオペレーティング・システム・シャットダウン
  - 即時 / 指定の遅延後 /n 秒後の電源オン
- ▶ システムの一般状態情報の照会
  - システム状態の安定 / 不安定
  - システム電源のオン / オフ
  - 再始動の回数
  - 電源オンの時間数
  - Universal unique ID (UUID)
  - 青色の表示ライトのオン / オフ
  - Light Path LED 機能中
- ▶ 使用または再使用される複数のコマンドを含むスクリプトの作成。スクリプトを実行すると、その中の各コマンドが実行されます。
- ▶ 構成できる機能
  - LDAP
  - Serial over LAN (SOL)
  - シリアル・ポート
  - コマンド・モード・インターフェース

- ▶ 詳細な権限
  - HTTP をリセットする権限
  - コマンド・モード・ポートの可用性を確認する権限
  - ホスト・オペレーティング・システムの取得と設定の権限
  - 管理モジュール・シャーシ VPD を検索する権限
  - プロセッサ・ブレード・アセンブリーを検索する権限。ブレード・アセンブリーは、ユーザーがプロセッサ・スロットに追加または除去する、結合された単一ユニットを表します。

### 6.3.3 制限

MPCLI は、Linux 環境では次のような制限があります。

- ▶ インストールのデフォルト・ロケーションは /opt/IBMmpcli/ directory から変更できません。
- ▶ CLI を開始した後、上矢印 / 下矢印キーを使用してコマンドを再呼び出しできません。

### 6.3.4 MPCLI のサポートされるプラットフォーム

MPCLI は、次のプラットフォームでサポートされます。

- ▶ Red Hat 2.1 AS、WS、ES
- ▶ Red Hat 3.0 AS、WS、ES
- ▶ SUSE LINUX Enterprise Server 8.0 (SP3)
- ▶ Microsoft Windows 2000 Server (SP3 以降)
- ▶ Microsoft Windows 2000 Professional (SP3 以降)
- ▶ Microsoft Windows 2000 AS (SP3 以降)
- ▶ Microsoft Windows XP Professional (SP1 以降)
- ▶ Microsoft Windows Server 2003、Standard Edition
- ▶ Microsoft Windows Server 2003、Enterprise Edition

最新のサポートされるオペレーティング・システム・プラットフォームについては、「*MPCLI User's Guide*」を参照してください。これは、次のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>

### 6.3.5 MPCLI のインストール

このセクションでは、Windows および Linux プラットフォームでの MPCLI のインストール方法について説明します。

次のサイトから MPCLI をダウンロードします。

<http://www.ibm.com/pc/support/site.wss/MIGR-54216.html>

Windows 版と Linux 版の両方ともこのサイトから入手できます。

## Windows オペレーティング・システム上のインストール

コマンド・ライン・インターフェースは、InstallShield ウィザードを使用してインストールすることもできますし、無人でインストールを実行することもできます。

InstallShield を使用したインストールは、他の標準的な Windows のインストールと同じです。

無人（サイレント）インストールを実行するには、上記の URL からインストール・プログラムをダウンロードして一時ディレクトリに保管し、次のコマンドを実行して、MPCLI をインストールします。

```
26r0684.exe /S /v/qn
```

インストールが正常に完了したことを知らせるメッセージは受け取らないことに注意してください。

インストールした後、MPCLI を開始するために、「スタート」→「プログラム」→「IBM」→「MPCLI」をクリックします。

## Linux オペレーティング・システム上のインストール

インストールを開始する前に、次の事項に注意してください。

- ▶ V1 または V2 から V3 へのアップグレード・パスはありません。シェル・プロンプトで次のコマンドを入力して、前にインストールしたものをアンインストールする必要があります。

```
rpm -e mpcli
```

- ▶ ユーザーが root ユーザーでない場合、または root ユーザー・グループのメンバーでない場合、コマンド・ライン・インターフェースのインストールやアンインストールを実行できない場合があります。

MPCLI をインストールするには、シェル・プロンプトから次のコマンドを実行します。

```
rpm -ivh mpcli-2.0-1.0.i386.rpm
```

インストールが完了した後、次のコマンドを入力して MPCLI の使用を開始します。

```
/opt/IBMmpcli/bin/MPCLI.bsh
```

ユーザーは、root ユーザーであるか、root ユーザー・グループのメンバーであることが必要です。MPCLI を開始したときにエラーが戻された場合は、スクリプト・ファイルの実行許可を持っていない可能性があります。実行許可を追加するには、シェル・プロンプトで `chmod +x MPCLI.bsh` と入力します。

## 6.3.6 MPCLI の使用

**注:** MPCLI を使用してリモート管理する場合、サービス・プロセッサのログイン信用証明情報を知っている必要があります。

- ▶ IP アドレス
- ▶ ユーザー ID
- ▶ パスワード

Windows 環境で MPCLI を開始するには、「スタート」→「プログラム」→「IBM」→「MPCLI」をクリックします。Linux 環境では、次のコマンドを入力します。

```
/opt/IBMmpcli/bin/MPCLI.bsh
```

これにより、MPCLI プロンプトが表示され、コマンドを受け入れる準備ができます。

```
mp>
```

Linux 環境では、ユーザーは root ユーザー、または root ユーザー・グループのメンバーのいずれかでなければなりません。

MPCLI を使用して、システム上のサービス・プロセッサまたはシステムに接続されたサービス・プロセッサにログオンし、システム・ヘルスおよび構成の管理とモニター、システム状況に関する情報の照会、あるいはシステムの動作パラメーターの設定を行うことができます。

### コマンド構文

コマンドはすべて、次のような基本構造を持っています。

```
command -option parameter
```

同じコマンドを繰り返し入力しなくても済むように、コマンドには 1 行に複数のオプションを追加します。例えば、次のように指定します。

```
command -option1 parameter -option2 parameter -option3 parameter
```

各オプションに対する情報は、入力された順序で戻され、それぞれ別の行に表示されます。

主要な構文規則は、次のとおりです。

- ▶ コマンドとオプションはすべて小文字で、大文字小文字の区別をします。ただし、ブール・パラメーター (**true** と **false**) およびストリング・パラメーターは大 / 小文字の区別をしません。
- ▶ スペースを含むストリング・パラメーターは、“Lesley Bain” のように、二重引用符で囲む必要があります。ストリングの最大長さは 15 文字 (スペースを含めて) です。長さが 15 文字を超えるストリング値は、切り捨てられます。

ヒント: MPCLI V3 は、SMASH コマンド・ライン・プロトコル (CLP) 構文もサポートします。「*MPCLI User's Guide*」に、サポートされる特定の SMASH コマンドが説明されています。SMASH についての詳細は、次のサイトを参照してください。

<http://www.dmtf.org/standards/smash>

## 既知の問題点

コマンド・ライン・インターフェースには現在、次のような問題点があります。

- ▶ RS-485 インターコネクトを使用してリモート・サービス・プロセッサにログオンした場合、一定期間活動が途絶えると、接続が失われることがあります。
- ▶ **setmpclock -gmtoffset** コマンドを使用しているときに、-12 から +12 の範囲外の無効なパラメーターを使用した場合、コマンドは失敗したにもかかわらず、コマンドが正常に実行されたことを示すメッセージが表示されることがあります。
- ▶ リモート管理アダプターにログオンしてコマンド・ライン・インターフェースを実行している場合、RS-485 インターコネクトでの内蔵システム管理プロセッサへのログオンに失敗すると、コマンド・ライン・インターフェースがすべての機能を失うことがあります。コマンド・ライン・インターフェースを再始動し、再度ログオンすることが必要になります。
- ▶ **setsmnetwork** コマンドを使用しているときに、いずれかのオプションを使用して変更を行った場合、**setsmnetwork -enable** コマンドが **true** に設定されていても (保留されている変更を適用するはずですが)、変更が保留状態のままになります。代わりに、**setsmnetwork -enable true** を入力すると、コマンドの送信に問題があったことを示すメッセージが戻されることがあります。
- ▶ x455 サーバーでは、**logonlocal** コマンドはサポートされません。
- ▶ IBM BladeCenter 内のプロセッサ・ブレードでは、管理モジュールを再始動しないと、変更されたテキスト ID は適用されません。ブレード・サー



バーで **setmpid** コマンドを使用するたびに、その後にブレード・サーバーに対して **restartmp** コマンドを実行する必要があります。

- ▶ ASM サービス・プロセッサの場合、**getvpd -postbios** および **getlightpath** コマンドは、誤ったエラーを報告するためサポートされません。

## サービス・プロセッサへのログイン

MPCLI の使用を開始する前の最初のタスクは、管理するサービス・プロセッサにログインすることです。このタスクを実行するには、さまざまな方法があります。

**重要:** 他のサービス・プロセッサへの複数のログインが許可されます。ただし、別のサービス・プロセッサにアクセスするまでは、実行されるコマンドはすべて、最新にアクセスしたサービス・プロセッサに影響を与えません。

- ▶ ローカル・サービス・プロセッサへのログオンは、次のコマンドを入力します。

```
logonlocal
```

- ▶ イーサネット・ネットワーク経由のアウト・オブ・バンドのログオンは、アドレス、ユーザー ID、およびパスワードを指定します。

```
logonip -hostname hostname -userid userid -password password
```

例えば、次のように指定します。

```
logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
```

- ▶ ASM インターコネクト・ネットワーク (RS-485) 経由のアウト・オブ・バンドのログオン。

RS-485 接続を介してサービス・プロセッサにログオンする前に、**logonlocal** または **logonip** を使用して、ゲートウェイ・サービス・プロセッサに接続する必要があります。

ゲートウェイ装置にログオンした後、次のコマンドを実行して、RS-485 を介して接続されている他のサービス・プロセッサのリストを表示します。

```
logonrs485 -query
```

**query** コマンドからの結果を使用して、次のようにインデックス番号またはリモート・サービス・プロセッサの名前を指定して、リモート・サービス・プロセッサに接続できます。

```
logonrs485 -index RSindex -userid userid -password password
```

```
logonrs485 -name RSname -userid userid -password password
```

ここで、*RSindex* は、**-query** コマンドによって戻された装置の番号で、*RSname* は装置の名前です。

**ヒント** : ISM プロセッサにログオンする場合は、**-userid** と **-password** パラメーターは必要ありません。

- ▶ RXE-100 内のサービス・プロセッサにログオンするには、**logonrx** コマンドを使用します。
  - **logonrx -query** - システムに接続された RXE-100 拡張装置のリストを入手します。
  - **logonrx -index RXindex -query** コマンドの出力から入手したインデックスを指定して、IBM RXE-100 拡張装置にログオンします。

現行セッションからログオフして、サービス・プロセッサから切断するには、次のコマンドを入力します。

logoff

## コマンド

以下のコマンドは、MPCLI の動作を制御します。これらのコマンドは、アプリケーションの出力と機能に影響を与えますが、サービス・プロセッサには直接影響を与えません。

表 6-5 MPCLI の動作を制御するためのメタ・コマンド

コマンド	説明
<b>help</b>	使用可能なヘルプ・コマンドを表示します。
<b>help-cli</b>	アプリケーション制御のログオンおよびログオフ・コマンドを表示します。
<b>help-cmd</b>	サービス・プロセッサにログオンした後に使用可能なすべてのコマンドを表示します。
<b>help-cmd <i>command</i></b>	指定されたコマンド名のすべてのコマンドを表示します。
<b>verbose</b>	デバッグ情報をオン/オフに切り替えます。デバッグは、コマンドの成功や失敗に関する詳細など、追加情報を提供します。デフォルトでは、 <b>verbose</b> は <b>off</b> です。
<b>sleep <i>milliseconds</i></b>	メイン実行スレッドが、指定された期間 (ミリ秒数) スリープ・モードに入ることを許可します。
<b>exit</b>	サービス・プロセッサへの接続をクローズして、プログラムを終了します。

コマンド	説明
<b>connectionblocks</b>	logon/logoff ブロック内でコマンドのグループ化を切り替えます。connectionsblocks が enabled のときに、logon が失敗した場合、logoff が検出されるまですべてのコマンドが無視されます。この機能は、主としてスクリプト記述に使用されます。

MPCLI コマンドの詳しい説明は、「*MPCLI User's Guide*」に記載されています。これは、次の URL から入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>

MPCLI コマンドは、次のグループに分けることができます。

- ▶ **BladeCenter 格納装置コマンド**  
BladeCenter によってサポートされる機能の読み取りと構成に使用されます。
- ▶ **ネットワーク・インターフェース・コマンド**  
SNMP、PPP、IP、ネットワーク・ハードウェア、DHCP、および DNS など、ネットワーク・プロトコルおよびハードウェアの構成に使用されます。
- ▶ **シリアル・ポート構成コマンド**  
シリアル・ポートのハードウェアおよびソフトウェア構成の読み取り / 書き込みアクセスを使用可能にするのに使用されます。
- ▶ **サービス・プロセッサ構成コマンド**  
サービス・プロセッサのクロック（テキスト ID）の読み取りと設定、ファームウェアの更新、デフォルト構成へのリセット、およびサービス・プロセッサの再始動を可能にします。
- ▶ **サービス・プロセッサ・イベント・コマンド**  
ダイヤルアウト / ダイヤルイン・アラート構成設定の読み取りと変更、イベント・ログの読み取りと消去に使用できます。また、サービス・プロセッサのアラート・トリガーの読み取り、使用可能化、または使用不可化にも使用できます。
- ▶ **システム電源コマンド**  
サーバー・タイムアウト、リモート電源制御、プリブート実行環境（PXE）リブートなど、システム電源オプションの読み取りまたは設定に使用できます。
- ▶ **システム統計コマンド**  
システム統計（サービス・プロセッサによって維持）の表示、青色の表示ライト機能の設定、および Light Path 診断状態の表示に使用します。

- ▶ システム・コンポーネント・コマンド  
サービス・プロセッサがモニターしているシステム・コンポーネント（メモリー、パワー・サプライ、ハード・ディスク・バックプレーン、プロセッサなど）に関する情報を提供します。
- ▶ システム・ヘルスおよび環境コマンド  
電圧、温度、ファン速度など、システム・ヘルスおよび環境情報を提供します。サービス・プロセッサがモニターしているシステム・ハードウェアの現行値としきい値にアクセスできます。

## MPCLI コマンドを使用したスクリプト記述

各コマンドを一度に1つずつ入力する代わりに、スクリプトを使用できます。例えば、サービス・プロセッサへのログインを容易にするには、ログオン・スクリプトを作成して、ホスト名、ユーザー ID、およびパスワードを繰り返し入力しなくても済むようにします。

スクリプトは、1行に1つのコマンドが記述されたテキスト・ファイルです。ファイルには、任意のファイル名と拡張子を付けることができます。スクリプトは、テキスト・エディターを使用して作成することもできますし、次のコマンドを使用して、MPCLI をレコード・モードに入れて作成することもできます。

```
commandfile outputfilename
```

ここで、*outputfilename* は、作成するスクリプト・ファイルの完全修飾名です。スクリプトの記録を停止するには、次のコマンドを発行して、スクリプト・コマンドの書き込みを停止します。

```
commandfile
```

スクリプトを作成した後は、MPCLI 内から次のコマンドを使用して呼び出すことができます。

```
inputfile inputfilename
```

ここで、*inputfilename* は、実行するスクリプト・ファイルの完全修飾名です。

また、スクリプトに記述されたコマンドの出力を表示する場所も制御できます。

- ▶ **outfile *outputfilename*** - 後続のコマンドの出力を、コマンド・ウィンドウではなく、指定されたファイルに転送します。失敗も含めて、すべての

結果が出力ファイルに取り込まれるため、MPCLI ウィンドウにはそれ以上のメッセージは表示されません。

- ▶ **resetoutput** - コマンド出力を、**outputfile** コマンドで指定された出力ファイルからコマンド・ウィンドウに戻します。

## MPCLI サンプル・スクリプト

以下のサンプル・スクリプトは、ユーザーの要件に合わせて変更して使用することもできますし、ユーザー独自のスクリプトを作成するための参考として利用することもできます。以下のサンプル・スクリプトでは、パラメーターは例に過ぎません。ご使用の環境に固有のパラメーターを選択して使用してください。

**注:** コマンドを操作するには、サービス・プロセッサにログオンする必要があります。

コマンドの詳しい解説は、「*MPCLI User's Guide*」を参照してください。

### ネットワーク・ハードウェア構成を取得して設定する

図 6-2 は、ネットワーク・ハードウェア構成を取得して設定するスクリプトを示しています。

```
outputfile ./enetcfgresults.txt
getmpid
getmpclock
setnethw -interface 1 -enabled false
setdhcp -enabled false
setnethw -interface 1 -linetype "ENET" -enabled true
setip -interface 1 -hostname X
setip -interface 1 -ipaddress 9.67.37.00
setip -interface 1 -subnet 255.255.255.128
setnethw -interface 1 -datarate "AUTO"
setnethw -interface 1 -duplex "AUTO"
setnethw -interface 1 -adminmac "00 00 00 00 00 00"
setnethw -interface 1 -gateway 9.67.37.1
setnethw -interface 1 -enabled true
resetoutput
restartmp
```

図 6-2 ネットワーク・ハードウェア構成を取得して設定するスクリプト

### ログオンしてサービス・プロセッサ情報を取得する

図 6-3 は、ログオンして SP 情報を取得するスクリプトを示しています。

```
outputfile ./getaccess.txt
logonip -hostname SPbatman -userid gisellem -password s0ngb1rd
getmpid -text
getmpclock -timeanddate
getdialinentry -index 12
logoff
exit
```

図 6-3 ログオンして SP 情報を取得するスクリプト

### **サービス・プロセッサ情報を取得してログに記録する**

200 ページの図 6-4 は、SP 情報を取得してログに記録するスクリプトを示しています。

```
outputfile ./mplog.txt
getmpid
getmpclock
getmplog -first
getmplog -all
resetoutput
```

図 6-4 SP 情報を取得してログに記録するスクリプト

### **さまざまなポリシーを取得して設定し、開始オプションを設定する**

図 6-5 は、ポリシーを取得して設定し、BladeCenter シャーシ内のオプションを開始するスクリプトを示しています。

```
getpbpolicy -localpower 2
setpbpolicy -localpower 2,false
getpbpolicy -localpower 2
setpbpolicy -localpowerall true
getpbpolicy -localpower 2
getpbpolicy -localkvm 2
setpbpolicy -localkvm 2,false
getpbpolicy -localkvm 2
setpbpolicy -localkvmall true
getpbpolicy -localkvm 2
getpbpolicy -localusb 2
setpbpolicy -localusb 2,false
getpbpolicy -localusb 2
setpbpolicy -localusball true
getpbpolicy -localusb 2
bootoptions -get 2
bootoptions -set 2,"pxe,cdrom,floppy"
bootoptions -get 2
getkvm
setkvm -owner 2
getkvm
setkvm -park
getkvm
```

図 6-5 ポリシーを取得して設定し、BladeCenter シャーシ内のオプションを開始するスクリプト

### ログオンしてサービス・プロセッサをフラッシュする

202 ページの図 6-6 は、ログオンして、イーサネット経由でサービス・プロセッサをフラッシュするスクリプトを示しています。

```

outputfile ./rsaflash.txt
logonip -hostname 192.168.1.100 -userid gisellem -password s0ngblrd
getmpid -text
getvpd -mpboot
getvpd -mprom
fwupdate -mn d:¥firmware¥x220¥batman¥CNETMNUS.PKT
logoff
sleep 15000
logonip -hostname 192.168.1.100 -userid gisellem -password s0ngblrd
fwupdate -br d:¥firmware¥x220¥batman¥CNETBRUS.PKT
logoff
sleep 15000
logonip -hostname 192.168.1.100 -userid gisellem -password s0ngblrd
fwupdate -vnc d:¥firmware¥x220¥batman¥CNETRGUS.PKT
logoff
exit

```

図 6-6 ログオンして、イーサネット経由でサービス・プロセッサをフラッシュするスクリプト

### ログオンしてユーザー ID を作成する

図 6-7 は、ログオンして、ダイヤルイン構成を設定するスクリプトを示しています。

```

outputfile ./setaccess.txt
logonip -hostname svcprocella -userid gisellem -password s0ngblrd
getmpid -text
getmpclock -timeanddate
setdialinentry -index 12 -id gisellem -password s0ngblrd -readonly
false
logoff
exit

```

図 6-7 ログオンして、ダイヤルイン構成を設定するスクリプト

### スイッチ・モジュール構成を取得して設定する

203 ページの図 6-8 は、スイッチ・モジュール構成を取得して設定するスクリプトを示しています。



```

getsmnetwork -currentconfig 1
getsmnetwork -currentmethod 1
getsmnetwork -pendingconfig 1
getsmnetwork -pendingmethod 1
switchmodule -getpoweron 1
switchmodule -getmemdiagson 1
switchmodule -getcfgotherports 1
switchmodule -gettextportson 1
switchmodule -ping 1
switchmodule -getpostresults 1
setsmnetwork -ipaddress 1, 192.168.1.125
setsmnetwork -gateway 1, 192.168.1.126
setsmnetwork -subnet 1,255.255.255.0
setsmnetwork -method 1, "static"
setsmnetwork -pending 1,false
setsmnetwork -pending 1,true
switchmodule -setpoweron 1,true
switchmodule -setmemdiagson 1,true
switchmodule -setcfgotherports 1,true
switchmodule -settextportson 1,true
switchmodule -ping 1
switchmodule -getpostresults 1

```

図 6-8 スイッチ・モジュール構成を取得して設定するスクリプト

## ネストされたスクリプトの作成

MPCLI は、ネストされたスクリプトに対応しています。つまり、スクリプトの内部から別のスクリプトを呼び出すことができます。この方法の利点は、1 つのスクリプトを複数の大きいスクリプトの中に入れることができ、スクリプト・ライブラリー全体の管理が容易になることです。例えば、サービス・プロセッサへのアクセスに使用するユーザー ID のパスワードを定期的に変更する場合、この情報はスクリプトのライブラリーとは別のファイルに保管すると便利です。サーバー FILE1 のサービス・プロセッサにログオンするためのスクリプトは、図 6-9 のようになります。

```
logonip -hostname file1sp -userid USERID -password PASSWORD
```

図 6-9 スクリプト・ファイル logon-file1.txt

ご使用のシステムごとに別々のログオン・スクリプトを作成します。その後、それぞれの管理スクリプトで、このスクリプトを呼び出すだけです。たとえば、複数のサービス・プロセッサをフラッシュするには、202 ページの図 6-6 のスクリプトを図のように変更できます（変更された行が強調表示されています）。

```
outputfile ./rsaflash.txt

getmpid -text
getvpd -mpboot
getvpd -mprom
fwupdate -mn d:¥firmware¥x220¥batman¥CNETMNUS.PKT
logoff
sleep 15000

fwupdate -br d:¥firmware¥x220¥batman¥CNETBRUS.PKT
logoff
sleep 15000

fwupdate -vnc d:¥firmware¥x220¥batman¥CNETRGUS.PKT
logoff
exit
```

図 6-10 ログオンして、イーサネット経由でサービス・プロセッサをフラッシュするスクリプト

後でパスワードを変更した場合、ログオン・スクリプトを更新するだけで済みます。

## 6.4 OSA SMBridge ユーティリティー

OSA System Management Bridge (SMBridge) は、BMC サービス・プロセッサが搭載されたサーバー上で、特定のリモート管理機能を実行できるユーティリティーです。このユーティリティーは、IPMI1.5 プロトコルおよび Serial Over LAN (SOL) プロトコルを使用して、サーバーのイーサネットまたはシリアル・インターフェースを介してサーバーを管理します。SMBridge の主な機能は、イーサネット経由でテキスト・モード・コンソールをリモート制御することです。

サポートされる xSeries サーバーは、BMC コントローラーを搭載したサーバーです (2 ページの表 1-1 のリストを参照)。

SMBridge ユーティリティーを使用するには、2 つの方法があります。すなわち、Telnet サーバーとして使用する方法と、BMC への直接コマンド・ライン・イン

ターフェースとして使用する方法です。この2つの方法が、206 ページの図 6-11 に示されています。

▶ **Telnet サーバー接続**

Telnet サーバーとして使用する場合、SMBridge は、ご使用のネットワーク上のシステム（通常は、BMC を搭載したサーバーでない）で、バックグラウンド・サービスまたはデーモンとして開始します。まず Telnet サーバーに接続し、そこからサーバーのイーサネット・ポートを介して BMC に接続します。

SMBridge は、Serial Over LAN プロトコルを使用して、テキスト・モードのタスク（POST メッセージ、BIOS セットアップ、およびオペレーティング・システムのテキスト・モード・タスクなど）を、管理者がリモート側で制御できるようにします。実行できるタスクには、次のものがあります。

- リモート・サーバーとのテキスト・モード・コンソール・セッションの確立
- サーバーの電源オン、電源オフ（即時および正常）、またはリブート
- 点滅するシステム ID のオン/オフ
- 現在の電源状況の表示
- イベント・ログの表示

標準 Telnet クライアント・アプリケーション（Microsoft Windows 上の HyperTerminal、または Linux 上の Telnet）を使用して、サーバーの機能にアクセスできます。

SOL プロトコルとリモート・システムの BIOS コンソール・リダイレクトを一緒に使用すると、管理者は LAN 経由で BIOS 設定を表示して、変更できます。Linux シリアル・コンソールと Microsoft の Emergency Messaging Service (EMS) /Special Administration Console (SAC) インターフェースにも、SOL を使用して LAN 経由でアクセスできます。

これについては、212 ページの 6.4.3、『Telnet サーバー経由の接続』で詳しく説明します。

▶ **コマンド・ライン・インターフェース**

この方法で SMBridge を使用すると、管理者はリモート側の BMC サービス・プロセッサ上で、次のタスクを実行できます。

- サーバーの電源オン、電源オフ（即時または正常）、またはリブート
- 点滅するシステム ID のオン/オフ
- 現在の電源状況の表示
- イベント・ログの表示または消去

CLI では、Telnet サーバーによって提供されるリモート・コンソール機能を除いて、すべての機能を実行できます。

これについては、229 ページの 6.4.7、『コマンド・ライン・インターフェースを介した接続』で詳しく説明します。

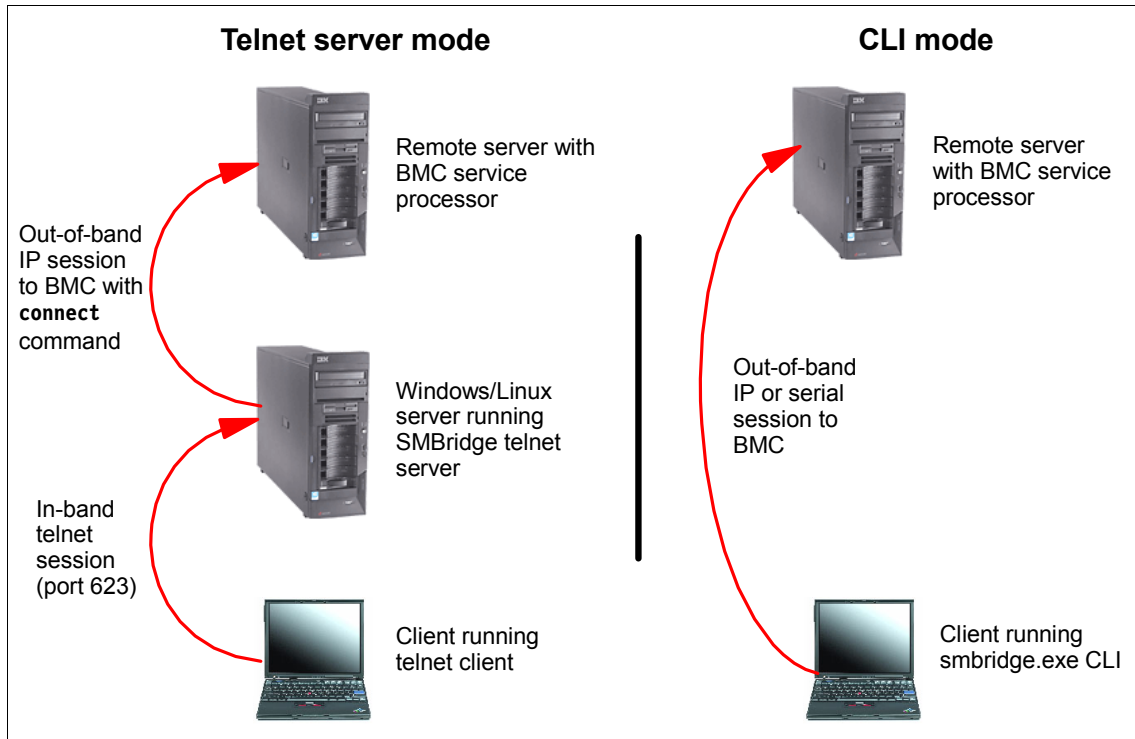


図 6-11 SMBridge ユーティリティの 2 つのモード

SMBridge は、次のサイトからダウンロードできます。

<http://www.ibm.com/pc/support/site.wss/MIGR-57729.html>

現行バージョンは、次のオペレーティング・システムをサポートします。

- ▶ Red Hat Linux 7.2
- ▶ Red Hat Linux 8.0
- ▶ Red Hat Linux 9.0
- ▶ Red Hat Enterprise Linux 3.0
- ▶ Microsoft Windows XP
- ▶ Microsoft Windows 2000 Professional
- ▶ Microsoft Windows 2000 Server
- ▶ Microsoft Windows Server 2003

「OSA System Management Bridge User's Guide」は、次のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-57816.html>

## 6.4.1 BIOS の構成

SMBridge を使用して SOL 経由でリモート・サーバーを管理する前に、リモート・サーバーの BMC および BIOS を、次のように設定しておく必要があります。

**注：**この手順は、サーバーの Gigabit ポート 1 の PXE ブートを使用不可にします。PXE を使用する計画の場合は、Gigabit ポート 2 をネットワークに接続し、リモート・インストール・プロシージャがそのポートを使用するように構成する必要があります。

1. ブート中にプロンプトで指示されたら F1 を押して、BIOS Setup に入ります。
2. まだ構成していない場合、35 ページの 2.3.5、『BIOS 内での BMC の構成』の説明に従って、BMC の固定 IP アドレス、サブネット・マスク、およびゲートウェイを構成します。
3. メインメニューから、「**Devices and I/O Ports**」を選択します。次のように設定します。
  - フィールド「Serial Port A」を「Auto-configure」に設定
  - フィールド「Serial Port B」を「Auto-configure」に設定
4. 「**Remote Console Redirection**」を選択します。次のように設定します。
  - 「Remote Console Active」を「Active」に設定
  - 「Remote Console Text Emulation」を「VT100/VT220」に設定
  - 「Remote Console Keyboard Emulation」を「VT100/VT220」に設定
  - 「Remote Console Active After Boot」を「Enabled」に設定
  - 「Remote Console Flow Control」を「Hardware」に設定

結果は、図 6-12 のようになります。

```

*****
*                               *
*           Remote Console Redirection           *
*                               *
*****
* Remote Console Active           [ Enabled ] *
* Remote Console COM Port        [ COM 1 ] *
* Remote Console Baud Rate       [ 19200 ] *
* Remote Console Data Bits       [ 8 ] *
* Remote Console Parity          [ None ] *
* Remote Console Stop Bits       [ 1 ] *
* Remote Console Text Emulation  [ VT100/VT220 ] *
* Remote Console Keyboard Emulation [ VT100/VT220 ] *
* Remote Console Active After Boot [ Enabled ] *
* Remote Console Flow Control    [ Hardware ] *
*****

```

図6-12 SOL を使用可能にするための「Remote Console Redirection」の設定

5. Esc を 2 回押してメインメニューに戻り、「**Start Options**」を選択します。次のように設定します。
  - 「Planar Ethernet 1 PXE」を「Disabled」に設定
  - 「Planar Ethernet 2 PXE」を「Enabled」に設定
  - 「Planar Ethernet PXE/DHCP」を「Planar Ethernet 2」に設定
  - 「Run PXE only on Selected Planar NIC」を「Enabled」に設定

ご使用のサーバーには、おそらく一部のオプションしか表示されないことに注意してください。例えば、x236 では、「Planar Ethernet PXE/DHCP」を「Planar Ethernet 2」に設定するだけです。
6. Esc を押してメインメニューに戻り、「**Advanced Options**」を選択し、次に「**Baseboard Management Controller (BMC) Settings**」を選択します。次のように設定します。
  - 「System-BMC Serial Port Sharing」を「Enabled」に設定
  - 「BMC Serial Port Access Mode」を「Dedicated」に設定
7. BIOS 設定を保管して、サーバーをリブートします。

## 6.4.2 インストール

このセクションでは、Windows および Linux プラットフォーム上の SMBridge ユーティリティーのインストール方法について説明します。ユーティリティーの最新バージョンは、次のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-57729.html>

## Microsoft Windows

プロシージャーは、CLI のインストールと、Telnet サーバーをインストールして使用可能にする操作の両方を行います。

**ヒント:** このインストールは通常、Telnet サーバーとして働かせる予定のサーバー上で実行します (206 ページの図 6-11 を参照してください)。CLI を使用する計画の場合、CLI を実行するために必要なファイルは `smbridge.exe` と `smbridge.cfg` だけであるため、実際にはツールをインストールする必要はありません。

そのため、他のシステム上で CLI を使用する計画の場合は、次のいずれかを使用できます。

- ▶ Telnet サーバーからファイル `smbridge.exe` と `smbridge.cfg` をコピーする。
- ▶ SMBridge をインストールした後、サービスを使用不可にする。

1. Setup を実行し、ライセンスに同意して、インストール・ディレクトリーを指定します。
2. IP アドレスと TCP/IP ポート番号の入力を求めるプロンプトが出ます (209 ページの図 6-13)。

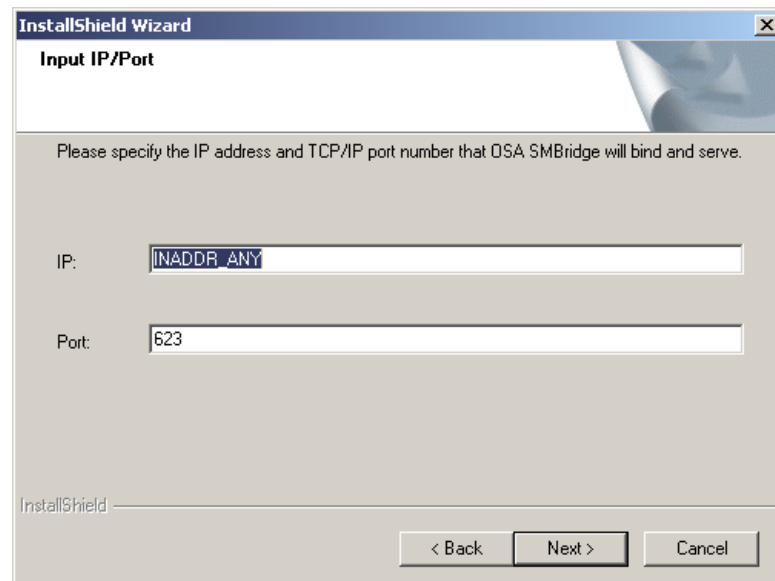


図6-13 IP アドレスとポート番号のウィンドウ

値は、次のとおりです。

- 「IP」は、SMBridge のバインド先サーバーの IP アドレスを指定します。  
サーバーは複数の有効な IP アドレスを持っている場合があるため、SMBridge では、単一の IP アドレスを指定することにより、サーバーへのアクセスを限定できます。SMBridge を複数の IP アドレスのいずれかにバインドしても構わない場合は、IP アドレスとして INADDR\_ANY を指定します。SMBridge がローカル接続のみを受け入れる場合は、IP アドレスとして 127.0.0.1 または localhost を指定します。SMBridge を特定の IP アドレスのみにバインドする必要がある場合は、その特定の IP アドレスを指定します。
- 「Port」は、SMBridge が listen するサーバー上のポート番号を指定します。

**注：**この2つの値は、SMBridge をサービス・デーモンとして自動的に始動するために、smbridge.cfg ファイルに記録されます。

3. 次に、Telnet セッション（分数）と電源オフ・コマンド（秒数）のタイムアウト値を指定するように要求されます（210 ページの図 6-14）。

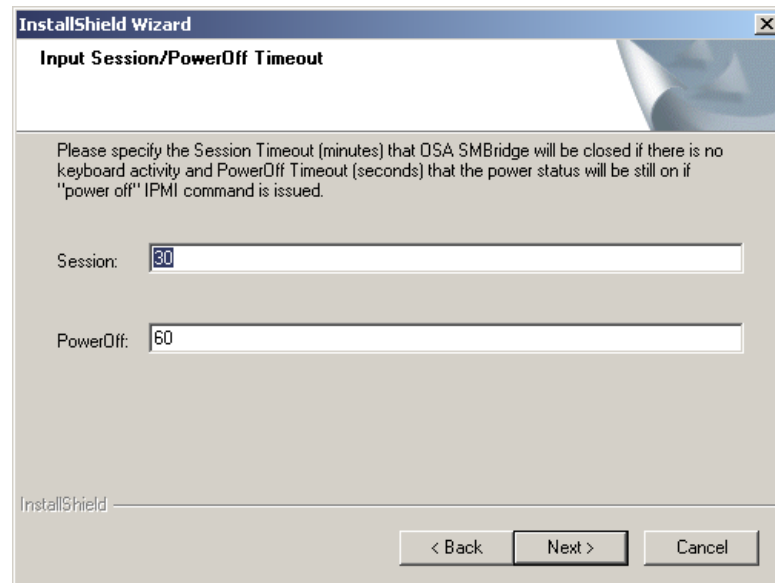


図 6-14 セッションおよび電源オフのタイムアウト設定のウィンドウ

値は、次のとおりです。

- 「Session」は、確立された Telnet セッションを終了する前に、キーボード活動が何も生じなかった分数を指定します。



- 「PowerOff」は、IPMI 電源オフ・コマンド（正常または強制）を実行する前に待つ秒数を指定します。時間がタイムアウト値を超過しても電源状況がオンのままの場合、電源オフ・コマンドが失敗した可能性があることを示すエラー・コードが戻されます。
4. 「Next」をクリックして選択を確認し、インストールを開始します。インストールが完了したら、「Finish」をクリックして、インストーラーを終了します。

OSA SMBridge サービスが自動的に開始し、サーバーが始動するたびに自動的に開始するように構成されています。これは、「コントロールパネル」→「管理ツール」→「サービス」を選択して変更できます。

## Linux プラットフォーム上のインストール

Linux 上で SMBridge をインストールするには、次の手順に従います。

1. root としてログインします。
2. SMBridge RPM ファイルが CD に入っている場合、CD をドライブに挿入し、次のコマンドを入力して、ドライブをマウントし、CD のルート・ディレクトリに変更します。

```
mount /mnt/cdrom
cd /mnt/cdrom
```

3. 次のコマンドを使用してインストールを実行します（rpm ファイルのファイル名が異なっている場合は、ご使用のファイル名で置き換えてください）。

```
rpm -i osasmbridge-1.0.3-1.i386.rpm
```

インストール・プロセスが正常に終了すると、次のディレクトリにファイルがコピーされています。

- ▶ /etc/init.d/smbbridge
- ▶ /etc/smbbridge.cfg
- ▶ /usr/bin/smbbridge
- ▶ /var/log/smbbridge
- ▶ /var/log/smbbridge/LICENSE

さらに、シンボリック・リンク /usr/sbin/smbbridge も作成されています。

テキスト・ファイル /etc/smbbridge.cfg には、多数の SMBridge ランタイム・パラメーターが入っており、ユーザーはそれを検討して、必要であれば変更できます。

デーモンを開始するには、ディレクトリー /etc/int.d に移動します。ここで、次のコマンドを使用して、OSA SMBridge デーモン・サービスを開始または停止します。

```
smbridge start  
smbridge stop
```

次のコマンドを使用して、デーモンを開始することもできます。

```
smbridge -d -c config-file
```

ここで、*config-file* は、Telnet サーバー構成を含んでいるファイルの名前です。デフォルトでは、/etc/smbridge.cfg です。このファイルについての詳細は、「*SMBridge User's Guide*」の「付録 C」を参照してください。

### 6.4.3 Telnet サーバー経由の接続

206 ページの図 6-11 に示されているように、SMBridge を BMC への Telnet インターフェース（または、「ブリッジ」）として使用できます。Telnet サーバー（SMBridge がインストールされている）に接続し、そこから Serial Over LAN（SOL）接続を使用して BMC に接続します。

SOL 接続を使用して、通常はサーバーのシリアル・ポートに直接接続した場合にのみ実行できるすべてのタスクを、LAN 接続経由で実行できます。

- ▶ BIOS 設定の変更
- ▶ Linux シリアル・コンソール
- ▶ Microsoft からの Emergency Messaging Service（EMS）
- ▶ Microsoft からの Special Administration Console（SAC）

Microsoft EMS に関する情報は、次のサイトから入手できます。

[http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS\\_topnode.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_topnode.asp)

実行できる SAC コマンドの説明は、次のサイトにあります。

[http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS\\_SAC\\_commands.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_SAC_commands.asp)

リモート・サーバー上の「BIOS console redirection to serial port」を「enabled」に設定すると、BIOS を使用してシステム・コンソールへの読み取り / 書き込みを行うアプリケーションは、その入出力がシリアル・ポートに転送されます。SOL を使用して、BMC ファームウェアはシリアル・ポートに書き込まれたデータを読み取り、それを LAN パケットとして SMBridge に送信します。SMBridge は、そのデータを TCP/IP パケットとして Telnet クライアントに転送します。

1 つの SMBridge セッションは、一度に 1 つの BMC を使用して 1 つの SOL セッションをサポートします。

## Telnet クライアント

SMBridge Telnet サーバーにアクセスするには、ポート 623（または、このデフォルトから変更した場合は、インストール時に選択したポート）を使用して接続します。例えば、次のように指定します。

```
telnet smbridge-server 623
```

**注：**デフォルトでは、SMBridge Telnet サーバーは、ポート 623 で listen します。

VT100 端末エミュレーションをサポートする Telnet クライアントを使用して、SMBridge を介して BMC にアクセスできます。これには、次のものが含まれません。

### ▶ Windows の **telnet** コマンド・ライン・ユーティリティー

追加情報：

- テストでは、Windows XP システムでキーボードの F1 を押すと、F1 はリモート・サーバーに正しく送信されることが示されました（例えば、BIOS Setup に入る）。ご使用の Telnet クライアントがこのような機能しない場合は（Windows Server 2000 の **telnet** コマンドなど）、F1 キーと F2 キーを、2 つの方法でシミュレートできます。F1 をシミュレートするには、次のいずれかを使用します。

- Esc、次に Numeric+1（つまり、数字キーパッドの 1）
- Esc、次に Shift+O、次に Shift+p

F2 をシミュレートするには、次のいずれかを使用します。

- Esc、次に Numeric+2（つまり、数字キーパッドの 2）
- Esc、次に Shift+O、次に Shift+q

**ヒント：**この Telnet クライアントは、Windows の実行中に使用することをお勧めします。これは、Telnet の標準実装で、カラーもサポートします。

### ▶ Windows の HyperTerminal

追加情報：

- Windows Server 2003、Enterprise Edition に付属の HyperTerminal は、正常に機能しない場合があります。Private パージョンにアップグレードする必要があります。
- Windows 2000 Server に付属の HyperTerminal は、ランダム文字を表示し、一部のテキストが失われます。このクライアントは使用しないことをお勧めします。
- 新規接続を作成する場合、ドロップダウン・メニューを使用して、「Connect」で「TCP/IP (WinSock)」を選択します。Telnet サーバーの IP ア

ドレスを入力し、ポート 623（または、SMBridge のインストール時に指定したポート）を指定します。

- 「ファイル」→「プロパティ」→「設定」→「ASH」→「設定」で、「Wrap lines that exceed terminal width」のチェック・ボックスをクリアして、自動折り返しをオフにします。
- 「プロパティ」ウィンドウで、VT100 端末をエミュレートするための接続を構成します。

▶ Linux の csh または ksh の一部としての **telnet** コマンド

F1 および F2 キーは、特に X-Windows 環境の外部では、正常に機能しない場合があります。VT100 キー・ストロークを生成するように、X-Windows を再構成できる場合もあります。例えば、KDE では、「Settings」を使用してキーボードを再構成します。

## 接続

このセクションでは、ラボのサーバーを参照しながら、プロセスを説明します。SMBridge Telnet サーバーはアドレス 9.42.171.121 のシステムにインストールし、リモート・サーバーは、アドレス 9.24.171.237 を使用するように構成された BMC を装備しています。BMC は、デフォルトの USERID/PASSWORD 認証を使用します。

BMC に接続するには、次のようにします（本書の例のアドレスを使用）。

1. 次のコマンドを発行して、Telnet サーバーのポート 623 に接続します。  
`telnet 9.42.171.121 623`
2. 次のようなプロンプトが表示されます。

Username:

3. Telnet サーバーの有効な管理者ユーザー ID とパスワードを入力します（例えば、Administrator または root）。

**注** : SMBridge Telnet サーバーをローカル・システムで実行している場合、SMBridge は、ログオンしている現行ユーザーの権限を使用するため、このプロンプトは表示されません。

4. 次のようなウェルカム・メッセージが表示されます。

```
Username:Administrator
Password:

Administrator login successful.

OSA System Management Bridge (SMBridge), Version 1.0.3.1
Copyright (c) 2004 - OSA Technologies, an Avocent Company. All
Rights Reserved.

SMBridge>
```

5. **connect** コマンドを使用して、管理するサーバー上の BMC に接続します。

```
SMBridge>connect -ip 9.42.171.237 -u USERID -p PASSWORD
SMBridge>
```

このユーザー ID とパスワードは、BMC にログインできるユーザーとして以前に構成されたものです。

コマンドが正常に実行された場合、**SMBridge** コマンド・プロンプトに戻ります。

6. これで、リモート BMC に対してコマンドを発行できるようになりました。コマンドについては、以下で説明します。
7. 終了するには、**exit** コマンドを入力します。

## 使用可能なコマンド

コマンドは、コマンド・ライン・インターフェースのコマンドのスーパーセットで、表 6-6 にリストされています。コマンドについての詳細なヘルプ情報を入力するには、**help** コマンドを発行します。例えば、次のように入力します。

```
help power
```

**ヒント** : Telnet インターフェースで使用可能なコマンドのほとんどは、CLI で使用されるコマンドと同じです。追加される Telnet コマンドは、**console**、**sol**、および **reboot** です。

表 6-6 SMBridge Telnet サブコマンド

サブコマンド	説明と構文
<p><b>console</b></p>	<p>BMC との Serial Over LAN (SOL) セッションを開始し、コンソールからシリアル・ポートに転送されたテキストを表示します。パラメーターはありません。</p> <p><b>console</b> コマンドを入力すると、次のような表示が出ます。</p> <pre>Activating remote console now. Remote console is now active and ready for user input.</pre> <p>Telnet セッションに戻るには、次のように、波形記号キーの後に、ピリオド・キーを押します。</p> <pre>~.</pre>
<p><b>sol</b></p>	<p>Serial Over LAN を使用可能または使用不可に設定し、シリアル・パラメーターをリモート・サーバーの BIOS の「Console Redirection」パラメーターに一致するように構成します。オプションは、次のとおりです。</p> <pre>sol enable sol disable sol config [-baud <i>baud_rate</i>] [-priv <i>privilege_level</i>] [-retry count <i>retry_count</i>] [-retry interval <i>retry_interval</i>]</pre>
<p><b>reboot</b></p>	<p>電源オフ (正常シャットダウン)、電源オン、次にリモート・コンソールを始動するのと同等の操作を実行します。オプションは、次のとおりです。</p> <pre>reboot reboot -force</pre> <p>x236、x336、および x346 は、正常シャットダウン・オプションをサポートしません。これらのサーバーでは、<b>-force</b> パラメーターが必須です。</p>
<p><b>sysinfo</b></p>	<p>サーバーと BMC に関連した一般システム情報を表示します。オプションは、次のとおりです。</p> <pre>sysinfo fru sysinfo id</pre> <p><b>id</b> は、パラメーターが指定されていない場合のデフォルトです。</p>

サブコマンド	説明と構文
<b>identify</b>	<p>サーバーのフロント・パネルの青色の識別 LED を制御します。オプションは、次のとおりです。</p> <pre>identify on [-t &lt;seconds&gt;] identify off</pre> <p><b>on</b> は、パラメーターが指定されていない場合のデフォルトです。</p>
<b>power</b>	<p>サーバーの電源オプションを制御します。オプションは、次のとおりです。</p> <pre>power status power on power cycle power reset power off [-force]</pre> <p><b>status</b> は、パラメーターが指定されていない場合のデフォルトです。</p> <p>x236、x336、および x346 は、正常シャットダウン・オプションをサポートしないことに注意してください。これらのサーバーでは、<b>-force</b> パラメーターが必須です。</p>
<b>sel</b>	<p>システム・イベント・ログ (SEL) を使用する操作を実行します。オプションは、次のとおりです。</p> <pre>sel status sel get set get -last &lt;n&gt; sel get -begin &lt;index1&gt; -end &lt;index2&gt; sel get -begin &lt;index1&gt; -max &lt;count&gt; sel clear sel set -time &lt;YYYY/MM/DD hh:mm:ss&gt;</pre> <p><b>status</b> は、パラメーターが指定されていない場合のデフォルトです。</p>
<b>help</b>	<p>すべてのコマンドの一般ヘルプ、または特定のコマンドに関するヘルプを表示します。</p>

#### 6.4.4 SOL をサポートするための Windows Server 2003 の構成

SMBridge Telnet サーバーを使用して BMC に接続すると、テキスト・コンソールをリモート側で制御できます。SOL の使用により、Windows Server 2003 や Linux のようなオペレーティング・システムでも、これが可能になります。

Windows Server 2003 は、SMBridge および BMC と連動してオペレーティング・システムへのアウト・オブ・バンド・アクセスを提供する、2つのコンポーネントを備えています。

- ▶ Microsoft Emergency Messaging Service (EMS)
- ▶ Microsoft Special Administration Console (SAC)

Microsoft EMS に関する情報は、次のサイトから入手できます。

[http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS\\_topnode.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_topnode.asp)

実行できる SAC コマンドの要約を表 6-7 に示します。

表 6-7 Windows Server 2003 Special Administration Console (SAC) コマンド

コマンド	説明
ch	すべてのチャンネルをリストします。
cmd	コマンド・プロンプト・チャンネルを作成します。ログオンするように要求されます。
crashdump	手動で Stop エラー・メッセージを生成し、メモリー・ダンプ・ファイルの作成を強制します。
d	現行カーネル・ログをダンプします。
f	t-list コマンドによって出力される情報を、プロセスのみの表示とプロセスとスレッドの表示の間で切り替えます。
i	すべてのネットワーク・インターフェースの TCP/IP の詳細をリストして、指定のネットワーク・インターフェースの IP アドレス、サブネット・マスク、およびゲートウェイを構成できるようにします。パラメーターを変更するには、次のように指定します。  network# IPaddress subnet gateway
id	サーバーの識別情報を表示します。
k pid	指定のプロセスを終了します。pid は、ユーザーが指定するプロセス識別番号です。
L pid	プロセス (および関連の子プロセス) の優先順位を可能な最下位レベルに下げます。
lock	Emergency Management Services コマンド・プロンプト・チャンネルへのアクセスを制限します。チャンネルのロックを解除するには、有効なログオン信用証明情報を提供する必要があります。



コマンド	説明
<code>m pid mb-allow</code>	プロセス ( および関連の子プロセス ) のメモリー使用量を、指定されたメガバイト数に制限します。 <i>mb</i> は、ユーザーが指定するメガバイト数です。
<code>p</code>	1 つのフルスクリーン情報が表示された後、 <code>t-list</code> コマンドの出力を休止します。
<code>r pid</code>	プロセスおよび関連の子プロセスの優先順位を 1 レベル上げます。
<code>restart</code>	サーバーを再始動します。
<code>s</code>	システム時刻を表示または設定します。時刻の設定には、次のフォーマットを使用します。  mm/dd/yyyy hh:mm
<code>shutdown</code>	シャットダウンして、サーバーの電源をオフにします。コンソール・セッションを終了し、 <b>SMBridge</b> プロンプトに戻ります。
<code>t</code>	現在実行中のプロセスとスレッドをリストします。
? または <code>help</code>	使用可能なコマンドをリストします。

SOL を終了して **SMBridge** プロンプトに戻るには、波形記号キーとピリオド・キー (つまり、`~.`) を押します。

詳細情報は、次のサイトを参照してください。

[http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS\\_SAC\\_commands.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_SAC_commands.asp)

Windows Server 2003 上の EMS を使用可能にするには、次のようにします。

1. 管理者として Windows にログインします。
2. コマンド・プロンプトを立ち上げて、コマンド **bootcfg** を入力します。

```
C:¥>bootcfg

Boot Loader Settings
-----
timeout:30
default:multi(0)disk(0)rdisk(0)partition(1)¥WINDOWS

Boot Entries
-----
Boot entry ID: 1
OS Friendly Name: Windows Server 2003, Enterprise
Path: multi(0)disk(0)rdisk(0)partition(1)¥WINDOWS
OS Load Options: /fastdetect
```

図6-15 bootcfg コマンドからの出力

- 出力を調べます。複数のブート・エントリーがある場合は、「Boot Loader Settings」の下の **default** 行を見てデフォルト・エントリーを調べ、「Boot Entry」の「Path」値が一致しているかどうかを調べる必要があります。この例の場合は、ブート・エントリーは1つだけです（ブート・エントリー1）。
- /id** パラメーターをご使用のブート・エントリー番号で置き換えて（本書の例のように1ではない場合）、次のコマンドを発行します。

```
bootcfg /ems on /port com1 /baud 19200 /id 1
```

```
C:¥>bootcfg /ems on /port com1 /baud 19200 /id 1
SUCCESS: Changed the redirection port in boot loader section.
SUCCESS: Changed the redirection baudrate in boot loader section.
SUCCESS: Changed the OS entry switches for line "1" in the
BOOT.INI file.
```

図6-16 ブート構成の変更

- bootcfg** コマンドを再発行して、結果を見ます。例の中の変更箇所が強調表示されています。

```
C:\>bootcfg /ems on /port com1 /baud 19200 /id 1
SUCCESS: Changed the redirection port in boot loader section.
SUCCESS: Changed the redirection baudrate in boot loader section.
SUCCESS: Changed the OS entry switches for line "1" in the BOOT.INI
file.

C:\>bootcfg

Boot Loader Settings
-----
timeout:          30
default:          multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
redirect:         COM1
redirectbaudrate:19200

Boot Entries
-----
Boot entry ID:    1
OS Friendly Name: Windows Server 2003, Enterprise
Path:             multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options: /fastdetect /redirect
C:\>
```

図 6-17 EMS を使用可能にした後の bootcfg コマンド

6. サーバーをリブートして、変更を有効にします。

**注:**再度 EMS オフにするには、次のコマンドを発行します。

```
bootcfg /ems off /id 1
```

ここで、1 は、上のステップで変更したブート・エントリーです。リブートして、変更をオンラインにします。

リブートして、SMBridge コンソールと連動させると (216 ページの表 6-6 の **console** コマンドを参照)、EMS コンソールが表示されます。

```
<?xml version="1.0"?>
<machine-info>
Computer is booting, SAC started and initialized.
<processor-architecture>x86</processor-architecture>
<os-version>5.2</os-version>
<os-build-number>3790</os-build-number>

SAC>
```

図 6-18 Microsoft Emergency Messaging Service コンソール

これで、218 ページの表 6-7 に記述されているさまざまな SAC コマンドを実行できるようになりました。例えば、コマンド・プロンプトを開始するには、コマンドは次のようになります (223 ページの図 6-19)。

**ヒント :** SMBridge コンソールの始動後に、ブランク画面しか表示されない場合は、Enter を数回押して、SAC> プロンプトを表示してください。

```

SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT: A new channel has been created. Use "ch -?" for channel help.
Channel: Cmd0002
SAC>ch
Channel List

(Use "ch -?" for information on using channels)

# Status Channel Name
0 (AV) SAC
1 (AV) Cmd0002
SAC>ch -si 1
Name: Cmd0002
Description: Command Prompt
Type: <Esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.

Please enter login credentials.
Username:
Domain:
Password:

Attempting to authenticate...

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003

C:¥WINDOWS¥system32>

```

図 6-19 コマンド・プロンプト・チャンネルを立ち上げる SAC コマンド

コマンド・プロンプト・チャンネルをクローズするには、`exit` を入力します。チャンネルをオープンしたまま、SAC プロンプトに戻るには、`Esc+Tab+0`（数字のゼロ・キー）（3つのキーを順に）押します。リモート・コンソールを出て、SMBridge に戻るには、波形記号 + ピリオド（つまり、`~`）を押します。

## 6.4.5 SOL をサポートするための Red Hat Linux の構成

Red Hat Linux を構成して、Linux 初期化（ブート）プロセスを公開する必要があります。これにより、ユーザーは SOL セッションを通して Linux コンソールにログインし、出力をシリアル・コンソールに送信できるようになります。以下の手順は、Red Hat Enterprise Linux ES 2.1 または 3.0 で SOL を使用可能にする場合を示しています。

1. root としてログインします。
2. `/etc/inittab` ファイルを変更して `# Run gettys in standard runlevels` セクションの最後に次の行を追加し、ユーザーが SOL コンソールでログインできるようにします。  

```
7:2345:respawn:/sbin/agetty -h ttyS1 19200 vt102
```
3. `/etc/securetty` ファイルを変更して次の行を追加し、ユーザーが SOL コンソールで root としてログインできるようにします。  

```
ttyS1
```

*LILO* ユーザーの場合（GRUB ユーザーは 226 ページのステップ 1 に進んでください。）

1. `/etc/lilo.conf` ファイルを変更します。
  - a. 最初の `default` 行に `-Monitor` を追加します。
  - b. `map` 行をコメント化します。
  - c. `message` 行をコメント化します。
  - d. 最初の `Image` セクションで、`label` 行に `-Monitor` を付加し、次の行を追加します。  

```
append="console=ttyS1,19200n8 console=tty1"
```
  - e. 2 つの `Image` セクションの間に、以下の行を追加します。  

```
# This will allow you to Interact with the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
label=linux-Interact
initrd=/boot/initrd-2.4.9-e.12smp.img
read-only
root=/dev/hda6
append="console=tty1 console=ttyS1,19200n8"
```

結果は、225 ページの図 6-20 のようになります。変更箇所が強調表示されています。

```

prompt
timeout=50
default=linux-Monitor
boot=/dev/hda
#map=/boot/map
install=/boot/boot.b
#message=/boot/message
linear

# This will allow you to only Monitor the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
label=linux-Monitor
initrd=/boot/initrd-2.4.9-e.12smp.img
read-only
root=/dev/hda6
append="console=ttyS1,19200n8 console=tty1"

# This will allow you to Interact with the OS boot via SOL
image=/boot/vmlinuz-2.4.9-e.12smp
label=linux-Interact
initrd=/boot/initrd-2.4.9-e.12smp.img
read-only
root=/dev/hda6
append="console=tty1 console=ttyS1,19200n8"

image=/boot/vmlinuz-2.4.9-e.12
label=linux-up
initrd=/boot/initrd-2.4.9-e.12.img
read-only
root=/dev/hda6

```

図6-20 lilo.conf ファイルの変更

2. lilo と入力して、新規の LILO 構成を保管し、アクティブにします。
3. Linux を再起動します。

オペレーティング・システムがブートを開始すると、通常の GUI インターフェースの代わりに、LILO boot: プロンプトが表示されるようになります。このプロンプトが表示されている間に Tab キーを押すと、ブート・オプションが表示されます。対話式モードでオペレーティング・システムをロードするには、次のように入力します。

```
linux-Interact
```

## GRUB ユーザーの場合

1. /boot/grub/grub.conf ファイルを、次のように変更します。
  - a. splashimage 行をコメント化します。
  - b. 最初の title 行の前に、次のコメントを追加します。

```
# This will allow you to only Monitor the OS boot via SOL
```
  - c. 最初の title 行に、SOL Monitor を付加します。
  - d. 最初の title セクションの kernel 行の最後に、次のテキストを付加します。

```
console=ttyS1,19200 console=tty1
```
  - e. 2 つの title セクションの間に、以下の行を追加します。

```
# This will allow you to Interact with the OS boot via SOL
title Red Hat Linux (2.4.9-e.12smp) SOL Interactive
root (hd0,0)
kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=tty1
  console=ttyS1,19200
initrd /initrd-2.4.9-e.12smp.img
```

結果は、227 ページの図 6-21 のようになります。変更箇所が強調表示されています。

2. Linux を再起動します。



```

#grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#           all kernel and initrd paths are relative to /boot/, eg.
#           root (hd0,0)
#           kernel /vmlinuz-version ro root=/dev/hda6
#           initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
# This will allow you to only Monitor the OS boot via SOL
title Red Hat Enterprise Linux ES (2.4.9-e.12smp) SOL Monitor
    root (hd0,0)
    kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=ttyS1,19200 console=tty1
    initrd /initrd-2.4.9-e.12smp.img

# This will allow you to Interact with the OS boot via SOL
title Red Hat Linux (2.4.9-e.12smp) SOL Interactive
    root (hd0,0)
    kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/hda6 console=tty1 console=ttyS1,19200
    initrd /initrd-2.4.9-e.12smp.img

title Red Hat Enterprise Linux ES-up (2.4.9-e.12)
    root (hd0,0)
    kernel /vmlinuz-2.4.9-e.12 ro root=/dev/hda6
    initrd /initrd-2.4.9-e.12.img

```

図 6-21 grub.conf ファイルの変更

## 6.4.6 SOL をサポートするための SUSE LINUX の構成

SUSE LINUX を構成して、Linux 初期化（ブート）プロセスを公開する必要があります。これにより、ユーザーは SOL セッションを通して Linux コンソールにログインし、出力をシリアル・コンソールに送信できるようになります。以下の手順は、SUSE LINUX Enterprise Server 8.0 で SOL を使用可能にする場合を示しています。

1. root としてログインします。
2. /etc/inittab ファイルを変更して #getty-programs for the normal runlevels セクションの最後に次の行を追加し、ユーザーが SOL コンソールでログインできるようにします。

```
7:2345:respawn:/sbin/agetty -h ttyS1 19200 vt102
```

3. `/etc/securetty` ファイルを変更して `tty6` 行の後に次の行を追加し、ユーザーが SOL コンソールで `root` としてログインできるようにします。

```
ttyS1
```

4. `/boot/grub/menu.lst` ファイルを、次のように変更します。

- a. `gfxmenu` 行をコメント化します。

- b. 最初の `title` 行の前に、次のコメント行を追加します。

```
# This will allow you to only Monitor the OS boot via SOL
```

- c. 最初の `title` 行に、`SOL Monitor` を付加します。

- d. 最初の `title` セクションの `kernel` 行に、次のテキストを付加します。

```
console=ttyS1,19200 console=tty1
```

- e. 最初の 2 つの `title` セクションの間に、以下の行を追加します。

```
# This will allow you to Interact with the OS boot via SOL
```

```
title linux SOL Interactive
```

```
kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot vga=791
```

```
console=tty1 console=ttyS1,19200
```

```
initrd (hd0,1)/boot/initrd
```

結果は、229 ページの図 6-22 のようになります。変更箇所が強調表示されています。

5. Linux を再起動します。

```

#gfxmenu (hd0,1)/boot/message
color white/blue black/light-gray
default 0
timeout 8

# This will allow you to only Monitor the OS boot via SOL
title linux SOL Monitor
# Note: The following "kernel" line is all one line, not two separate lines
# The text has wrapped in this example
kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot vga=791
console=ttyS1,19200 console=tty1
initrd (hd0,1)/boot/initrd

# This will allow you to Interact with the OS boot via SOL
title linux SOL Interactive
# Note: The following "kernel" line is all one line, not two separate lines
# The text has wrapped in this example
kernel (hd0,1)/boot/vmlinuz root=/dev/hda2 acpi=oldboot vga=791 console=tty1
console=ttyS1,19200
initrd (hd0,1)/boot/initrd

title floppy
root
chainloader +1
title failsafe
kernel (hd0,1)/boot/vmlinuz.shipped root=/dev/hda2 ide=nodma apm=off vga=normal
nosmp disableapic maxcpus=0 3
initrd (hd0,1)/boot/initrd.shipped

```

図 6-22 menu.lst ファイルの変更

### 6.4.7 コマンド・ライン・インターフェースを介した接続

OSA SMBridge は、コマンド・ライン・ツールの `smbridge.exe` も提供します。これを使用すると、Telnet サーバーを使用して実行できる機能のサブセットを実行できます。具体的には、欠けているタスクは、SOL を介してサーバーのテキスト・コンソールをリモート側で制御する機能です。ただし、CLI では、シリアル接続を介してサーバーに接続できません。

CLI モードでは、SMBridge は LAN またはシリアル・ポート経由で、一度に 1 つのサーバーへのアウト・オブ・バンド・アクセスをサポートします。ただし、

同じリモート・サーバー上で複数の IPMI セッションを同時に実行できます。  
LAN 接続はイーサネット経由、シリアル接続は通常はヌル・モデム経由です。

SMBridge を CLI モードで実行するには、単に SMBridge のインストール先ディレクトリーでコマンド・プロンプト/シェル・プロンプトを開いて、**smbridge** コマンドを実行するだけです。

- ▶ Windows では、SMBridge はデフォルトで `c:\Program Files\OSA` にインストールされます。
- ▶ Linux では、デフォルトで `/usr/sbin` にインストールされます。

イーサネット接続またはシリアル接続の場合、構文は以下のようになります。

イーサネット接続の場合

```
smbridge -ip address -u user -p password subcommand
```

ここで、

- ▶ **-ip address** は、リモート・サーバーの IP アドレスまたはホスト名です。
- ▶ **-u user -p password** は、サービス・プロセッサの有効なユーザー ID とパスワード（デフォルトは、USERID/PASSWORD）です。

シリアル接続の場合

```
smbridge -com serialport [-baud baudrate] [-flow flowcontrol] -u user  
-p password subcommand
```

ここで、

- ▶ **-com serialport** は、リモート・サーバー上のシリアル・ポートを指定します。Windows システムでは、COM1 の場合は 1、COM2 の場合は 2 というように指定します。Linux システムでは、ttyS0、ttyS1 というようになります。
- ▶ **-baud baudrate** は、通信速度（9600、19200 など）を指定します。これは、リモート・サーバーの BIOS で設定された通信速度（「Remote Console Redirection」ウィンドウ）と一致しなければなりません。指定しない場合、デフォルトの 19200 になります。
- ▶ **-flow flowcontrol** は、フロー制御を指定します。指定しない場合、デフォルトの CTS（ハードウェア・フロー制御）が使用されます。オプションは、次のとおりです。
  - CTS = ハードウェア・フロー制御
  - XON = ソフトウェア・フロー制御
  - NONE = フロー制御なし

有効なサブコマンドとコマンドの構文が、231 ページの表 6-8 にリストされています。構文の詳しい説明を見るには、**-help** コマンドを発行します。例えば、次のように入力します。

```
smbridge -help power
```

表 6-8 *SMBridge CLI* サブコマンド

サブコマンド	説明と構文
<b>sysinfo</b>	<p>サーバーと BMC に関連した一般システム情報を表示します。オプションは、次のとおりです。</p> <pre>sysinfo fru sysinfo id</pre> <p><b>id</b> は、パラメーターが指定されていない場合のデフォルトです。</p>
<b>identify</b>	<p>サーバーのフロント・パネルの青色の識別 LED を制御します。オプションは、次のとおりです。</p> <pre>identify on [-t &lt;seconds&gt;] identify off</pre> <p><b>on</b> は、パラメーターが指定されていない場合のデフォルトです。</p>
<b>power</b>	<p>サーバーの電源オプションを制御します。オプションは、次のとおりです。</p> <pre>power status power on power cycle power reset power off [-force]</pre> <p><b>status</b> は、パラメーターが指定されていない場合のデフォルトです。</p> <p>注: x236、x336、および x346 は、正常シャットダウン・オプションをサポートしません。これらのサーバーでは、<b>-force</b> パラメーターが必須です。</p>

サブコマンド	説明と構文
<b>sel</b>	<p>システム・イベント・ログ (SEL) を使用する操作を実行します。オプションは、次のとおりです。</p> <pre> sel status sel get sel get -last &lt;n&gt; sel get -begin &lt;index1&gt; -end &lt;index2&gt; sel get -begin &lt;index1&gt; -max &lt;count&gt; sel clear sel set -time &lt;YYYY/MM/DD hh:mm:ss&gt; </pre> <p><b>status</b> は、パラメーターが指定されていない場合のデフォルトです。</p>

## 6.5 Web インターフェース

Remote Supervisor Adapter II および BladeCenter 管理モジュールは、Web サーバーを標準装備しており、ユーザーは Web ブラウザーを使用してサービス・プロセッサにアクセスできます。

次のブラウザーは、RSA II および BladeCenter 管理モジュールでの使用がサポートされます。

- ▶ Microsoft Internet Explorer 5.5 (最新サービス・パック搭載) 以降
- ▶ Netscape Navigator 4.72 以降 (Version 6.x はサポートされません)
- ▶ Mozilla 1.3 以降 (RSA II の Remote Control 機能はサポートされません)

ブラウザーは、Java 対応で、JavaScript 1.2 以降をサポートし、Java 1.4.1 プラグインがインストール済みであることが必要です。

**ヒント:** Web ブラウザーの使用時に最良の結果が得られるように、モニターの解像度は最低 800x600、少なくとも 256 色であることを確認してください。

Java ランタイムが必要です。ご使用のコンピューターがインターネット接続を装備していない場合、別のコンピューターを使用して、次のサイトから Java ソフトウェアをダウンロードできます。

<http://www.java.com/en/download/manual.jsp>

インターネット接続を装備している場合は、ブラウザに Java ソフトウェアのダウンロードを強制できます。次の例は、Windows と Internet Explorer を使用しています。

1. ブラウザーを立ち上げて、RSA II または BladeCenter 管理モジュールに接続します。
2. ログインします (デフォルトのユーザー ID/ パスワードは、USERID/PASSWORD)。
3. ナビゲーション・フレームで、「Tasks」 → 「Remote Control」をクリックします。
4. 「Start Remote Control in Single User Mode」をクリックします。

新しいブラウザ・ウィンドウが表示され、セキュリティー警告がポップアップ表示されます。このようにならず、ブラウザからエラー・メッセージを受け取る場合は、ブラウザが Java 対応であり、Java スクリプトがサポートされていることを確認してください。

5. その後は画面の指示に従って、インストールを完了します。

### 6.5.1 Web インターフェースの構造

サービス・プロセッサによって使用される Web ページはすべて、類似の構造を持っています。234 ページの図 6-23 の番号を参照してください。

1. 上部には、接続されているサービス・プロセッサのタイプが表示されません。
2. 左側はナビゲーション・フレームで、階層構造のメニューが表示されます。
3. ウィンドウの残りの部分は、アクティブ・メニューに関連した情報です。

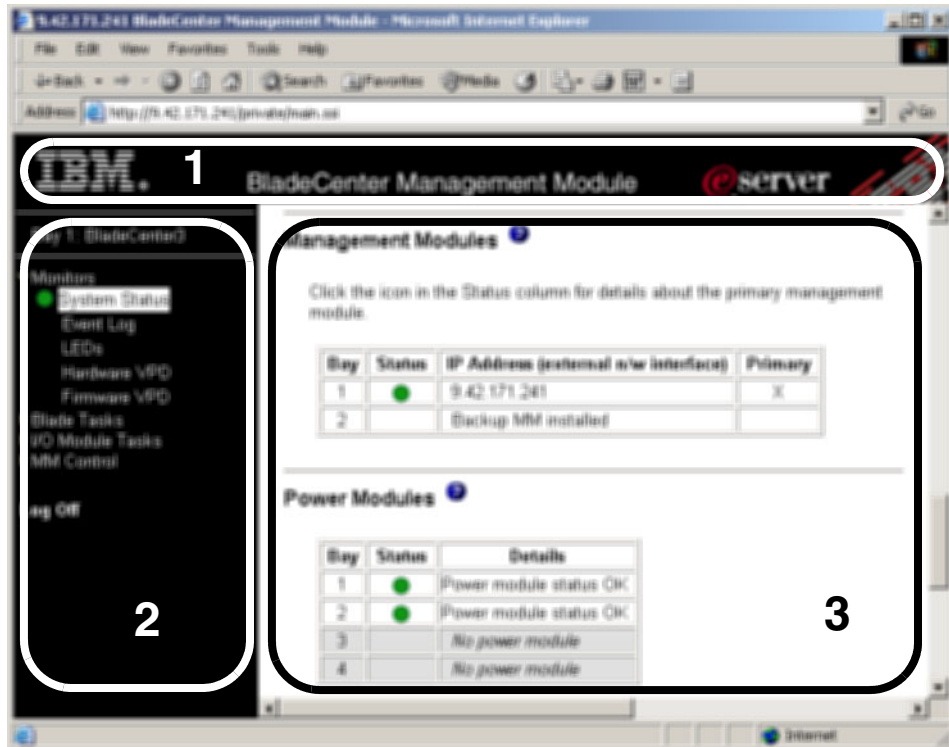


図 6-23 Web インターフェースの構造

## 6.6 Telnet インターフェース

232 ページの 6.5、『Web インターフェース』で説明した Web インターフェースに加えて、一部の xSeries サービス・プロセッサには内蔵インターフェースも装備され、サービス・プロセッサに応じて、次の接続を通してアクセス可能です。

- ▶ イーサネット経由 Telnet
- ▶ イーサネット経由 SSH
- ▶ シリアル経由 ANSI 端末

**注：**インターフェースは、telnet、ssh、および ANSI 端末セッションを介して使用できますが、単純化するために、まとめて Telnet と呼ぶことにします。

これらのインターフェースをサポートするサービス・プロセッサは、次のとおりです。



- ▶ BladeCenter 管理モジュール
- ▶ Remote Supervisor Adapter II
- ▶ Remote Supervisor Adapter II SlimLine
- ▶ Remote Supervisor Adapter II-EXA
- ▶ Remote Supervisor Adapter
- ▶ ASM PCI アダプター (Telnet と ANSI のみ)
- ▶ ASM プロセッサ (ASM インターコネクト・ネットワーク経由の Telnet のみ)

xSeries BMC サービス・プロセッサは Telnet をサポートしますが、SMBridge 経由でのみサポートします。204 ページの 6.4、『OSA SMBridge ユーティリティー』を参照してください。eServer BMC は、Telnet セッションをサポートしません。

このインターフェースは、Web インターフェースで提供される管理機能のサブセットを提供します。他のインターフェースと同様に、コマンドを実行する前に認証が必要です。

RSA II、RSA II SlimLine、および BladeCenter 管理モジュールのサービス・プロセッサの場合、Telnet インターフェースは、コマンド・ライン・ベースです。コマンドのフォーマットは、次のとおりです。

command [arguments] [-options]

注：

- ▶ コマンド構文は大 / 小文字の区別をします。
- ▶ コマンド名は常に小文字です。
- ▶ オプションは常にハイフンで始まります。
- ▶ 1 行に 1 つのコマンドを記述します。

コマンド **help** を発行すると、すべての使用可能なコマンドを表示します。例 6-5 は、RSA II で使用可能なコマンドをリストしています。

例 6-5 RSA II のコマンド (help コマンドの出力)

---

```

? -- Display command list
clearcfg -- Resets the ASM to its default settings
clearlog -- Clear ASM event log
clock -- Display/set date, time, GMT offset, and dst setting
console -- Exit CLI, attach to serial console
dhcpinfo -- View DHCP server assigned settings
exit -- Exit CLI (log off)
fans -- Displays the fan speed for all system fans
help -- Display command list
history -- Display history of last 8 commands
ifconfig -- Ethernet and PPP configuration

```

```

portcfg -- Serial port configuration.
power -- Control server power
readlog -- Displays the ASM event log, five entries at a time
reset -- Reset server
resetsp -- Reset ASM
slp -- View/edit SLP parameters
srcfg -- Serial redirection configuration
syshealth -- System Health
tcpcmdmode -- View/edit TCP command mode config.
temps -- Display system temperatures
timeouts -- Server timeouts configuration
users -- User profile configuration
update -- Update firmware
volts -- Displays all the voltages and voltage thresholds
vpd -- Display VPD

```

---

例 6-6 は、BladeCenter 管理モジュールを使用して使用可能なコマンドをリストしています。

例 6-6 BladeCenter 管理モジュールのコマンド (*help* コマンドの出力)

---

```

?- Display commands
alertentries- View/edit remote alert recipients
boot- Boot target
clear- Clear the config
clearlog- Clear the event log
console- Start SQL session to a blade
dhcpinfo- View DHCP server assigned settings
displaylog- Display log entries
dns- View/edit DNS config
env- Set persistent command target
exit- Log off
fuelg- Power management
health- View system health status
help- Display command list
history- Display command history
identify- Control target location LED
ifconfig- View/edit network interface config
info- Display identity and config of target
list- Display installed targets
power- Control target power
reset- Reset target
shutdown- Shutdown target
slp- View/edit SLP parameters
smtp- View/edit SMTP config

```

```
snmp- View/edit SNMP config
sol- View SOL status and view/edit SOL config
tcpcmdmode- View/edit TCP command mode config
telnetcfg- View/edit telnet config
update- Update firmware from TFTP server
users- View/edit user login profiles
```

---

-h パラメーターを付けてコマンドを発行すると、そのコマンドの構文に関するヘルプ情報が提供されます。例 6-7 は、**ifconfig -h** コマンドの出力を示しています。

*例 6-7 ifconfig コマンドの構文のヘルプ情報の表示 (RSA II)*

---

```
x345rsa2> ifconfig -h
usage:
  ifconfig eth0 [-options] - ethernet interface configuration
  ifconfig ppp [-options] - ppp interface configuration
eth0 options:
  -state <enabled|disabled> - interface status
  -c <dhcp|static|dthens> - configuration method
  -i <ip_addr> - IP address
  -g <ip_addr> - gateway
  -s <ip_addr> - subnet mask
  -n <hostname> - host name
  -r <10|100|auto> - data rate
  -d <full|half|auto> - duplex mode
  -m <num> - MTU
  -l <mac_addr> - LAA
Note: The -b option in the ifconfig display is for the burned-in
      MAC address and is read-only

ppp options:
  -state <enabled|disabled> - interface status
  -i <ip_addr> - IP address
  -ri <ip_addr> - remote IP address
  -s <ip_addr> - subnet mask
  -a <pap|chap|cthenp> - authentication method
```

---

使用法の例として、例 6-8 を使用して、現行イーサネット構成を表示し、ホスト名を変更した後、サービス・プロセッサを再始動する例を示します。

*例 6-8 イーサネット・インターフェースのホスト名の変更*

---

```
x345rsa2> ifconfig eth0
-state enabled
```

```
-c dthens
-i 9.42.171.7
-g 9.42.171.3
-s 255.255.255.0
-n ASMA00096B5E1209
-r auto
-d auto
-m 1500
-b 00:09:6B:5E:12:09
-l 00:08:04:06:4B:4F
x345rsa2> ifconfig eth0 -n x345rsa2
These configuration changes will become active after the next reset of
the ASM.
x345rsa2> resetsp
Submitting reset request
x345rsa2>
Connection to host lost.
```

---

Telnet インターフェースには、次のような制限があります。

- ▶ コマンド構文は大 / 小文字の区別をします。
- ▶ 最大限で、一度に 2 つの Telnet と 2 つの ssh セッションが許可されます。
- ▶ 1 行に 1 つのコマンドを記述できます。スペースを含めて 160 文字の制限があります。
- ▶ 長いコマンドのための継続文字はありません。唯一の編集機能は、入力したばかりの文字を消去するための Backspace キーです。
- ▶ 上矢印キーと下矢印キーを使用して、最新の 8 つのコマンドをブラウズできます。**history** コマンドは、最新の 8 つのコマンドのリストを表示し、感嘆符 (!) を使用してコマンドを再発行できます。**history** によって表示された 4 番目のコマンドを再発行するには、!**4** を入力します。

RSA II や BladeCenter 管理モジュールとは異なり、Remote Supervisor Adapter の Telnet インターフェースはメニュー方式です (239 ページの図 6-24 を参照)。ASM PCI アダプターの Telnet インターフェースもメニュー方式ですが、これよりも初歩的です。

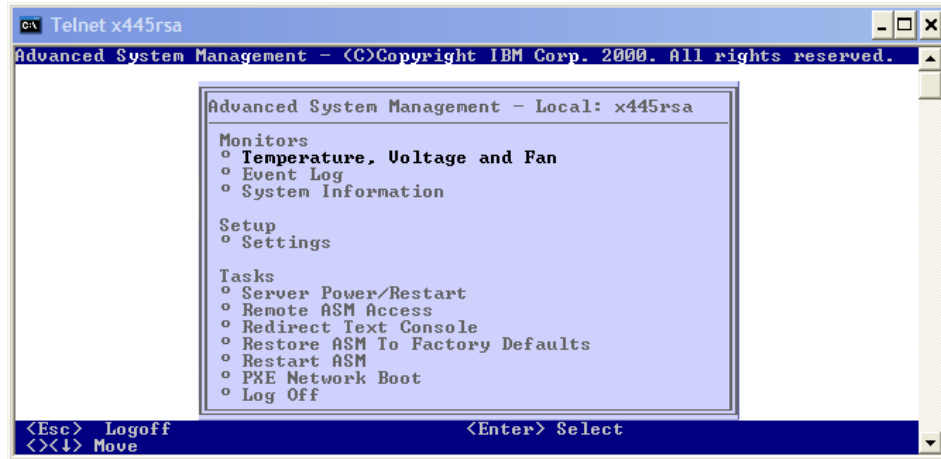


図 6-24 Remote Supervisor Adapter (xSeries 445) の Telnet インターフェース

## 6.7 IBM Director の統合

xSeries および BladeCenter システムの完全なシステム管理のために推奨されるツールは、IBM Director です。IBM Director を使用すると、システム管理ハードウェアに完全にアクセスできるだけでなく、イベント管理、インベントリー、配備など、他の管理タスクも実行できます。

IBM Director は、IBM のお客様のために、以下のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-57057.html>

IBM Director コンソールは、240 ページの図 6-25 に示すように、3 つのペインに分かれています。左側にはグループ、中央にはグループ・メンバー（例えば、サーバー）、右側には使用可能なタスクが表示されます。

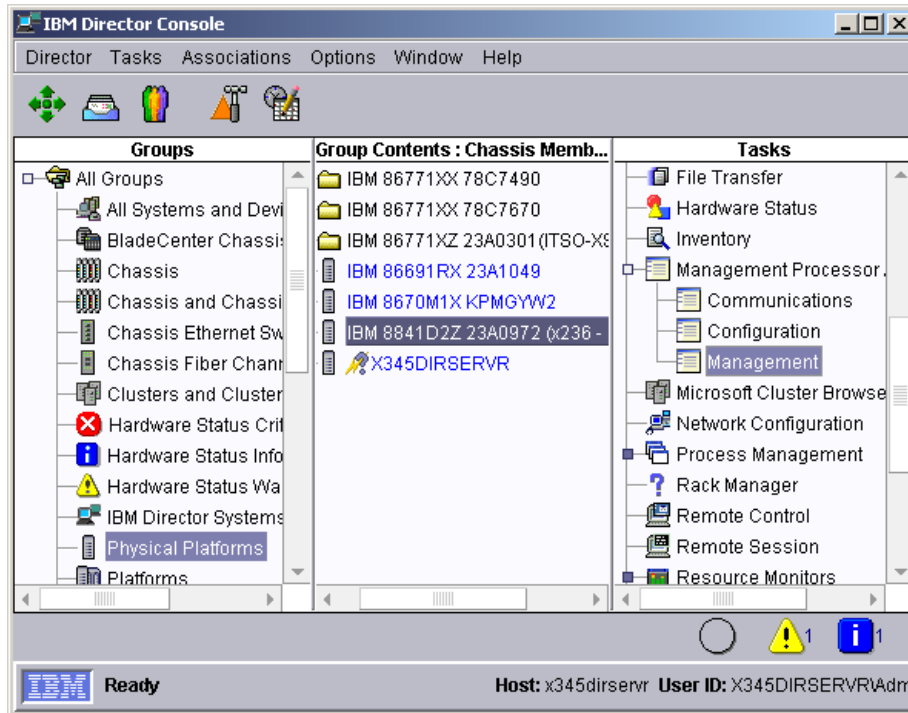


図 6-25 IBM Director コンソール

IBM Director 内で、特にサービス・プロセッサの管理用に使用されるコンポーネントは、管理プロセッサです。241 ページの 6.7.1、『管理プロセッサ』を参照してください。

IBM Director を使用して xSeries サーバー内のサービス・プロセッサにアクセスするには、最初にターゲット・サーバーに IBM Director エージェントと該当するサービス・プロセッサ・ドライバがインストールされている必要があり、オペレーティング・システムは稼働中でなければなりません。

**ヒント:** プロセス間通信 (IPC) を使用して IBM Director コンポーネント (コンソール、エージェント、およびサーバー) 間で行う通信方法を、インバンド通信といいます。その他の通信 (例えば、Web インターフェースを使用したイーサネット経由のハードウェアへの通信) は、すべてアウト・オブ・バンド通信といいます。IBM Director 関連の資料では、この表現が使用されています。

BladeCenter 管理モジュールにアクセスするには、エージェントやドライバをインストールする必要はありません。システム管理プロセッサとは異なり、管理モジュールは専用のイーサネット接続を備えているためです。

IBM Director についての詳しい情報は、次の資料を参照してください。

- ▶ IBM Redbook 「*Implementing Systems Management Solutions using IBM Director*, SG24-6188」
- ▶ 製品資料 「*IBM Director Systems Management Guide*」。これは、IBM Director CD 上の docs ディレクトリーにあります。

### 6.7.1 管理プロセッサ

管理プロセッサ (MPA) は、サービス・プロセッサの構成と管理を行うための IBM Director のインターフェースです。このインターフェースは、以下のサービス・プロセッサを 1 台以上搭載した IBM サーバーと連動します。

- ▶ システム管理プロセッサ (ASMP)
- ▶ システム管理 PCI アダプター (ASMA)
- ▶ 内蔵システム管理プロセッサ (ISMP)
- ▶ Intelligent Platform Management Interface (IPMI) ベースボード管理コントローラー (BMC)
- ▶ リモート管理アダプター (RSA)
- ▶ リモート管理アダプター II (RSA II)

**ヒント:** MPA を使用するには、IBM Director エージェントをターゲット・サーバーにインストールする必要があります。ブレード・サーバーをターゲットとして使用している場合は、MPA の代わりに BladeCenter アシスタントを使用します。242 ページの 6.7.2、『BladeCenter アシスタント』を参照してください。

MPA を立ち上げるには、次のようにします。

1. タスク「Management Processor Assistant」の前にある小さい黒丸をクリックして、メニューを展開します。
2. 「**Management**」または「**Configuration**」を左マウス・ボタンでクリックし、システム管理コンポーネントを管理するサーバーの上に、それをドラッグ・アンド・ドロップします。

「Management Processor Assistant」ウィンドウ (242 ページの図 6-26) が表示されます。左側のペインで、実行するタスクを選択します。プルダウン・メニューから、「Management」、「Configuration」、または「Communication」を選択します。

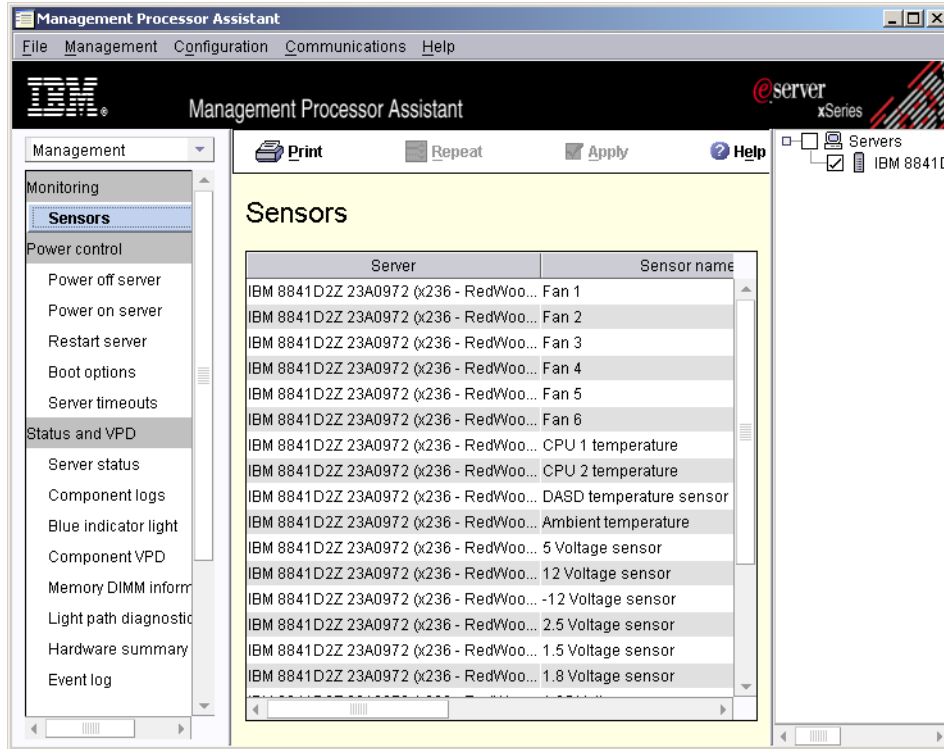


図 6-26 IBM Director の管理プロセッサ

MPA は、RSA II の Web インターフェースに非常によく似ていることが分かります。

## 6.7.2 BladeCenter アシスタント

IBM Director の BladeCenter アシスタントは、MPA と同様の働きをします。さらに、BladeCenter に固有の追加のタスクがいくつかあります。BladeCenter アシスタントを立ち上げるには、次のようにします。

1. タスク「BladeCenter Assistant」の前にある小さい黒丸をクリックして、メニューを展開します。
2. 「BladeCenter Management」または「BladeCenter Configuration」をクリックします。
3. 「BladeCenter Management」または「BladeCenter Configuration」をクリックして、管理する BladeCenter の上に、それをドラッグ・アンド・ドロップします。



「Management Processor Assistant for BladeCenter」ウィンドウが表示されます。左側のペインで、プルダウン・メニューから実行するタスクを選択します。「Management」または「Configuration」を選択します。

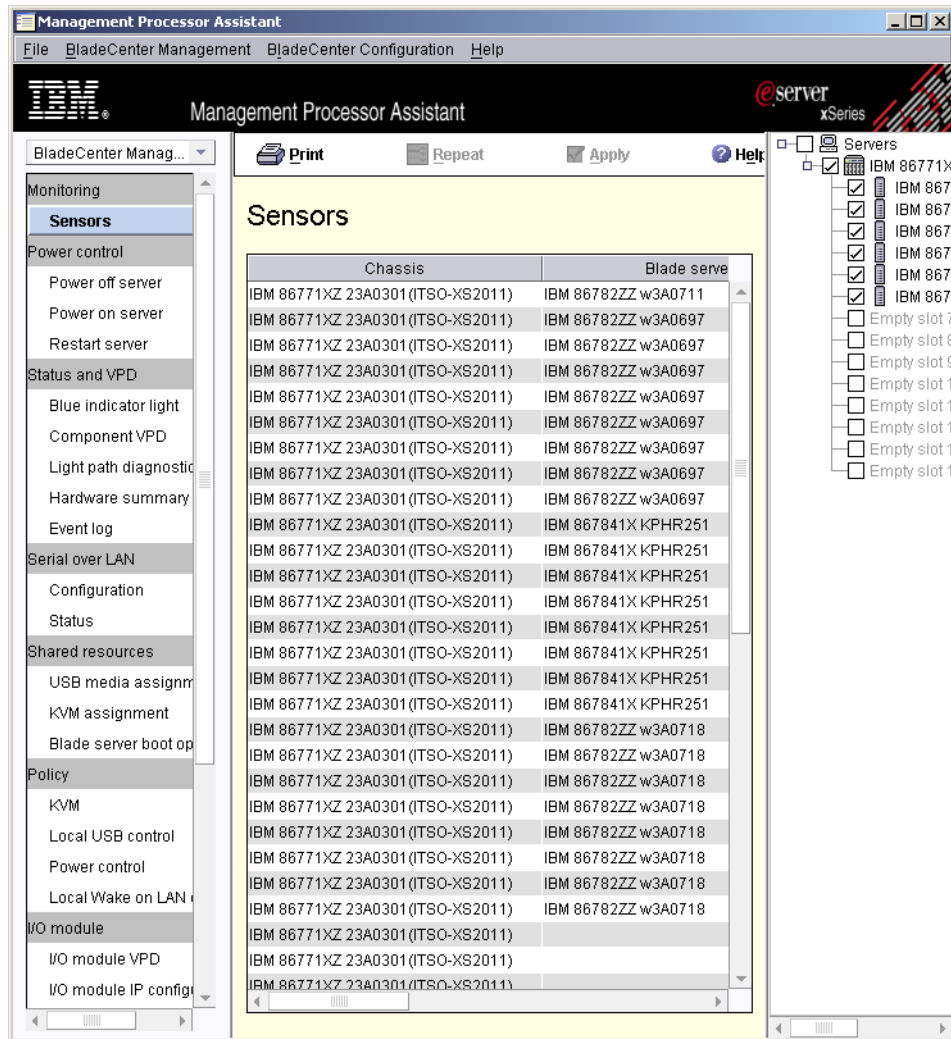


図 6-27 IBM Director の BladeCenter アシスタント

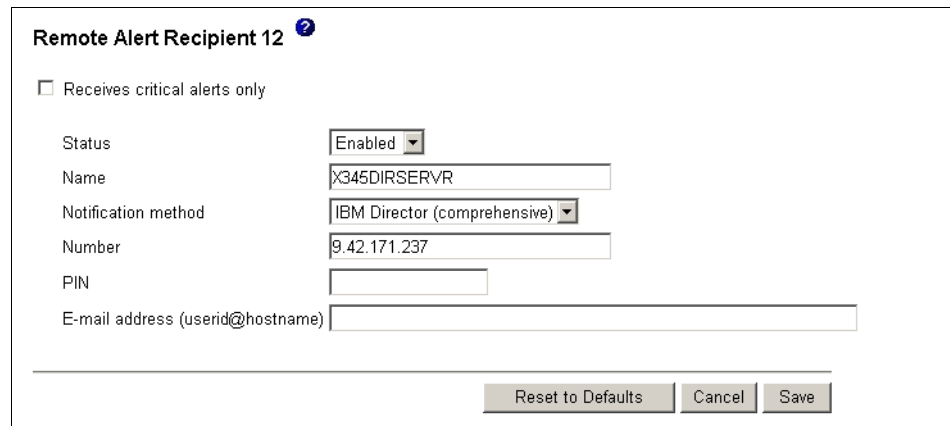
### 6.7.3 アラート転送

IBM Director は、xSeries サービス・プロセッサおよび管理モジュールのアラート宛先として機能します。システム管理ハードウェアがアラートを IBM

Director サーバーに送信するようには、ハードウェアを次のように構成します。

IBM Director にアラートを転送するようには、次のようにします。

1. Web インターフェースを立ち上げます。
2. ログインします。
3. ナビゲーション・フレームで、「**ASM Control**」(BladeCenter 管理モジュールを使用している場合は、「**MM Control**」) → 「**Alerts**」 をクリックします。
4. 「**~not used ~**」 項目の 1 つをクリックします。



Remote Alert Recipient 12 ?

Receives critical alerts only

Status: Enabled

Name: X345DIRSERVR

Notification method: IBM Director (comprehensive)

Number: 9.42.171.237

PIN:

E-mail address (userid@hostname):

Reset to Defaults Cancel Save

図 6-28 アラート転送の構成

5. 次のようにして、値を入力します。

クリティカル・アラートのみを受信する場合は、「**Receives critical alerts only**」をクリックします。クリティカル・アラートのリストを表示するには、ナビゲーション・フレームで「**Alerts**」リンクをクリックし、「**Monitored Alerts**」セクションまでスクロールダウンします。そこに、クリティカル・アラートがリストされます。

この受信側にアラートを送信することを許可する場合は、プルダウン・ボタンをクリックして、「**Enabled**」を選択します。

アラートを受信する人またはシステムの名前を入力します。

「Notification method」プルダウンから、「**IBM Director over LAN**」または「**IBM Director (comprehensive)**」を選択します。「comprehensive」項目を選択した場合、IBM Director は自動的にシステム管理ハードウェアを検出します。他方の項目を選択した場合は、IBM Director に検出を強制する必要があります。

フィールド「Number」に、IBM Director サーバーの IP アドレスまたはホスト名を入力します。ホスト名を入力する場合は、ネーム・レゾリューションが機能することを確認してください。

6. 終了したら、「Save」をクリックします。

IBM Director がアラートを受信すると、アラートは自動的にイベント・ログに追加されます。

**ヒント:** RSA II が ASM ネットワークの一部である場合、接続されたシステム管理プロセッサのゲートウェイとして機能できます。ゲートウェイとして機能させるには、「Alert Forwarding」セクションで「**Make this ASM the Gateway**」をクリックします。1 つの ASM ネットワークにつき 1 つだけゲートウェイを使用できます。

機能をテストするには、「Remote alert recipients」セクションで、「**Generate Test Alert**」をクリックします。IBM Director のイベント・ログで、テストの入力項目を確認します。

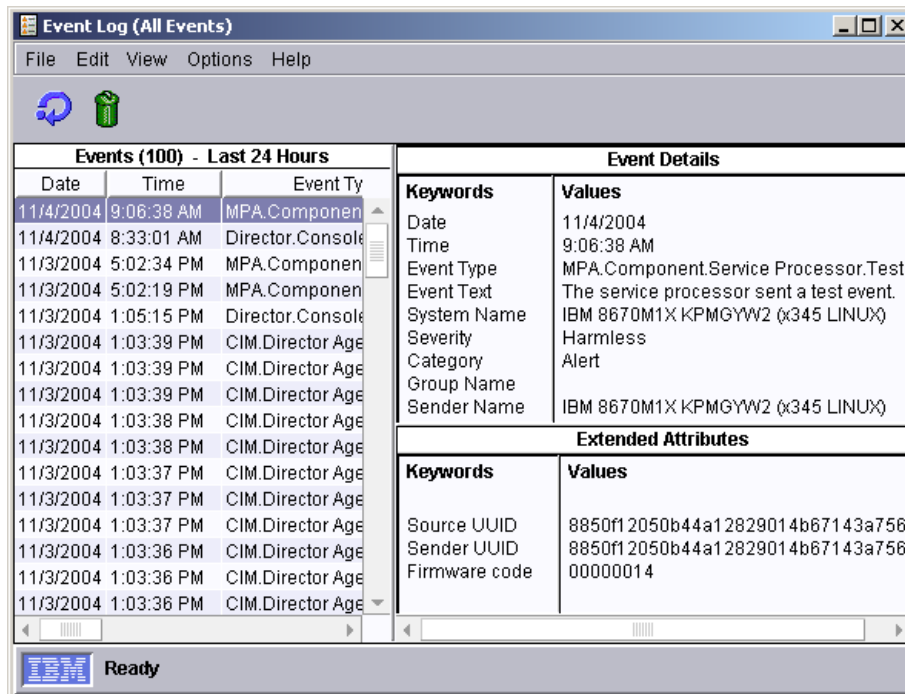



図 6-29 テスト・アラートの IBM Director イベント・ログ項目

これで、イベントは IBM Director に送信されるようになりました。次のステップは、イベント・アクション・プランを使用してこれらのイベントを処理する

ように、IBM Director を構成することです。このアクティビティーについての詳細は、「*Implementing Systems Management Solutions using IBM Director, SG24-6188*」を参照してください。



## シナリオおよびベスト・プラクティス

この章では、サービス・プロセッサと管理インターフェースを正常に機能させるための方策を、例を使って説明します。この章のトピックは、次のとおりです。

- ▶ 248 ページの 7.1、『セキュアな通信と認証』
- ▶ 251 ページの 7.2、『構成のバックアップとリストア』
- ▶ 255 ページの 7.3、『すべての BladeCenter モジュールへのリモート・アクセスの提供』
- ▶ 259 ページの 7.4、『マルチ・サブネット環境』
- ▶ 262 ページの 7.5、『ユーザー ID とパスワードの一括構成』
- ▶ 264 ページの 7.6、『RSA II の出荷時のデフォルト値へのリセット』
- ▶ 269 ページの 7.7、『リモート側での ASU の使用法』
- ▶ 273 ページの 7.8、『リモート側での BIOS とファームウェアの更新』
- ▶ 291 ページの 7.9、『UpdateXpress firmware update scripts for BladeCenter』

## 7.1 セキュアな通信と認証

システム管理ハードウェアを使用して、通信と認証をセキュアにするために取ることができるステップがあります。このセクションでは、この分野でのベスト・プラクティスの要約を示します。詳細については、137 ページの第 5 章、『セキュリティーおよび認証』を参照してください。

**注:**ここに記載するステップは、ご使用の環境を完全にセキュアにできるわけではありません。システム管理ハードウェアの持つ機能を利用して、可能な限り最良の保護を実現することが目的です。

ユーザー ID、パスワード、構成ファイルなどのデータは暗号化によって保護し、アクセスを制限する必要があります。

### 7.1.1 一般的な考慮事項

パスワードを選択する際には、password、ibm、rsa、会社名など、簡単に推測できる表現は使用しないでください。パスワードは安全な場所に保管し、パスワードへのアクセスが制限されていることを確認してください。社内のパスワード・ポリシーをインプリメントしてください。

その他の一般的な問題として、以下のことを考慮する必要があります。

- ▶ 実現可能であれば、システム管理ハードウェアは別のサブネットに配置してください。その LAN 内のユーザー（通常は、管理者グループ）だけが、それにアクセスできるようにします。通常のユーザーが誤ってシステム管理ハードウェアの Web インターフェースにアクセスしないようにする必要があります。
- ▶ サービス・プロセッサごとに、デフォルト・ユーザー USERID のパスワードを変更してください。さらに良い方法は、異なる ID とパスワードを使用して新規のスーパーバイザー・ユーザーを作成し、各サービス・プロセッサ上のデフォルト・ユーザー USERID を削除することです。MPCLI を使用すると、バッチでこれを実行できます。186 ページの 6.3、『管理プロセッサ・コマンド・ライン・インターフェース』を参照してください。
- ▶ LDAP サーバーが使用可能な場合、LDAP をサポートするすべてのサービス・プロセッサで (RSA II、BladeCenter 管理モジュール)、ユーザー認証用に LDAP を構成してください。LDAP 通信の SSL をアクティブにします (『セキュア LDAP クライアントの構成』(143 ページ)、および 148 ページの 5.2、『LDAP を使用した認証』を参照してください)。LDAP に問題があった

場合に備えて、各サービス・プロセッサ上でローカルに、少なくとも1名のスーパーバイザー・ユーザーを定義してください。

- ▶ 異なるユーザーに対しては、異なる権限レベルを使用してください。すべてのユーザーが同じスーパーバイザー・ユーザー ID を使用するのを許可してはなりません。
- ▶ BladeCenter シャーシの場合、リダンダント管理モジュールを搭載して、1次管理モジュールに障害が起きてもアクセスを確保できるようにします。103 ページの 4.3、『リダンダント管理モジュール』を参照してください。
- ▶ BladeCenter イーサネット・スイッチ・モジュール (ESM) の外部管理ポートを使用可能にしないでください。これにより、管理トラフィックを実動 LAN トラフィックから確実に分離できます。代わりに、管理モジュールの ESM の内部イーサネット・インターフェースへの接続を使用してください。
- ▶ サーバーに BMC と RSA II SlimLine が搭載されている場合、BMC の IP アドレスを 0.0.0.0 に設定して、BMC への非セキュアな直接接続を使用不可にしたことを確認してください。詳しくは、55 ページの 3.2.3、『Remote Supervisor Adapter II SlimLine』を参照してください。
- ▶ IBM Director を使用している場合、サーバーとエージェント間の暗号化通信を使用可能にしたことを確認してください。IBM Redbook 「*Implementing Systems Management Solutions using IBM Director*, SG24-6188」の第5章を参照してください。
- ▶ 少なくとも重要なファームウェア更新はインストール済みであることを確認してください。使用可能な更新については、IBM Support Web サイト <http://www.pc.ibm.com/support> を参照してください。

IBM UpdateXpress Server を使用して、ご使用のネットワーク上のサーバーから更新を使用可能にすることもできます。UpdateXpress Server は Web ベースのプログラムで、これを使用すると、ご使用のネットワーク内の中央リポジトリから IBM デバイス・ドライバーおよびファームウェア更新の複数のバージョンを管理できます。IBM UpdateXpress Server は、次のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-57426.html>

- ▶ 何らかの変更を行った後は、サービス・プロセッサの構成のバックアップを取ってください。詳しくは、251 ページの 7.2、『構成のバックアップとリストア』を参照してください。

## 7.1.2 Web インターフェース

RSA II または BladeCenter 管理モジュールの Web インターフェースをセキュアにするには、SSL を使用します。SSL の構成について詳しくは、138 ページの 5.1.1、『Secure Sockets Layer (SSL)』を参照してください。

さらに、HTTPS プロトコルのポートを変更すると、セキュリティーを一層強化できます。これは、次の方法で行えます。

1. ナビゲーション・フレームで、「**ASM Control**」（または、管理モジュールを使用している場合は、「**MM Control**」）→「**Port Assignments**」をクリックします。
2. HTTPS のポート番号を変更します。
3. 「**Save**」をクリックします。
4. 変更をアクティブにするために、「**Restart ASM**」（または、「**Restart MM**」）をクリックします。

新しいポート番号を使用して、次の URL で Web インターフェースにアクセスできるようになります（例えば、選択したポートが 4711 の場合）。

`https://9.42.171.241:4711`

### 7.1.3 コマンド・ライン・インターフェース

すべてのコマンド・ライン・インターフェース (CLI) は、デフォルトではセキュアではありません。この例外は、セキュア・シェル (SSH) です。

#### Telnet とセキュア・シェル (SSH)

RSA II の Telnet サービスを使用不可にして、代わりに SSH をアクティブにしてください。SSH をアクティブにする方法と使用法については、143 ページの 5.1.2、『セキュア・シェル (SSH)』を参照してください。

RSA II を搭載したサーバーを使用している場合、最初にそのサーバーが SSH 接続をサポートするかどうかを確認してから、Telnet サービスを使用不可にしてください。一部の古いサーバーは SSH をサポートしません。サーバーが SSH をサポートしない場合は、代わりに Web インターフェースを使用してください。

**ヒント:** ご使用のサーバーと RSA II の組み合わせで SSH が使用可能かどうかを検査するには、Web インターフェースを立ち上げて、「**ASM Control**」→「**Security**」をクリックし、「**Secure Shell (SSH) Server**」セクションがあるかどうかを調べます。

BladeCenter 管理モジュールを使用している場合は、Telnet プロトコルを使用不可にできません。SSH プロトコルをアクティブにし、Telnet のポートを変更して、Telnet の代わりに SSH を使用します。Telnet などのプロトコルのポートを変更する方法については、249 ページの 7.1.2、『Web インターフェース』を参照してください。



## MPCLI

本書の出版日現在、MPCLI の最新バージョンは、通信を暗号化する手段を提供していません。

## ASU

Advanced Settings ユーティリティ (ASU) は、サーバー上でローカルでのみ機能します。ASU とサーバー間の通信には、ネットワーク接続は使用しません。この通信はセキュアにする必要はありません (サーバー自体がセキュアであることを前提として)。

## 7.2 構成のバックアップとリストア

RSA II または BladeCenter 管理モジュールの構成作業を終了した後、構成のバックアップを取って、リストアが必要になったときに備えることをお勧めします。

### 7.2.1 バックアップ手順

構成をファイルに保管するには、Web インターフェースを立ち上げます。

1. ナビゲーション・フレームで、「**ASM Control**」(管理モジュールを使用している場合は、「**MM Control**」) → 「**Configuration File**」をクリックします。
2. 「**Backup**」をクリックして、構成を保管します。

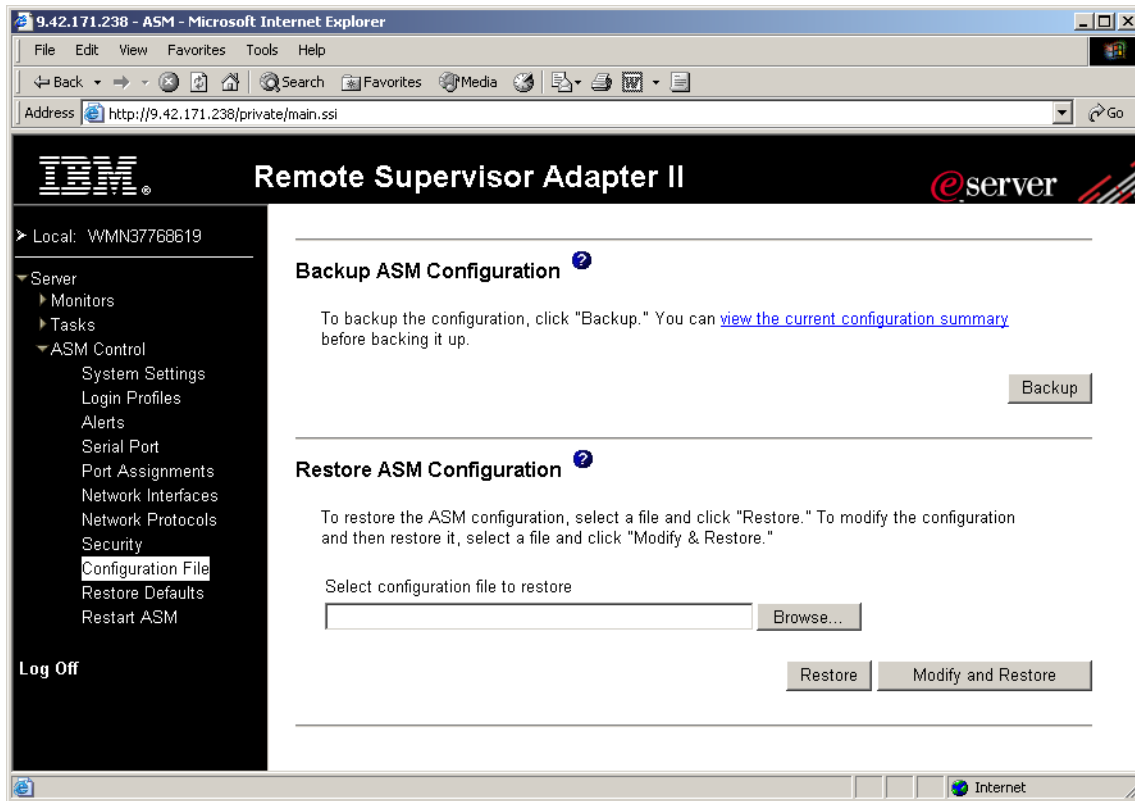


図7-1 構成のバックアップ

3. 「file download」ウィンドウがポップアップ表示されます。ファイルのフォルダーとファイル名を選択して、「Save」をクリックします。

**ヒント:** 1つのディレクトリーに複数のシステム管理ハードウェアの構成ファイルを保管する場合、バックアップ・ファイルの名前を適切に付けてください。サービス・プロセッサを搭載したサーバーまたは BladeCenter に対応したファイル名を選択してください。構成をリストアする必要があるときに、正しいファイルを容易に見付けることができます。

## 7.2.2 リストア手順

構成をリストアする必要がある場合、252 ページの図 7-1 に示したのと同じパネルを使用します。

1. ナビゲーション・フレームで、「**ASM Control**」（管理モジュールを使用している場合は、「**MM Control**」）→「**Configuration File**」をクリックします。252 ページの図 7-1 が表示されます。
2. 「Restore ASM Configuration」セクションで、「**Browse**」をクリックして、リストアする構成ファイルを選択します。
3. 元の設定をリストアする場合は「**Restore**」をクリックし、リストアする前に設定を表示または変更する場合は「**Modify and Restore**」をクリックします。
4. 「**Modify and Restore**」をクリックした場合、図 7-2 が表示され、ここで変更内容を入力できます。「**Restore Configuration**」をクリックして、先に進みます。

---

### Restore ASM Configuration

**ASM Information**

Name:

ID number:

Contact:

Location:

Host OS:

~~~~~ Section(s) Hidden ~~~~~

**Ethernet**

Interface:

DHCP:

Hostname:

**Static IP Configuration**

IP address:

Subnet mask:

Gateway address:

Data rate:

Duplex:

MTU:

Locally admin. address:

図7-2 構成ファイルのリストア

5. リストアした後、RSA II または管理モジュールを再始動する必要があります。「**Restart ASM**」（管理モジュールを使用している場合は、「**Restart MM**」）をクリックします。

**ヒント：**構成がよく似ている場合、保管されたファイルを1つのRSA II から別のRSA II にリストアしたり、1つの管理モジュールから別の管理モジュールにリストアすることもできます。リストアする前に、構成ファイル内の情報とIP構成パラメーターを変更したことを確認してください。

## 7.3 すべての BladeCenter モジュールへのリモート・アクセスの提供

BladeCenter 内のスイッチ・モジュールにアクセスして管理するには、管理モジュール（外部および内部インターフェース）とスイッチ・モジュールが同じ IP サブネット上にあることが必要です。

**注：**リダンダント管理モジュールを搭載している場合、IP 構成はアクティブ・モジュールから検索されます。リダンダント・モジュールの IP 設定は構成しないでください。管理機能がリダンダント・モジュールにフェイルオーバーされた場合、リダンダント・モジュールは障害を起こした 1 次モジュールの IP 構成を引き継ぎます。

管理モジュールは、256 ページの図 7-3 に示すように、外部および内部イーサネット・インターフェースを備えています。

- ▶ 外部イーサネット：DHCP 構成または固定（デフォルトは、192.168.70.125）
- ▶ 内部：固定（デフォルトは、192.168.70.126）

管理モジュールから、ベイ 1、2、3、4 のイーサネット・スイッチ・モジュール（ESM）の Web インターフェースにも接続できます。ESM のデフォルト・アドレスは、次のとおりです。

- ▶ 192.168.70.127（ベイ 1）
- ▶ 192.168.70.128（ベイ 2）
- ▶ 192.168.70.129（ベイ 3）
- ▶ 192.168.70.130（ベイ 4）

デフォルトでは、スイッチ・モジュールの外部実動ポートからは ESM にアクセスできません。これはこのままの状態に保ち、シャード管理の単一入り口点（管理モジュール経由の）を維持することをお勧めします。これを使用可能に設定する場合は、ご使用の実動ネットワーク上で有効なアドレスを構成する必要があります。

管理モジュールの内部インターフェースは、ベイ 1 から 4 の ESM の管理インターフェースに接続されています。スイッチ・モジュールへの接続のアドレスは、256 ページの図 7-3 に示されています。

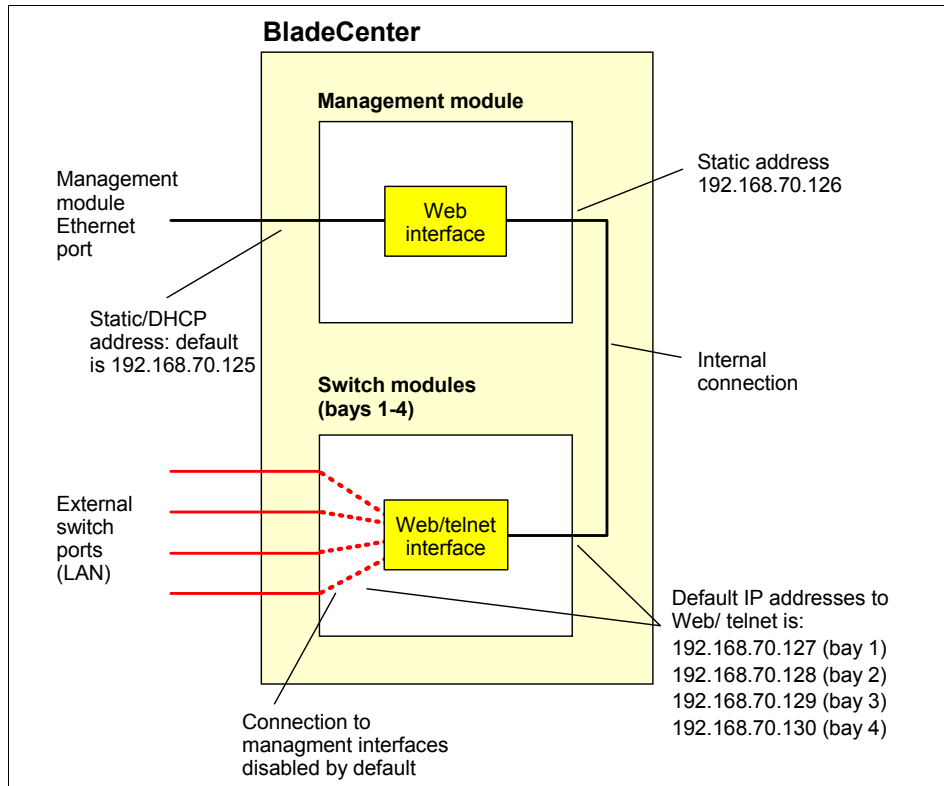


図 7-3 BladeCenter 内部イーサネット

ESM は、管理用に構成できる追加の外部インターフェースを備えています。この外部インターフェースは、デフォルトでは使用不可になっています。BladeCenter の単一管理点を確保するために、このインターフェースは使用可能してはなりません。このことは、特に、管理モジュールが管理 LAN に接続され、ESM 外部インターフェースが実動 LAN に接続されている場合に重要です。

**ヒント:** 管理タスクを実動 LAN から分離するには、管理目的の専用のイーサネット・セグメントを構築する必要があります。これは、VLAN でも、物理的に分離された LAN でも構いません。専用の管理 LAN を設けると、ユーザーやコンピューターによるシステム管理ハードウェアへのアクセスを容易に制御できます。

さらに、リモート・メディアを使用しても（例えば、インストールの目的で）、実動 LAN は影響を受けません。システム管理用に追加のソフトウェアを使用する場合は、専用の PCI ネットワーク・アダプターを使用して、ご使用のサーバーを管理 LAN に接続してください。

管理モジュールの外部イーサネット・インターフェースの構成方法についての詳細は、98 ページの 4.2.2、『ネットワーク設定』を参照してください。

次のステップは、管理モジュールと他のすべてのスイッチ・モジュールの内部 IP アドレスを構成することです。すべての内部インターフェースは、デフォルトの IP アドレスを持っています。これを変更するには、管理モジュールの Web インターフェースを立ち上げて、以下のステップを実行します。

1. 「**MM Control**」 → 「**Network Interfaces**」をクリックします。
2. 「**Internal Network Interface (eth1)**」までスクロールダウンします。
3. インターフェースが使用可能であることを確認します。
4. IP 構成パラメータを入力します。
5. 「**Save**」をクリックします。

次に、搭載されたすべてのモジュールの内部 IP インターフェースを構成します。

1. 「**I/O Module Tasks**」 → 「**Management**」をクリックします。
2. IP 構成パラメータを入力します。
3. 「**Save**」をクリックします。
4. 搭載されたすべてのモジュールについて、ステップ 2 と 3 を繰り返します。

The screenshot shows the IBM BladeCenter Management Module interface. The left sidebar contains a navigation menu with options like 'Monitors', 'Blade Tasks', 'I/O Module Tasks', and 'MM Control'. The main content area is titled 'I/O Module Management' and includes a section for 'Bay 1 (Ethernet SM)'. Under this section, there are two sub-sections: 'Current IP Configuration' and 'New Static IP Configuration'. The 'Current IP Configuration' shows a static IP of 9.42.171.243. The 'New Static IP Configuration' section has a status of 'Enabled' and a text instruction: 'To change the IP configuration for this switch module, fill in the following fields and click "Save". This will save and enable the new IP configuration.' Below this are three input fields: 'IP address' (9.42.171.243), 'Subnet mask' (255.255.255.0), and 'Gateway address' (9.42.171.3). A 'Save' button is located at the bottom right of the page.

図 7-4 入出力モジュールの IP 設定の構成

構成をテストするために、すべてのスイッチ・モジュールについて、以下を実行します。

1. 「**Advanced Management**」をクリックします。
2. 「**Send Ping Requests**」をクリックします。
3. 「**Ping Switch Module**」をクリックします。次の図のようになります。



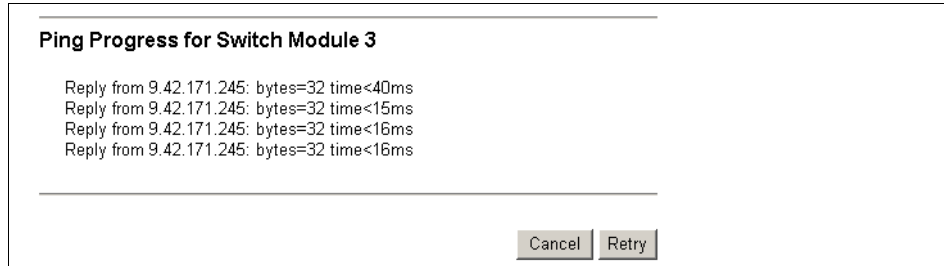


図 7-5 ping 要求

すべてのスイッチ・モジュールが ping 要求に応答したことを確認します。これで、管理モジュールを介して、またはモジュールの IP アドレスを指定してブラウザを立ち上げることによって、各モジュールの Web インターフェースにアクセスできるようになりました。

スイッチ・モジュールの管理については、モジュールに付属の資料を参照してください。

## 7.4 マルチ・サブネット環境

このシナリオでは、ネットワークは 3 つの分離されたサブネット（実動、テスト、管理）に分けられています。ユーザーは、ハードウェア・ベースのシステム管理ソリューションを実装する必要があります。

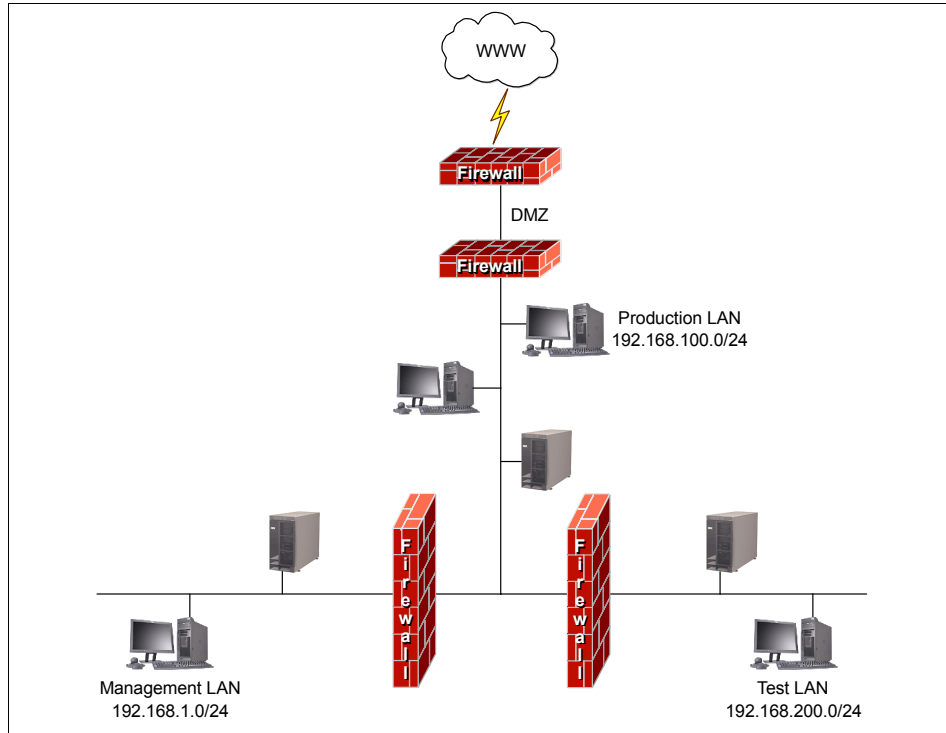


図7-6 3つのサブネットを持つネットワークの例

## 7.4.1 一般的な考慮事項

RSA II アダプターと BladeCenter 管理モジュールのイーサネット・ポートを管理 LAN に接続します。

内蔵 BMC を備えたサーバー (x236、x336、または x346) が RSA II SlimLine を搭載していない場合、BMC はシステム・イーサネット・ポートの 1 つをオペレーティング・システムと共用するため、BMC は実動ネットワークに接続されるという事実を理解しておくことが重要です。この場合、2 つの可能性があります。

**ヒント:** 2 つのイーサネット・ポートのうち、どちらのポートを BMC が使用するかについては、サーバーに付属の資料を参照してください。通常、BMC が使用するイーサネット・ポートは、パワー・サプライに近い方のポートです。

- ▶ 1 つだけのイーサネット・ポートをオペレーティング・システム用に使用し、他方のポートは BMC 専用にする。
  - a. 管理 LAN の IP 設定を使用して BMC を構成し、イーサネット・ケーブルを接続します。
  - b. オペレーティング・システム内で、BMC 用に使用されるイーサネット・ポートを使用不可に設定します。
- ▶ 両方のイーサネット・ポートをオペレーティング・システム用に使用し、そのうちの 1 つのポートを BMC と共有する。
  - a. 実動ネットワークの IP 設定を使用して BMC を構成します。
  - b. BMC が管理 LAN に（および、その逆に）到達できることを確認します。

**注：**オペレーティング・システムにリダンダント・イーサネット接続を持たせるために、2 番目のオプションを使用することをお勧めします。リダンダント・イーサネット・ポートの要件を備えていない場合は、最初のオプションを使用してください。

## 7.4.2 他のサブネットへのアクセス

例えば、実動ネットワーク上の管理者のデスクトップから管理ネットワークに接続するには、接続装置（ルーターとファイアウォール）を正しく構成する必要があります。

**ping** コマンドを使用して、TCP/IP のルーティングをテストします。ping (ICMP) パケットがファイアウォールを通過できることを確認してください。ポートのオープンが必要な場合もあります。該当するポート番号については、91 ページの 3.6、『リモート管理アダプター II によって使用されるポート』、および 134 ページの 4.6、『管理モジュールによって使用されるポート』を参照してください。

**ヒント：**MPCLI は、IBM Director コマンドと同じポート（TCP ポート 6090）を使用します。

必ず、実際に必要であり、使用されるポートのみをオープンしてください。ポートは、サービス・プロセッサにアクセスする必要があるユーザー・グループに対してのみオープンしてください。

## 7.4.3 異なるサブネット内の DHCP

DHCP サーバーがインストールされている場合、DHCP サーバーは、通常はルーターによって転送されないブロードキャストを扱うため、同じサブネット内の DHCP クライアントの IP アドレスのみを提供します。ルーターが RFC 1542

準拠の場合（つまり、DHCP ディスカバー・パケットを他のサブネットに転送できる場合）は、ルーターが機能するため、以下のオプションを考慮する必要はありません。ルーターが RFC 1542 準拠でない場合、他の 2 つのサブネット内で DHCP を使用可能にするには、2 つの選択肢があります。

- ▶ 他の 2 つのサブネットのそれぞれに DHCP サーバーを 1 つインストールする。
- ▶ 他の 2 つのサブネットに DHCP リレー・エージェントをインストールする。DHCP リレー・エージェントは、例えば Windows または Linux を実行しているサーバーにインストールできます。

プリブート実行環境（PXE）を IBM Remote Deployment Manager（RDM）のような開発サービスと一緒に使用する場合は、DHCP サーバーが BOOTP プロトコルも提供することを確認してください。

## 7.5 ユーザー ID とパスワードの一括構成

このシナリオでは、RSA II および BladeCenter 管理モジュールのユーザー ID とパスワードを一括構成する方法を見てみます。多数のサーバーを構成する必要がある場合、あるいは会社の方針でパスワードを定期的に変更する場合、このシナリオは非常に役立ちます。

このシナリオで使用するユーティリティは、MPCLI です。これについては、186 ページの 6.3、『管理プロセッサ・コマンド・ライン・インターフェース』で説明しています。

### スクリプト・ファイルの作成

最初に、例 7-1 に示すような、スクリプト・ファイル `chnguidpwd.script` を作成します。このスクリプトは、サーバー 9.42.171.216 上のユーザー ID ADMIN3 を変更（または、作成）します。

**ヒント:** テキスト・エディターを使用してスクリプトを作成する代わりに、**commandfile** コマンドを使用して、対話式モードでスクリプトを生成することもできます。『MPCLI コマンドを使用したスクリプト記述』（198 ページ）を参照してください。

例 7-1 Script `c:\IBM\chnguidpwd.script`

---

```
logonip -hostname 9.42.171.216 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
```

---

ご使用の環境にあるサーバーの数だけ、この3行のコマンドを追加していきます。それぞれのRSA/BCMMを変更した後で、必ずlogoffを指定してください。例えば、このシナリオの場合は維持するシステムが4つあるため、スクリプトは次のようになります。

*例7-2 4つのシステムのすべてに対して実行するように変更したスクリプト*

---

```
logoff
logonip -hostname 192.168.70.120 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
logonip -hostname 192.168.70.121 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
logonip -hostname 192.168.70.122 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
logonip -hostname 192.168.70.123 -userid USERID -password PASSWORD
setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
logoff
```

---

**ヒント:** スクリプト・ファイルにはコメントも含めることができ、それぞれのコメント行を#文字で開始します。例えば、次のように入力します。

```
#Ensure you are not logged into another Service Processor.
logoff
```

スクリプトを実行するには、mp>プロンプトで、次のコマンドを実行します。

```
inputfile c:¥IBM¥chnguidpwr.script
```

スクリプト・ファイル内の各コマンドの出力が、画面に表示されます。このシナリオの例では、出力は次のようになります。

*例7-3 例のスクリプトからの出力*

---

```
mp> inputfile c:¥ibm¥chngspuid.script
FAILURE: You are not logged in.
SUCCESS: logonip -hostname 9.42.171.238 -userid USERID -password PASSWORD
SUCCESS: setdialinentry -index 2 -id ADMIN2 -password ADMIN2 -dialback false -readonly false
SUCCESS: setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
SUCCESS: setdialinentry -id ADMIN3
true
SUCCESS: setdialinentry -password ADMIN3
true
SUCCESS: setdialinentry -dialback false
true
SUCCESS: setdialinentry -readonly false
true
```

```
SUCCESS: logoff
SUCCESS: logonip -hostname 9.42.171.216 -userid USERID -password PASSWORD
SUCCESS: setdialinentry -index 2 -id ADMIN2 -password ADMIN2 -dialback false -readonly false
SUCCESS: setdialinentry -index 3 -id ADMIN3 -password ADMIN3 -dialback false -readonly false
SUCCESS: setdialinentry -id ADMIN3
true
SUCCESS: setdialinentry -password ADMIN3
true
SUCCESS: setdialinentry -dialback false
true
SUCCESS: setdialinentry -readonly false
true
SUCCESS: logoff
mp>
```

**注:** 上記の出力で、状態が **FAILURE** であっても、これは実際に失敗したわけではありません。ユーザーがログオンせずにログオフしようとする、MPCLI はこの出力を表示します。

コマンドが正常に実行されたかどうかを検査する場合、特定のサーバーの Web インターフェースを介して検査できます。上記の変更を使用して更新された Web インターフェースの例は、264 ページの図 7-7 を参照してください。

| Login ID                        | Access     |
|---------------------------------|------------|
| 1. <a href="#">USERID</a>       | Read/Write |
| 2. <a href="#">ADMIN2</a>       | Read/Write |
| 3. <a href="#">ADMIN3</a>       | Read/Write |
| 4. <a href="#">~ not used ~</a> |            |
| 5. <a href="#">~ not used ~</a> |            |
| 6. <a href="#">~ not used ~</a> |            |
| 7. <a href="#">~ not used ~</a> |            |

図 7-7 スクリプト・ファイルの実行後の RSA II ログイン・プロファイルの変更の表示

## 7.6 RSA II の出荷時のデフォルト値へのリセット

このセクションでは、RSA または RSA II を出荷時のデフォルト値に戻す方法について説明します。

**注:**行われる変更には、次のものが含まれます。

- ▶ ユーザー ID とパスワードをデフォルト設定 USERID と PASSWORD (0 はゼロで、文字の O ではありません) にリセットします。
- ▶ RSA II の場合、IP アドレスの設定をデフォルトの DHCP に戻し、固定 IP アドレス 192.168.70.125 とサブネット・マスク 255.255.255.0 を設定します。
- ▶ RSA の場合、IP アドレスを DHCP のデフォルト設定に戻し、固定アドレスのバックアップは使用しません。
- ▶ ホスト名を ASMA + サービス・プロセッサの MAC アドレス (例えば、ASMA00096b0a8469) に戻します。

リセット後にこれらのサービス・プロセッサを再構成する容易な方法は、ASM インターコネクト・ネットワーク接続を介して接続することです。

このタスクを実行するには、4 とおりの方法があります。

- ▶ ASU: 下記を参照。
- ▶ IBM Director: 『IBM Director の使用』 (266 ページ) を参照。
- ▶ MPCLI: 『MPCLI の使用』 (268 ページ) を参照。
- ▶ Web インターフェース (ナビゲーション・メニューから、「**Restore Defaults**」を選択します)。

ASU 方式と IBM Director 方式は、サービス・プロセッサ上の有効なユーザー ID とパスワードを知っている必要はありません。ただし、MPCLI の場合、ユーザーはこの情報を知っている必要があります。

## 7.6.1 ASU の使用

ASU を使用して RSA または RSA II を出荷時のデフォルト値に戻す必要が生じるのは、管理者がサービス・プロセッサの IP アドレス、ユーザー ID、またはパスワードを忘れ (あるいは、会社を離れ)、会社が IBM Director を実装していない場合です。

ASU を使用して、アダプターを出荷時のデフォルト値にリセットするには、次のようにします。

1. サーバー上にローカルで ASU をインストールします (170 ページの 6.2、『Advanced Settings ユーティリティ』を参照してください)。
2. RSAI/RSII 定義ファイルを ASU に追加します (173 ページの 6.2.4、『ASU 定義ファイルの使用』を参照してください)。
3. 次のコマンドを入力して、サービス・プロセッサをリセットします。
  - Windows の場合 : **asu resetrsa**

- Linux の場合: `./asu resetrsa`
4. サービス・プロセッサは、出荷時のデフォルト値にリセットされた後、再始動されます。
  5. ASU を使用して、一部の基本設定も構成できます。
    - DHCP の使用不可化
    - 固定 IP アドレス、サブネット・マスク、およびゲートウェイの設定
    - デフォルト・ユーザー ID の新規ユーザー ID への置き換え（例えば、`u=lesley`、`p=baln`）。

例 7-4 のような SET コマンドを使用します（Linux の場合は、**asu** の代わりに `./asu` を使用します）。SET コマンドの全リストは、177 ページの例 6-1 を参照してください。

*例7-4 基本RSA 設定を構成するためのASU コマンド*

---

```
asu set RSA_DHCP1 Disabled
asu set RSA_Network1 Enabled
asu set RSA_HostIPAddress1 xxx.xxx.xxx.xxx
asu set RSA_HostIPSnet1 xxx.xxx.xxx.xxx
asu set RSA_GatewayIPAddress1 xxx.xxx.xxx.xxx
asu set RSAString_loginId1 "lesley"
asu set RSAString_Password1 "baln"
```

---

ヒント: これらのコマンドをバッチで実行する方法については、185 ページの 6.2.8、『ASU バッチ・コマンド』を参照してください。

## 7.6.2 IBM Director の使用

IBM Director も、RSA と RSA II の設定を出荷時のデフォルト設定にリセットする機能を備えています。次の要件を満たす必要があります。

- ▶ リセットするサービス・プロセッサを搭載したサーバー（これをターゲット・サーバーと呼びます）上に、IBM Director エージェントがインストールされている。
- ▶ ご使用のサーバー用の適切なサービス・プロセッサ・ドライバがインストールされている。
- ▶ ご使用のネットワーク内のサーバー上に IBM Director サーバーがインストールされている。

IBM Director を使用して、アダプターを出荷時のデフォルト値にリセットするには、次のようにします。

1. IBM Director 管理コンソールを使用して、ターゲット・サーバーが IBM Director によって検出されたことを確認します。



2. 「Tasks」 ペインで、「**Management Processor Assistant**」 タスクを展開します。
3. 「**Configuration**」 サブタスクを選択し、それをターゲット・サーバー上にドラッグ・アンド・ドロップします。267 ページの図 7-8 が開きます。サービス・プロセッサに接続できない場合は、ポップアップ・メッセージが表示されます。サービス・プロセッサのドライバーが正しくインストールされていることを確認します。

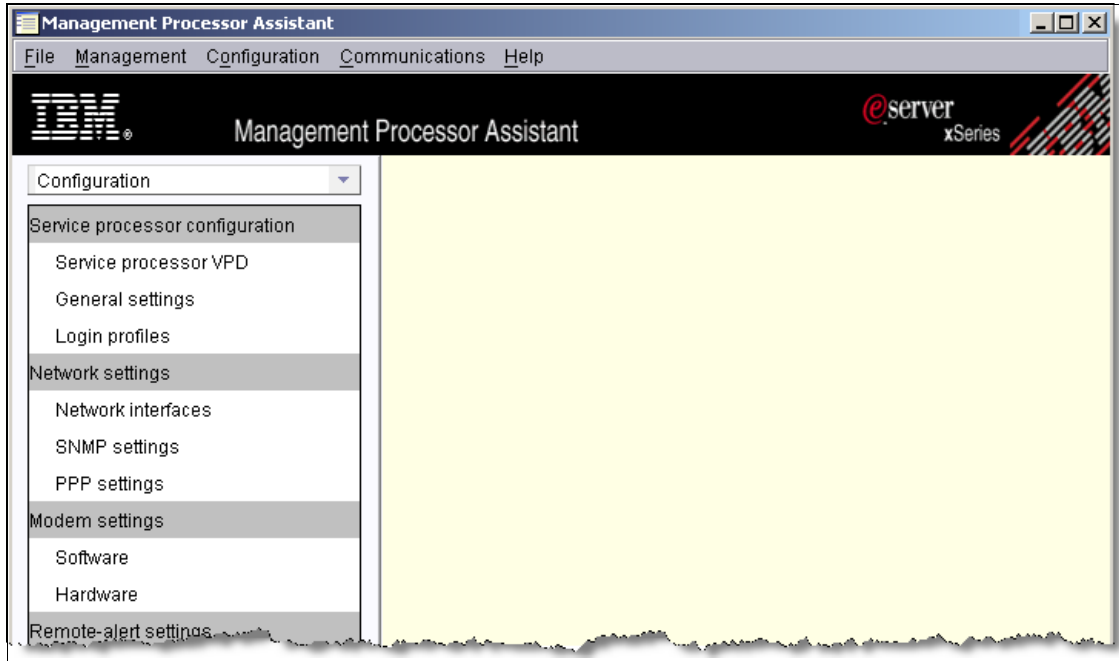


図 7-8 IBM Director の MPA 構成ビュー

4. サービス・プロセッサを出荷時のデフォルト値に復元するには、「**General settings**」をクリックします。図 7-9 が表示されます。

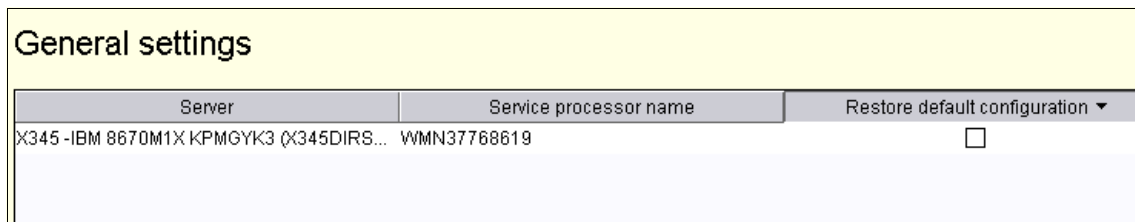


図 7-9 「MPA configuration」 ウィンドウ内の 「General settings」 ウィンドウ

5. 「Reset default configuration」の見出しの下のチェック・ボックスにチェック・マークを付けます（必要な場合は、右にスクロールしてください。図 7-9 を参照）。
6. 上記のメニューで、「Apply」をクリックして、サービス・プロセッサへの変更を保管します。
7. これで再度、すべての出荷時デフォルト値が設定され、このインターフェースを使用して、またはユーザーが選択した別のインターフェースを使用して、再構成を行う準備が整いました。

**注：**RSA または RSAII アダプターをリセットするための上記のタスクは、いずれもセキュリティ上のリスクはありません。ASU はローカル・ツールであり、会社のシステム管理者のみがインストールするのでセキュアです。IBM Director は、IBM Director 管理コンソールにログオンするためにユーザー ID とパスワードが必要なので、完全にセキュアです。

### 7.6.3 MPCLI の使用

サービス・プロセッサの IP アドレス、ユーザー ID、およびパスワードを知っている場合、MPCLI ユーティリティを使用して、構成を出荷時のデフォルト設定にリセットできます。ユーザーがログインできるオペレーティング・システムがサーバーにインストールされていない場合、MPCLI が役立ちます。

MPCLI を使用して、アダプターを出荷時のデフォルト値にリセットするには、次のようにします。

1. MPCLI を別のワークステーションにインストールします。詳しくは、191 ページの 6.3.5、『MPCLI のインストール』を参照してください。
2. MPCLI を開始します。
  - Windows: 「スタート」→「プログラム」→「IBM」→「MPCLI」→「MPCLI」
  - Linux: `/opt/IBMmpcli/bin/MPCLI.bsh`
3. MPCLI コマンド・プロンプトで、次のコマンドを入力します（サービス・プロセッサの IP アドレス、ユーザー ID、およびパスワードは、ユーザー自身の値で置き換えてください）。  
**logonip -hostname xxx.xxx.xxx.xxx -userid userid -password password**
4. 次のコマンドを入力して、サービス・プロセッサをリセットします。  
`resetmp`

注：デフォルトのネットワーク構成は、次のとおりです。

- ▶ RSA II: DHCP サーバーに到達できる場合は、DHCP を使用します。それに失敗する場合は、固定アドレス 192.168.70.125、サブネット 255.255.255.0 に設定します。
- ▶ RSA: DHCP を使用します。DHCP サーバーが見つからない場合、IP アドレスは割り当てられません。

5. MPCLI を使用して、一部の基本設定も構成できます。

- DHCP の使用不可化
- 固定 IP アドレス、サブネット・マスク、およびゲートウェイの設定
- デフォルト・ユーザー ID の新規ユーザー ID への置き換え（例えば、u=lesley、p=ba1n）

このタスクには、スクリプトを使用できます。『MPCLI コマンドを使用したスクリプト記述』（198 ページ）を参照してください。このタスクに使用されるコマンドを、例 7-5 に示します（該当する場合、**logonip** コマンドの DHCP が割り当てたサービス・プロセッサのアドレスを置き換えてください）。

例 7-5 基本的なデフォルト値を設定するための MPCLI コマンド

```
logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
setnethw -interface 1 -enabled true
setdhcp -enabled false
setip -interface 1 -method static
setip -interface 1 -ipaddress xxx.xxx.xxx.xxx
setip -interface 1 -gateway xxx.xxx.xxx.xxx
setip -interface 1 -subnet xxx.xxx.xxx.xxx
setdialinentry -index 1 -id userid -password password -dialback false -readonly false
```

注：RSA II に適用できる 3 つの method タイプがあります（RSA は最初の 2 つだけをサポートします）。

- ▶ static - 固定 IP アドレスを使用します。
- ▶ dhcp - DHCP サーバーから割り当てられた IP アドレスを取得します。
- ▶ dhcpstatic - DHCP サーバーが使用不可の場合、固定 IP アドレスを使用します。

## 7.7 リモート側での ASU の使用法

170 ページの 6.2、『Advanced Settings ユーティリティ』で説明したように、ASU は、ローカル側でサーバーにインストールして実行するように設計された

ユーティリティーです。ただし、IBM Director の「File Transfer」および「Remote Console」タスクを一緒に使用すると、リモート側で ASU ツールをインストールして使用できるようになります。

このシナリオは、完全自動のリモート環境において、サーバーを再起動せずにサーバーの CMOS または RSA/RSA II アダプターの設定を変更する必要がある場合に役立ちます。

このシナリオは、以下のことを前提としています。

- ▶ ご使用の環境に IBM Director 管理サーバーがインストール済みである。
- ▶ ASU ユーティリティーを使用するサーバー上に IBM Director エージェントがインストール済みである。
- ▶ リモート・ロケーションで、例えば、ご使用のラップトップに IBM Director コンソールがインストール済みであり、IBM Director サーバーに接続できる。
- ▶ IBM Director 管理サーバーから IBM Director エージェントを検出できる。
- ▶ 必要な ASU コードをラップトップまたはリモート・ロケーションにダウンロード済みである。必要なコードについての詳細は、173 ページの 6.2.3、『ASU と定義ファイルのダウンロード』を参照してください。

IBM Director のエージェントとサーバーの部分のインストールについて詳しくは、「*IBM Director Installation Guide*」を参照してください。

リモート側での ASU の使用は、次のようにして行います。

1. リモート・コンソールから IBM Director サーバーをオープンし、接続します。
2. 接続した後、右側のペインでタスク「**File Transfer**」を選択して、ASU を使用するサーバーの上に、これをドラッグ・アンド・ドロップします。「File Transfer」ウィンドウが開きます。図 7-10 を参照してください。

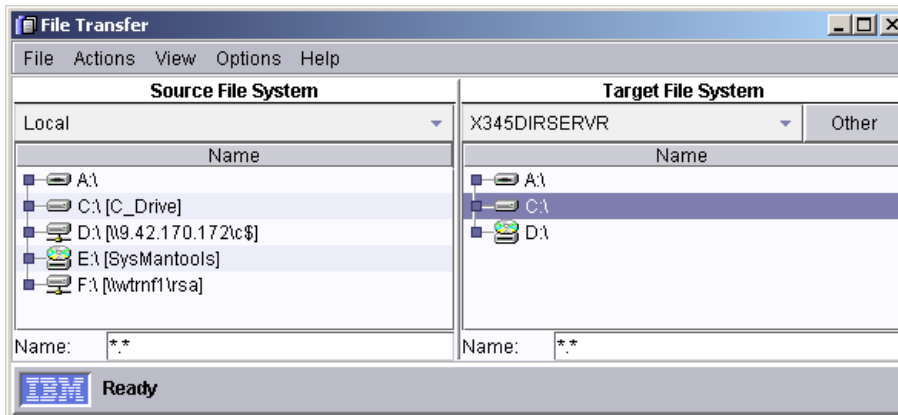


図7-10 「File transfer」 ウィンドウ

3. 「Local」 (左側) ペインから、ASU ツールのダウンロード先のディレクトリーまでナビゲートし、ディレクトリーを展開します。271 ページの図 7-11 を参照してください。

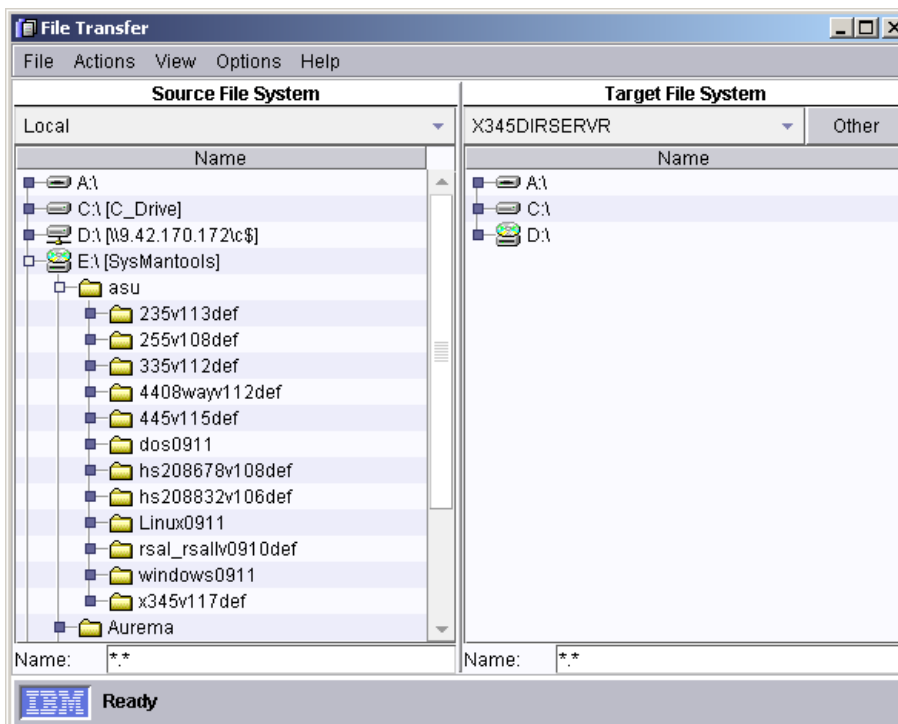
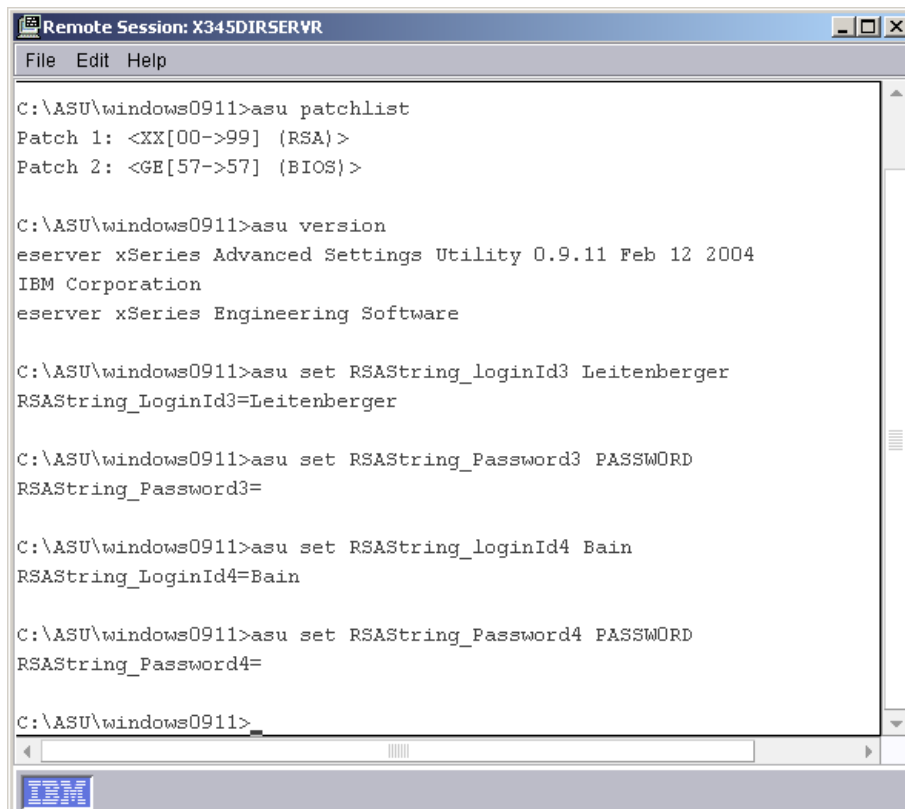


図7-11 ローカル上のASU ダウンロード・ディレクトリー・ロケーション

4. リモート・サーバー上の ASU ファイルのコピー先ディレクトリーを展開します。
5. ローカル・システムから ASU ファイルを選択して、リモート・ディレクトリー・ロケーションに、それをドラッグ・アンド・ドロップします。
6. これで、このリモート・サーバーに ASU をインストールする準備ができました。ASU ファイルのアンパック方法については、173 ページの 6.2.3、『ASU と定義ファイルのダウンロード』、ASU への必要な定義の追加方法については、173 ページの 6.2.4、『ASU 定義ファイルの使用』を参照してください。
7. ASU の構成を完了すると、リモート側で操作を開始できるようになります。
8. Director コンソールから、「**Remote Session**」タスクを選択して、ASU を使用するシステム上に、それをドラッグ・アンド・ドロップします。リモート・セッションがオープンします。これで、リモート側で操作を開始し、サーバーに対して ASU コマンドを発行できるようになりました。IBM Director の「Remote Session」タスクを使用して、リモート側で ASU コマンドを実行する例は、272 ページの図 7-12 を参照してください。



```
Remote Session: X345DIRSERVER
File Edit Help
C:\ASU\windows0911>asu patchlist
Patch 1: <XX[00->99] (RSA)>
Patch 2: <GE[57->57] (BIOS)>

C:\ASU\windows0911>asu version
eserver xSeries Advanced Settings Utility 0.9.11 Feb 12 2004
IBM Corporation
eserver xSeries Engineering Software

C:\ASU\windows0911>asu set RSAString_loginId3 Leitenberger
RSAString_LoginId3=Leitenberger

C:\ASU\windows0911>asu set RSAString_Password3 PASSWORD
RSAString_Password3=

C:\ASU\windows0911>asu set RSAString_loginId4 Bain
RSAString_LoginId4=Bain

C:\ASU\windows0911>asu set RSAString_Password4 PASSWORD
RSAString_Password4=

C:\ASU\windows0911>
```

図 7-12 リモート側で ASU を実行している IBM Director の「Remote Session」

## 7.8 リモート側での BIOS とファームウェアの更新

どのような環境も、変更管理の手順を確立しておく必要があります。それによって、サーバーの BIOS、ファームウェア、デバイス・ドライバーを、常に最新リリースに更新された状態に保つことができます。

サーバーのサービス・プロセッサのファームウェアとシステム BIOS をアップグレードするには、さまざまな方法があります。

- ▶ MPCLI (273 ページの 7.8.1、『MPCLI を使用したファームウェアの更新』で説明)
- ▶ IBM Director ソフトウェア配布 (275 ページの 7.8.2、『IBM Director を使用したファームウェア更新』で説明)
- ▶ UpdateXpress RemoteUX (283 ページの 7.8.3、『UpdateXpress RemoteUX を使用したファームウェアの更新』で説明)
- ▶ RSA II Web インターフェース
- ▶ RSA II Telnet/ 端末インターフェース
- ▶ Remote Deployment Manager

このシナリオでは、最初の 3 つの方法を説明します。表 7-1 は、この 5 つのツールを使用して実行できる更新をリストしています。

表 7-1 リモート側で SP ファームウェアとシステム BIOS を更新する方法

| 方式                        | SP ファームウェアの更新 | システム BIOS の更新 |
|---------------------------|---------------|---------------|
| MPCLI                     | 可             | 不可            |
| IBM Director ソフトウェア配布     | 可             | 可             |
| UpdateXpress RemoteUX     | 可             | 可             |
| RSA II Web インターフェース       | 可             | 不可            |
| RSA II Telnet/ 端末インターフェース | 可             | 不可            |
| Remote Deployment Manager | 可             | 可             |

### 7.8.1 MPCLI を使用したファームウェアの更新

MPCLI を使用した場合、RSA、RSA II、および BladeCenter 管理モジュールのファームウェアのみをアップグレードできます。

ファームウェアは、次のサイトからダウンロードできます。

<http://www.pc.ibm.com/support>

必要なファイルは、次の方法で入手できます。

- ▶ **BladeCenter 管理モジュール** : BCMM ファームウェア更新 PKT ファイルは、ZIP ファイルとしてダウンロードできます。必ず、ご使用の構成で使用される特定の管理モジュール用のファームウェア更新をダウンロードしてください。
- ▶ **RSA** : RSA ファームウェア更新ファイルは、EXE ファイルとしてダウンロードできます。EXE ファイルを実行すると、PKT ファイルが入っているディスクレットが作成されます。EXE ファイルは2つあります (アップグレードに必要な各ディスクレット用に1つずつ)。必ず、ご使用のサーバー用の特定の RSA ファームウェア更新をダウンロードしてください。
- ▶ **RSA II** : RSA II ファームウェア更新 PKT ファイルは、ZIP ファイルとしてダウンロードできます。必ず、ご使用のサーバー用の特定の RSA II ファームウェア更新をダウンロードしてください。

このシナリオでは、リモート側で **BladeCenter 管理モジュール** のファームウェアをバージョン 1.14 から 1.15 にアップグレードします。

1. 「スタート」→「プログラム」→「IBM」→「MPCLI」とクリックして、MPCLI を開始します。
2. RSA、RSAII、または BCMM のファームウェアをアップグレードする場合、次の3つのコンポーネントをアップグレードする必要があります。
  - メイン・アプリケーション : CNETMNUS.PKT
  - ブート ROM : CNETBRUS.PKT
  - リモート制御 : CNETRGUS.PKT
3. この更新を実行するために必要な MPCLI コマンドを、例 7-6 に示します。

**注** : IP アドレス、ユーザー ID、パスワード、および PKT ファイルのディレクトリーの場所は、ユーザー自身の設定値で置き換える必要があります。

#### 例 7-6 管理モジュールのファームウェアを更新するためのコマンド

```
mp> logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
mp> fwupdate -mn d:¥bladecenter¥CNETMNUS.PKT
mp> fwupdate -br d:¥bladecenter¥CNETBRUS.PKT
mp> fwupdate -vnc d:¥bladecenter¥CNETRGUS.PKT
mp> restartmp
mp> logoff
```

各コマンドの出力を例 7-7 に示します。



```
mp> logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
SUCCESS: logonip -hostname 192.168.70.125 -userid USERID -password PASSWORD
mp> fwupdate -mn d:¥bladecenter¥CNETMNUMS.PKT
Interrupting the firmware update can damage your system!
Please DO NOT cancel the operation while in progress.
FIRMWARE UPDATE: Started.
You must update ALL available firmware for Management Module and then must issue 'restartmp'
from the command line in order for 'fwupdate' to take affect.
mp> fwupdate -br d:¥bladecenter¥CNETBRUS.PKT
Interrupting the firmware update can damage your system!
Please DO NOT cancel the operation while in progress.
FIRMWARE UPDATE: Started.
You must update ALL available firmware for Management Module and then must issue 'restartmp'
from the command line in order for 'fwupdate' to take affect.
mp> fwupdate -vnc d:¥bladecenter¥CNETRGUS.PKT
Interrupting the firmware update can damage your system!
Please DO NOT cancel the operation while in progress.
FIRMWARE UPDATE: Started.
You must update ALL available firmware for Management Module and then must issue 'restartmp'
from the command line in order for 'fwupdate' to take affect.
mp> restartmp
SUCCESS: restartmp
PASSED: The management processor has been successfully restarted. Please Logoff and
reconnect.
mp> logoff
SUCCESS: logoff
```

---

4. これで、BladeCenter MM はアップグレード済みのレベルになっているはず  
です。

## 7.8.2 IBM Director を使用したファームウェア更新

IBM Director を使用する場合は、アップグレードを実行する時期をスケ  
ジュールできることです。また、一度に複数のサーバーをアップグレードでき  
るのも有利です。

このシナリオでは、x345 のすべてのファームウェアをアップグレードします。  
これには、次のものが含まれます。

- ▶ x345 システム BIOS
- ▶ x345 ISMP ファームウェア
- ▶ x345 診断
- ▶ x345 RSA II ファームウェア

このシナリオは、以下のことを前提としています。

- ▶ ご使用の環境に IBM Director 管理サーバーがインストール済みである。
- ▶ アップグレードするサーバーに IBM Director エージェントがインストール済みである。
- ▶ リモート・ロケーションで、例えば、ご使用のラップトップに IBM Director コンソールがインストール済みであり、IBM Director サーバーに接続できる。
- ▶ IBM Director 管理サーバーから IBM Director エージェントを検出できる。

IBM Director のエージェント部分とサーバー部分のインストールについての詳細は、「*IBM Director Installation Guide*」を参照してください。

さらに、UpdateXpress の最新リリースもダウンロードする必要があります。これは、次のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-53046.html>

UpdateXpress は、自動開始プログラムが入っている CD-ROM です。これを使用すると、システムのファームウェアと Windows デバイス・ドライバを CD 上に定義された最新レベルに維持することができ、不要なシステム停止を防止するのに役立ちます。

UpdateXpress は、現行のデバイス・ドライバとファームウェアのレベルを自動的に検出し、ユーザーに提示します。次に、ユーザーが特定のアップグレードを選択するか、または UpdateXpress がアップグレードの必要性を検出したすべてのシステム・レベルを更新するかを選択するオプションが提供されます。

UpdateXpress CD に収容された更新ファイルは、IBM Director の「Software Distribution」タスクにインポートすることもできます。このシナリオでは、この方法を使用します。

以下の手順に従って、x345 のファームウェアをアップグレードします。

1. リモート・ロケーションで、UpdateXpress CD をご使用の CD ドライブに挿入します。
2. IBM Director コンソールをオープンし、Director サーバーにログインします。
3. 「Software Distribution」タスクを選択し、タスクを右クリックして、「Open」を選択します。「Software Distribution Manager」ウィンドウが開きます。「Wizards」ファイルを展開します。詳細は、図 7-13 を参照してください。

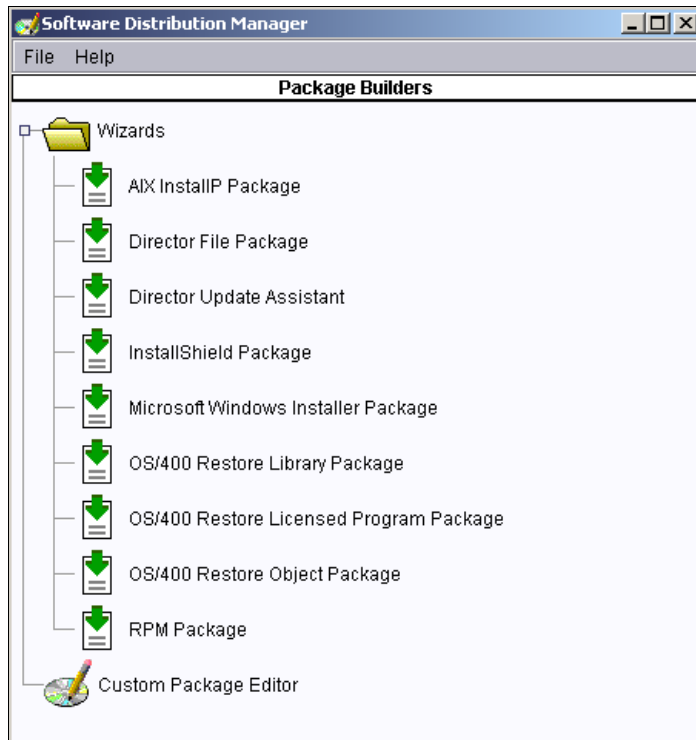


図 7-13 「Software Distribution Manager」 ウィンドウ

4. 「**Director Update Assistant**」をダブルクリックします。「Director Update Assistant」ウィンドウが開きます。詳細は、278 ページの図 7-14 を参照してください。

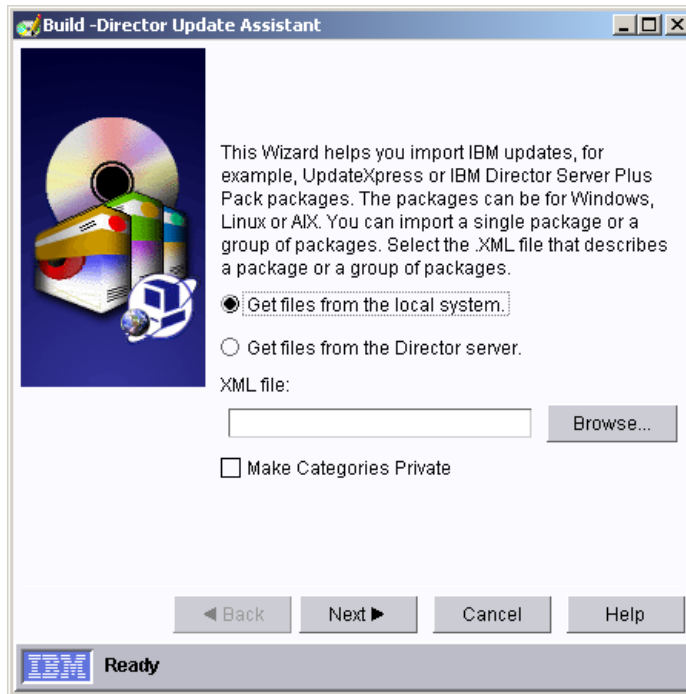


図 7-14 「Director Update Assistant」 ウィンドウ

5. 「**Get files from the local system**」を選択します。
6. 「**Browse**」をクリックします。これにより、ルート・ディレクトリー検索ウィンドウが開きます。
7. UpdateXpressが入っている CD-ROM ドライブまでナビゲートし、ルート・ディレクトリーで「**index.xml**」を選択して、「**OK**」をクリックします。
8. 「**Next**」をクリックして、続行します。
9. 「IBM eServer xSeries 345」という名前のフォルダーに達するまで、パッケージのリストをスクロールダウンし、ツリーを展開します。279 ページの図 7-15 のようなビューが表示されます。

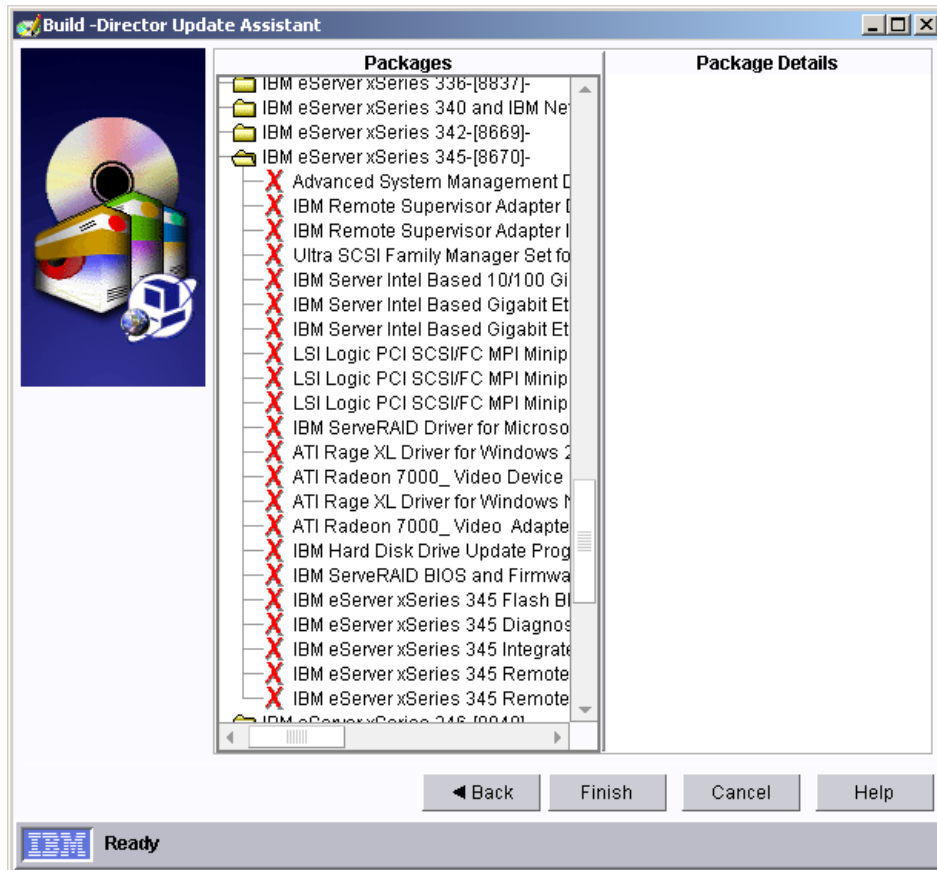


図 7-15 ダウンロードできる x345 ファイル

10. 実行する必要がある更新を見つけます。ファームウェア更新の横の **X** をクリックして、「**Select Item**」をクリックします。**X** が **✓** に変わります。
11. 必要なファームウェア更新をすべて選択した後、「**Finish**」をクリックします。
12. この時点で、これらの更新が処理され、IBM Director の「**Software Distribution**」タスクに追加されて、サーバーの更新に使用可能になります。
13. すべてのイメージの処理が完了すると、このウィンドウは自動的に閉じて、「**Software Distribution Manager**」ウィンドウ (277 ページの図 7-13) に戻ります。「**File**」→「**Close**」を選択してこのウィンドウを閉じ、IBM Director コンソールに戻ります。
14. 「**Software Distribution**」タスクを選択し、ツリーを展開して、新しいイメージを見ます。詳細は、280 ページの図 7-16 を参照してください。

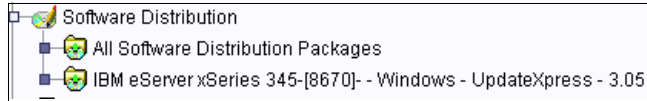


図 7-16 UX v3.05a CD からインポートされた x345 用のファームウェア

15. x345 ツリーを展開すると、279 ページの ステップ 10 で選択した項目が表示されます。図 7-17 を参照してください。このファームウェア更新を管理対象システムにプッシュして即時に実行することもできますし、IBM Director スケジューラーを使用して後で実行することもできます。オプションを管理対象システムにドラッグすると、すぐに実行されます。

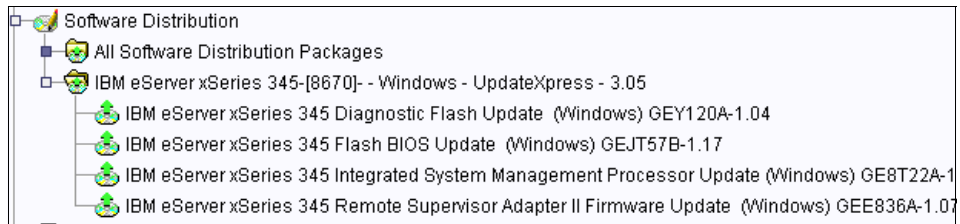


図 7-17 x345 用のファームウェアの詳細

16. これで、x345 サーバーの更新を実行する準備ができました。
17. 4 つの x345 ファームウェア更新のルート・タスクを選択し、それを x345 サーバー上にドラッグ・アンド・ドロップします (単一更新の場合)。x345 サーバー・グループを更新する必要がある場合は、ファームウェア更新を x345 サーバーのグループ・アイコンの上にドラッグ・アンド・ドロップします。
18. 図 7-18 のような質問が表示されます。ファームウェア更新を別の時間にスケジュールする場合は、「**Schedule**」をクリックし、ファームウェアを即時に更新する場合は、「**Execute Now**」をクリックします。

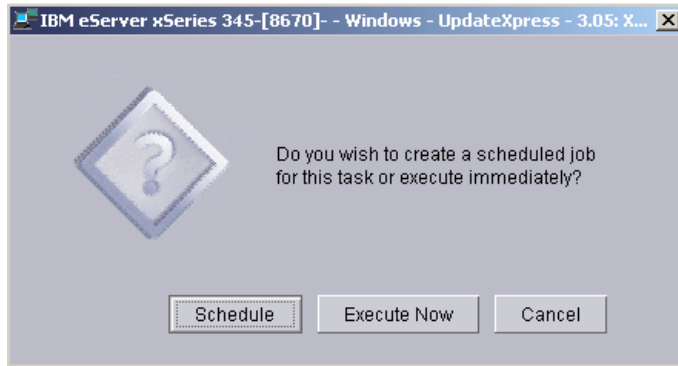


図 7-18 更新をスケジュールするか、すぐに実行するかについての質問

19. 「**Schedule**」をクリックした場合、図 7-19 のウィンドウが表示されます。このウィンドウで、新規にスケジュールされたジョブの詳細を入力できます。

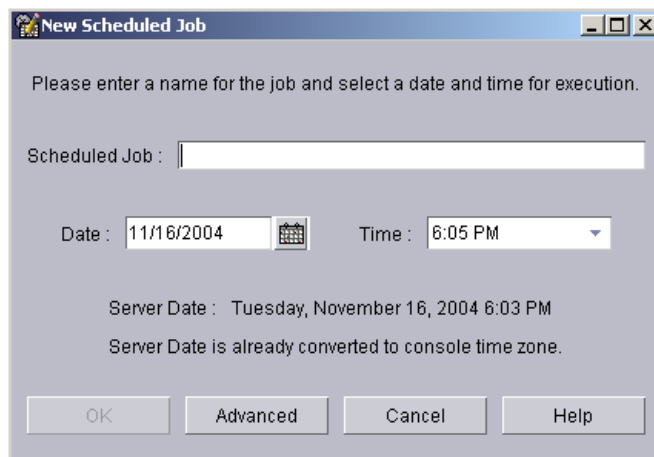


図 7-19 新規にスケジュールされたジョブ

20. スケジュールされたジョブの適切な名前を入力します。この例では「x345 firmware updates」を使用し、ジョブを実行する時刻を選択します。図 7-20 を参照してください。

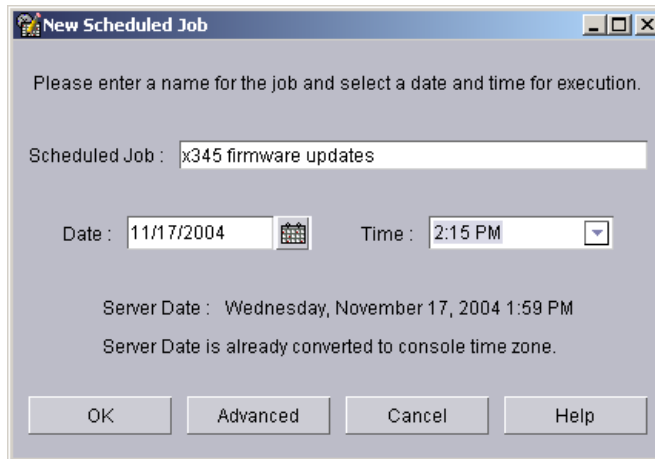



図 7-20 ジョブの詳細

21. スケジュールされた時刻が適切であれば、「**OK**」をクリックします。
22. スケジュールされたタスクを保管することの確認を求めるプロンプトが出ます。「**OK**」をクリックします。
23. これで、ジョブはサーバーに適用されました。これを確認するには、**IBM Director** コンソールのメイン・ウィンドウの中央ペインに表示されるビューを変更して、スケジュール済みのジョブをすべて表示し、ジョブに関連付けられたサーバーを確認します。中央ペインのフリー・スペースで右クリックして、「**Associate by Job**」をクリックします。
24. 「**Agent**」の横にツリー・ボックスが表示されたら、ツリーを展開して、適用されたジョブを表示します。詳細は、図 7-21 を参照してください。



図 7-21 ジョブ別の関連付け

25. ジョブが完了した後、実行履歴を見ることができます。履歴を入手するには、**IBM Director** のアイコン・メニューからスケジューラー・アイコン  を選択します。
26. ジョブを見つけて、それを右クリックします。これにより、メニューが開きます。「**Open Execution History**」をクリックします。
27. このウィンドウから、「**File**」→「**View Log**」を選択します。
28. ジョブ実行履歴が開きます。表示の詳細は、デフォルトでは「**low**」に設定されていますが、「**View**」→「**Detail**」→「**High**」を選択することによ



り、詳細を「high」に変更できます。これによって、283 ページの図 7-22 に示すように、実行履歴の完全な明細を受け取ることができます。

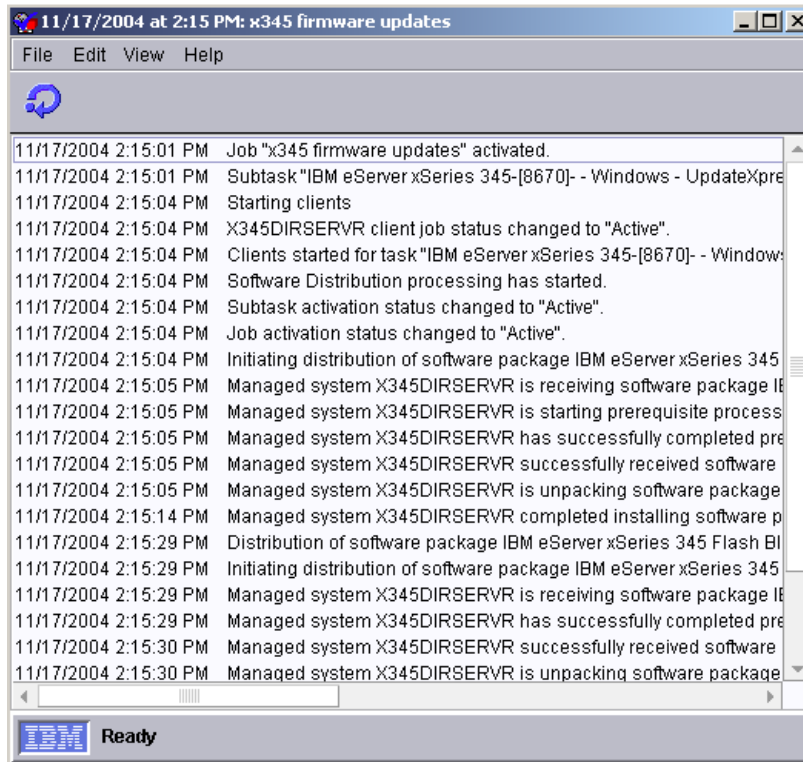


図 7-22 ジョブ実行履歴の高度の詳細の表示

### 7.8.3 UpdateXpress RemoteUX を使用したファームウェアの更新

UpdateXpress は、自動開始プログラムが入っている CD-ROM です。これを使用して、システムのファームウェアと Windows デバイス・ドライバを CD 上に定義された最新レベルに維持することができ、不要なシステム停止を防止するのに役立ちます。UpdateXpress は、次のサイトから入手できます。

<http://www.ibm.com/pc/support/site.wss/MIGR-53046.html>

UpdateXpress は、現行のデバイス・ドライバとファームウェアのレベルを自動的に検出し、ユーザーに提示します。次に、ユーザーが特定のアップグレードを選択するか、または UpdateXpress がアップグレードの必要性を検出したすべてのシステム・レベルを更新するかを選択するオプションが提供されます。

UpdateXpress CD を使用するには、3 とおりの方法があります。

- ▶ ローカル側のサーバーで CD からブートする
- ▶ ローカル側で Windows から CD をロードする (autorun)
- ▶ リモート側で CD 上の RemoteUX コマンド・ライン・ユーティリティーを使用する

このセクションでは、RemoteUX の使用法について説明します。

RemoteUX は、Windows ベースのサーバーとのみ連動し、管理共用 (C\$, ADMIN\$) を介してサーバーにリモート接続します。ファームウェアの更新は、PowerQuest 仮想ブート環境を使用して、リモート・サーバー内のディスクの最初のトラックの使用可能なセクターにデータを書き込むことによって実行されます。

**注:** RemoteUX は、Windows ワークステーション上でのみ機能し、Windows NT 4.0、Windows 2000 Server、および Windows Server 2003 を実行するリモート・サーバーとのみ連動します。

図 7-23 は、リモート側で UpdateXpress を実行する標準的なネットワーク図を示しています。

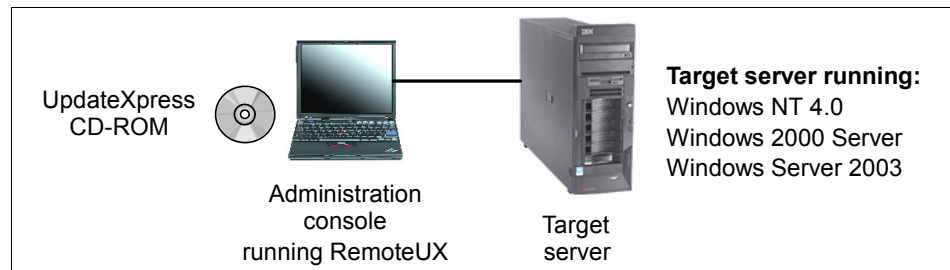


図 7-23 リモート側で実行される UpdateXpress

UpdateXpress CD-ROM は、ローカル管理者のワークステーションのドライブに挿入するか、またはネットワーク共有にコピーします。ネットワーク共有オプションを使用する場合は、そのロケーションを RemoteUX コマンドの一部として指定します。

**ヒント:** このセクションでは、CD-ROM または CD-ROM のすべてのファイルを含んでいるネットワーク共有から、RemoteUX を使用するプロセスを説明します。ネットワーク共有を使用するが、使用されるスペースを最小限にとどめたい場合は、次の URL から入手できる資料「Automating System Firmware Updates with RemoteUX and UpdateXpress Version 3.02A」の指示に従って、不要なファイルを削除してください。

<http://www.ibm.com/pc/support/site.wss/MIGR-54033.html>

RemoteUX の構文は、次のとおりです。

```
remoteux ¥¥targetserver parameters command
```

オプションは、接続方法と UpdateXpress ファイルのソースの場所を指定します。

パラメーターを表 7-2 に示します。パラメーターを指定しない場合、以下の設定が使用されます。

- ▶ UpdateXpress ファイルは現行のローカル・ディレクトリーにある。
- ▶ リモート・サーバーの c\$¥temp を一時スペースとして使用する。
- ▶ 現行ユーザー ID/ パスワードを使用してリモート・サーバーにログインする。

表7-2 RemoteUX のパラメーター

| オプション                                | 意味                                                                                                                                                                  |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r:path<br>-remote:path              | ターゲット・サーバーのステージングまたは作業ディレクトリー・パスを指定します。デフォルトは、C\$¥temp です。フォーマットは、shareName¥path です。                                                                                |
| -l:path<br>-local:path               | UpdateXpress CD イメージの保管場所のパスを指定します。デフォルトは、現行ディレクトリーです。                                                                                                              |
| -n<br>-nowait                        | RemoteUX は、リモート・プロセスが完了するのを待たずに終了することを指定します。システムの再始動を必要とする更新 (ファームウェア更新) の場合、待機 (waiting) は、更新がスケジュールされると、またはエラーによりスケジュールに失敗すると、すぐに RemoteUX アプリケーションを終了することを意味します。 |
| -u:user<br>-user:user                | リモート・サーバーに接続するための管理者ユーザー ID を指定します。デフォルトは、現行ユーザー名です。                                                                                                                |
| -p:password<br>-pwd:password<br>-p:* | 接続に使用するパスワードを指定します。* を指定すると、RemoteUX は、ユーザーにパスワードの入力を求めるプロンプトを出します。                                                                                                 |

ユーザーは種々のコマンドを実行して、インストールされているファームウェアとドライバーのレベルを照会し、更新を適用することができます。

使用できるコマンドを表 7-3 に示します。

表 7-3 RemoteUX コマンド

| コマンド                                           | 意味                                                                                                                                                                                            |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-c</b><br><b>-compare</b>                   | リモート・システム上のファームウェアとデバイス・ドライバーのレベルを、UpdateXpress CD 上で使用可能なレベルと比較して、表示します。                                                                                                                     |
| <b>-e</b><br><b>-examine</b>                   | 現行のファームウェアとドライバーのレベルを表示します。リモート・サーバーの型式番号も報告します。                                                                                                                                              |
| <b>-pkg:pkg.exe</b><br><b>-package:pkg.exe</b> | リモート側で pkg.exe を実行します。これは「Package for the Web」パッケージです。リモート・サーバー上に保留にできるのは、一度に 1 つの更新に限られます。必要な場合は、 <b>-local</b> パラメーターを使用して、ローカル・ディレクトリーを指定します。 <b>-a</b> を使用すると、追加の引数をパッケージ・ファイルに渡すことができます。 |
| <b>-a args</b>                                 | オプションの引数をパッケージ更新に渡します。頻繁に使用される引数リストは、 <b>-a -r</b> で、これは更新パッケージをスケジュールした後、即時に再始動を実行します。このコマンドは、更新を適用した後、システムをリブートします。完全なリストは、表 7-4 を参照してください。                                                 |
| <b>-d</b><br><b>-drivers</b>                   | リモート・サーバー上のデバイス・ドライバーを更新します。このコマンドは、該当するデバイス・ドライバーを CD からターゲットにプッシュし、リモート側で UpdateXpress を立ち上げます。UpdateXpress は、各システムに必要な更新を識別し、自動的にサーバーを更新します。                                               |
| <b>-f</b><br><b>-firmware</b>                  | リモート・サーバー上のすべてのファームウェアを更新します。このコマンドは、ファームウェア更新を CD からターゲットにプッシュします。更新を適用するためにリブートがスケジュールされます。あるいは、 <b>-f -a -r</b> パラメーターを使用して、即時リブートを強制することもできます。                                            |
| <b>-g</b><br><b>-getlog</b>                    | リモート・サーバーから ux.log ファイルを取得します。このファイルは、リモート・サーバーの c\$¥uxlog¥ux.log にあります。                                                                                                                      |
| <b>-clr</b><br><b>-clearlog</b>                | リモート・サーバー上の ux.log ファイルを削除します。                                                                                                                                                                |

**-a** コマンドを使用すると、「Package for the Web」パッケージにパラメーターを渡すことができます。構文は、以下のようになります。

ドライバーの更新の場合、オプションの引数は、次のとおりです。

`[-s] [-a [-s] | [-x directory] ]`

ファームウェアの更新の場合、オプションの引数は、次のとおりです。

`[-s] [-a [-s] | [-r] | [-c] | [-x directory] | [-xd] ]`

インストール・パッケージに渡すために `-a` 引数を使用されている点に注意してください。

表 7-4 `-a` コマンドのパラメーター

| 引数                  | ドライバー | ファームウェア | 意味                                                                                                                                                                                     |
|---------------------|-------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-s</code>     | 可     | 可       | パッケージ・ソフトウェアをサイレント・インストールし、 <code>%temp%</code> ディレクトリー内のファイルを上書きする必要があっても、プロンプトを出しません。                                                                                                |
| <code>-a</code>     | 可     | 可       | パッケージの後続のコマンドをすべてインストール・パッケージに渡します。                                                                                                                                                    |
| <code>-s</code>     | 可     | 可       | (2 番目の <code>-s</code> パラメーター) 更新を無人でサイレント・インストールします。ドライバーは即時にインストールされますが、更新を適用するにはリポートが必要な場合があります。ファームウェアの場合は、更新は次回のリポート時に実行するようにスケジュールされます。 <code>-r</code> オプションを使用すると、リポートを強制できます。 |
| <code>-x dir</code> | 可     | 可       | 更新をディレクトリーに抽出します。デフォルトは、リモート・サーバーの <code>%TEMP%</code> ディレクトリーです。                                                                                                                      |
| <code>-r</code>     | 不可    | 可       | 更新をスケジュールして ( <code>-s</code> オプション付き、または、なしで使用できます)、即時にリポートします。                                                                                                                       |
| <code>-c</code>     | 不可    | 可       | スケジュールされたファームウェア更新を取り消して、ログ・ファイルに項目を書き込みます。                                                                                                                                            |

**ヒント:** 一度に 1 つだけのファームウェア・パッケージをスケジュールできます。現在スケジュールされているファームウェア更新パッケージの代わりに、別のファームウェア更新を適用する必要がある場合、ファームウェア・パッケージに対して `-c` オプションを実行して、現行の更新パッケージを取り消してから、該当のファームウェア更新を実行してください。

たとえば、リモート xSeries 345 上のファームウェアとドライバーの現行レベルを表示し、それを UpdateXpress CD と比較するには、次のコマンドを使用します。

```
remoteux ¥¥9.42.171.144 -u:Administrator -p:* -c
```

#### 例7-8 比較コマンドの結果

```
H:¥UX¥Disk 1>remoteux ¥¥9.42.171.144 -u:Administrator -p:* -c
RemoteUX V1.2 for Windows 2003/2000/NT4
Password:
Connecting to remote service....
Remote Machine=¥¥9.42.171.144 Model Number=8670 Server Type=xSeries 345
Copying examination tools to remote server.
Please wait.....
Comparing system levels in server ¥¥9.42.171.144 started at 10:45 AM on 03/21/20
05 against UpdateXpress 3.06
NOTE: Some versions of the IBM Service Processor may not be compatible with this
utility.
```

| Type | Name                | System Level | CD Level   | New |
|------|---------------------|--------------|------------|-----|
| F    | POST/BIOS           | 61A          | 60A        |     |
| F    | System diagnostics  | T20          | T20        |     |
| F    | ISMP                | 20A          | 22A        | X   |
| D    | symmpi.sys          | 1.08.18.00   | 1.09.06.00 | X   |
| F    | IBM RSA II Firmware | GEE840A      | GEE836A    |     |
| D    | e1000325.sys        | 6.3.6.31     | 7.3.13.0   | X   |
| D    | IBM RSA II Driver   | 5.33         | 5.32       |     |

比較コマンドの出力の最初の列は、項目がファームウェアであるか、ドライバーであるかを指定します。最後の列は、ご使用のバージョンの UpdateXpress 更新するのに適格な項目を示します。上の例では、1つのファームウェア (ISMP) の更新が必要であり、2つのドライバー (LSI Logic SCSI ドライバー symmpi.sys と Intel Gigabit ドライバー e1000325.sys) の更新が必要です。

リモート・サーバーのファームウェアを更新するには、**-f** (または **-firmware**) コマンドを実行します。

```
remoteux ¥¥9.42.171.144 -u:Administrator -p:* -f
```

#### 例7-9 リモート・サーバー上のすべてのファームウェアを更新するファームウェア・コマンドからの出力

```
Connecting to remote service....
Remote Machine=¥¥9.42.171.144 Model Number=8670 Server Type=xSeries 345

Copying required UpdateXpress source to ¥¥9.42.171.144.
Please wait.....
Running UpdateXpress on the remote machine...
```

ファームウェアは通常、リブートを必要とします。これを確認するには、**-getlog** コマンドを使用して、UpdateXpress のログを取得します。

*例 7-10 リブート前の getlog コマンドからの出力*

---

```
Connecting to remote service....
Remote Machine=¥¥9.42.171.144 Model Number=8670 Server Type=xSeries 345
03:10:2005 13:31:34,Update=BIOS,New=1.19,Status=Success,ReturnCode=0
[Remote UpdateXpress Firmware Update]
Scheduled at 17:15:32 - 03:21:2005 returns=0
```

---

上記の出力から、更新は後の時刻にスケジュールされていることが分かります。スケジュールされた時刻は制御できませんが、必要であれば、手動でその時刻より前にサーバーをリブートできます。代わりに、即時にリブートするように指定しておくこともできます。

```
remoteux ¥¥9.42.171.144 -u:Administrator -p:* -f -a -r
```

リブートして更新した後、**-getlog** コマンドの出力の内容は、次のようになります (例 7-11)。

*例 7-11 更新が適用された後の getlog コマンドからの出力*

---

```
Connecting to remote service.....
Remote Machine=¥¥9.42.171.144 Model Number=8670 Server Type=xSeries 345
03:10:2005 13:31:34,Update=BIOS,New=1.19,Status=Success,ReturnCode=0
[Remote UpdateXpress Firmware Update]
Scheduled at 17:15:32 - 03:21:2005 returns=0

03:21:2005 12:38:12,Update=Tape drive microcode,Old=,New=Many, Status=No supported tape device
found,Error,ReturnCode=2
03:21:2005 12:38:12,Update=SCSI hard disk drive microcode,Old=,New=Many, Status=Error,
ReturnCode=1
03:21:2005 12:38:12,Update=RSA II Video BIOS,Old=Unknown,New=001, Status=Error, ReturnCode=2
03:21:2005 12:38:12,Update=Integrated Systems Management,Old=20A,New=22A,
Status=Success, ReturnCode=0
12:38:12.42p 03-21-2005, Update=RemoteUX Firmware, Status=Complete, ReturnCode=0
```

---

ログから (また、更新プロセス中の表示からも)、さまざまな更新が試行されたことが分かります。戻りコードは、表 7-5 の該当するセクションにリストされています。

- ▶ テープ・ドライブ・マイクロコード: テープ・ドライブが見つからない (RC=2)
- ▶ SCSI ディスク・ドライブ・マイクロコード: 失敗 (RC=1)
- ▶ RSA II ビデオ BIOS: 失敗 (RC=2)

▶ ISMP サービス・プロセッサ : 正常に更新 (RC=0)

表 7-5 は、更新パッケージの戻りコードをリストしています。

表7-5 .UpdateXpress パッケージの戻りコード

| 戻りコード                           | 意味                           |
|---------------------------------|------------------------------|
| <b>IBM サービス・プロセッサ・ドライバー</b>     |                              |
| 0                               | 成功、リブートは不要                   |
| 1                               | 成功、リブートが必要                   |
| 2                               | エラー、インストールに失敗                |
| 8                               | ハードウェアが見つからない                |
| <b>テープ・ドライブ・ファームウェア</b>         |                              |
| 0                               | 成功                           |
| 1                               | エラー、磁気テープ装置の更新に失敗            |
| 2                               | サポートされる磁気テープ装置が見つからない        |
| 3                               | 磁気テープ装置はすでに最新である             |
| 4                               | 磁気テープ装置に無関係のリカバリー不能エラー       |
| 5                               | オペレーターが自動更新を取り消した            |
| 6                               | 磁気テープ装置は代替方式による更新が必要         |
| 7                               | 磁気テープ装置は DOS 専用モードで更新する必要がある |
| 8                               | 磁気テープ装置は別のプログラムによって使用中       |
| 9                               | 磁気テープ装置はアクセス不能               |
| <b>ハード・ディスク・マイクロコード・ファームウェア</b> |                              |
| 0                               | 成功                           |
| 1                               | エラー、ハード・ディスク装置の更新に失敗         |
| 3                               | ハード・ディスク装置はすでに最新である          |

表 7-6 は、RemoteUX の戻りコードをリストしています。

表7-6 リモート UpdateXpress 戻りコード

| 戻りコード | 意味                              |
|-------|---------------------------------|
| 0     | UpdateXpress は正常に開始した (注 1 を参照) |



| 戻りコード                                                                                                                                                                   | 意味                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| 2                                                                                                                                                                       | エラー、ファイルが見つからない(注2を参照) |
| 3                                                                                                                                                                       | エラー、パスが見つからない(注2を参照)   |
| 5                                                                                                                                                                       | エラー、アクセスが拒否された(注2を参照)  |
| 39                                                                                                                                                                      | エラー、ディスクが満杯(注2を参照)     |
| <b>注:</b><br>1. UpdateXpress は、ゼロ以外のコードを戻す場合、そのエラー・コードを説明するメッセージを表示します。<br>2. 0 の戻りコードは、必ずしも更新が正常に適用されたことを示すものではなく、更新が正常にスケジュールされたことをのみを示します。ログ・ファイルを見て、更新の結果を確認してください。 |                        |

UpdateXpress の機能や、障害が発生した場合の原因の判別方法についての詳しい情報は、UpdateXpress CD-ROM から `index.htm` を立ち上げると利用できるオンライン・ヘルプを参照してください。

**注: -clearlog** コマンドを使用して、ログ・ファイルを定期的に消去する必要があります。ファイルのサイズが 4 MB に達すると、更新の出力がファイルに書き込まれなくなります。

## 7.9 UpdateXpress firmware update scripts for BladeCenter

UpdateXpress Firmware Update Scripts for BladeCenter (UXBC) は、以下にリストするコンポーネントのファームウェア更新を、リモート側で、単一の BladeCenter シャーシ上で無人で実行することを可能にするプロセスです。

- ▶ 管理モジュール (1 台または 2 台)
- ▶ 4 ポート・イーサネット・スイッチ・モジュール
- ▶ Nortel Layer 2-7 Gigabit Ethernet スイッチ・モジュール

スクリプトは、シャーシ内のサポートされるすべてのコンポーネントを、指定されたファームウェアに更新します。更新するシャーシ内のコンポーネントを選択することはできません。

開始する前に、更新プロセスを立ち上げるためのコマンド・ライン・パラメーターが必要です。このソリューションは、Python スクリプト言語で書かれた最上位スクリプト (`ChassisUpdate.py`) で構成され、これが他のサブスクリプトを駆動して実行させます。

## 要件

UXBC は、Python スクリプトを通して制御され、実行されます。Python インタープリター（バージョン 2.3 以降）は、管理システムにのみインストールする必要があります。ご使用のオペレーティング・システム用の Python インタープリターは、次の Web サイトからダウンロードできます。

<http://www.python.org>

モジュール（スイッチなど）のファームウェア更新を取得するために、TFTP サーバーが必要です。TFTP サーバーは、更新を必要とするスイッチがアクセス可能なネットワーク上の任意の場所にインストールできます。

使用可能な TFTP サーバーの 1 つは SolarWinds TFTP サーバーで、まだお持ちでない場合は、次のサイトから入手できます。

[http://www.solarwinds.net/Tools/Free\\_tools/TFTP\\_Server/](http://www.solarwinds.net/Tools/Free_tools/TFTP_Server/)

UXBC スクリプトは、ファイアウォールの背後の LAN で実行することをお勧めします。LAN 環境の TCP/IP と FTP をサポートする、信頼できるメディアおよび伝送タイプがサポートされます。

UXBC スクリプトは、管理システムにインストールされた次のオペレーティング・システムから実行できます。

- ▶ Windows 2000
- ▶ Windows XP
- ▶ Windows Server 2003
- ▶ Red Hat Enterprise Linux 2.1
- ▶ Red Hat Enterprise Linux 3.0
- ▶ SUSE LINUX Enterprise Server 8.0

## はじめに

スクリプトをインストールする必要はありません。Windows 環境では、追加のレジストリー項目または共用 DLL は必要ありません。

UXBC コードを入手するには、IBM Support Web サイトから ZIP ファイルをダウンロードします。

<http://www.ibm.com/pc/support/site.wss/MIGR-57201.html>

ZIP ファイルの内容を解凍し、解凍プロセスで大文字小文字とファイル許可が保存されたことを確認します。PY 拡張子を持つファイルはすべて実行可能ファイルです。

UXBC ファイルを解凍すると、次のディレクトリーが作成されます（例えば、C:\¥ directory に解凍された場合）。

**c:\¥BladeCenterUpdates**

ルート・ディレクトリー

|                                        |                          |
|----------------------------------------|--------------------------|
| <b>c:\BladeCenterUpdates\Common</b>    | 共通機能 / 定義                |
| <b>c:\BladeCenterUpdates\IOModules</b> | 入出力モジュール (スイッチなど) のスクリプト |
| <b>c:\BladeCenterUpdates\MM</b>        | 管理モジュールに関するスクリプト         |

ヒント : c:\BladeCenterUpdates\にあるサンプル応答ファイル BladeCenterUpdates.rsp を、参照用として例 7-12 に示します。ご使用のカスタム応答ファイルを作成する際に、このファイルを手近に置いて参考にしてください。ファイル内のパラメーターについての追加情報が組み込まれています。

#### 例 7-12 BladeCenterUpdates.rsp ファイル

```
# BladeCenterUpdates.rsp
# UpdateXpress firmware update scripts for BladeCenter response file
# Copyright IBM Corporation, 2004
# The format of this file is straight forward. Lines begining with a # # are considered
comments and ignored. Lines beginning with white space are also ignored. Every option is
specified using a key-value pair seperated by an = character. Keys cannot be used without
values associated with them (e.g. mmipaddr= is not a valid key-value pair, mmipaddr=192.168.1.1
is).
# Some of the options are mandatory. Others are mandatory only with certain BladeCenter
configurations (e.g. Firmware update filenames are mandatory for switches to get updated).
Most options have a default value that is used if the option is not specified. The defaults
are listed in the description ofeach option below.

### MANDATORY Fields ###
# These fields must be specified.
# This is a mandatory field that specifies the hostname or the dotted IP address of the
BladeCenter Management Module.
# ex. mmipaddr=10.1.1.100 or mmipaddr=hostname.host.com
mmipaddr=

### OPTIONAL Fields ###
# These fields may be necessary depending on the BladeCenter configuration.
# This is an optional field that specifies the username for the BladeCenter Management Module.
If not specified (i.e. commented out), the defaultusername (USERID) is assumed. Otherwise, a
value MUST be specified.
## ex. mmuser=USERID
#mmuser=

# This is a optional field that contains the password of the specified usernamefor the
BladeCenter Management Module. If not specified If not specified (i.e. commented out), the
default password (PASSWORD) is assumed. Otherwise,a value MUST be specified.
#
# ex. mmpass=PASSWORD
#mmpass=
```

```

# This is an optional field that is the fully qualified path to the BladeCenter Management
Module firmware update files. By default the scripts will look in the current directory for
the firmware. To use this field, remove the comment character (#) and add the fully qualified
path. Note: Packet files must be in ALLCAPS, and must be named CNETBRUS.PKT, CNETMNUS.PKT, and
CNETRGUS.PKT
#
# ex. mmFileLocation=c:\¥images
#mmFileLocation=

# The IP address of the TFTP server containing the firmware update files.This address MUST be
specified as a valid dotted IP address, hostnames are not allowed. This field is required for
updating any switch in the BladeCenter.

# ex. tftpipaddr=192.168.1.2
#tftpipaddr=

# This is a optional field that contains the username for the first I/O module.If not specified
(i.e. commented out), the default username (USERID) is assumed. Otherwise, a value MUST be
specified.
#
# ex. ioluser=USERID
#ioluser=

# This is a optional field that contains the password for the username of the first I/O module.
If not specified (i.e. commented out), the default password (PASSWORD) is assumed. Otherwise, a
value MUST be specified.
#
# ex. iolpass=PASSWORD
#iolpass=

# The full path(s) and filename(s) of the first I/O module FLASH file(s) on the TFTP server.
If only one filename necessary use io1Filename1 and leave io1Filename2 commented out.
#
# ex. io1Filename1=ibmrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io1Filename1 and the boot image by
io1Filename2.
#
# ex. io1Filename1=GbESM-AOS-20.1.1.0-os.img
# io1Filename2=GbESM-AOS-20.1.1.0-boot.img
#io1Filename1=
#io1Filename2=

# This is an optional field that contains the username for the second I/O module. If not
specified (i.e. commented out), the default username (USERID)is assumed. Otherwise, a value
MUST be specified.
#
# ex. io2user=USERID

```

```

#io2user=

# This is an optional field that contains the password for the username of the second I/O
module. If not specified (i.e. commented out), the default password (PASSWORD) is assumed.
Otherwise, a value MUST be specified.
#
# ex. io1pass=PASSWORD
#io2pass=

# The full path(s) and filename(s) of the second I/O module FLASH file(s) on the TFTP server.
If only one filename necessary use io2Filename1 and leave io2Filename2 commented out.
#
# ex. io2Filename1=ibmrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io2Filename1 and the boot image by
io2Filename2.
#
# ex. io2Filename1=GbESM-AOS-20.1.1.0-os.img
# io2Filename2=GbESM-AOS-20.1.1.0-boot.img
#io2Filename1=
#io2Filename2=

# This is an optional field that contains the username for the third I/O module. If not
specified (i.e. commented out), the default username (USERID) is assumed. Otherwise, a value
MUST be specified.
#
# ex. io3user=USERID
#io3user=

# This is an optional field that contains the password for the username of the third I/O
module. If not specified (i.e. commented out), the default password(PASSWORD) is assumed.
Otherwise, a value MUST be specified.
#
# ex. io3pass=PASSWORD
#io3pass=

# The full path(s) and filename(s) of the third I/O module FLASH file(s) on the TFTP server.
If only one filename necessary use io3Filename1 and leaveio3Filename2 commented out.
#
# ex. io3Filename1=ibmrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io3Filename1 andthe boot image by
io3Filename2.
#
# ex. io3Filename1=GbESM-AOS-20.1.1.0-os.img
# io3Filename2=GbESM-AOS-20.1.1.0-boot.img
#io3Filename1=
#io3Filename2=

```

```

# This is an optional field that contains the username for the fourth I/O module. If not
specified (i.e. commented out), the default username (USERID) is assumed. Otherwise, a value
MUST be specified.
#
# ex. io4user=USERID
#io4user=

# This is an optional field that contains the password for the username of the fourth I/O
module. If not specified (i.e. commented out), the default password (PASSWORD) is assumed.
Otherwise, a value MUST be specified.
#
# ex. io4pass=PASSWORD
#io4pass=

# The full path(s) and filename(s) of the fourth I/O module FLASH file(s) on the TFTP server.
If only one filename necessary use io4Filename1 and leave io4Filename2 commented out.
#
# ex. io4Filename1=ibmrun.095
#
# For a Nortel switch, the OS image MUST be the specified by io4Filename1 and the boot image by
io4Filename2.
#
# ex. io4Filename1=GbESM-AOS-20.1.1.0-os.img
#      io4Filename2=GbESM-AOS-20.1.1.0-boot.img
#io4Filename1=
#io4Filename2=

# This option specifies that if the Management Module is configured via DHCP, FLASHing of the
I/O modules should occur automatically even if it is not possible to FLASH the Management
Module. To enable, simply uncomment the following line. To disable, comment the line or
specify FALSE.
#continueIO=TRUE

# Some management applications may cause the 6090 TCP port of the Management Module to remain
in a locked state and inaccessible by applications, such as these scripts. If you uncomment
the forceMMreboot option, you will permit these scripts to reboot the Management Module and
release this port. To enable, simply uncomment the following line. To disable, comment the
line or specify FALSE.
#forceMMreboot=TRUE

```

---

以下のステップを実行して、UpdateXpress Firmware Update Scripts for BladeCenter  
で使用するファームウェア更新を入手します。

1. 管理モジュールの最新のファームウェア更新を IBM Support Web サイトから  
ダウンロードします。

BladeCenter: <http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>

BladeCenter T: <http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>

2. BladeCenterUpdates ディレクトリーを除いて (README ファイルが上書きされることになるため)、管理システムがアクセスできる任意の場所にパッケージを解凍し、ファイル拡張子 .PKT を持つすべてのファイルを入れます。その後で、すべての .PKT ファイルを UXBC パッケージのデフォルト・ディレクトリー (¥BladeCenterUpdates) に移動しても構いません。

.PKT ファイルを代替場所に置いた場合は、パスをメモしてください。この情報は、後で応答ファイルに入力する必要があります。

3. 入出力モジュール用の最新のファームウェア更新をダウンロードします。入出力モジュール用のファームウェアは、IBM Support Web サイトから入手できます。

4 ポート・イーサネット・スイッチ・モジュール :

<http://www.ibm.com/pc/support/site.wss/MIGR-50457.html>

Nortel Networks Layer 2-7 GbE スイッチ・モジュール :

<http://www.ibm.com/pc/support/site.wss/MIGR-53058.html>

4. ファームウェア更新を TFTP サーバーに解凍します。次の情報を記録してください。
  - 解凍されたファームウェア・ファイルへのパス
  - 入出力モジュールのファームウェア・ファイルの名前

## 手動による BladeCenterUpdates.rsp ファイルの作成

BladeCenter シャーシのファームウェア更新を実行するには、大量の情報が必要です。UXBC ソフトウェアは、以前に作成された応答ファイルからの情報を使用して、更新の実行に必要なパラメーターを取得します。この応答ファイルのデフォルト名は、BladeCenterUpdates.rsp です。

サンプル応答ファイルが UXBC パッケージの ¥BladeCenterUpdates ディレクトリーに提供されており、293 ページの例 7-12 に複製されています。

このサンプル・ファイルを検討して、ご使用の環境用に変更してください。サンプル・ファイルには、フィールドごとに詳細情報が記述されています。応答ファイルに別のファイル名とパスを使用する場合は、UXBC プロセスの開始時に、コマンド行で名前とパスを指定してください。

応答ファイルを更新した後、メイン・スクリプト (ChassisUpdate.py) を実行できます。更新プロセスは、応答ファイル内の情報をスクリプトへの入力として使用します。

**ヒント :** BladeCenter シャーシ用の最初の応答ファイルを作成した後、IP アドレスやファームウェア・ファイルの名前などの情報が変更された場合、同じ応答ファイルを使用する将来のファームウェア更新プロセスでは、変更が必要になることがあります。

## PYTHONPATH 環境変数の設定

UXBC を実行するためには、PYTHONPATH 環境変数を BladeCenterUpdates ディレクトリーの上位のディレクトリーに設定する必要があります。例えば、次のように設定します。

- ▶ Microsoft Windows コマンド・プロンプト  

```
set PYTHONPATH=c:\uxbcu¥
```
- ▶ Linux BASH 環境  

```
export PYTHONPATH=/root/uxbcu
```

## 更新プロセスの開始

UXBC プロセスを開始するには、**ChassisUpdate.py** を実行します。ChassisUpdate スクリプトを実行するには、メイン・スクリプトを直接呼び出すか、または Python インタープリターを通してメイン・スクリプトを呼び出します。コマンド・プロンプトから、次のいずれかのコマンドを入力して、Enter を押します。コマンドは、大/小文字の区別をします。

**重要**：更新する BladeCenter シャーシ内にあるブレードから ChassisUpdate.py を実行してはなりません。ファームウェア更新は、BladeCenter システムの支持構造の一部であるコンポーネントに対して実行されるため、ファームウェア更新プロセスは、完全に独立したシステムから実行する必要があります。

- ▶ メイン・スクリプトを呼び出す場合は、次のように入力します。  
`ChassisUpdate.py options`
- ▶ Python インタープリターを通してメイン・スクリプトを呼び出す場合は、次のように入力します。  
`python ChassisUpdate.py options`

**ChassisUpdate** コマンドのオプションを 298 ページの表 7-7 にリストします。

表 7-7 ChassisUpdate スクリプトのコマンド・ライン・オプション

| オプション (リストされたバリエーションはすべて有効)                                              | 説明                                                                                                              |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <code>--responseFile &lt;file&gt;</code><br><code>-r &lt;file&gt;</code> | 応答ファイルを指定します。ここで、<file> は、応答ファイルのパスと名前を指定します。応答ファイルを指定しない場合、デフォルトの応答ファイル名とパスである BladeCenterUpdates.rsp が使用されます。 |
| <code>-V</code><br><code>--version</code>                                | スクリプトのバージョン番号を表示します (注: -V は、大文字の V です (verbose モードを表す -v ではありません))。                                            |



|                             |                          |
|-----------------------------|--------------------------|
| オプション (リストされたバリエーションはすべて有効) | 説明                       |
| -h<br>--help<br>-?          | ヘルプ情報を表示します。             |
| -v<br>--verbose             | 実行中に、更新プロセスに関する情報を表示します。 |

## 戻りコード

ファームウェア更新プロセスについての情報はすべて、BladeCenterUpdates.log ファイルに記録されます。ログ・ファイル項目のフォーマットは、次のとおりです。

<time\_and\_date> - <message>

ChassisUpdate スクリプトには、次の戻りコードがあります (表 7-8)。

表 7-8 ChassisUpdate からの戻りコード

| 戻りコード | 意味                                      |
|-------|-----------------------------------------|
| -1    | 一般的な更新障害。                               |
| 0     | 更新が正常に完了しました。                           |
| 1     | 指定の Telnet 接続に対して無効な IP アドレスが指定されました。   |
| 2     | Telnet セッションを開始しようとしたときにソケット・エラーがありました。 |
| 3     | Telnet セッションから無効な応答を受け取りました。            |
| 4     | Telnet セッションに対して無効なログイン名とパスワードが指定されました。 |
| 5     | 管理モジュールに対して無効な IP アドレスが指定されました。         |
| 6     | BCMM に接続しようとしたときにソケット・エラーがありました。        |
| 7     | BCMM に接続しようとしたときに不明のエラーがありました。          |
| 8     | BCMM から戻された暗号鍵が無効です。                    |
| 9     | BCMM に対して無効なログイン名とパスワードが指定されました。        |
| 10    | BCMM から無効な応答を受け取りました。                   |
| 11    | BCMM にコマンドを送信する際に 3 回の試行限度を超えました。       |

| 戻りコード | 意味                                          |
|-------|---------------------------------------------|
| 12    | 管理モジュールに対して不明のコマンド・タイプを指定しました。              |
| 13    | 管理モジュールのコマンドの長さと応答が一致していません。                |
| 14    | BCMM から送信されたコマンドと BCMM から受信したコマンドが一致していません。 |
| 15    | BCMM へのデータ送信にエラーがありました。                     |
| 16    | BladeCenter シャーシの無効なスロット番号が指定されました。         |
| 17    | 照会で無効なコード・レベルが指定されました。                      |
| 18    | 指定された管理モジュール・パケット・ファイルが見つかりません。             |
| 19    | 無効なパケット・ファイルが指定されました。                       |
| 20    | パケット・ファイルに無効なヘッダーが含まれています。                  |
| 21    | TFTP ダウンロードのタイムアウト。                         |
| 22    | TFTP サーバーが見つかりません。                          |
| 23    | TFTP サーバーとの接続が失われました。                       |
| 24    | TFTP サーバーの IP アドレスが無効です。                    |
| 25    | 入出力モジュールへの接続に失敗しました。                        |
| 26    | 更新イメージ・ファイルが見つかりません。                        |
| 27    | イメージ・ファイルが無効です。                             |

## 制限

UXBC には、次のような制限があります。

- ▶ 管理モジュール
  - ▶ リダンダント管理モジュールが装備され、IP アドレスを DHCP を通じて取得している場合、既存のファームウェア・レベルが 57 K より低い場合は、管理モジュールを更新できません。
  - ▶ 検出されたコード・レベルによっては、更新プロセス中に管理モジュールの再始動が複数回行われることがあります。UXBC ツールを使用して、管理モジュールのファームウェアを下位レベルにすることはできません。
  - ▶ 応答ファイル内の管理モジュールのパスワード（293 ページの例 7-12 のサンプル応答ファイルでは、mmpass）は、5 文字より多く、16 文字より少ない英数字でなければなりません。

- ▶ IBM ESM 構成
  - ▶ 0.081 (バージョン 1.04) より前のファームウェア・レベルから 0.081 以降のファームウェア・レベルにアップグレードする場合、ESM スイッチ構成の設定値がリセットされる可能性があります。リンク・アグリゲーションの設定は、このファームウェア更新の間に失われ、デフォルト値にリセットされます。
  - ▶ リンク・アグリゲーションの設定またはポート・トランキングをデフォルト設定とは異なる値に設定する場合、後で手動でスイッチを再構成できない場合には、UXBC を使用しないでください。
  - ▶ ごくまれに、UXBC ツールは、ESM スイッチのファームウェア更新が完了したことを確認できない場合があります。この場合、BladeCenterUpdates.log ファイルに、Update completion could not be verified という警告が記録されます。UXBC ツールがフラッシュの完了を確認できなかった場合に実施したテストでは、ESM スイッチはすべて正常に更新されていました。ただし、ユーザーは手動で、ESM スイッチが正しいレベルであることを確認する必要があります。
- ▶ 一般

管理システムから一度に複数の BladeCenter シャーシに対して ChassisUpdate スクリプトの複数インスタンスを実行すると、望ましくない結果が生じる可能性があります、これはサポートされません。



# 省略語および頭字語

|               |                                                                            |               |                                                     |
|---------------|----------------------------------------------------------------------------|---------------|-----------------------------------------------------|
| <b>ADS</b>    | Active Directory Service                                                   | <b>DIMM</b>   | dual inline memory module                           |
| <b>ADSI</b>   | Active Directory Service Interfaces                                        | <b>DLL</b>    | ダイナミック・リンク・ライブラリー (dynamic linked library)          |
| <b>ANSI</b>   | 米国規格協会 (American National Standards Institute)                             | <b>DMI</b>    | Desktop Management Interface                        |
| <b>ASCII</b>  | 情報交換用米国標準コード (American National Standard Code for Information Interchange) | <b>DMTF</b>   | Distributed Management Task Force                   |
| <b>ASF</b>    | Alert Standard Format                                                      | <b>DN</b>     | 識別名 (distinguished name)                            |
| <b>ASM</b>    | システム管理 (advanced system management)                                        | <b>DNS</b>    | ドメイン・ネーム・システム (Domain Name System)                  |
| <b>ASMA</b>   | システム管理アダプター (Advanced System Management Adapter)                           | <b>DOS</b>    | ディスク・オペレーティング・システム (disk operating system)          |
| <b>ASMP</b>   | システム管理プロセッサ (Advanced System Management Processor)                         | <b>DSA</b>    | digital signature algorithm                         |
| <b>ASR</b>    | 自動サーバー再始動 (automatic server restart)                                       | <b>EEPROM</b> | electrically erasable programmable read only memory |
| <b>ASU</b>    | Advanced Settings ユーティリティ (Advanced Settings Utility)                      | <b>EMEA</b>   | 欧州、中東、アフリカ (Europe, Middle East, Africa)            |
| <b>BCMM</b>   | BladeCenter 管理モジュール                                                        | <b>EMS</b>    | Emergency Messaging Service                         |
| <b>BIOS</b>   | 基本入出力システム (basic input output system)                                      | <b>ESM</b>    | イーサネット・スイッチ・モジュール (Ethernet switch modules)         |
| <b>BMC</b>    | Baseboard Management Controller                                            | <b>EXA</b>    | Enterprise X-Architecture™                          |
| <b>BOOTP</b>  | ブート・プロトコル (boot protocol)                                                  | <b>GUI</b>    | グラフィカル・ユーザー・インターフェース (graphical user interface)     |
| <b>CD-ROM</b> | compact disk read only memory                                              | <b>HDD</b>    | ハード・ディスク (hard disk drive)                          |
| <b>CIM</b>    | Common Information Model                                                   | <b>HID</b>    | human interface device                              |
| <b>CLI</b>    | コマンド・ライン・インターフェース (command-line interface)                                 | <b>IBM</b>    | International Business Machines Corporation         |
| <b>CPU</b>    | 中央演算処理装置 (central processing unit)                                         | <b>ICMB</b>   | Intelligent Chassis Management Bus                  |
| <b>CSR</b>    | 証明書署名要求 (Certificate Signing Request)                                      | <b>ICMP</b>   | internet control message protocol                   |
| <b>CTS</b>    | 送信可 (clear to send)                                                        | <b>IP</b>     | インターネット・プロトコル (internet protocol)                   |
| <b>DEN</b>    | Directory Enabled Network                                                  | <b>IPMB</b>   | Intelligent Platform Management Bus                 |
| <b>DHCP</b>   | 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)                         | <b>IPMI</b>   | Intelligent Platform Management Interface           |
|               |                                                                            | <b>IRQ</b>    | 割り込み要求 (interrupt request)                          |
|               |                                                                            | <b>ISM</b>    | 内蔵システム管理 (integrated system management)             |

|              |                                                                         |               |                                                     |
|--------------|-------------------------------------------------------------------------|---------------|-----------------------------------------------------|
| <b>ISMP</b>  | 内蔵システム管理プロセッサ (Integrated System Management Processor)                  | <b>OS</b>     | オペレーティング・システム (operating system)                    |
| <b>ISO</b>   | 国際標準化機構 (International Organization for Standards)                      | <b>PCI</b>    | Peripheral Component Interconnect                   |
| <b>ITSO</b>  | International Technical Support Organization                            | <b>PET</b>    | Platform Event Trap                                 |
| <b>IXA</b>   | 統合 xSeries アダプター (Integrated xSeries Adapter)                           | <b>PKT</b>    | パケット (packet)                                       |
| <b>KVM</b>   | キーボード・ビデオ・マウス (keyboard video mouse)                                    | <b>PPP</b>    | point-to-point protocol                             |
| <b>LAA</b>   | ローカル管理アドレス (locally administered address)                               | <b>PXE</b>    | プリブート実行環境 (preboot execution environment)           |
| <b>LAN</b>   | ローカル・エリア・ネットワーク (local area network)                                    | <b>RAID</b>   | 新磁気ディスク制御機構 (redundant array of independent disks)  |
| <b>LDAP</b>  | Lightweight Directory Access Protocol                                   | <b>RAM</b>    | ランダム・アクセス・メモリー (random access memory)               |
| <b>LDAPS</b> | セキュア LDAP (secure LDAP)                                                 | <b>RDM</b>    | Remote Deployment Manager                           |
| <b>LED</b>   | 発光ダイオード (light emitting diode)                                          | <b>RFC</b>    | request for comments                                |
| <b>MAC</b>   | メディア・アクセス制御 (media access control)                                      | <b>RISC</b>   | reduced instruction set computing                   |
| <b>MB</b>    | メガバイト (megabyte)                                                        | <b>ROM</b>    | 読み取り専用メモリー (read-only memory)                       |
| <b>MCSE</b>  | Microsoft 認定システム・エンジニア (Microsoft Certified Systems Engineer)           | <b>RPM</b>    | Red Hat Package Manager                             |
| <b>MMC</b>   | Microsoft 管理コンソール (Microsoft Management Console)                        | <b>RSA</b>    | リモート管理アダプター (Remote Supervisor Adapter)             |
| <b>MPA</b>   | 管理プロセッサ (Management Processor Assistant)                                | <b>SAC</b>    | Special Administration Console                      |
| <b>MPCLI</b> | 管理プロセッサ・コマンド・ライン・インターフェース (management processor command line interface) | <b>SAN</b>    | storage area network                                |
| <b>MTU</b>   | 最大伝送単位 (maximum transmission unit)                                      | <b>SCSI</b>   | small computer system interface                     |
| <b>NEBS</b>  | network equipment building system                                       | <b>SLES</b>   | SUSE LINUX Enterprise Server                        |
| <b>NIC</b>   | ネットワーク・インターフェース・カード (network interface card)                            | <b>SLP</b>    | Service Location Protocol                           |
| <b>NMI</b>   | マスク不可能割り込み (non-maskable interrupt)                                     | <b>SMASH</b>  | Systems Management Architecture for Server Hardware |
| <b>OEM</b>   | 他装置製造者 (other equipment manufacturer)                                   | <b>SMBIOS</b> | システム管理 BIOS (system management BIOS)                |
| <b>OOB</b>   | アウト・オブ・バンド (out of band)                                                | <b>SMI</b>    | Structure of Management Information                 |
|              |                                                                         | <b>SMTP</b>   | Simple Mail Transfer Protocol                       |
|              |                                                                         | <b>SNMP</b>   | Simple Network Management Protocol                  |
|              |                                                                         | <b>SOL</b>    | serial over LAN                                     |
|              |                                                                         | <b>SP</b>     | サービス・プロセッサ (service processor)                      |
|              |                                                                         | <b>SSH</b>    | セキュア・シェル (secure shell)                             |
|              |                                                                         | <b>SSL</b>    | secure sockets layer                                |
|              |                                                                         | <b>UDF</b>    | Universal Disk Format                               |

|              |                                         |
|--------------|-----------------------------------------|
| <b>UPN</b>   | ユーザー・プリンシパル名 (User Principal Name)      |
| <b>UPS</b>   | 無停電電源装置 (uninterruptible power supply)  |
| <b>URL</b>   | Uniform Resource Locator                |
| <b>USB</b>   | universal serial bus                    |
| <b>UX</b>    | UpdateXpress                            |
| <b>VESA</b>  | Video Electronics Standards Association |
| <b>VPD</b>   | 重要プロダクト・データ (vital product data)        |
| <b>VRM</b>   | 電圧調節モジュール (voltage regulator module)    |
| <b>WAN</b>   | 広域ネットワーク (wide area network)            |
| <b>WEBEM</b> | Web-based Enterprise Management         |
| <b>WOL</b>   | wake on LAN                             |
| <b>XON</b>   | 送信オン (transmitter on)                   |





# 関連資料

ここに掲載する資料は、このレッドブックで取り上げている問題をさらに詳しく検討するのに特に適していると考えられる資料です。

## IBM Redbook

これらの資料の注文方法については、『IBM Redbook の入手方法』（311 ページ）を参照してください。ここに記載されている資料の一部のものは、ソフトコピーでのみ入手できる場合があります。

- ▶ *IBM @server xSeries BMC — Firmware and Drivers Cheatsheet, TIPS0532*
- ▶ *Implementing Systems Management Solutions using IBM Director, SG24-6188*
- ▶ *Netfinity Server Management, SG24-5208*
- ▶ *Remote Supervisor Adapter II Family — Firmware and Drivers Cheatsheet, TIPS0532*
- ▶ *Service Processors Supported in IBM Netfinity and IBM @server xSeries Servers, TIPS0146*

## その他の資料

次の資料も関連の情報源として利用できます。

- ▶ *Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-57091.html>
- ▶ *IBM Remote Supervisor Adapter II Technical Update for Linux, 2nd Edition*  
<http://www.ibm.com/pc/support/site.wss/MIGR-50314.html>
- ▶ *BladeCenter Management Module User's Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-45153.html>
- ▶ *BladeCenter Management Module Installation Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-52227.html>

- ▶ *BladeCenter and BladeCenter T Management Module Command-Line Interface Reference Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-54667.html>
- ▶ *BladeCenter and BladeCenter T Serial over LAN Setup Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-54666.html>
- ▶ *Lightweight Directory Access Protocol User's Guide for IBM @server BladeCenter Management Module and IBM Remote Supervisor Adapters*  
<http://www.ibm.com/pc/support/site.wss/MIGR-55014.html>
- ▶ *Management Command Line Interface User's Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-54214.html>
- ▶ *OSA System Management Bridge User's Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-57816.html>
- ▶ *IBM Director Installation Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-50460.html>
- ▶ *IBM Director Systems Management Guide*  
<http://www.ibm.com/pc/support/site.wss/MIGR-50461.html>
- ▶ *Whitepaper: Automating System Firmware Updates with RemoteUX and UpdateXpress*  
<http://www.ibm.com/pc/support/site.wss/MIGR-54033.html>
- ▶ *Technical update: Connecting an x335 to an ASM interconnect network*  
<http://www.ibm.com/pc/support/site.wss/MIGR-54747.html>
- ▶ *IPMI Version 1.5 specification*  
[ftp://download.intel.com/design/servers/ipmi/IPMIv1\\_5rev1\\_1-012904markup.pdf](ftp://download.intel.com/design/servers/ipmi/IPMIv1_5rev1_1-012904markup.pdf)
- ▶ *Active Directory Programmer's Guide*  
<http://go.microsoft.com/fwlink/?LinkId=142>

## オンライン・リソース

次の Web サイトと URL も関連の情報源として役立ちます。

### IBM Web ページ

- ▶ *BladeCenter Standby Capacity on Demand*  
[http://www.ibm.com/servers/eserver/bladecenter/scod/more\\_info.html](http://www.ibm.com/servers/eserver/bladecenter/scod/more_info.html)

- ▶ ServerProven System Management Upgrades  
<http://www.pc.ibm.com/us/compat/xseries/upgrades/smmatrix.html>
- ▶ Software and device drivers matrix for xSeries and BladeCenter  
<http://www.ibm.com/pc/support/site.wss/MIGR-4JTS2T.html>
- ▶ RETAIN tip H177279, RSA II PS/2 mouse does not work during Red Hat Linux installation  
<http://www.ibm.com/pc/support/site.wss/MIGR-50413.html>
- ▶ BladeCenter 4-Port Ethernet Switch Module Firmware  
<http://www.ibm.com/pc/support/site.wss/MIGR-50457.html>
- ▶ UpdateXpress CD  
<http://www.ibm.com/pc/support/site.wss/MIGR-53046.html>
- ▶ BladeCenter Nortel Networks Layer 2-7 GbE Switch Module Firmware  
<http://www.ibm.com/pc/support/site.wss/MIGR-53058.html>
- ▶ Management Processor Command Line Interface Utility  
<http://www.ibm.com/pc/support/site.wss/MIGR-54216.html>
- ▶ Management Module Firmware for BladeCenter  
<http://www.ibm.com/pc/support/site.wss/MIGR-54939.html>
- ▶ Management Module Firmware for BladeCenter T  
<http://www.ibm.com/pc/support/site.wss/MIGR-56054.html>
- ▶ RSA II remote mounting issues with Linux  
<http://www.ibm.com/pc/support/site.wss/MIGR-55671.html>
- ▶ Advanced Settings Utility for Microsoft Windows  
<http://www.ibm.com/pc/support/site.wss/MIGR-55019.html>
- ▶ Advanced Settings Utility for Linux  
<http://www.ibm.com/pc/support/site.wss/MIGR-55020.html>
- ▶ Advanced Settings Utility for DOS  
<http://www.ibm.com/pc/support/site.wss/MIGR-55021.html>
- ▶ Advanced Settings Utility definition files for RSA and RSA II  
<http://www.ibm.com/pc/support/site.wss/MIGR-55027.html>
- ▶ Advanced Settings Utility definition files for x345  
<http://www.ibm.com/pc/support/site.wss/MIGR-55778.html>

- ▶ Advanced Settings Utility definition files for x235  
<http://www.ibm.com/pc/support/site.wss/MIGR-55803.html>
- ▶ Advanced Settings Utility definition files for x335  
<http://www.ibm.com/pc/support/site.wss/MIGR-55804.html>
- ▶ Advanced Settings Utility definition files for x445  
<http://www.ibm.com/pc/support/site.wss/MIGR-55944.html>
- ▶ Advanced Settings Utility definition files for x255  
<http://www.ibm.com/pc/support/site.wss/MIGR-56393.html>
- ▶ Advanced Settings Utility definition files for BladeCenter HS20 8832  
<http://www.ibm.com/pc/support/site.wss/MIGR-56555.html>
- ▶ Advanced Settings Utility definition files for x440  
<http://www.ibm.com/pc/support/site.wss/MIGR-56858.html>
- ▶ Advanced Settings Utility definition files for BladeCenter HS20 8678  
<http://www.ibm.com/pc/support/site.wss/MIGR-56860.html>
- ▶ IBM Director 4.20.2  
<http://www.ibm.com/pc/support/site.wss/MIGR-57057.html>
- ▶ UpdateXpress firmware update scripts for BladeCenter  
<http://www.ibm.com/pc/support/site.wss/MIGR-57201.html>
- ▶ IBM UpdateXpress Server  
<http://www.ibm.com/pc/support/site.wss/MIGR-57426.html>
- ▶ System Management Bridge utility  
<http://www.ibm.com/pc/support/site.wss/MIGR-57729.html>

## その他の Web ページ

- ▶ Distributed Management Task Force 標準  
<http://www.dmtf.org/standards>  
<http://www.dmtf.org/standards/smash>
- ▶ Intelligent Platform Management Interface  
<http://www.intel.com/design/servers/ipmi>
- ▶ Java ランタイム環境のダウンロード  
<http://www.java.com/en/download/manual.jsp>
- ▶ CD-ROM ISO ツール  
<http://www.smart-projects.net/isobuster>

<http://www.magiciso.com>

- ▶ PuTTY telnet/SSH クライアント  
<http://www.chiark.greenend.org.uk/~sgtatham/putty>
- ▶ Windows Emergency Management Services  
[http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS\\_topnode.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_topnode.asp)
- ▶ Windows Special Administration Console および SAC コマンド  
[http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS\\_SAC\\_commands.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/EMS_SAC_commands.asp)
- ▶ SolarWindws TFTP サーバー  
[http://www.solarwinds.net/Tools/Free\\_tools/TFTP\\_Server](http://www.solarwinds.net/Tools/Free_tools/TFTP_Server)
- ▶ Python  
<http://www.python.org>

## IBM Redbook の入手方法（英語版のみ）

次の Web サイトでは、Redbook、Redpaper、ヒント、ドラフト資料、追加資料などを、検索、表示、またはダウンロードできます。

[ibm.com/redbooks](http://ibm.com/redbooks)

## IBM のヘルプ

IBM サポートおよびダウンロード

[ibm.com/support](http://ibm.com/support)

IBM グローバル・サービス

[ibm.com/services](http://ibm.com/services)



# 索引

## 数字

13N0382、RSA II-EXA 54  
59P2984、RSA II 53  
73P9341、RSA II SlimLine 55

## A

Active Directory 138, 151  
ASF 5  
ASM PCI アダプター  
    ASM インターコネクト・ネットワーク 57  
    IBM Director 241  
    MPCLI 186  
    Telnet インターフェース 235  
    サポートされるサーバー 2  
ASM インターコネクト・ネットワーク 57-63, 50  
    ゲートウェイ 61  
    管理モジュール 94  
ASU 170-186  
    patchadd コマンド 173  
    resetrsa コマンド 265  
    RSA II の構成 184  
    set コマンド 184  
    オペレーティング・システム 171  
    構文 174  
    コマンド 175  
    サポートされるサーバー 171  
    出荷時のデフォルト値 265  
    使用 184  
    スクリプト 185  
    設定の表示 176  
    ダウンロード 173  
    他のツールとの比較 170  
    定義ファイル 173  
    バッチ・コマンド 185  
    リモート、使用 269

## B

BIOS  
    BMC イベント・ログ 36  
    BMC 構成 35  
    Remote Console Redirection 207  
    SMBridge 構成 207  
BladeCenter

BladeCenter アシスタント 242  
UpdateXpress スクリプト 291  
UXBC 292  
オンデマンド活動化 128  
管理モジュール  
    「管理モジュール」を参照  
デフォルト・アドレス 255  
モジュールへのリモート・アクセス 255  
BMC 7-48  
eServer BMC 9-18  
    IBM Director 14  
    IBM Director アラート 13  
    IPMI ドライバー 17  
    lancfg 11  
    MAC アドレス 12  
    ping コマンド 9  
    アラート転送 16  
    アラートの宛先 13  
    構成 11  
    接続 9  
    デフォルトのユーザー ID 13  
    ドライバー 17  
    パッドロック・アイコン 15  
    ファームウェアのアップグレード 10  
    ユーザーの追加 15  
ISM プロセッサとの比較 8  
xSeries BMC 18-47  
    ASM コネクタ 21  
    BIOS 内での構成 35  
    bmc\_cfg 23  
    IBM Director 38  
        アラートの送信先 26, 41  
        構成 38  
    IP アドレスの設定 25  
    IPMI ドライバー 42  
    PET アラート 27  
    ping コマンド 19  
    RS-485 コネクタ 21  
    RSA II SlimLine、両方を搭載 249  
    SEL 36  
    SNMP コミュニティ 28  
    TCP/IP ポート 47  
    宛先タイプ 27

- アラートの宛先 26
- イベント・ログ 36
- 機能 19
  - クロック 36
  - ゲートウェイ 26
  - サブネット・マスク 26
  - 使用不可化 20
  - 接続 19
  - チャンネル番号 25
  - デフォルトのユーザー ID 24
  - デフォルト・ゲートウェイ 26
  - 特権 33
  - ドライバー 42
  - パッドロック・アイコン 39
  - ファームウェアの更新 22
  - 物理プラットフォーム 38
  - ポート 19, 47
  - ユーザーの追加 28, 39
  - ユーザー・アクセス 31
  - リモート制御 42
  - SMBridge 204–232
- 機能 8
- サポートされるサーバー 2
- bmc\_cfg 23–35
  - IP アドレスの設定 25
  - SNMP コミュニティ 28
  - 宛先アドレス 26
  - 宛先タイプ 27
  - サブネット・マスク 26
  - チャンネル番号 25
  - デフォルト・ゲートウェイ 26
  - 特権 33
  - ユーザーの追加 28
  - ユーザー・アクセス 31
- bootcfg コマンド 219

## C

- C2T 61
- CIM 5
- CLI
  - ASU 170–186
  - MPCLI 186–204
  - RemoteUX 283
  - SMBridge 204–232
  - Telnet インターフェース 234–238
  - セキュア化 250
  - 比較 168
- CLIs
  - bmc\_cfg 23–35

## D

- DEN 5
- DMI 5
- DMTF 5

## E

- Emergency Messaging Service 212

## I

- IBM Director 239–246
  - BladeCenter アシスタント 242
  - BMC 構成
    - eServer BMC 14
    - xSeries BMC 38
  - BMC の追加 14
  - File Transfer 270
  - アラート転送 243
  - 暗号化 249
  - 管理プロセッサ 39, 241
  - 出荷時のデフォルト値 266
  - スケジューラー 281
  - パッドロック・アイコン 15, 39
  - ファームウェアの更新 275
  - 物理プラットフォーム・オブジェクト 15, 38
  - ユーザーの追加
    - eServer BMC 15
    - xSeries BMC 39
  - MPA 239–242
- IPMI 6
- IPMI ドライバー
  - BladeCenter サーバー 127
  - eServer BMC 17
  - xSeries BMC 42
- ISM プロセッサ
  - BMC との比較 8
  - MPCLI サポート 186
  - インターコネクト・バス 60
  - 機能 8, 47
  - ゲートウェイ装置 61, 48
  - サポートされるサーバー 2
  - 制限 48

## J

- Java ランタイム 72

## L

- lancfg ユーティリティ 11
- LDAP 148–166



- miscellaneous parameters 162
- MPCLI 190
- user search base DN 162
- クライアント 160
- グループ・フィルター 163
- 構成のテスト 158
- スキーマ 152
- 認証属性 149
- バインド方式 163

Linux

- ASU サポート 171
- GNOME 78, 111
- KDE 78, 111
- MPCLI サポート 191
- OpenLDAP 138
- RSA II
  - Remote Control 75
    - ドライバー 71
    - リモート CD-ROM 87
    - リモート・イメージ・ファイル 90
    - リモート・ディスクレット 84
- SMBridge 211
- telnet 214
- XDM 77, 111
- 管理モジュール
  - Remote Control 110
    - リモート CD-ROM 121
    - リモート・イメージ・ファイル 125
    - リモート・ディスクレット 116

**M**

- MIB ファイル
  - RSA II 72
  - 管理モジュール 103
- MPCLI 186-204
  - LDAP 190
  - Linux
    - インストーラ 192
    - 制限 191
  - Serial over LAN 190
  - SP 情報の例 200
  - SP 設定の変更 189
  - Windows 上のインストーラ 192
  - イーサネット構成の例 199
  - イベント・ログ 190
  - イベント・ログの例 200
  - インストーラ 191
  - 開始 193
  - 管理モジュールの例 201

- 機能 189
- 構文 193
- コマンド 196
- サポートされるサーバー 186
- サンプル・スクリプト 199
- シナリオ 262
- 出荷時のデフォルト値 268
- 使用例 262
- スクリプト記述 190, 198
  - ネストされたスクリプト 203
- 制限 194
- 接続 195
- 他のツールとの比較 170
- 電源制御 190
- バッチ・コマンド 198
- ファームウェアの更新 202, 273
- ヘルス状況 190
- ユーザー ID の作成 202
- ログオン 195

## O

- OpenLDAP 138
- OSA SMBridge
  - 「SMBridge」を参照。
- 「Other OS」設定、RSA II 65

## P

- PET トラップ 13
- PKT ファイル
  - MPCLI、使用 201, 273
  - RSA II 67
  - 管理モジュール 274
- PowerQuest 284
- PuTTY 146

## R

- Red Hat
  - ASU サポート 171
  - MPCLI サポート 191
  - RSA II
    - Remote Control 76
      - リモート CD-ROM 88
      - リモート・イメージ・ファイル 91
      - リモート・ディスクレット 86
  - SMBridge サポート 206
  - SMBridge のインストーラ 211
  - SOL、使用可能化 224
  - 管理モジュール

- Remote Control 111
    - リモート CD-ROM 122
    - リモート・イメージ・ファイル 126
    - リモート・ディスクレット 119
  - Redbooks Web サイト 311
    - Contact us xi
  - Remote Control
    - 管理モジュール 106-127
  - RemoteUX 283
    - Windows サポート 284
    - コマンド 286
    - パラメーター 285
    - 戻りコード 290
  - RSA
    - ASU サポート 171
    - MPCLI サポート 187
    - Telnet インターフェース 238
    - サポートされるサーバー 2
    - 「RSA II」も参照。
  - RSA II 49-92
    - ASM インターコネクト・ネットワーク 50, 57, 59
    - ASU サポート 171
    - DHCP 65
    - IBM Director 241
    - IBM Director へのアラート転送 243
    - ISM プロセッサのゲートウェイ 62
    - Java ランタイム 72
    - LDAP 148-166
    - LDAP を使用した認証 148-166
    - Linux
      - インストール 71
      - リモート・メディア 80
    - MIB ファイル 72
    - MPCLI サポート 187
    - Remote Control 72-91
      - Linux サポート 75
    - RSA II-EXA 54
    - SNMP MIB ファイル 72
    - SSH (セキュア・シェル) 143
    - SSL 138, 249
    - TCP ポート 91
    - Telnet インターフェース 235
    - USB ケーブル 51, 64
    - Web インターフェース
      - セキュア化 100, 249
      - 使用 232
    - Windows ドライバー 69
    - アラート 50
  - 暗号化 138-148
  - イベント・ログ 50
  - インターコネクト・ネットワーク 50, 59, 60
  - 機構 53
  - 機能 50
    - グローバル・ログイン設定 166
  - 構成 63
    - 構成のバックアップ 251
    - 構成のリストア 253
    - 固定アドレス 65
    - コネクター 53
    - サポートされるサーバー 2, 51
    - システム・ボード・コネクター 51
    - 出荷時のデフォルト値 264
    - 証明書 139
    - セキュリティ 138-148
    - デフォルトのユーザー ID 67
    - ドライバ 69
    - ネットワーク設定 64
    - ビデオ速度 74
    - ファームウェアの更新 66, 274
    - ブルー・スクリーン 50
    - ブレイクアウト・ケーブル 54
    - ヘルス・モニター 50
    - ポート 91
      - ユーザー ID の一括構成 262
      - ユーザー ID の一括変更 262
    - リモート・メディア 79-91
      - ディスクレット 83
      - ファイル 88
      - リモート CD-ROM 86
    - 「Other OS」設定 65
    - 「RSA」も参照。
    - 取り付け 63
  - 「Other OS」設定、RSA II 65
  - RSA II SlimLine 55
    - ASM インターコネクト・ネットワーク 57
    - 機能 50
    - サポートされるサーバー 2
    - 「RSA II」も参照。
- ## S
- SAC コマンド 218
  - Serial over LAN
    - MPCLI 190
    - SMBridge 204, 216
    - 管理モジュール 132
  - ServerProven 73
  - SMASH 5

- SMBIOS 5
- SMBridge 204–232
  - BIOS 設定 207
  - bootcfg コマンド 219
  - CLI 205, 229
  - console コマンド 216
  - EMS 212, 218
  - EMS、使用可能化 219
  - GRUB 226
  - LILO 224
  - Linux サポート 206
  - PXE ブート 207
  - Red Hat、SOL の使用可能化 224
  - SAC 218
  - SAC コマンド 218
  - SAC サポート 212
  - Serial over LAN 216
  - SOL の終了 219
  - Telnet クライアント 213
  - Telnet サーバー 205, 212
  - Telnet の F1 キー 213
  - Windows SOL 217
  - イベント・ログ 217
  - インストール 208
  - コマンド 215, 231
  - コンソール・リダイレクト 207
  - サービス 211
  - 接続 214
  - タイムアウト値 210
  - 他のツールとの比較 170
  - デーモン 212
  - 電源制御 216
  - 認証 215
  - ポート 210
  - リモート・コンソール・リダイレクト 207
- SNMP 6
  - MIB ファイル
    - RSA II 72
    - 管理モジュール 103
  - xSeries BMC 28
- Special Administration Console 212
- SSH (セキュア・シェル) 143
- SSL 138
- SUSE LINUX
  - ASU サポート 172
  - MPCLI サポート 191
  - RSA II
    - Remote Control 76
    - リモート CD-ROM 88

- リモート・イメージ・ファイル 90
- リモート・ディスクット 85
- SOL、使用可能化 227
- 管理モジュール
  - Remote Control 111
  - リモート CD-ROM 121
  - リモート・ディスクット 117
  - リモート・ファイル・イメージ 125

## T

- TCP ポート
  - RSA II 91
  - 管理モジュール 134
- TCP/IP ポート
  - xSeries BMC 47
- Telnet インターフェース 234–238
  - SMBridge 205
  - コマンド 235
  - 他のツールとの比較 170
- TFTP サーバー 170, 292

## U

- UpdateXpress 276, 283
  - BladeCenter 291
  - RemoteUX 283
  - UXBC 292

## W

- Web インターフェース 232, 232–234
  - セキュア化 100, 249
  - 他のツールとの比較 170
- WEBEM 5
- Windows
  - ASU サポート 171
  - bootcfg コマンド 219
  - EMS 212
    - 使用可能化 219
  - eServer BMC ドライバー 17
  - MPCLI サポート 191
  - RSA II
    - ドライバ 69
    - リモート CD-ROM 87
    - リモート・イメージ・ファイル 90
    - リモート・ディスクット 84
  - SAC 212
  - SAC コマンド 218
  - SMBridge
    - インストール 209

- サポート 206
- SOL サポート 217
- xSeries BMC ドライバー 42
- 管理モジュール
  - リモート CD-ROM 120
  - リモート・イメージ・ファイル 125
  - リモート・ディスク 116

## X

- xSeries サーバー
  - サポート一覧表 2

## あ

- 暗号化 138–148

## い

- イーサネット・スイッチ・モジュール 255
- イベント・ログ、BMC 36
- インターコネクト・ネットワーク 50, 57–63
  - RSA II 54
  - 管理モジュール 94

## お

- オペレーター権限
  - eServer BMC 16
  - xSeries BMC 33, 41
- オンデマンド活動化
  - BladeCenter 128

## か

- カスタム権限
  - eServer BMC 16
- 監視許可権限
  - eServer BMC 16
  - xSeries BMC 41
- 管理 LAN 256
- 管理者権限
  - eServer BMC 16
  - xSeries BMC 33, 41
- 管理プロセッサ 39, 241–242
- 管理モジュール 93–136
  - BladeCenter アシスタント 242
  - DHCP 98
  - IBM Director へのアラート転送 243
  - IP アドレス、デフォルト 98, 99
  - KVM 制御 131
  - KVM 接続 105
  - LDAP 148–166

- LDAP を使用した認証 148–166
- MAC アドレス 98
- MIB ファイル 103
- MPCLI サポート 187
- MPCLI の例 201
- Remote Control 106–127
  - Linux サポート 110
  - 位相調整 109
  - 画面調整 109
  - キーボード・セレクター 110
  - メディア・トレイ 109
- Serial over LAN 132
- SNMP MIB ファイル 103
- SSH (セキュア・シェル) 143
- SSL 138, 249
- TCP ポート 134
- Telnet インターフェース 235
- wake on LAN 131
- Web インターフェース
  - セキュア化 100, 249
- 暗号化 138–148
- イーサネット・インターフェース 104
- 機構 94
  - グローバル・ログイン設定 166
  - 構成 97, 127
  - 構成のバックアップ 251
  - 構成のリストア 253
  - コネクタ 94
  - 再始動 100
  - 出荷時のデフォルト値 136
  - 出荷時のデフォルト値へのリセット 136
  - 手動切り替え 104, 105
  - 証明書 139
  - セキュリティ 138–148
  - デフォルト IP アドレス 98, 99
  - デフォルト・ホスト名 98
  - 電源制御 131, 132
  - 取り付け 97
  - 入出力モジュール
    - ファームウェアの更新 134
    - タスク 132
  - ネットワーク設定 98
  - ファームウェアの更新 101, 103, 274
    - 個別のブレード 130
  - フェイルオーバー 105
  - ブレード情報 130
  - ポート 134
  - ポリシー設定 131
  - メディア・トレイ 109

モジュールへのリモート・アクセス 255  
ユーザー ID の一括構成 262  
ユーザー権限 95  
ユーザー ID の一括変更 262  
リダンダント管理モジュール 103  
リモート・メディア 112-127, 106  
  CD-ROM 120  
  イメージ・ファイル 123  
  ディスクレット 115

## き

業界標準 4

## け

ゲートウェイ、ASM インターコネクト・ネットワーク  
61

## こ

コールバック権限  
  xSeries BMC 33  
コンソール・リダイレクト 207

## さ

サービス・プロセッサへの ANSI インターフェース  
234-238  
サービス・プロセッサ  
  BladeCenter 管理モジュール 93-136  
  eServer BMC 9-18  
  ISM プロセッサ 47-48  
  RSA II 49-92  
  xSeries BMC 18-47  
サブネット、複数の 259  
サポートされるサーバー 2  
  RSA II 51  
  ユーティリティ 168

## し

シナリオ 247-301  
出荷時のデフォルト値  
  RSA II 264  
  管理モジュール 136

## す

スクリプト記述  
  ASU 185  
  MPCLI 198

## せ

セキュリティ 138-148  
  シナリオ 248

## つ

ツール  
  ASU 170-186  
  bmc\_cfg 23-35  
  IBM Director 239-246  
  lancfg 11  
  MPCLI 186-204  
  RemoteUX 283  
  SMBridge 204-232  
  Telnet インターフェース 234-238  
  Web インターフェース 232-234  
  セキュア化 250  
  比較 168

## て

電源制御  
  MPCLI 190  
  SMBridge 216  
  Telnet インターフェース 236  
  サポートするツール 170

## と

統合 xSeries アダプター 21  
ドライバー  
  BladeCenter サーバー 127  
  eServer BMC 17  
  RSA II 69  
  xSeries BMC 42

## に

認証  
  LDAP 148-166  
  xSeries BMC 28, 39  
  シナリオ 248

## ね

ネットワーク  
  複数のサブネット 259

## は

パスワード 248

## ひ

標準 4

## ふ

ファームウェアのアップグレード  
eServer BMC 10  
ファームウェアの更新  
IBM Director 275  
MPCLI 202, 273  
RemoteUX 283  
RSA II 66  
Telnet クライアント 236  
UpdateXpress 291  
xSeries BMC 22  
管理モジュール 101  
ブレード・サーバー 130  
例 273  
ブルー・スクリーン 50

## へ

ベースボード管理コントローラー  
「BMC」を参照。

## ほ

ポート  
RSA II 91  
xSeries BMC 47  
管理モジュール 134

## ゆ

ユーザー権限  
xSeries BMC 33  
ユーティリティ  
ASU 170-186  
bmc\_cfg 23-35  
MPCLI 186-204  
SMBridge 204-232  
Telnet インターフェース 234-238  
Web インターフェース 232-234  
IBM Director 239-242  
lancfg 11  
RemoteUX 283  
セキュア化 250  
比較 168

## よ

読み取り専用権限  
eServer BMC 16

xSeries BMC 41

## り

リモート制御  
BMC 42  
リモート・コンソール・リダイレクト 207  
リモート・メディア  
RSA II 79  
CD-ROM 86  
イメージ・ファイル 88  
ディスクレット 83  
管理モジュール 112  
CD-ROM 120  
イメージ・ファイル 123  
ディスクレット 115

## れ

例 247-301





# IBM @server xSeries および BladeCenter サーバー管理



**RSA II アダプター、  
BMC、BladeCenter  
管理モジュールを  
使用した管理**

**ハードウェア装置を  
使用するための  
ユーザー・インター  
フェースの解説**

**ツールの使用法の  
事例を掲載**

IBM @server xSeries および BladeCenter サーバーに搭載されるシステム管理ハードウェアは、お客様の総合的な管理計画に重要な役割を果たします。このハードウェアは、サーバーまたは BladeCenter シャーシに組み込まれるか、工場アダプターとして取り付けられ、オプションとしても入手可能です。システム管理ハードウェアは、管理者に重要な情報を提供し、オペレーティング・システムが稼働中でなくても、管理者はリモート側でサーバーを制御できるようになります。

この IBM Redbook では、現在 xSeries および BladeCenter システムで使用できる管理ハードウェアの全機種を紹介し、内蔵ベースボード管理コントローラー、リモート管理アダプター II ファミリーのアダプター、および BladeCenter 管理モジュールについて説明します。また、このハードウェアにアクセスするために使用するユーザー・インターフェースについて詳しく解説し、セキュリティ機能 (SSL など) と認証機能 (LDAP など) の構成方法も説明します。

本書は、システム管理ハードウェアの機能、その構成方法、使用法を理解してサーバー管理の向上を目指す、お客様、IBM ビジネス・パートナー、および IBM 社員を対象としています。

## INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

**実際の経験  
に基づいた  
技術情報の開発**

IBM Redbooks は IBM International Technical Support Organization が制作しています。世界各国の IBM、お客様、パートナーが協力して、専門家が現実的なシナリオに基づきタイムリーな技術情報を提供します。ユーザーの環境に効果的に IT ソリューションをインプリメントするのに役立つ具体的な推奨を提示します。

**詳細情報：  
[ibm.com/redbooks](http://ibm.com/redbooks)**

SG88-8550-00

