Power Systems

ハードウェア管理コンソールのインストールおよび構成

IBM

Power Systems

ハードウェア管理コンソールのインストールおよび構成

IBM

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、 vii ページの『安全上の注意』、 95 ページの『特記事項』、資料「*IBM Systems Safety Notices*」(G229-9054)、および「*IBM Environmental Notices and User Guide*」(Z125–5823) に記載されている情報をお読みください。

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。

本書は、IBM ハードウェア管理コンソールのバージョン 7 リリース 7.7.0 保守レベル 0 および新版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

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： Power Systems
Installing and configuring the
Hardware Management Console

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2013.9

目次

安全上の注意

安全上の注意は、このガイド全体を通じて記載されています。

- **危険**の注記は、人間に致命的または極めて危険な損傷を与える可能性のある状態について注意を促します。
- **注意**の注記は、何らかの状況が原因の、人間に危険な損傷を与える可能性のある状態について注意を促します。
- **重要**の注記は、プログラム、装置、システム、あるいはデータに損傷を与える可能性があることを示します。

ワールド・トレードの安全上の注意

国によっては、製品資料に記載される安全上の注意を自国語で提示するよう要求しています。 この要求がお客様の国に適用される場合は、製品に付属の資料パッケージ (印刷された資料または DVD で、あるいは製品の一部として) に安全上の注意についての文書が含まれます。この文書には、英語原典に準拠した、各国語による安全上の注意が記載されています。 この製品の取り付け、操作、または保守のために英語の資料をご使用になる場合は、まず、関連している安全上の注意についての文書をよくお読みください。また、英語版資料の安全上の注意が明確に理解できない場合も、必ずこの文書を参照してください。

安全上の注意についての文書の差し替え版または追加のコピーについては、IBM ホットライン (1-800-300-8751) に連絡して入手することができます。

レーザーに関する安全上の注意

IBM® サーバーは、レーザーまたは LED を使用する、光ファイバー・ベースの I/O カードまたはフィーチャーを使用することができます。

レーザーに関する準拠

IBM サーバーは、IT 装置ラックの内部または外部に取り付けることができます。

危険

システムまたはその周辺で作業をする場合は、以下の予防措置を確認してください。

電源ケーブルや電話線、通信ケーブルからの電圧および電流は危険です。 感電を防ぐために次の事項を守ってください。

- **電源と装置を接続する場合は、必ず IBM 提供の電源コードを使用してください。 IBM 提供の電源コードを他の製品に使用しないでください。**
- **電源装置アセンブリーを開いたり、保守しないでください。**
- **雷雨の間はケーブルの接続や切り離し、または本製品の設置、保守、再構成を行わないでください。**
- **この製品は複数の電源コードを備えていることがあります。 危険な電圧をすべて除去するには、すべての電源コードを取り外してください。**
- **すべての電源コードは正しく配線され接地されたコンセントに接続してください。 コンセントがシステム定格プレートに従った正しい電圧および相回転を供給していることを確認してください。**
- **ご使用の製品に接続するすべての装置を、正しく配線されたコンセントに接続してください。**
- **シグナル・ケーブルの接続または切り離しは可能なかぎり片手で行ってください。**
- **火災、水害、または建物に構造的損傷の形跡が見られる場合は、どの装置の電源もオンにしないでください。**
- **取り付けおよび構成手順で特別に指示されている場合を除いて、装置のカバーを開く場合はその前に、必ず、接続されている電源コード、通信システム、ネットワーク、およびモデムを切り離してください。**
- **ご使用の製品または接続されたデバイスの取り付け、移動、またはカバーの取り外しを行う場合には、次の手順に従ってケーブルの接続および取り外しを行ってください。**

  ケーブルの切り離し手順:
  1. **すべての電源をオフにします (別に指示される場合を除く)。**
  2. **電源コードを電源コンセントから取り外します。**
  3. **シグナル・ケーブルをコネクターから取り外します。**
  4. **すべてのケーブルをデバイスから取り外します。**

  ケーブルの接続手順:
  1. **すべての電源をオフにします (別に指示される場合を除く)。**
  2. **すべてのケーブルをデバイスに接続します。**
  3. **シグナル・ケーブルをコネクターに接続します。**
  4. **電源コードをコンセントに接続します。**
  5. **デバイスの電源をオンにします。**

  (D005)

危険

IT ラック・システムやその周辺で作業をする場合は、以下の予防措置を確認してください。

- **重量のある装置の場合、取り扱いを誤ると身体傷害または設備の損傷を引き起こす可能性があります。**
- **ラック・キャビネットのレベル・パッドは必ず下げておきます。**
- **ラック・キャビネットには必ずスタビライザー・ブラケットを取り付けてください。**
- **釣り合いがとれていない機械的荷重による危険な状態を避けるため、最も重いデバイスを常に、ラック・キャビネットの下部に取り付けます。 必ず、サーバーおよびオプション・デバイスはラック・キャビネットの下部側から取り付けてください。**
- **ラック・マウント型デバイスを棚やワークスペースとして使用しないでください。 ラック・マウント型デバイスの上には何も置かないでください。**

- **各ラック・キャビネットには複数の電源コードが付いていることがあります。 保守する際に電源を切断するように指図された場合、ラック・キャビネットのすべての電源コードを抜いてください。**
- **ラック・キャビネット内のすべてのデバイスは、同一ラック・キャビネットに取り付けられている電源デバイスに接続します。 あるラック・キャビネットに取り付けられているデバイスの電源コードを、別のラック・キャビネットにある電源デバイスに接続しないでください。**
- **正しく配線されていない電源コンセントは、システムまたはシステムに接続されたデバイスの金属部品に危険な電圧をかける可能性があります。 感電を避けるためにコンセントが正しく配線および接地されていることの確認は、お客様の責任で行ってください。**

注意

- **ラック内部の温度が、すべてのラック・マウント型デバイスに対する製造者推奨の周辺温度を超えるようなラック内には、装置を取り付けないでください。**
- **空気の流れが妨げられているラック内には、装置を取り付けないでください。 装置内で空気の流れのために使用される装置のいずれかの側面、前面、または背面で、空気の流れが妨げられたり減速されたりしないようにしてください。**
- **回路の過負荷によって電源配線や過電流保護が破損しないように、電源回路への機器の接続には十分注意してください。 ラックに正しく電源を接続するには、ラック内の機器の定格ラベルで、電源回路の総消費電力を確認してください。**
- *(引き出し式ドロワーの場合。)* **ラック・スタビライザー・ブラケットがラックに取り付けられていない場合は、ドロワーまたはフィーチャーを引き出したり、取り付けたりしないでください。 一度に複数のドロワーを引き出さないでください。 一度に複数のドロワーを引き出すと、ラックが不安定になる可能性があります。**
- *(固定式ドロワーの場合。)* **このドロワーは固定ドロワーなので、製造元の指定がない限り、保守のために動かさないでください。 ラックからドロワーの一部または全部を引き出そうとすると、ラックが不安定になったり、ドロワーがラックから落下する可能性があります。**

(R001)

注意:
ラック・キャビネット内の上の方の位置からコンポーネントを取り外すと、再配置中のラックの安定性が改善されます。 格納されたラック・キャビネットを部屋または建物内で再配置するときは必ず、以下の一般ガイドラインに従ってください。

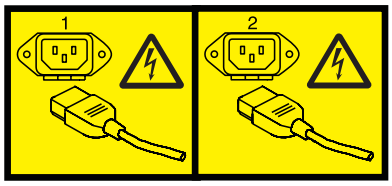
- **ラック・キャビネットの上部から順に装置を取り外すことにより、ラック・キャビネットの重量を減らします。 可能な場合は、ラック・キャビネットを納品時のラック・キャビネットの構成に復元します。この構成がわからない場合は、以下の手順を実行する必要があります。**
  - **32U 位置以上にあるすべてのデバイスを取り外します。**
  - **最も重いデバイスがラック・キャビネットの下部に取り付けられていることを確認します。**
  - **ラック・キャビネット内で 32U レベルより下に取り付けられたデバイス間に空の U レベルがないことを確認します。**
- **再配置しているラック・キャビネットが、一組のラック・キャビネットの一部である場合は、そのスイートからラック・キャビネットを切り離します。**
- **通る予定の経路を検査して、障害になる可能性があるものを取り除きます。**
- **選択する経路が、搭載されたラック・キャビネットの重量を支えることができるか検査します。 搭載されたラック・キャビネットの重量については、ラック・キャビネットに付属の資料を参照してください。**
- **すべてのドアの開口部が少なくとも 760 x 230 mm 以上であることを確認します。**
- **すべてのデバイス、シェルフ、ドロワー、ドア、およびケーブルが安定していることを確認します。**
- **4 つのレベル・パッドが最も高い位置に上がっていることを確認します。**
- **移動時にスタビライザー・ブラケットがラック・キャビネットに取り付けられていないことを確認します。**
- **傾斜が 10 度を超えるスロープは使用しないでください。**
- **ラック・キャビネットが新しい場所に置かれたら、次の手順を実行します。**
  - **4 つのレベル・パッドを下げます。**
  - **スタビライザー・ブラケットをラック・キャビネットに取り付けます。**
  - **ラック・キャビネットからデバイスを取り外してあった場合は、ラック・キャビネットの最も低い位置から最も高い位置へと格納していきます。**
- **長距離の移動が必要な場合は、ラック・キャビネットを納品時のラック・キャビネットの構成に復元します。 ラック・キャビネットを元の梱包材、またはそれと同等のもので梱包します。 また、レベル・パッドを下げて、キャスターをパレットから離れるように持ち上げ、ラック・キャビネットをパレットにボルトで止めます。**

(R002)

(L001)

(L002)

(L003)



または

すべてのレーザーは、クラス 1 のレーザー製品について規定している米国の保健社会福祉省連邦規則 21 副章 J (DHHS 21 CFR Subchapter J) の要件に準拠していることが認証されています。 米国以外の国では、レーザーは、クラス 1 レーザー製品として IEC 60825 に準拠していることが認証されています。 レーザー認証番号および承認情報については、各部品のラベルをご覧ください。

注意:
この製品には、クラス 1 のレーザー製品である CD-ROM ドライブ、DVD-ROM ドライブ、DVD-RAM ドライブ、またはレーザー・モジュールの各デバイスのうち 1 つ以上が含まれていることがあります。 次の情報に注意してください。

- **カバーを外さないこと。 カバーを取り外すと有害なレーザー光を浴びることがあります。 この装置の内部には保守が可能な部品はありません。**
- **本書に記述されている以外の手順、制御または調節を行うと有害な光線を浴びることがあります。**

(C026)

注意:
データ処理環境には、クラス 1 のパワー・レベルより高いレベルで作動するレーザー・モジュールを備えるシステム・リンク上で伝送する装置が含まれることがあります。 この理由から、光ファイバー・ケーブルの先端、またはコンセントの差込口を覗き込まないでください。 (C027)

注意:
この製品には、クラス 1M のレーザーが含まれています。 光学装置を用いて直接見ないでください。 (C028)

注意:
一部のレーザー製品には、クラス 3A またはクラス 3B のレーザー・ダイオードが組み込まれています。 次の点に注意してください。カバーを開くとレーザー光線の照射があります。 光線を見つめたり、光学装置を用いて直接見たり、光線を直接浴びることは避けてください。 (C030)

注意:
このバッテリーにはリチウムが含まれています。 爆発することがありますので、バッテリーを火中に入れたり、充電したりしないでください。

次の行為は絶対にしないでください。

- **___ 水に投げ込む、あるいは浸す**
- **___ 100℃ (華氏 212 度) を超える過熱**
- **___ 修理または分解**

IBM 承認の部品のみと交換してください。 バッテリーのリサイクルまたは廃棄については、地方自治体の条例に従ってください。 米国では、IBM がこのバッテリーの回収プロセスを設けています。 詳しくは、1-800-426-4333 にお問い合わせください。 お問い合わせの前に、このバッテリー・ユニットの IBM 部品番号をご用意ください。 (C003)

NEBS (Network Equipment-Building System) GR-1089-CORE の電源および配線の情報

以下のコメントは、NEBS (Network Equipment-Building System) GR-1089-CORE 準拠として指定された IBM サーバーに適用されます。

装置は、以下での設置に適しています。

- ネットワーク通信設備
- NEC (National Electrical Code) が適用される場所

この装置のイントラビルディング・ポートは、イントラビルディングまたは屋外に露出していない配線またはケーブル接続にのみ適しています。 この装置のイントラビルディング・ポートを OSP (屋外施設) やその配線に接続されているインターフェースの金属部と接続しないでください。 これらのインターフェース

は、イントラビルディング・インターフェース (GR-1089-CORE 記載のタイプ 2 ポートまたはタイプ 4 ポート) としてのみ使用するように設計されており、屋外に露出した OSP 配線とは分離する必要があります。 1 次保護装置を追加しても、これらのインターフェースと OSP 配線の金属部の接続を十分に保護することはできません。

注: すべてのイーサネット・ケーブルは、シールドされ、両端が接地されている必要があります。

AC 電源システムに、外部サージ保護装置 (SPD) を使用する必要はありません。

DC 電源システムは、分離 DC 帰還 (DC-I) 設計を採用しています。 DC バッテリー帰還端子をシャーシまたはフレーム・アースに接続しないでください。

ハードウェア管理コンソールのインストールおよび構成

HMC ハードウェアのインストール方法、その管理対象システムへの接続および使用上の構成方法について説明します。これらの作業は、お客様自身で行うこともできますが、サービス・プロバイダーに依頼することもできます。この作業に関して、サービス・プロバイダーがお客様に費用を請求させていただく場合があります。

取り付けおよび構成のタスク

HMC のさまざまな取り付けおよび構成のタスクに関連付けられたタスクについて説明します。

このセクションでは、HMC の取り付けおよび構成を行う際に実行する必要がある高水準のタスクについて説明します。さまざまな方法で HMC の取り付けおよび構成を行うことができます。実行するタスクに最適な状態を見つけてください。

注: POWER7® プロセッサー・ベースのサーバーを管理する場合、HMC はバージョン 7.7.2 以降でなければなりません。詳しくは、75 ページの『HMC マシン・コードのバージョンおよびリリースの判別』を参照してください。

新しいサーバーを用いた新規 HMC の取り付けおよび構成

新しいサーバーを用いて新規 HMC の取り付けおよび構成を行う際に実行する必要がある高水準タスクについて詳しく説明します。

表 1. 新しいサーバーを用いて新規 HMC の取り付けおよび構成を行う際に実行する必要があるタスク

作業	関連情報の入手先
1. 情報を収集し、プリインストール構成ワークシートへの記入を完了する。	19 ページの『HMC 用のプリインストール構成ワークシート』 18 ページの『HMC 構成の準備』
2. ハードウェアを開梱する。	
3. HMC ハードウェアをケーブル接続する。	26 ページの『スタンドアロン HMC の配線』 37 ページの『ラック・マウント HMC の配線』
4. 電源ボタンを押し、HMC の電源をオンにする。	
5. HMC Web アプリケーションにログインし、起動する。	
6. ガイド付きセットアップ・ウィザードにアクセスするかまたは HMC メニューを使用して、HMC を構成する。	54 ページの『ガイド付きセットアップ・ウィザードによる高速パスを使用した HMC の構成』 55 ページの『HMC メニューを使用した HMC の構成』
7. サーバーを HMC に接続する。	

HMC コードの更新およびアップグレード

ご使用の HMC コードを更新およびアップグレードする際に実行する必要がある高水準タスクについて詳しく説明します。

HMC が既に存在し、ご使用の HMC コードを更新またはアップグレードする場合は、以下の高水準タスクを実行する必要があります。

表 2. HMC コードを更新またはアップグレードする際に実行する必要があるタスク

作業	関連情報の入手先
1. アップグレードを入手する。	79 ページの『HMC ソフトウェアのアップグレード』
2. 既存の HMC マシン・コード・レベルを表示する。	
3. 管理対象システムのプロファイル・データをバックアップする。	
4. HMC データをバックアップする。	
5. 現行 HMC 構成情報を記録する。	
6. リモート・コマンドの状況を記録する。	
7. アップグレード・データを保管する。	
8. HMC ソフトウェアをアップグレードする。	
9. HMC マシン・コード・アップグレードが正常にインストールされたことを確認する。	

HMC バージョン 6 コードから HMC バージョン 7 コードへの移行

HMC バージョン 6 から HMC バージョン 7 に移行する際に実行する必要がある高水準タスクについて詳しく説明します。

HMC が既に存在し、バージョン 6 からバージョン 7 に移行する場合は、以下の高水準タスクを実行する必要があります。

表 3. HMC バージョン 6 から HMC バージョン 7 に移行する際に実行する必要があるタスク

作業	関連情報の入手先
1. ご使用の HMC ハードウェアが HMC バージョン 7 コードをサポートするか確認する。	
2. ご使用の HMC コード・レベルが 6.12 以降であるか確認する。コード・レベルが 6.12 以降でない場合は、既存の HMC コードをアップグレードする必要があります。	75 ページの『HMC マシン・コードのバージョンおよびリリースの判別』 79 ページの『HMC ソフトウェアのアップグレード』
3. ご使用の HMC をバージョン 7 にアップグレードする。	79 ページの『HMC ソフトウェアのアップグレード』
4. オプション: 管理対象システムのファームウェア・レベルを使用可能な最も高いレベルにアップグレードする。	2
5. 2 番目の HMC がある場合は、その HMC に対してステップ 1 から 4 を実行する。	

既存の取り付け環境への 2 番目の HMC の追加

管理対象システムに 2 番目の HMC を追加する際に実行する必要がある高水準タスクについて詳しく説明します。

HMC および管理対象システムが既に存在し、2 番目の HMC をこの構成に追加する場合は、次のようにします。

表 4. 2 番目の HMC を既存のインストール・システムに追加する際に実行する必要があるタスク

作業	関連情報の入手先
1. ご使用の HMC ハードウェアが HMC バージョン 7 コードをサポートするか確認する。	
2. 情報を収集し、プリインストール構成ワークシートへの記入を完了する。	19 ページの『HMC 用のプリインストール構成ワークシート』
3. ハードウェアを開梱する。	
4. HMC ハードウェアをケーブル接続する。	26 ページの『スタンドアロン HMC の配線』 37 ページの『ラック・マウント HMC の配線』
5. 電源ボタンを押し、HMC の電源をオンにする。	
6. HMC にログインする。	
7. 各 HMC コードのレベルが一致する必要があります。1 つの HMC のコードを変更して、他の HMC のコードと一致させます。	75 ページの『HMC マシン・コードのバージョンおよびリリースの判別』 79 ページの『HMC ソフトウェアのアップグレード』
8. ガイド付きセットアップ・ウィザードにアクセスするかまたは HMC メニューを使用して、HMC を構成する。	55 ページの『HMC メニューを使用した HMC の構成』
9. コール・ホーム・セットアップ・ウィザードを使用して、この HMC をサービス用に構成する。	66 ページの『HMC を構成してサービスおよびサポートに連絡できるようにする方法』
10. サーバーを HMC に接続する。	

HMC ネットワーク接続

いくつかのタイプのネットワーク接続を使用して、ご使用の HMC を管理対象システムに接続することができます。 HMC をネットワークに接続できるように構成する方法の詳細については、 54 ページの『HMC の構成』を参照してください。ネットワーク上での HMC の使用について詳しくは、以下をお読みください。

HMC ネットワーク接続のタイプ

ここでは、ネットワークを使用しての HMC リモート管理およびサービス機能の使用方法について説明します。

HMC は、以下のタイプの論理通信をサポートします。

HMC から管理対象システムへ

このタイプの通信は、大部分のハードウェア管理機能を実行するために使用されます。HMC は、管理対象システムのサービス・プロセッサーを介してコントロール機能要求を出します。 HMC とサービス・プロセッサーとの間の接続は、サービス・ネットワーク と呼ばれる場合があります。この接続は、管理対象システムの管理に必要とされます。

HMC から論理区画へ

このタイプの通信は、論理区画で稼働中のオペレーティング・システムからプラットフォーム関連の情報 (ハードウェア・エラー・イベント、ハードウェア・インベントリー) を収集したり、特定のプラットフォーム活動 (動的 LPAR、並行修理) をそれらのオペレーティング・システム間で調整したりするのに使用されます。サービス・フィーチャーおよびエラー通知フィーチャーを使用したい場合には、この接続を作成する必要があります。

HMC からリモート・ユーザーへ

このタイプの通信は、リモート・ユーザーが HMC 機能にアクセスできるようにします。リモート・ユーザーは、以下のようにして HMC にアクセスすることができます。

- SSH (Secure Socket Shell) を使用して、リモートで HMC コマンド行機能にアクセスする。

HMC からサービス・プロバイダーへ

このタイプの通信は、サービス・プロバイダーとの間で、ハードウェア・エラー報告、インベントリー・データ、およびマイクロコード更新などのデータを送受信するために使用されます。この通信パスを使用して、自動サービス呼び出しを行うことができます。

HMC は、モデルに応じて最大 4 つの独立した物理イーサネット・インターフェースをサポートします。スタンドアロン・バージョンの HMC では、1 つの内蔵イーサネット・アダプターおよび最大 2 つのプラグイン・アダプターを使用して、3 つの HMC インターフェースのみをサポートします。これらのインターフェースをそれぞれ、以下のように使用してください。

- サービス・プロセッサーへのネットワーク・インターフェースは SSL (Secure Sockets Layer) プロトコルで暗号化されており、パスワードで保護されていますが、別の専用ネットワークがあれば、これらのインターフェースに対して、より高水準のセキュリティーを提供することができます。
- HMC と論理区画間の通信では、オープン・ネットワーク・インターフェースが、HMC と管理対象システム上の論理区画の間でのネットワーク接続に通常使用されます。このオープン・ネットワーク・インターフェースを使用して、HMC をリモートで管理することもできます。
- オプションで、3 番目のインターフェースを使用して、論理区画に接続し、HMC をリモートで管理することができます。この 3 番目のインターフェースは、異なるグループの論理区画に別の HMC 接続を持たせるためにも使用することができます。例えば、すべての通常のビジネス・トランザクションを実行している LAN とは別の管理 LAN を持つこともできます。リモート管理者は、この方式を使用して、HMC および他の管理対象装置にアクセスすることもできます。場合によっては、論理区画が、おそらくはファイアウォールの背後で異なるネットワーク・セキュリティー・ドメイン内にあることがあり、これら 2 つのドメインのそれぞれに対して異なる HMC ネットワーク接続を持つこともできます。

HMC の Web ブラウザー要件

ハードウェア管理コンソール (HMC) は、Microsoft Internet Explorer (IE) バージョン 6.0 および 7.0、Firefox バージョン 1.5.0.7 および 2.0 でサポートされます。

ご使用のブラウザーがインターネット・プロキシーを使用するように構成されている場合は、例外リストにローカル IP アドレスを指定する必要があります。例外リストについての詳細は、ネットワーク管理者にお問い合わせください。プロキシーを使用して HMC にアクセスする必要がある場合は、「インターネットオプション」ウィンドウの「詳細設定」タブで「プロキシ接続で HTTP 1.1 を使用する」を有効にしてください。

注: Firefox バージョン 2.0 の場合は、JavaScript オプションの「ウィンドウのフォーカス (前面か背面か) を切り替える」および「ウィンドウの移動または大きさの変更」を有効にしてください。この機能により、HMC タスクを容易に切り替えることができます。 Javascript オプションを有効にするには、以下の手順を実行します。

1. 「ツール」を選択して、「オプション」をクリックします。
2. 「コンテンツ」を選択して、「詳細設定」をクリックします。
3. 「ウィンドウの移動または大きさの変更」および「ウィンドウのフォーカス (前面か背面か) を切り替える」を選択します。
4. 「OK」をクリックします。

HMC にリモート接続されている場合に ASMI が作動するように、セッション Cookie を有効にする必要があります。 ASM のプロキシー・コードは、セッション情報を保管して使用します。セッション Cookie を有効にするには、以下の手順に従います。

Internet Explorer の場合は、以下のようにして、セッション Cookie を有効にします。

1. 「ツール」を選択して、「インターネット オプション」をクリックします。
2. 「プライバシー」を選択して、「詳細設定」をクリックします。
3. 「常にセッション Cookie を許可する」にチェック・マークが付いていることを確認します。チェック・マークが付いていない場合は、「自動 Cookie 処理を上書きする」と「常にセッション Cookie を許可する」を選択します。
4. 「ファースト パーティの Cookie」および「サード パーティの Cookie」で「ダイアログを表示する」を選択します。
5. 「OK」をクリックします。

Firefox の場合は、以下のようにして、セッション Cookie を有効にします。

1. 「ツール」を選択して、「オプション」をクリックします。
2. 「Cookie」をクリックします。
3. 「サイトから送られてきた Cookie を保存する (Allow sites to set cookies)」を選択します。
4. 「例外サイト」を選択して、HMC を追加します。
5. 「OK」をクリックします。

HMC 環境でのプライベート・ネットワークおよびオープン・ネットワーク:

HMC は、オープン・ネットワークおよびプライベート・ネットワークを使用するように構成できます。プライベート・ネットワークを使用すると、ルーティング不能な IP アドレスの範囲を指定して使用できるようになります。パブリック ・ネットワークまたは「オープン」ネットワークとは、全論理区画に対する HMC と、お客様が通常使用するネットワークにある他システムとの間のネットワーク接続を表しています。

プライベート・ネットワーク

HMC プライベート・ネットワーク上にある装置は、HMC 自身と、その HMC の接続先の各管理対象システムのみです。HMC は、各管理対象システムの FSP (Flexible Service Processor) に接続されます。

大部分のシステム上では、この FSP は 2 つのイーサネット・ポート (**HMC1** および **HMC2** のラベルが付いている) を装備しています。これを使用して最大 2 つの HMC に接続可能となります。

一部のシステムには、デュアル FSP オプションがあります。この状態の場合、2 番目の FSP は「冗長」バックアップとして機能します。2 つの FSP を搭載したシステムに対する基本的なセットアップ要件は、2 番目の FSP がない場合の要件と本質的には同じです。HMC は各 FSP に接続する必要があります。このため、複数の FSP がある場合、または複数の管理対象システムがある場合は、追加のネットワーク・ハードウェア (例えば、LAN スイッチまたはハブ) が必要になります。

注: 管理対象システム上の各 FSP ポートは、1 台の HMC にのみ接続する必要があります。

パブリック・ネットワーク

オープン・ネットワークは、インターネットに接続するためにファイアウォールまたはルーターに接続することができます。インターネットへの接続により、報告が必要となるすべてのハードウェア・エラー発生時に、HMC が「コール・ホーム」することが可能となります。

HMC 自身は、自分自身のファイアウォールをその各ネットワーク・インターフェース上で提供します。「HMC ガイド付きセットアップ・ウィザード」の実行時に基本的なファイアウォールが自動的に構成されますが、初期の HMC インストールと構成の完了後にファイアウォール設定をカスタマイズする必要があります。

DHCP サーバーとしての HMC:

HMC を動的ホスト構成プロトコル (DHCP) サーバーとして使用することができます。

注: IPv6 を使用している場合、ディスカバリー・プロセスは手動で行う必要があります。 IPv6 では自動ディスカバリーはありません。

コール・ホーム・サーバーに使用する接続方式の決定

コール・ホーム・サーバーの使用時に適用できる接続オプションについて説明します。

HMC を構成して、ハードウェア保守関連情報を IBM に送信することができます。これを行うには、LAN ベースのインターネット接続またはモデム経由のダイヤルアップ接続を使用します。

LAN ベースのインターネット接続を構成する場合、2 つの通信上の選択肢があります。最初の選択肢は、標準 SSL (Secure Sockets Layer) の使用です。SSL 通信を使用すれば、お客様のプロキシー・サーバー経由でインターネットに接続できます。SSL 接続を使用すると、企業のセキュリティー・ガイドラインに準拠できる可能性が一層高くなります。2 番目の選択肢は VPN 接続の使用です。

注: ご使用のオープン・ネットワーク・インターフェース接続で、インターネット・プロトコル・バージョン 6 (IPv6) のみが使用されている場合、インターネット VPN を使用してサポートに接続することはできません。使用されるプロトコルの詳細については、8 ページの『インターネット・プロトコルの選択』を参照してください。

インターネット接続を使用した場合のメリットは、以下のとおりです。

- 非常に高速な伝送速度
- お客様のコスト負担の軽減 (例えば、専用のアナログ電話回線のコストに対して)
- 一層高い信頼性

選択した接続方式に関係なく、以下のセキュリティー上の特性が有効となります。

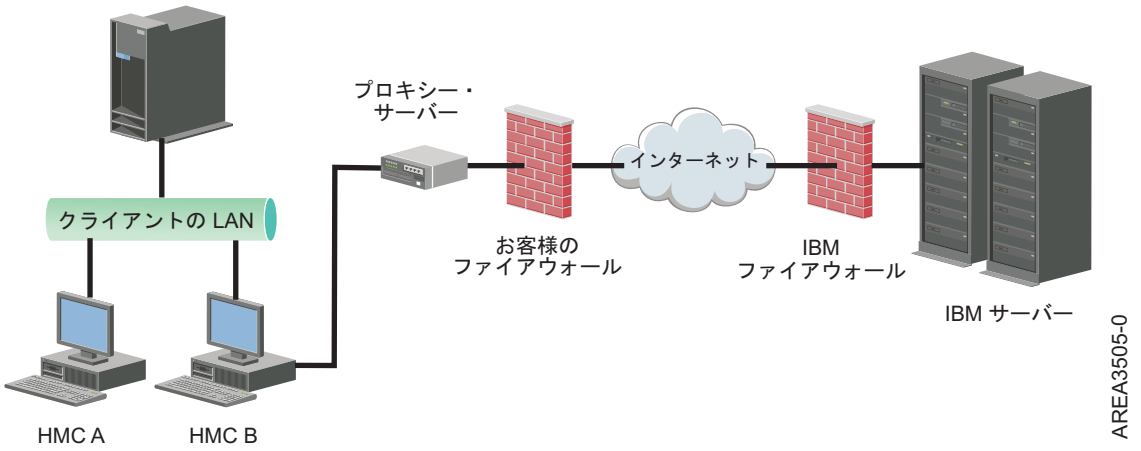
- リモート・サポート機能の要求は、常に、HMC から開始されて IBM に送信されます。インバウンド接続が、IBM Service Support System から開始されることは決してありません。
- HMC と IBM Service Support System 間で転送される全データは、高度な暗号化機能を使用して暗号化されています。選択した接続方式に応じて、SSL または IPSec Encapsulating Security Payload (ESP) のいずれかを使用して暗号化されます。
- 暗号化された接続の開始時に、HMC はターゲットとなる宛先を IBM Service Support System の宛先として認証します。

IBM Service Support System に送信されるデータには、単にハードウェア障害および構成に関する情報が入っているだけです。アプリケーションまたはお客様データは、IBM には伝送されません。

プロキシー・サーバー経由での間接インターネット接続の使用

お客様のインストール環境で、HMC をプライベート・ネットワーク上で使用する必要がある場合、SSL プロキシーを使用してインターネットに間接的に接続することもできます。これにより、各要求をインターネットにフォワードすることができます。SSL プロキシーを使用した場合に考えられる他の利点の 1 つとしては、プロキシーによりロギングと監査の機能がサポートされることです。

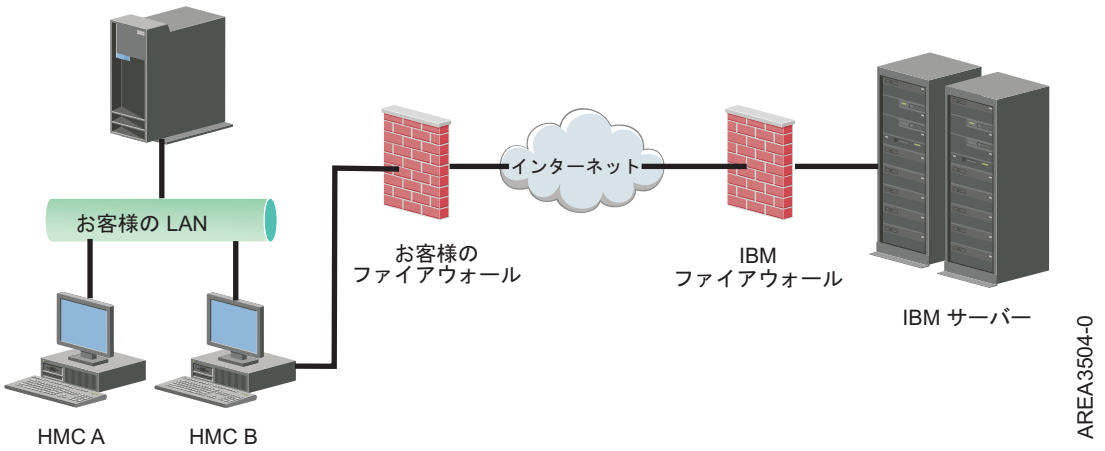
SSL ソケットをフォワードするには、そのプロキシー・サーバーは基本プロキシー・ヘッダー機能 (RFC 2616 に記載あり) と CONNECT メソッドをサポートする必要があります。オプションとして、基本プロキシー認証 (RFC 2617) を、プロキシー・サーバー経由でソケットを転送しようとする前に HMC が認証するように構成することができます。



HMC が通信を正常に行うためには、そのクライアントのプロキシー・サーバーはポート 443 に接続可能でなければなりません。プロキシー・サーバーを構成して、HMC が接続可能な IP アドレスを特定のものに限定することができます。IP アドレス・リストは、 8 ページの『インターネット SSL アドレス・リスト』 を参照してください。

直接のインターネット SSL 接続の使用

HMC をインターネットに接続可能な場合で、かつ、外部ファイアウォールをセットアップして、確立された TCP パケットが 8 ページの『インターネット SSL アドレス・リスト』に記載された宛先に向けてアウトバウンドに伝送できる場合、直接的なインターネット接続を使用できます。



インターネット SSL を使用してリモート・サポートに接続する方法

すべての通信は、HMC により開始された TCP ソケットを通じて処理され、高度な SSL を使用して伝送データを暗号化します。宛先 TCP/IP アドレスは公開されています (『インターネット SSL アドレス・リスト』参照)。それによって、これらの接続を許可するように外部ファイアウォールを構成します。

注: 標準 HTTPS ポート 443 は、すべての通信に対して使用されます。

HMC は、インターネットに直接接続するか、またはお客様提供のプロキシー・サーバーから間接的に接続するように対応可能です。どちらの方式がお客様のシステム環境に最適であるかは、お客様のセキュリティー要件とネットワーキング要件により異なります。HMC は、インターネット SSL 接続を使用するように構成されている場合、 (直接または SSL プロキシー経由で) 以下のアドレスを使用します。

インターネット・プロトコルの選択

HMC がサービス・プロバイダーに接続する際に使用される IP アドレスのバージョンを決定します。

ほとんどのユーザーは、インターネット・プロトコル・バージョン 4 (IPv4) を使用してサービス・プロバイダーに接続します。 IPv4 アドレスは、IPv4 アドレスの 4 つのバイトをピリオドで区切った形式 (例えば、9.60.12.123) で表わされ、インターネットへのアクセスに使用されます。サービス・プロバイダーに接続するには、インターネット・プロトコル・バージョン 6 (IPv6) を使用することもできます。 IPv6 は、固有のアドレス・スペースを確保するために、ネットワーク管理者がよく使用します。ご使用のシステムで使用されているインターネット・プロトコルが不明である場合は、ネットワーク管理者に問い合わせてください。各バージョンの使用について詳しくは、 61 ページの『IPv4 アドレスの設定』および 61 ページの『IPv6 アドレスの設定』を参照してください。

インターネット SSL アドレス・リスト

インターネット SSL 接続を使用する場合に HMC が使用するアドレスについて説明します。

HMC は、インターネット SSL 接続を使用するように構成されると、IBM サービスおよびサポートとの接続に以下の IPv4 アドレスを使用します。

以下の IPv4 アドレスは、すべての国と地域で使用されます。

- 129.42.26.224
- 129.42.34.224
- 129.42.42.224
- 170.225.15.41
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216

以下の IPv4 アドレスはアメリカ合衆国の場合に使用されます。

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

以下の IPv4 アドレスは、アメリカ合衆国以外のすべての国と地域で使用されます。

- 129.42.160.48

- 129.42.160.50
- 207.25.252.200
- 207.25.252.205

注: ファイアウォールを構成して HMC がこれらのサーバーに接続できるようにする場合、地理的な地域固有の IP アドレスだけが必要となります。

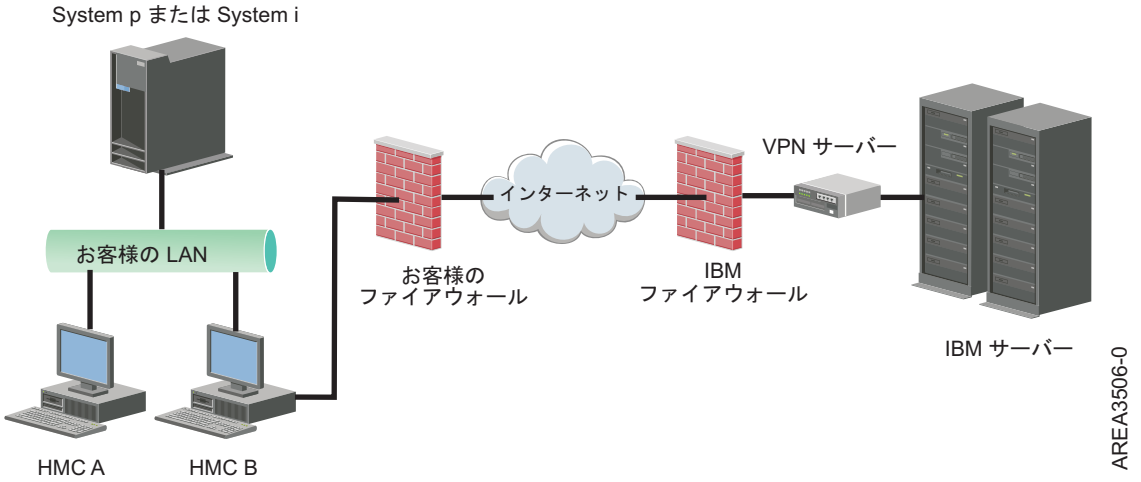
HMC は、インターネット SSL 接続を使用するように構成されると、IBM サービスおよびサポートとの接続に以下の IPv6 アドレスを使用します。

- 2620:0:6C0:1::1000
- 2620:0:6C1:1::1000
- 2620:0:6C2:1::1000

仮想プライベート・ネットワークを使用してリモート・サポートに接続する方法

仮想プライベート・ネットワーク (VPN) は、リモート・サポートへの接続時にセキュリティーを提供します。

VPN は、従来のプライベート・ネットワークによる物理的に分離されたネットワーク回線の代わりに、暗号化などのセキュリティー手段を使用することによって、分離されたネットワークのプライバシーを公衆回線上でユーザーに提供します。 VPN 接続は、アウトバウンド接続用に使用可能であることに加えて、必要に応じてリモート・サービス要求をサポートするように構成可能です。



インターネット接続を提供することは、システム管理者の責任です。このファイアウォールもまた、HMC が接続可能な特定 IP アドレスを限定することもできます。ファイアウォールが IP アドレスを限定するように構成する必要がある場合は、使用可能なアドレス・リストについては、『VPN サーバー・アドレス・リスト』を参照してください。

LAN ベースの VPN を使用してインターネットに接続する方法の詳細は、 56 ページの『HMC ネットワーク・タイプの構成』を参照してください。

VPN サーバー・アドレス・リスト

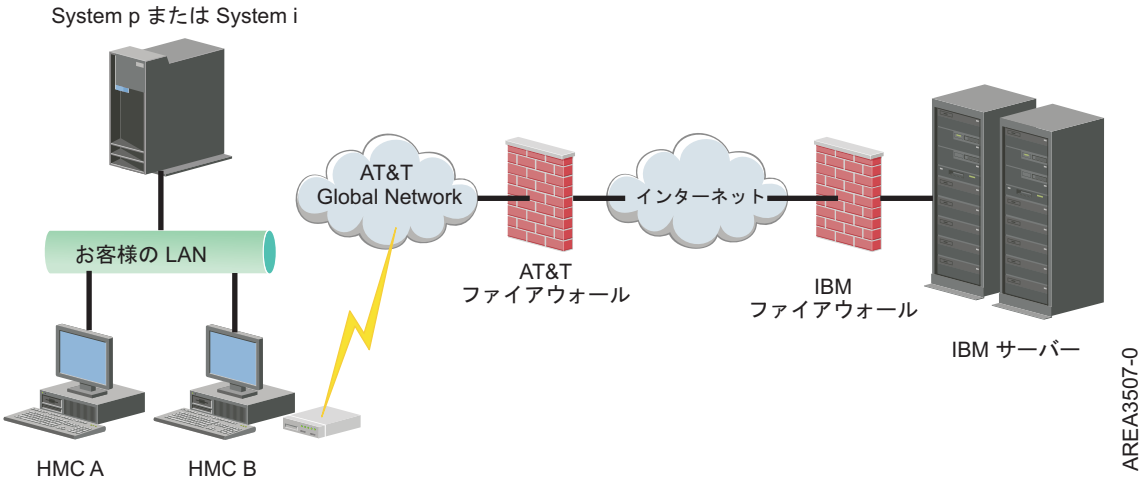
インターネット VPN 接続を使うように HMC を構成する場合、HMC が使用するサーバーをリストします。

インターネット VPN 接続を使うように HMC を構成すると、HMC は以下のサーバーを使用します。ネットワーク・アドレス変換 (NAT) ファイアウォールを使おうとする時に、すべての接続が ESP、およびポート 500 とポート 4500 上の UDP を使用します。

- 129.42.160.16 IBM VPN サーバー
- 207.25.252.196 IBM VPN サーバー

電話とモデムを使用してリモート・サポートに接続する方法

モデムを使用してリモート・サポートに接続したい場合は、専用のアナログ回線を使用して HMC モデムに接続する必要があります。 HMC はこのモデムを使用して、Global Network にダイヤルし、IBM サービスおよびサポートに接続します。



電話とモデムを使用してリモート・サポートに接続する方法の詳細は、 56 ページの『HMC ネットワーク・タイプの構成』を参照してください。

複数のコール・ホーム・サーバーの使用

このトピックでは、複数のコール・ホーム・サーバーの使用を決定した場合に知る必要のある事項を説明します。

Single Point of Failure を防ぐには、HMC を構成し、複数のコール・ホーム・サーバーを使用するようにします。最初に使用可能なコール・ホーム・サーバーが、各サービス・イベントの対処を試行します。このコール・ホーム・サーバーで接続または伝送の障害が起こった場合、他のコール・ホーム・サーバーのいずれかがサービス要求を正常に再試行するまで、またはすべてのコール・ホーム・サーバーが試行するまで、サービス要求が再試行されます。

当該管理対象システムの 1 次分析コンソールであると問題分析で識別された、接続済みの HMC が問題を報告します。この 1 次コンソールは、2 次 HMC がある場合はその HMC に問題報告書のレプリカを生成します。この 2 次 HMC は、ネットワーク上で 1 次 HMC によって認識されている必要があります。2 次 HMC が追加のコール・ホーム・サーバーとして 1 次 HMC に認識されるのは、以下の場合です。

- 1 次 HMC が「検出済みの」コール・ホーム・サーバーを使用するように構成されており、そのコール・ホーム・サーバーが 1 次 HMC と同じサブネット上にあるか、または同じシステムを管理しているか、いずれかの場合。

- コール・ホーム・サーバーが、アウトバウンド接続に使用可能なコール・ホーム・サーバー・コンソールのリストに手動で追加済みである場合。

HMC に関するネットワーク設定の選択

HMC 上で使用可能なネットワーク設定について説明します。

HMC ネットワーク接続

いくつかのタイプのネットワーク接続を使用して、ご使用の HMC を管理対象システムに接続することができます。 HMC をネットワークに接続できるように構成する方法の詳細については、 54 ページの『HMC の構成』を参照してください。ネットワーク上での HMC の使用について詳しくは、以下をお読みください。

HMC ネットワーク接続のタイプ

ここでは、ネットワークを使用しての HMC リモート管理およびサービス機能の使用方法について説明します。

HMC は、以下のタイプの論理通信をサポートします。

HMC から管理対象システムへ

このタイプの通信は、大部分のハードウェア管理機能を実行するために使用されます。HMC は、管理対象システムのサービス・プロセッサーを介してコントロール機能要求を出します。 HMC とサービス・プロセッサーとの間の接続は、サービス・ネットワーク と呼ばれる場合があります。この接続は、管理対象システムの管理に必要とされます。

HMC から論理区画へ

このタイプの通信は、論理区画で稼働中のオペレーティング・システムからプラットフォーム関連の情報 (ハードウェア・エラー・イベント、ハードウェア・インベントリー) を収集したり、特定のプラットフォーム活動 (動的 LPAR、並行修理) をそれらのオペレーティング・システム間で調整したりするのに使用されます。サービス・フィーチャーおよびエラー通知フィーチャーを使用したい場合には、この接続を作成する必要があります。

HMC からリモート・ユーザーへ

このタイプの通信は、リモート・ユーザーが HMC 機能にアクセスできるようにします。リモート・ユーザーは、以下のようにして HMC にアクセスすることができます。

- SSH (Secure Socket Shell) を使用して、リモートで HMC コマンド行機能にアクセスする。

HMC からサービス・プロバイダーへ

このタイプの通信は、サービス・プロバイダーとの間で、ハードウェア・エラー報告、インベントリー・データ、およびマイクロコード更新などのデータを送受信するために使用されます。この通信パスを使用して、自動サービス呼び出しを行うことができます。

HMC は、モデルに応じて最大 4 つの独立した物理イーサネット・インターフェースをサポートします。スタンドアロン・バージョンの HMC では、1 つの内蔵イーサネット・アダプターおよび最大 2 つのプラグイン・アダプターを使用して、3 つの HMC インターフェースのみをサポートします。これらのインターフェースをそれぞれ、以下のように使用してください。

- サービス・プロセッサーへのネットワーク・インターフェースは SSL (Secure Sockets Layer) プロトコルで暗号化されており、パスワードで保護されていますが、別の専用ネットワークがあれば、これらのインターフェースに対して、より高水準のセキュリティーを提供することができます。

- HMC と論理区画間の通信では、オープン・ネットワーク・インターフェースが、HMC と管理対象システム上の論理区画の間でのネットワーク接続に通常使用されます。このオープン・ネットワーク・インターフェースを使用して、HMC をリモートで管理することもできます。
- オプションで、3 番目のインターフェースを使用して、論理区画に接続し、HMC をリモートで管理することができます。この 3 番目のインターフェースは、異なるグループの論理区画に別の HMC 接続を持たせるためにも使用することができます。例えば、すべての通常のビジネス・トランザクションを実行している LAN とは別の管理 LAN を持つこともできます。リモート管理者は、この方式を使用して、HMC および他の管理対象装置にアクセスすることもできます。場合によっては、論理区画が、おそらくはファイアウォールの背後で異なるネットワーク・セキュリティー・ドメイン内にあることがあり、これら 2 つのドメインのそれぞれに対して異なる HMC ネットワーク接続を持つこともできます。

HMC の Web ブラウザー要件

ハードウェア管理コンソール (HMC) は、Microsoft Internet Explorer (IE) バージョン 6.0 および 7.0、Firefox バージョン 1.5.0.7 および 2.0 でサポートされます。

ご使用のブラウザーがインターネット・プロキシーを使用するように構成されている場合は、例外リストにローカル IP アドレスを指定する必要があります。例外リストについての詳細は、ネットワーク管理者にお問い合わせください。プロキシーを使用して HMC にアクセスする必要がある場合は、「インターネットオプション」ウィンドウの「詳細設定」タブで「プロキシ接続で HTTP 1.1 を使用する」を有効にしてください。

注: Firefox バージョン 2.0 の場合は、JavaScript オプションの「ウィンドウのフォーカス (前面か背面か) を切り替える」および「ウィンドウの移動または大きさの変更」を有効にしてください。この機能により、HMC タスクを容易に切り替えることができます。 Javascript オプションを有効にするには、以下の手順を実行します。

1. 「ツール」を選択して、「オプション」をクリックします。
2. 「コンテンツ」を選択して、「詳細設定」をクリックします。
3. 「ウィンドウの移動または大きさの変更」および「ウィンドウのフォーカス (前面か背面か) を切り替える」を選択します。
4. 「OK」をクリックします。

HMC にリモート接続されている場合に ASMI が作動するように、セッション Cookie を有効にする必要があります。 ASM のプロキシー・コードは、セッション情報を保管して使用します。セッション Cookie を有効にするには、以下の手順に従います。

Internet Explorer の場合は、以下のようにして、セッション Cookie を有効にします。

1. 「ツール」を選択して、「インターネット オプション」をクリックします。
2. 「プライバシー」を選択して、「詳細設定」をクリックします。
3. 「常にセッション Cookie を許可する」にチェック・マークが付いていることを確認します。チェック・マークが付いていない場合は、「自動 Cookie 処理を上書きする」と「常にセッション Cookie を許可する」を選択します。
4. 「ファースト パーティの Cookie」および「サード パーティの Cookie」で「ダイアログを表示する」を選択します。
5. 「OK」をクリックします。

Firefox の場合は、以下のようにして、セッション Cookie を有効にします。

1. 「ツール」を選択して、「オプション」をクリックします。

2. 「Cookie」をクリックします。
3. 「サイトから送られてきた Cookie を保存する (Allow sites to set cookies)」を選択します。
4. 「例外サイト」を選択して、HMC を追加します。
5. 「OK」をクリックします。

HMC 環境でのプライベート・ネットワークおよびオープン・ネットワーク:

HMC は、オープン・ネットワークおよびプライベート・ネットワークを使用するように構成できます。プライベート・ネットワークを使用すると、ルーティング不能な IP アドレスの範囲を指定して使用できるようになります。パブリック ・ネットワークまたは「オープン」ネットワークとは、全論理区画に対する HMC と、お客様が通常使用するネットワークにある他システムとの間のネットワーク接続を表しています。

プライベート・ネットワーク

HMC プライベート・ネットワーク上にある装置は、HMC 自身と、その HMC の接続先の各管理対象システムのみです。HMC は、各管理対象システムの FSP (Flexible Service Processor) に接続されます。

大部分のシステム上では、この FSP は 2 つのイーサネット・ポート (**HMC1** および **HMC2** のラベルが付いている) を装備しています。これを使用して最大 2 つの HMC に接続可能となります。

一部のシステムには、デュアル FSP オプションがあります。この状態の場合、2 番目の FSP は「冗長」バックアップとして機能します。2 つの FSP を搭載したシステムに対する基本的なセットアップ要件は、2 番目の FSP がない場合の要件と本質的には同じです。HMC は各 FSP に接続する必要があります。このため、複数の FSP がある場合、または複数の管理対象システムがある場合は、追加のネットワーク・ハードウェア (例えば、LAN スイッチまたはハブ) が必要になります。

注: 管理対象システム上の各 FSP ポートは、1 台の HMC にのみ接続する必要があります。

パブリック・ネットワーク

オープン・ネットワークは、インターネットに接続するためにファイアウォールまたはルーターに接続することができます。インターネットへの接続により、報告が必要となるすべてのハードウェア・エラー発生時に、HMC が「コール・ホーム」することが可能となります。

HMC 自身は、自分自身のファイアウォールをその各ネットワーク・インターフェース上で提供します。「HMC ガイド付きセットアップ・ウィザード」の実行時に基本的なファイアウォールが自動的に構成されますが、初期の HMC インストールと構成の完了後にファイアウォール設定をカスタマイズする必要があります。

DHCP サーバーとしての HMC:

HMC を動的ホスト構成プロトコル (DHCP) サーバーとして使用することができます。

注: IPv6 を使用している場合、ディスカバリー・プロセスは手動で行う必要があります。 IPv6 では自動ディスカバリーはありません。

コール・ホーム・サーバーに使用する接続方式の決定

コール・ホーム・サーバーの使用時に適用できる接続オプションについて説明します。

HMC を構成して、ハードウェア保守関連情報を IBM に送信することができます。これを行うには、LAN ベースのインターネット接続またはモデム経由のダイヤルアップ接続を使用します。

LAN ベースのインターネット接続を構成する場合、2 つの通信上の選択肢があります。最初の選択肢は、標準 SSL (Secure Sockets Layer) の使用です。SSL 通信を使用すれば、お客様のプロキシー・サーバー経由でインターネットに接続できます。SSL 接続を使用すると、企業のセキュリティー・ガイドラインに準拠できる可能性が一層高くなります。2 番目の選択肢は VPN 接続の使用です。

注: ご使用のオープン・ネットワーク・インターフェース接続で、インターネット・プロトコル・バージョン 6 (IPv6) のみが使用されている場合、インターネット VPN を使用してサポートに接続することはできません。使用されるプロトコルの詳細については、8 ページの『インターネット・プロトコルの選択』を参照してください。

インターネット接続を使用した場合のメリットは、以下のとおりです。

- 非常に高速な伝送速度
- お客様のコスト負担の軽減 (例えば、専用のアナログ電話回線のコストに対して)
- 一層高い信頼性

選択した接続方式に関係なく、以下のセキュリティー上の特性が有効となります。

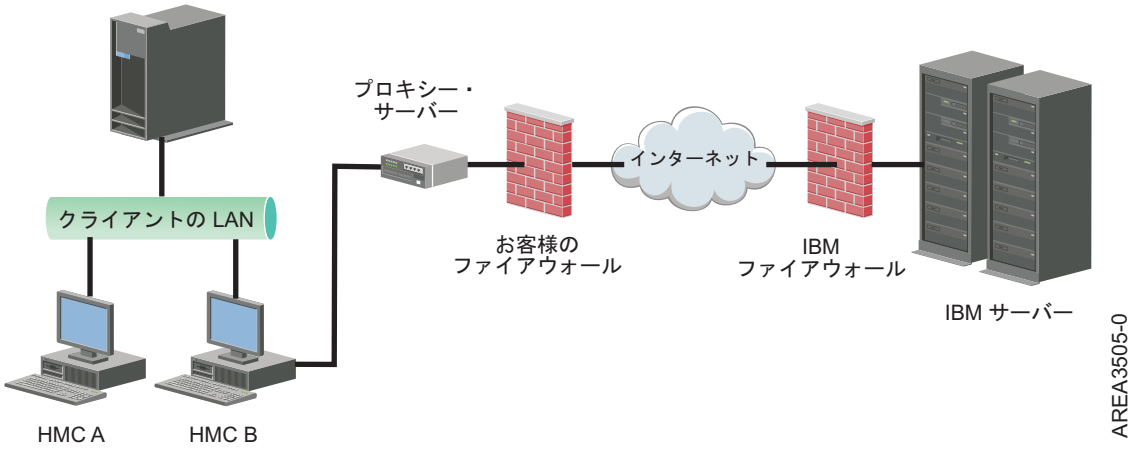
- リモート・サポート機能の要求は、常に、HMC から開始されて IBM に送信されます。インバウンド接続が、IBM Service Support System から開始されることは決してありません。
- HMC と IBM Service Support System 間で転送される全データは、高度な暗号化機能を使用して暗号化されています。選択した接続方式に応じて、SSL または IPSec Encapsulating Security Payload (ESP) のいずれかを使用して暗号化されます。
- 暗号化された接続の開始時に、HMC はターゲットとなる宛先を IBM Service Support System の宛先として認証します。

IBM Service Support System に送信されるデータには、単にハードウェア障害および構成に関する情報が入っているだけです。アプリケーションまたはお客様データは、IBM には伝送されません。

プロキシー・サーバー経由での間接インターネット接続の使用

お客様のインストール環境で、HMC をプライベート・ネットワーク上で使用する必要がある場合、SSL プロキシーを使用してインターネットに間接的に接続することもできます。これにより、各要求をインターネットにフォワードすることができます。SSL プロキシーを使用した場合に考えられる他の利点の 1 つとしては、プロキシーによりロギングと監査の機能がサポートされることです。

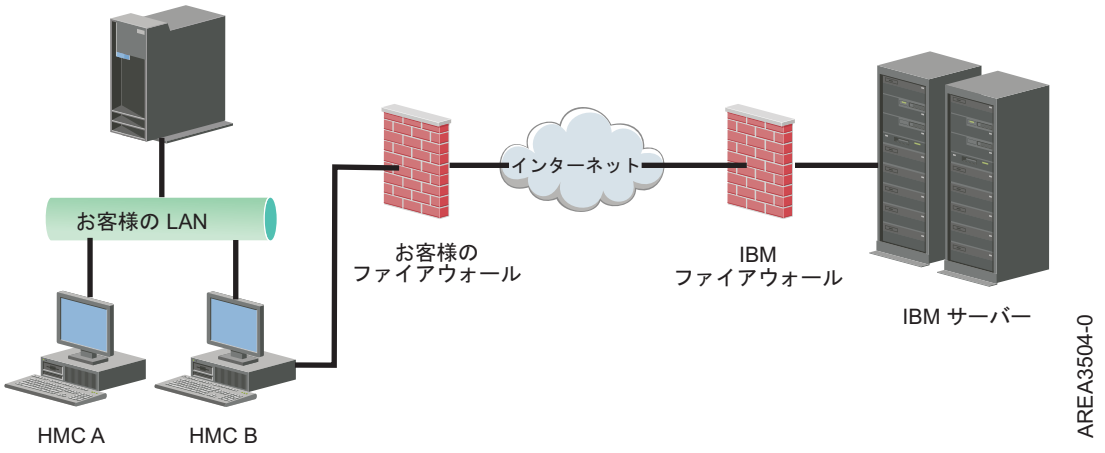
SSL ソケットをフォワードするには、そのプロキシー・サーバーは基本プロキシー・ヘッダー機能 (RFC 2616 に記載あり) と CONNECT メソッドをサポートする必要があります。オプションとして、基本プロキシー認証 (RFC 2617) を、プロキシー・サーバー経由でソケットを転送しようとする前に HMC が認証するように構成することができます。



HMC が通信を正常に行うためには、そのクライアントのプロキシー・サーバーはポート 443 に接続可能でなければなりません。プロキシー・サーバーを構成して、HMC が接続可能な IP アドレスを特定のものに限定することができます。IP アドレス・リストは、 8 ページの『インターネット SSL アドレス・リスト』 を参照してください。

直接のインターネット SSL 接続の使用

HMC をインターネットに接続可能な場合で、かつ、外部ファイアウォールをセットアップして、確立された TCP パケットが 8 ページの『インターネット SSL アドレス・リスト』に記載された宛先に向けてアウトバウンドに伝送できる場合、直接的なインターネット接続を使用できます。



インターネット SSL を使用してリモート・サポートに接続する方法

すべての通信は、HMC により開始された TCP ソケットを通じて処理され、高度な SSL を使用して伝送データを暗号化します。宛先 TCP/IP アドレスは公開されています (8 ページの『インターネット SSL アドレス・リスト』参照)。それによって、これらの接続を許可するように外部ファイアウォールを構成します。

注: 標準 HTTPS ポート 443 は、すべての通信に対して使用されます。

HMC は、インターネットに直接接続するか、またはお客様提供のプロキシー・サーバーから間接的に接続するように対応可能です。どちらの方式がお客様のシステム環境に最適であるかは、お客様のセキュリティー要件とネットワーキング要件により異なります。HMC は、インターネット SSL 接続を使用するように構成されている場合、 (直接または SSL プロキシー経由で) 以下のアドレスを使用します。

インターネット・プロトコルの選択

HMC がサービス・プロバイダーに接続する際に使用される IP アドレスのバージョンを決定します。

ほとんどのユーザーは、インターネット・プロトコル・バージョン 4 (IPv4) を使用してサービス・プロバイダーに接続します。 IPv4 アドレスは、IPv4 アドレスの 4 つのバイトをピリオドで区切った形式 (例えば、9.60.12.123) で表わされ、インターネットへのアクセスに使用されます。サービス・プロバイダーに接続するには、インターネット・プロトコル・バージョン 6 (IPv6) を使用することもできます。 IPv6 は、固有のアドレス・スペースを確保するために、ネットワーク管理者がよく使用します。ご使用のシステムで使用されているインターネット・プロトコルが不明である場合は、ネットワーク管理者に問い合わせてください。各バージョンの使用について詳しくは、 61 ページの『IPv4 アドレスの設定』および 61 ページの『IPv6 アドレスの設定』を参照してください。

インターネット SSL アドレス・リスト

インターネット SSL 接続を使用する場合に HMC が使用するアドレスについて説明します。

HMC は、インターネット SSL 接続を使用するように構成されると、IBM サービスおよびサポートとの接続に以下の IPv4 アドレスを使用します。

以下の IPv4 アドレスは、すべての国と地域で使用されます。

- 129.42.26.224
- 129.42.34.224
- 129.42.42.224
- 170.225.15.41
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216

以下の IPv4 アドレスはアメリカ合衆国の場合に使用されます。

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

以下の IPv4 アドレスは、アメリカ合衆国以外のすべての国と地域で使用されます。

- 129.42.160.48
- 129.42.160.50
- 207.25.252.200
- 207.25.252.205

注: ファイアウォールを構成して HMC がこれらのサーバーに接続できるようにする場合、地理的な地域固有の IP アドレスだけが必要となります。

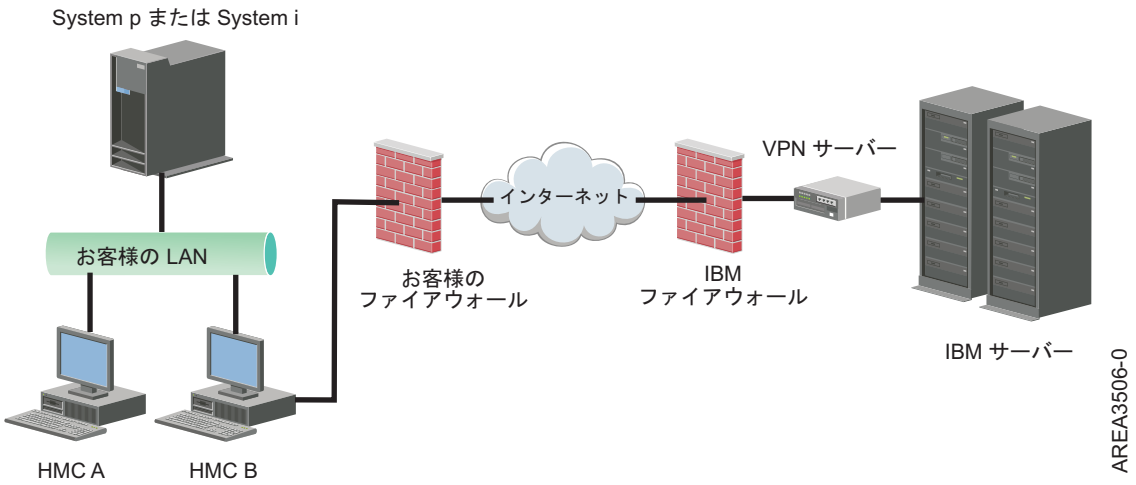
HMC は、インターネット SSL 接続を使用するように構成されると、IBM サービスおよびサポートとの接続に以下の IPv6 アドレスを使用します。

- 2620:0:6C0:1::1000
- 2620:0:6C1:1::1000
- 2620:0:6C2:1::1000

仮想プライベート・ネットワークを使用してリモート・サポートに接続する方法

仮想プライベート・ネットワーク (VPN) は、リモート・サポートへの接続時にセキュリティーを提供します。

VPN は、従来のプライベート・ネットワークによる物理的に分離されたネットワーク回線の代わりに、暗号化などのセキュリティー手段を使用することによって、分離されたネットワークのプライバシーを公衆回線上でユーザーに提供します。 VPN 接続は、アウトバウンド接続用に使用可能であることに加えて、必要に応じてリモート・サービス要求をサポートするように構成可能です。



インターネット接続を提供することは、システム管理者の責任です。このファイアウォールもまた、HMC が接続可能な特定 IP アドレスを限定することもできます。ファイアウォールが IP アドレスを限定するように構成する必要がある場合は、使用可能なアドレス・リストについては、9 ページの『VPN サーバー・アドレス・リスト』を参照してください。

LAN ベースの VPN を使用してインターネットに接続する方法の詳細は、56 ページの『HMC ネットワーク・タイプの構成』を参照してください。

VPN サーバー・アドレス・リスト

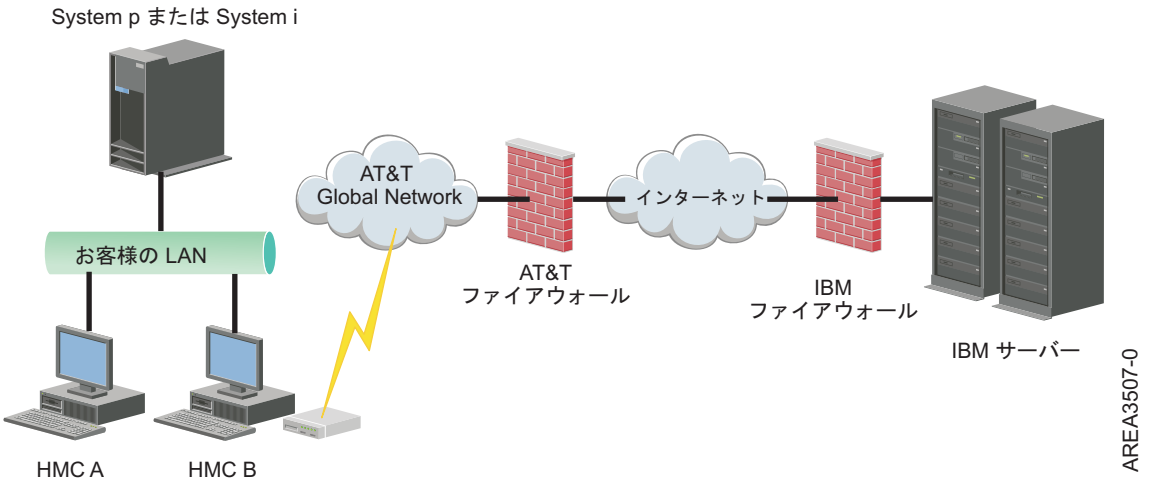
インターネット VPN 接続を使うように HMC を構成する場合、HMC が使用するサーバーをリストします。

インターネット VPN 接続を使うように HMC を構成すると、HMC は以下のサーバーを使用します。ネットワーク・アドレス変換 (NAT) ファイアウォールを使おうとする時に、すべての接続が ESP、およびポート 500 とポート 4500 上の UDP を使用します。

- 129.42.160.16 IBM VPN サーバー
- 207.25.252.196 IBM VPN サーバー

電話とモデムを使用してリモート・サポートに接続する方法

モデムを使用してリモート・サポートに接続したい場合は、専用のアナログ回線を使用して HMC モデムに接続する必要があります。 HMC はこのモデムを使用して、Global Network にダイヤルし、IBM サービスおよびサポートに接続します。



電話とモデムを使用してリモート・サポートに接続する方法の詳細は、 56 ページの『HMC ネットワーク・タイプの構成』を参照してください。

複数のコール・ホーム・サーバーの使用

このトピックでは、複数のコール・ホーム・サーバーの使用を決定した場合に知る必要のある事項を説明します。

Single Point of Failure を防ぐには、HMC を構成し、複数のコール・ホーム・サーバーを使用するようにします。最初に使用可能なコール・ホーム・サーバーが、各サービス・イベントの対処を試行します。このコール・ホーム・サーバーで接続または伝送の障害が起こった場合、他のコール・ホーム・サーバーのいずれかがサービス要求を正常に再試行するまで、またはすべてのコール・ホーム・サーバーが試行するまで、サービス要求が再試行されます。

当該管理対象システムの 1 次分析コンソールであると問題分析で識別された、接続済みの HMC が問題を報告します。この 1 次コンソールは、2 次 HMC がある場合はその HMC に問題報告書のレプリカを生成します。この 2 次 HMC は、ネットワーク上で 1 次 HMC によって認識されている必要があります。2 次 HMC が追加のコール・ホーム・サーバーとして 1 次 HMC に認識されるのは、以下の場合です。

- 1 次 HMC が「検出済みの」コール・ホーム・サーバーを使用するように構成されており、そのコール・ホーム・サーバーが 1 次 HMC と同じサブネット上にあるか、または同じシステムを管理しているか、いずれかの場合。
- コール・ホーム・サーバーが、アウトバウンド接続に使用可能なコール・ホーム・サーバー・コンソールのリストに手動で追加済みである場合。

HMC 構成の準備

構成手順を始める前に知っておかなければならない必要な構成設定値の収集に、このセクションを使用してください。

注: 追加の接続およびセキュリティー情報が使用可能です。詳しくは、『HMC Connectivity Security』を参照してください。

HMC 用のプリインストール構成ワークシート

このワークシートを使用して、インストールに必要なインストール情報を準備します。

ネットワーク設定

LAN インターフェース: サービスおよびサポート、およびリモート・ユーザーに接続するために、この HMC で使用する有効なアダプター (eth0、eth1 など) を選択します。詳細は、 3 ページの『HMC ネットワーク接続』を参照してください。HMC からの接続は、プライベート・ネットワークまたはオープン・ネットワークのいずれかの上で可能です。

イーサネット・アダプターのスピードと二重モード

必要とするイーサネット・アダプター・スピードと二重モードを入力します。自動検出オプションを使用すると、お客様がハードウェアにとってどのスピードと二重モードを選択するのが最適な結果となるかをよく知らなくとも、どのオプションが最適かを判別します。「Default = Autodetection Media」スピードでは、イーサネット・アダプターの二重モードでのスピードを指定します。メディア・スピードを固定的に指定する要件がある場合を除き、「自動検出」を選択してください。デフォルトの FSP 設定は変更できないため、FSP に接続されるデバイス (スイッチ/HMC) はすべて、自動 (スピード) または自動 (二重) モードにセットする必要があります。

	eth0	**eth1**	**eth2**	**eth3**
スピードと二重モードの選択				
メディア・スピード (自動検出、10/100/1000 全/半二重)				

プライベート・ネットワークとオープン・ネットワークの詳細については、 5 ページの『HMC 環境でのプライベート・ネットワークおよびオープン・ネットワーク』を参照してください。

	eth0	**eth1**	**eth2**	**eth3**
アダプターごとに、「**プライベート (Private)**」または「**オープン (Open)**」ネットワークを指定します。				

動的ホスト構成プロトコル (Dynamic Host Configuration Protocol (DHCP)) は、動的なクライアント構成をするための自動化された方式です。 DHCP サーバーとしてこの HMC を指定可能です。これが、プライベート・ネットワーク上での最初で唯一の HMC である場合は、DHCP サーバーとしてこの HMC を有効にします。これを行う場合、ネットワーク上の管理対象システムを、HMC が自動的に構成および検出することになります。

プライベート・ネットワークとして指定されたイーサネット・アダプターの場合は、以下のテーブルの入力を行います。

	eth0	**eth1**
DHCP サーバーとしてこの HMC を指定したいですか? (はい/いいえ)		

	eth0	eth1
「はい」の場合、使用する IP アドレスの範囲を記録します。		

オープン・ネットワークとして指定されたイーサネット・アダプターの場合は、以下のテーブルの入力を行います。別のインターネット・プロトコル・バージョンに関する詳細は、8 ページの『インターネット・プロトコルの選択』を参照してください。

IPv6 の使用

IPv6 を使用する場合、ネットワーク管理者に連絡し、IP アドレスの取得方法を決定してください。次に、以下のテーブルの入力を行います。

	eth0	eth1	eth2	eth3
静的に割り振られた IP アドレスを使用していますか?「はい」の場合、ここでそのアドレスを記録してください。				

	eth0	eth1	eth2	eth3
DHCP サーバーから IP アドレスを取得していますか?(はい/いいえ)				

	eth0	eth1	eth2	eth3
IPv6 ルーターから IP アドレスを取得していますか?				

IPv6 アドレスの設定について、詳しくは 61 ページの『IPv6 アドレスの設定』を参照してください。 IPv6 アドレスのみを使用する場合は、62 ページの『IPv6 アドレスのみの使用』を参照してください。

IPv4 の使用

IPv4 を使用するオープン・ネットワークとして指定されたイーサネット・アダプターの場合、次のテーブルの入力を行います。

	eth0	eth1	eth2	eth3
IP アドレスを自動的に入手したいですか?(はい/いいえ)				
「いいえ」の場合、以下に指定されたアドレスをリストします。				
TCP/IP インターフェース・アドレス:				

	eth0	eth1	eth2	eth3
TCP/IP インターフェース・ネットワーク・マスク:				
ファイアウォール設定:				
HMC のファイアウォール設定を構成したいですか?(はい/いいえ)				
「はい」の場合、ファイアウォールを通過するように許可するアプリケーションおよび IP アドレスをリストします。				

TCP/IP 情報

ユニークな TCP/IP アドレスが、サポート・エレメント (SE) と HMC の両方に対して各ノードごとに必要になります。ローカル・プライベート LAN の場合、デフォルトでは、割り当てられたネットワーク・マスクを使用してユニークなアドレスを生成します。各ノードが、管理された TCP/IP アドレスを使用して大規模ネットワークに接続される場合、使用するその TCP/IP アドレスをお客様が指定できます。このデフォルト設定は、システムにより生成されます。

ファイアウォール設定

HMC ファイアウォール設定を使用してセキュリティー・バリアを作成します。それによって、HMC 上の特定ネットワーク・アプリケーションへのアクセスを許可または拒否します。各物理ネットワーク・インターフェースごとにこれらの制御設定を個別に指定可能です。これにより、どの HMC ネットワーク・アプリケーションを各ネットワーク上でアクセス可能かを制御できるようになります。

オープン・ネットワーク・アダプターとして少なくとも 1 つのアダプターを構成済みの場合、以下の追加情報を指定して、ご使用の HMC が LAN にアクセスできるようにします。

ローカル・ホスト情報	
HMC ホスト名:	
ドメイン・ネーム:	
HMC の説明:	
ゲートウェイ情報	
ゲートウェイ・アドレス: (nnn.nnn.nnn.nnn)	
ゲートウェイ・デバイス:	
DNS の有効化	
DNS を使用したいですか? (はい/いいえ)	

ローカル・ホスト情報	
「はい」の場合、DNS サーバーのサーチ・オーダーを以下に指定します。	
1.	
2.	
ドメイン・サフィックス・サーチ・オーダー:	
1.	
2.	

ローカル・ホスト情報

ご使用の Hardware Management Console (HMC) をネットワークに対して認識させるには、HMC のホスト名とドメイン・ネームを入力します。お客様のネットワーク上でショート・ホスト名のみ使用している場合を除き、完全修飾のホスト名を入力してください。ドメイン・ネームの例: name.yourcompany.com

ゲートウェイ情報

デフォルト・ゲートウェイを定義するには、IP パケットのルーティング用に使用する TCP/IP アドレスを入力します。宛先ステーションが送信元と同じサブネット上に存在しない場合に、このゲートウェイ・アドレスを使って、データをいつ送信したらよいかを各コンピューターまたはネットワーク装置に通知します。

DNS の有効化

ドメイン・ネーム・システム (DNS) を使用して、IP ベースのコンピューターを探すための標準命名規則を指定します。DNS サーバーを定義すると、IP アドレスを使用せずにホスト名を使用してサーバーとハードウェア管理コンソール (HMC) を認識できるようになります。

DNS サーバー・サーチ・オーダー

サーチ対象の DNS サーバーの IP アドレスを入力して、ホスト名と IP アドレスをマッピングさせます。このサーチ・オーダーが使用できるのは、DNS が使用可能な場合に限ります。

ドメイン・サフィックス・サーチ・オーダー

使用対象のドメイン・サフィックスを入力します。HMC はドメイン・サフィックスを使用して、DNS サーチに対して非修飾名を追加します。各サフィックスは、それがリストされた順番にサーチされます。このサーチ・オーダーが使用できるのは、DNS が使用可能な場合に限ります。

電子メール通知

お客様のシステム上でハードウェア障害イベント発生時に電子メールを使って通知されることを望む場合は、電子メールの連絡先情報をリストします。

電子メール・アドレス:	
SMTP サーバー:	
ポート:	
通知対象となるエラー:	
コール・ホームの対象となる問題イベントのみ	
全部の問題イベント	

SMTP サーバー

サーバーの Simple Mail Transfer Protocol (SMTP) アドレスを入力して、システム・イベントに関する通知を受けます。SMTP サーバー名の例は、`relay.us.ibm.com` です。

SMTP は電子メールを送信するのに使用されるプロトコルです。SMTP 使用時は、SMTP プロトコルを使ってクライアントがメッセージを送信し、SMTP サーバーと通信します。

ご使用のサーバーの SMTP アドレスを知らないか、またはよく分からない場合は、お客様のネットワーク管理者に確認してください。

ポート サーバーのポート番号を入力して、システム・イベントに関する通知を受けます。あるいはデフォルトのポートを使用します。

通知を受ける対象の電子メール・アドレス

構成された電子メール・アドレスを入力して、システム・イベント発生時に通知を受けます。

- 「**コール・ホームの対象となる問題イベントのみ (Only call-home problem events)**」を選択して、コール・ホーム機能を作成するイベント発生時のみ通知を受けます。
- 「**全問題イベント (All problem events)**」を選択して、どのようなイベント発生時にも通知を受けます。

サービス連絡先情報

会社名	
管理者名	
電子メール・アドレス	
電話番号	
代替電話番号	
Fax 番号	
代替 FAX 番号	
所在地住所	
所在地住所 2	
市または地域	
県	
郵便番号	
国または地域	
HMC の場所 (上記管理者住所と同じ場合は、「同じ」と指定)	
所在地住所	
所在地住所 2	
市または地域	
県	
郵便番号	
国または地域	

サービス権限と接続性

サービス・プロバイダーに連絡するための接続タイプを選択してください。これらの方法の詳細 (セキュリティー特性と構成要件を含む) は、 6 ページの『コール・ホーム・サーバーに使用する接続方式の決定』を参照してください。

_____ インターネット経由の Secure Sockets Layer (SSL)

_____ ローカル HMC からのダイヤルアップ

_____ インターネットを介する仮想プライベート・ネットワーク (VPN)。

インターネット経由の Secure Sockets Layer (SSL):

お客様に HMC からの既存インターネット接続がある場合、その接続を使用してサービス・プロバイダーを呼び出すことができます。サービス・プロバイダーに直接接続することができます。これを行うには、既存インターネット接続を使用して、暗号化された Secure Sockets Layer (SSL) を使用します。SSL プロキシー経由の間接接続を使って、暗号化された SSL の使用を構成したい場合は、「**SSL プロキシーの使用 (Use SSL Proxy)**」を選択します。

SSL プロキシーの使用 ? (はい/いいえ)	
「はい」の場合、以下の情報をリストします。	
アドレス:	
ポート:	
SSL プロキシーにより認証 ?	
「はい」の場合、以下の情報をリストします。	
ユーザー:	
パスワード:	

使用されるインターネット接続プロトコル

別のインターネット・プロトコルに関する詳細は、 8 ページの『インターネット・プロトコルの選択』を参照してください。

___ IPv4

___ IPv6

___ IPv4 および IPv6

ローカル HMC からのダイヤルアップ

ダイヤルアップ情報を入力して、ローカル・モデムを構成します。どの電話番号を使ってサービス・プロバイダーにダイヤルするかを指定します。接続しようとする時点で、その電話番号がリストされた順序でダイヤルインされます。

アクセス番号: _____

トーン: _____

パルス: _____

ダイヤル音を待つ? _____

スピーカーを使用可能にする? _____

仮想プライベート・ネットワーク (VPN)

お客様に HMC からの既存インターネット接続がある場合、その接続を使用してサービス・プロバイダーを呼び出すことができます。既存インターネット接続を使用して、仮想プライベート・ネットワークによりサービス・プロバイダーに直接接続できます。

注: インターネット経由の仮想プライベート・ネットワークを選択すると、お客様には他のどのオプションも選択するように指示されません。

コール・ホーム・サーバー

コール・ホーム・サーバーとしてサービスおよびサポートに接続するように構成する HMC を決定します。複数のコール・ホーム・サーバーの使用について詳しくは、10 ページの『複数のコール・ホーム・サーバーの使用』を参照してください。

___ この HMC

___ 別の HMC

「**別の HMC**」にチェックマークを入れた場合は、コール・ホーム・サーバーとして構成済みの別の HMC を、ここで以下にリストしてください。

表 5. コール・ホーム・サーバーとして構成済みの別の HMC

コール・ホーム・サーバーとして構成済みの HMC ホスト名または IP アドレスのリスト

サポート上のさらなる利点

マイ・システムとプレミアム・サーチ

IBM ID のリスト _____

追加の IBM ID のリスト _____

エレクトロニック・サービス Web サイトの「マイ・システム (My Systems)」および「プレミアム・サーチ (Premium Search)」セクション内の有用なカスタマイズ・サポート情報にアクセスするには、IBM ID をこのシステムに登録する必要があります。お客様がまだ IBM ID を保有していない場合、www.ibm.com/account/profile でその ID に対して登録することができます。

注: IBM はパーソナライズされた Web 機能を提供して、その機能で、IBM Electronic Service Agent™ アプリケーションが収集した情報を使用します。これらの機能を使用するには、まず最初に、IBM 登録 Web サイト (http://www.ibm.com/account/profile) で登録を行う必要があります。

ユーザーによるエレクトロニック・サービス・エージェント情報の使用を許可して Web 機能をパーソナライズするには、IBM 登録 Web サイト上で登録した IBM ID を入力します。http://www.ibm.com/support/electronic にアクセスして、(IBM ID を自分のシステムに登録している) お客様にとって使用可能な価値あるサポート情報を参照します。

HMC のセットアップ

HMC ソフトウェアを構成する前に、HMC ハードウェアをセットアップする必要があります。デスクサイド HMC またはラック・マウント HMC のセットアップについて、さらに説明します。

スタンドアロン HMC の配線

HMC を配置して各ハードウェア・コンポーネントを配線します。

いずれかの POWER7 プロセッサー・ベースのシステムの管理に HMC が使用される場合、HMC は、C05 以降のスタンドアロン HMC でなければなりません。

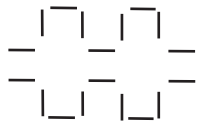
1. HMC は、必ず正しい位置に置くようにしてください。
2. モニター・コネクターにモニター・ケーブルを接続し、ねじを締めます。
3. 電源コードをモニターに接続します。
4. HMC の電圧選択スイッチが、お客様の国および地域の電圧に設定されているか確認します。電圧選択スイッチは赤色で、電源コネクターのそばにあります。お客様の地域で使用する電圧が表示できるようにスイッチを移動してください。
5. 電源コードのプラグを HMC に差し込みます。
6. キーボードおよびマウスを HMC に接続します。
7. 以下のようにして、オプションのモデムを接続します。

   注: HMC の取り付けおよび構成中、HMC がルーチン・コールアウト・プロシージャーを進めるのに合わせて、モデムが自動的にダイヤルアウトすることがあります。これは通常の動作です。

   オプションの外付けモデムを接続する場合は、以下のようにします。

   注: IBM にエラー情報を送信する場合、他の接続方式も使用できます。

   a. モデム・データ・ケーブルを外付け HMC モデムにまだ接続していない場合は、ここで行います。
   b. モデム・データ・ケーブルを、次の記号のラベルが付いた HMC のシステム・ポートに接続します。



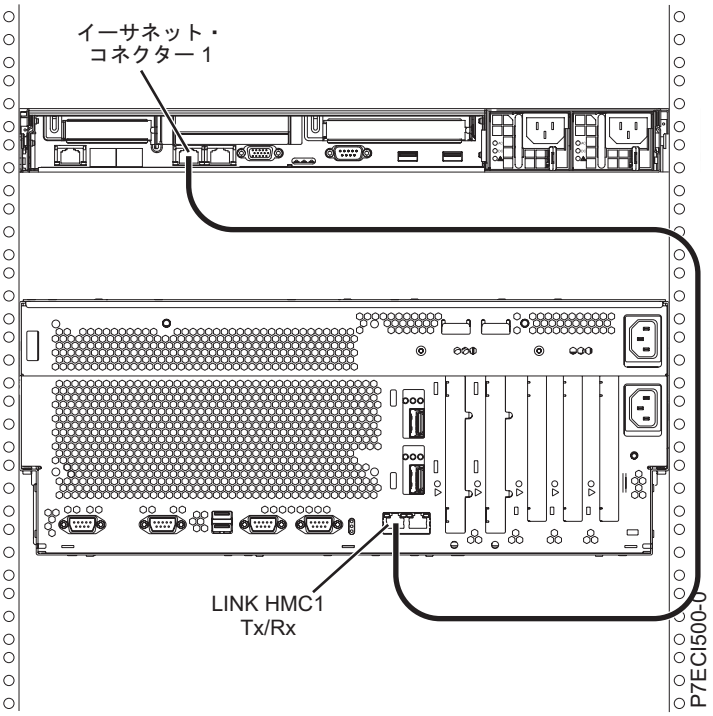
IPHAI522-0

   c. 電話ケーブルを使用して、外付けモデムの回線ポートを壁面のアナログ電話ジャックに接続します。

   オプションの内蔵モデムを接続する場合 は、データ・ケーブルを使用して、内蔵 HMC モデムを適切なデータ・ソースに接続します。例えば、電話ケーブルを使用して、HMC モデムの回線ポートを壁面のアナログ・ジャックに接続します。

   注: IBM にエラー情報を送信する場合、他の接続方式も使用できます。
8. 管理対象システムが既にインストール済みの場合は、イーサネット・ケーブル接続がアクティブ状態かどうかを確認できます。これを行うには、取り付けの進行中に、HMC および管理対象システムの両方のイーサネット・ポートの緑色の状況ライトを確認します。

9. HMC の**イーサネット・コネクター 1** を管理対象システムの **LINK HMC1** ポートに接続します。



10. 2 台目の HMC を管理対象サーバーに接続する場合は、管理対象サーバー上で **LINK HMC2** というラベルの付いたイーサネット・ポートに接続します。
11. 外付けモデムを使用する場合は、モデムの電源コードを HMC モデムに接続します。
12. モニター、HMC、および HMC 外付けモデムのそれぞれの電源コードをコンセントに差し込みます。この HMC を新しい管理対象システムに接続する場合は、この時点では、管理対象システムを電源に接続しないでください。

次に、HMC ソフトウェアを構成する必要があります。 54 ページの『HMC の構成』から続行します。

関連概念:

6 ページの『コール・ホーム・サーバーに使用する接続方式の決定』
コール・ホーム・サーバーの使用時に適用できる接続オプションについて説明します。

3 ページの『HMC ネットワーク接続』

7310-CR4 HMC のラックへの取り付け

このセクションでは、7310-CR4 HMC をラックに取り付ける方法について説明します。この作業はお客様が行う作業です。

いずれかの POWER7 プロセッサー・ベースのシステムの管理に HMC が使用される場合、HMC は、CR3 以降のモデルのラック・マウント HMC でなければなりません。

以下に 7310–CR4 の背面図を示します。

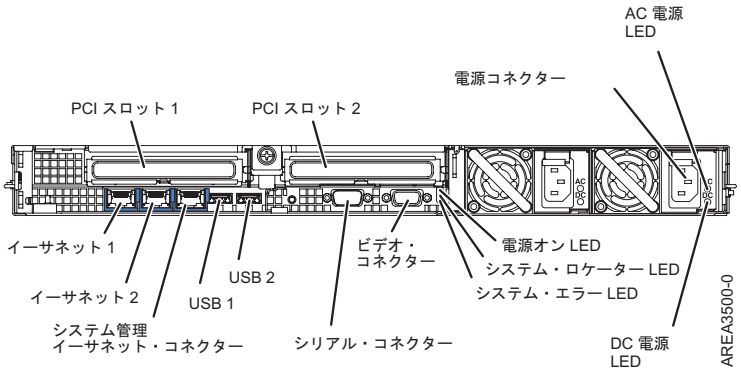


図 1. 7310–CR4 の背面図

7310-CR4 HMC をラックに取り付けるには、次のステップを実行します。

1. 部品目録を確認します。『部品目録の確認』を参照してください。
2. システム装置に組み込まれているラック取り付けハードウェア・キットとシステム・レール・アセンブリーを探します。

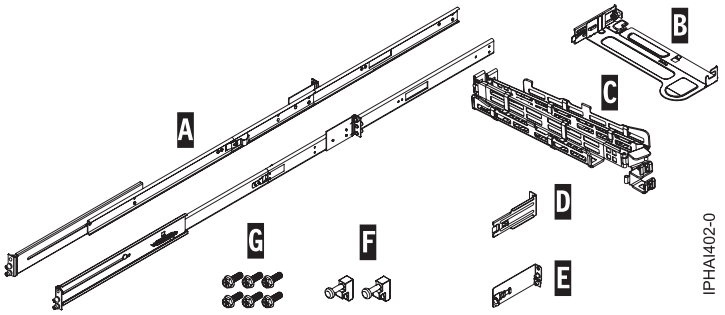


図 2. レール・キット

表 6. レール・キット部品

スライド・レール・キット部品

A スライド・レール

B ケーブル・マネージメント・アーム取り付けプレート

C ケーブル・マネージメント・アーム

D ケーブル・マネージメント・ブラケット

E ケーブル・マネージメント・サポート・ブラケットおよび保護タブ

F ラッチ受け座 (2)

G ねじ (6)

重要: このシステム装置は 1 台の EIA 装置の高さです。取り付けの完了にはこの情報が必要です。

部品目録の確認

部品目録を確認することが必要な場合があります。このセクションの手順を使用して、この作業を行ってください。

部品目録をまだ確認していない場合は、取り付けを始める前に確認してください。

1. アクセサリー・ボックスにあるキット一式のレポートを確認します。
2. オーダーしたすべての部品を受け取ったか確認します。

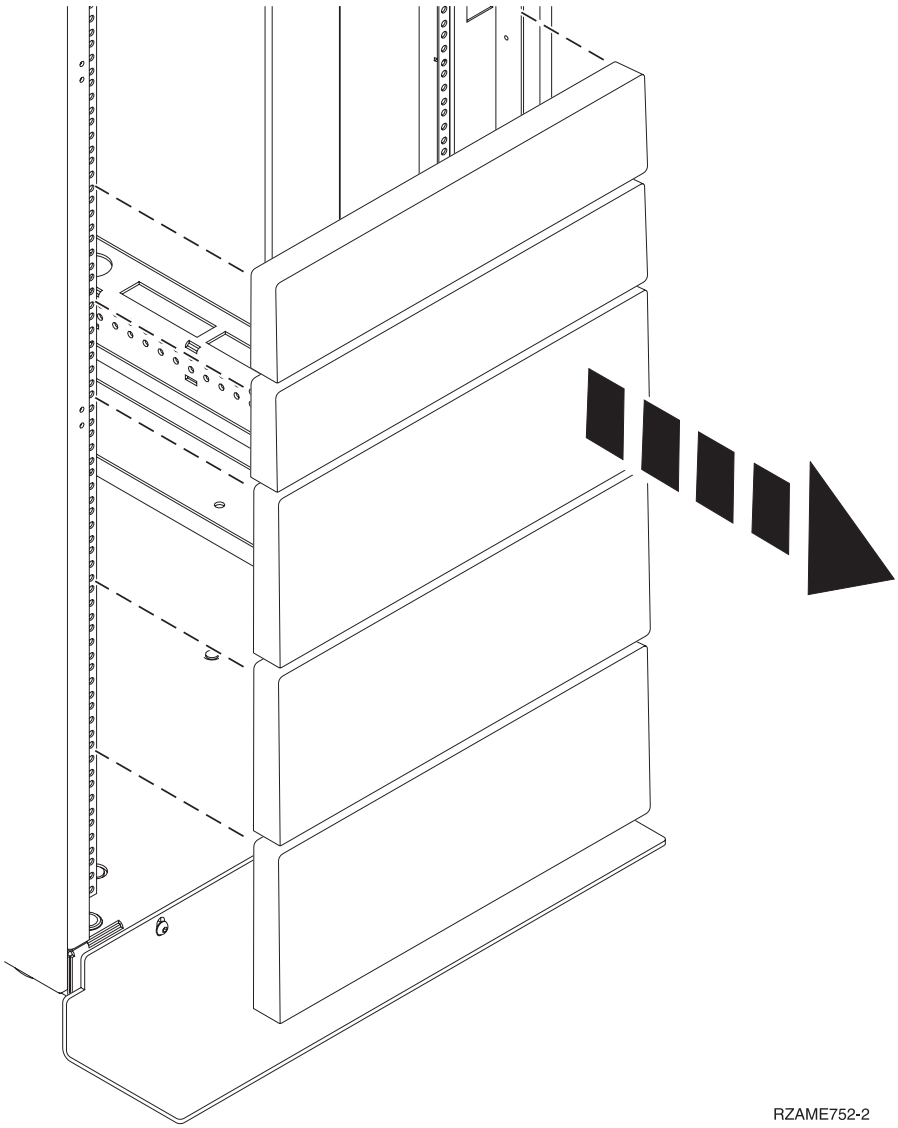
部品の間違い、欠落、または損傷がある場合は、IBM 販売店またはIBM 営業およびサポートにご連絡ください。

位置の決定

システムを取り付けるラック内の位置を判別することが必要になる場合があります。このセクションでは、お客様がこれらの作業を実施可能にするための手順を記載してあります。

HMC をラックに取り付ける前に、次のステップを実行します。

1. 装置の配置位置を決定します。大きくて重い装置をラックの低い段に配置してください。
2. ラックにフィラー・パネルが入っている場合はそれを取り外し、装置を配置しようとするラック・エンクロージャーの内部にアクセスできるようにします。



RZAME752-2

図 3. フィラー・パネルの取り外し

3. 必要な場合、前面および背面のラック・ドアを取り外します。
4. ラック取り付けテンプレートなしでの位置のマーク付けを参照しながら、テンプレートなしに位置にマーキングする手順に従います。

ラック・マウント・テンプレートを使用せずに位置にマークを付ける:

テンプレートを使用せずに、位置にマークを付けることができます。

このシステムには、ラック取り付けテンプレートは組み込まれていません。これらのシステムの高さは、1 EIA 単位です。

取り付け位置を決定するには、以下のステップを完了します。

1. ラック内にシステムを設置する場所を決定します。 EIA 位置を記録します。

   注: ラック上の EIA 装置は 3 つの穴のグループから構成されます。
2. ラックの前面に向き、右側から作業しながら、提供された接着ドットを EIA 装置の上部の穴の隣に付けます。

   注: この接着ドットは、ラック上での位置の識別をしやすくするために使用します。 手持ちのドットがない場合は、他のマーキング用具 (テープ、マーカー、鉛筆など) を、穴の位置の識別のために使用してください。スライド・レールを取り付ける場合は、各 EIA 装置の低い、中央の穴にマークまたは接着ドットを付けます。
3. もう 1 つの接着ドットをその上の EIA 単位の下部の穴の横に貼ります。

   注: 穴を数える場合、最初のドットで印された穴から数え始め、2 つ上の穴を数えます。 2 番目のドットを 3 番目の穴の隣に付けます。
4. ラック左側の対応する穴に対してもステップ 1 を繰り返します。
5. ラックの背面に回ります。
6. 右側で、ラック前面のマークを付けた下部 EIA 装置に対応する EIA 装置を見つけます。
7. 下部の EIA 装置に接着ドットを付けます。
8. EIA 装置の上部の穴に接着ドットを付けます。
9. ラックの左側で対応する穴にマークを付けます。

スライド・レールのラックへの取り付け

スライド・レールをラックに取り付けるには、以下の手順を使用します。

スライド・レールをラックに取り付けるには、以下のステップを完了します。

1. 右のマークが付いた右スライド・レール **(A)** を、ラックの背面右にあるラック取り付けフランジ **(B)** の位置に挿入します。 2 つのレール・ピンが、EIA 装置の下部および中央の穴 **(B)** から突き出ます。

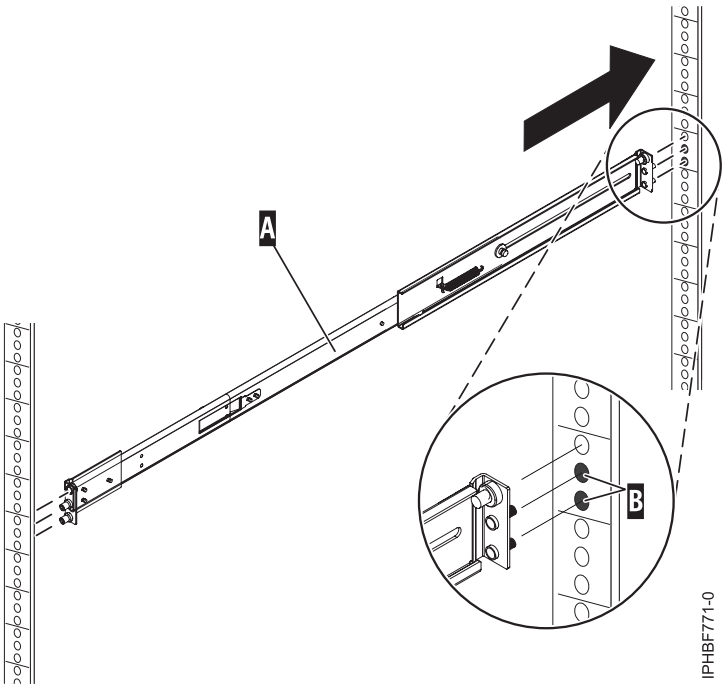


図 4. 右スライド・レールのラック背面への取り付け

2. レール **(A)** の端を押して、レールのバネ仕掛けのメカニズムを圧縮し、レールをラック右側にある取り付けフランジ **(B)** の位置に挿入します。レールの圧縮が解除され、2 つのレール・ピンが、EIA 装置の下部および中央の穴 **(B)** から突き出ます。

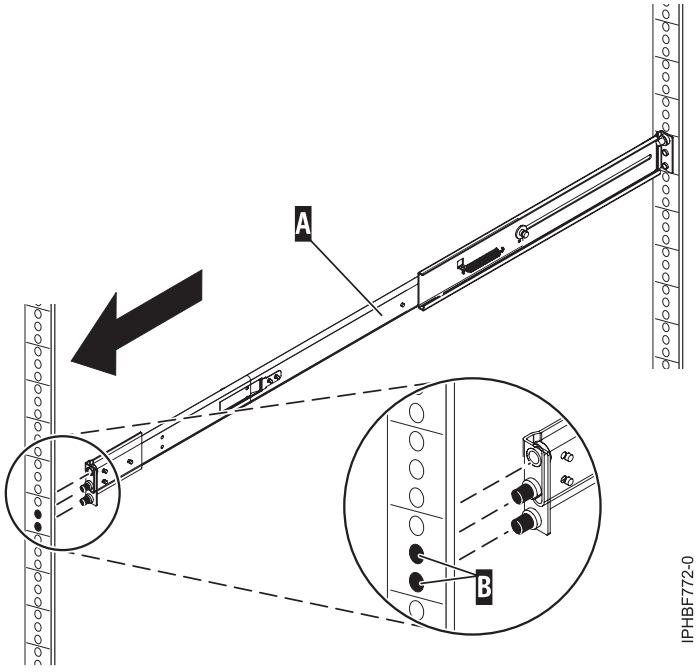


図 5. 右スライド・レールのラック前面への取り付け

3. ステップ 1 (30 ページ) から 2 (31 ページ) を繰り返して、左のマークが付いた左スライド・レールをラックに取り付けます。
4. ラック前面から、ラッチ受け座 **(C)** をこのピンの上に置きます。拘束ねじ **(D)** を、右側スライド・レール **(A)** の前面の上部ピンに入れ、指で締めてください。

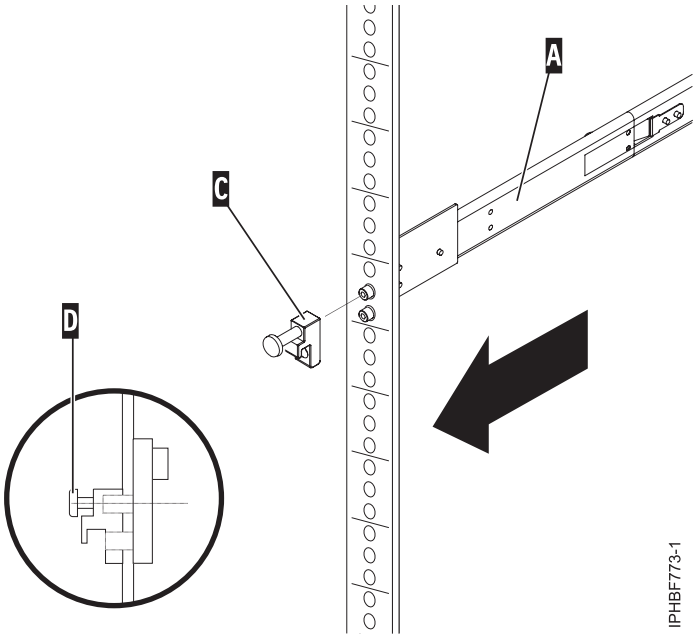


図 6. ラッチ・ストライクのレールの前面への取り付け

5. 前のステップを繰り返して、ラッチ・ストライクを左側のスライド・レールの前面に取り付けます。
6. ラックの背面に移動します。ねじ **(F)** を指で締めて、ケーブル・マネージメント・アーム取り付けブラケット **(E)** を左レール **(G)** の背面に取り付けます。

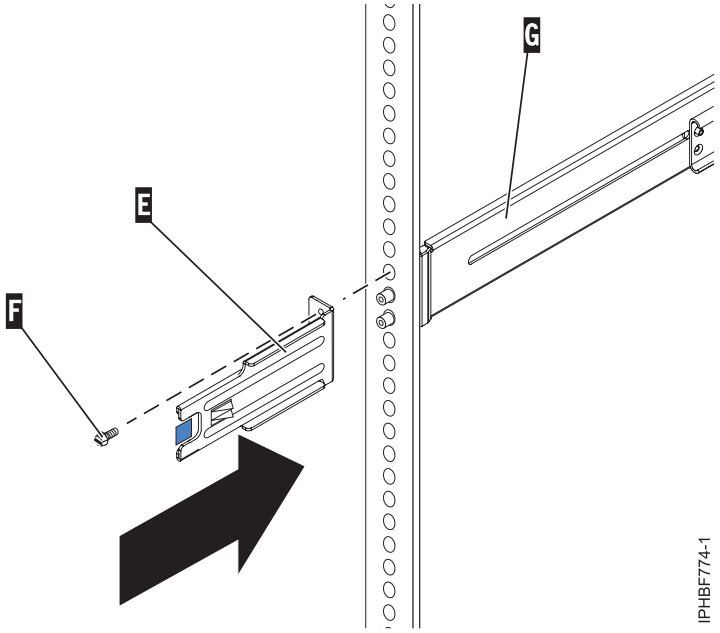


図 7. ケーブル・マネージメント・ブラケットの左背面レールへの接続

7. このシステムを輸送する計画がない場合は、 34 ページの『HMC のスライド・レールへの取り付け』を続行します。このシステムを輸送する計画がある場合は、ねじ **(I)** を挿入し、ケーブル・マネージメント・アーム・サポート・ブラケット **(H)** を、レール **(A)** の右背面に取り付けます。ねじを指で締めます。

   ケーブル・マネージメント・アームのサポート・ブラケットを使用して、輸送中にケーブル・マネージメント・アームを固定することができます。このメカニズムがケーブル・マネージメント・アームが取り付けられた後でかみ合わされた場合、システムをラックからスライドできなくなります。

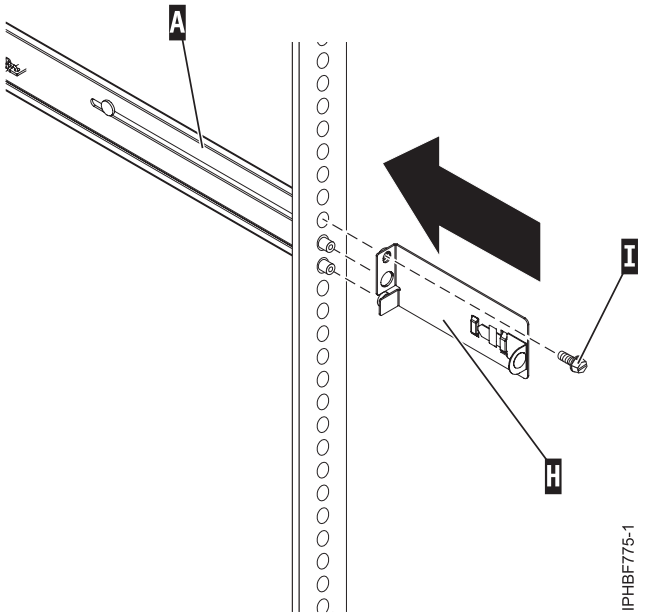


図 8. 右背面レールへのケーブル・マネージメント・サポート・ブラケットの接続。

HMC のスライド・レールへの取り付け

HMC のスライド・レールへの取り付けが必要になることがあります。この作業を実行するには、このセクションの手順を使用します。

HMC をスライド・レールに取り付ける前に、スタビライザーを延長し、ラック・スタビライザー・ブラケットがラックの下部前面に接続して、レールをラックから引き出したときに、ラックが前方に転倒しないようにしてください。

HMC をスライド・レール・アセンブリーに取り付ける場合は、以下のステップを完了します。

1. 電源装置を覆っている配送用ブラケットを、HMC の右背面から取り外します。この配送用ブラケットを取り外すには、ブラケットを右方に押して、配送用ブラケットをクルリと回して HMC から離します。
2. ラックの前面から、スライド・レールを、所定の延長した位置 **(A)** に固定されるまで十分延長します。

   重要: HMC をレールに取り付けるには、*その前に* レールの前面のラッチ・ストライクとケーブル・マネージメント・アーム・ブラケットを取り付けておく必要があります。これらの部品が取り付けられていない場合は、HMC を取り付けた際にレールが圧縮され、HMC がラックから外れることがあります。

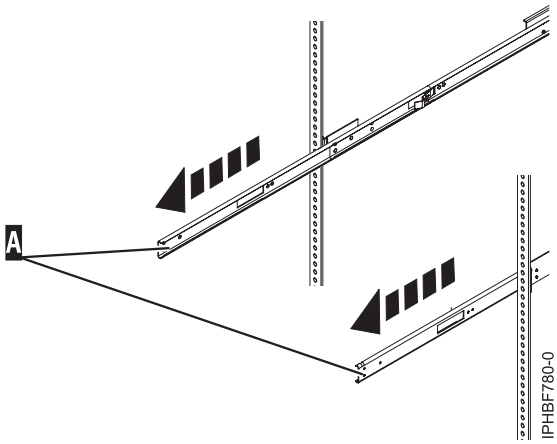


図 9. スライド・レールの延長

重要: この装置の重量は約 17 kg であり、HMC をラックに収めるときは、この重量を確実に支えることができるようにしてください。

3. HMC をレールの高さに持ち上げ、ホイール **(B)** のセットをレール・ガイド間の HMC の背面に置きます。

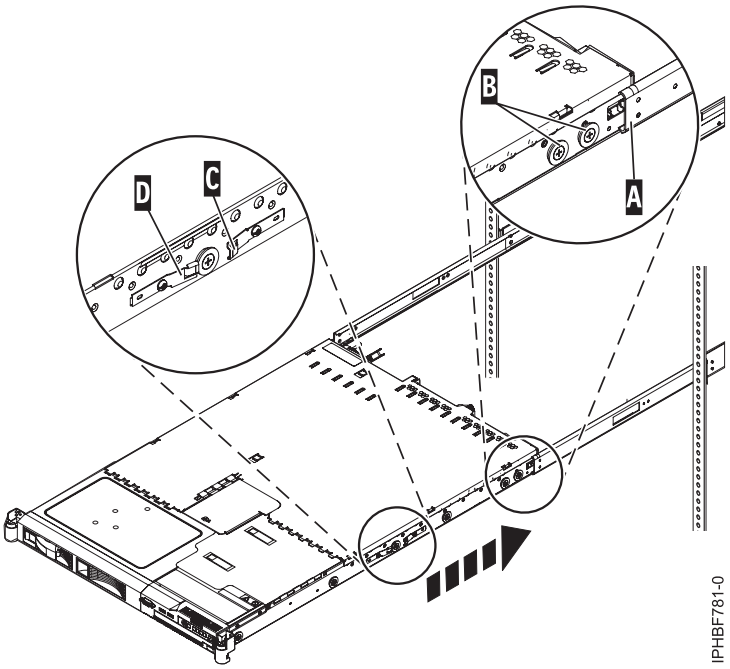


図 10. HMC のスライド・レールへの取り付け

4. HMC をスライド・レールに、スライド・リリース・キャッチ **(C)** が、所定の位置に固定されるまで押し込みます。これで、システムはこのスライドの保守位置に固定されます。カチッという音が聞こえます。
5. スライド・レールの両側にある、前面のスライド・レール・リリース・ラッチ **(D)** を押します。

6. HMC をスライドさせながらラック内に入れたり出したりして、HMC が制限されることなく自由に移動するか確認します。

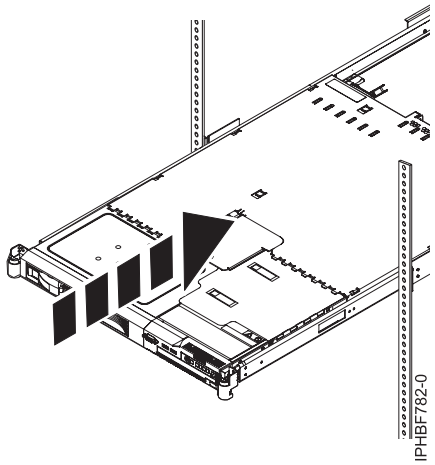


図 11. HMC のラック内へのスライド

重要: どのような場合も、HMC を無理にスライド・レールに押し込まないでください。 HMC がラック内に支障なく滑り込まない場合は、HMC をレールから完全に取り外してください。 HMC がレールから除かれた後、HMC の位置を変更してから、再度 HMC をレールに挿入します。 HMC が支障なくラックに滑り込むまでこのプロセスを繰り返します。

7. HMC を、ラック・ラッチ **(F)** が所定の位置に固定されるまで押し込みます。

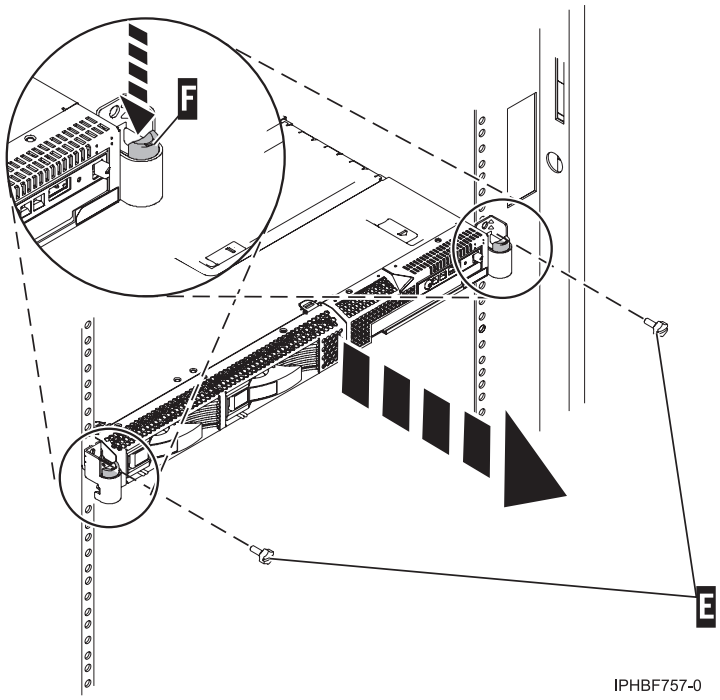


図 12. ラック・ラッチとねじ

8. 両側のレールの前面と背面に取り付けた 4 つのねじをそれぞれきつく締めます。
9. ラックを移動する場合は、2 つのラック保護ねじ **(E)** を挿入し、締め付けてください。

ケーブル・マネジメント・アームの取り付け

ケーブル・マネジメント・アームを取り付ける必要がある場合があります。 このセクションの手順を使用して、この作業を行ってください。

ケーブル・マネジメント・アームを取り付けるには、次の手順を実行してください。

1. ラックの背面から、左のシステム・レール・アセンブリーの固定された背面部分にある、ケーブル・マネージメント・アーム・フランジ **(A)** を (ラックの背面から見て) 見つけます。
2. ケーブル・マネージメント・アームの止め金 **(B)** を、所定の位置に固定されるまでレールに押し込み、レールに取り付けます。

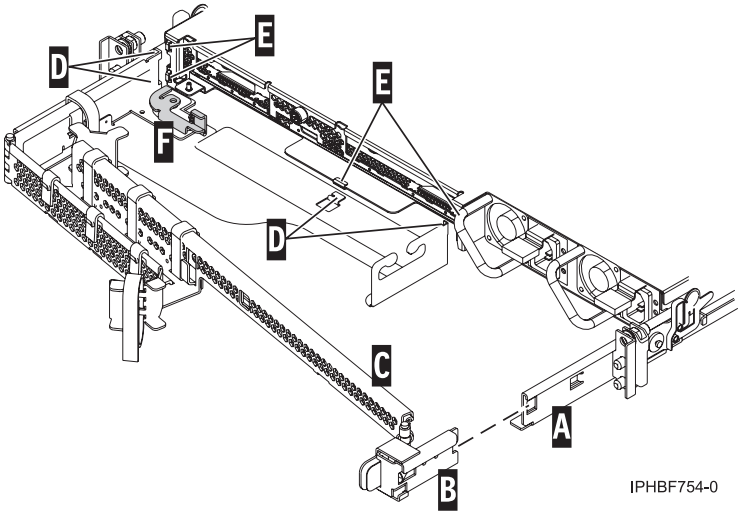


図 13. ケーブル・マネージメント・アームおよびシステム装置。

3. ケーブル・マネージメント・アーム **(C)** の別の端を HMC の背面に接続します。ケーブル・マネージメント・アームのタブ **(D)** を HMC の背面のスロット **(E)** の位置に合わせます。
4. ケーブル・マネージメント・アームを左にスライドさせ、所定の位置に固定します。すべてのタブがスロットに収まるようにしてください。
5. ロッキング・レバー **(F)** を、固定された位置に押し込みます。ケーブル・マネージメント・アーム **(C)** が、自由に移動するように水平にしてください。

ラック・マウント HMC の配線

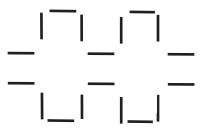
ラック・マウント HMC を物理的にインストールする方法について説明します。

1. HMC は、必ず正しい位置に置くようにしてください。
2. HMC をラックに取り付けます。詳しくは、 27 ページの『7310-CR4 HMC のラックへの取り付け』を参照してください。ラックへの HMC の取り付けが完了したら、次のステップに進みます。
3. 電源コードのプラグを HMC に差し込みます。
4. キーボード、モニター、およびマウスを接続します。
5. 以下のようにして、オプションのモデムを接続します。

   外付けモデムを接続する場合は、以下のようにします。

   注: IBM にエラー情報を送信する場合、他の接続方式も使用できます。詳しくは、 6 ページの『コール・ホーム・サーバーに使用する接続方式の決定』を参照してください。

a. 外付けモデムをラック内に取り付ける必要がある場合は、ここで行います。
b. モデム・データ・ケーブルを外付け HMC モデムにまだ接続していない場合は、ここで行います。
c. モデム・データ・ケーブルを、次の記号のラベルが付いた HMC のシステム・ポートに接続します。



IPHAI522-0

d. 電話ケーブルを使用して、外付けモデムの回線ポートを壁面のアナログ電話ジャックに接続します。
e. モデムの電源コードのプラグを HMC モデムに差し込みます。

内蔵モデムを接続する場合 は、データ・ケーブルを使用して、内蔵 HMC モデムを適切なデータ・ソースに接続します。 例えば、電話ケーブルを使用して、HMC モデムの回線ポートを壁面のアナログ・ジャックに接続します。

注: IBM にエラー情報を送信する場合、他の接続方式も使用できます。詳しくは、6 ページの『コール・ホーム・サーバーに使用する接続方式の決定』を参照してください。

6. 以下のようにして、HMC からのイーサネット (またはクロス) ケーブルを管理対象サーバーに接続します。

注: HMC ネットワーク接続の詳細については、3 ページの『HMC ネットワーク接続』を参照してください。

7. 管理対象システムが既にインストール済みの場合は、イーサネット・ケーブル接続がアクティブ状態かどうかを確認できます。これを行うには、取り付けの進行中に、HMC および管理対象システムの両方のイーサネット・ポートの緑色の状況ライトを確認します。
8. HMC のイーサネット・ポートを、管理対象サーバー上で **HMC1** というラベルの付いたイーサネット・ポートに接続します。
9. 2 台目の HMC を管理対象サーバーに接続する場合は、管理対象サーバー上で **HMC2** というラベルの付いたイーサネット・ポートに接続します。
10. モニター、HMC、および HMC 外付けモデムのそれぞれの電源コードをコンセントに差し込みます。

注: この HMC を新しい管理対象システムに接続する場合は、この時点では、管理対象システムを電源に接続しないでください。

次に、HMC ソフトウェアを構成する必要があります。54 ページの『HMC の構成』から続行します。

7042-CR5、7042-CR6、および 7042-CR7 のラックへの取り付け

このセクションでは、7042-CR5、7042-CR6、および 7042-CR7 HMC をラックに取り付ける方法について説明します。

いずれかの POWER7 プロセッサー・ベースのシステムの管理に HMC が使用される場合、HMC は、CR3 以降のモデルのラック・マウント HMC でなければなりません。

部品目録を確認します。次の図は、サーバーをラック・キャビネットの中に取り付けるために必要な品目を示しています。いずれかの品目が欠落または損傷している場合、購入先にお問い合わせください。

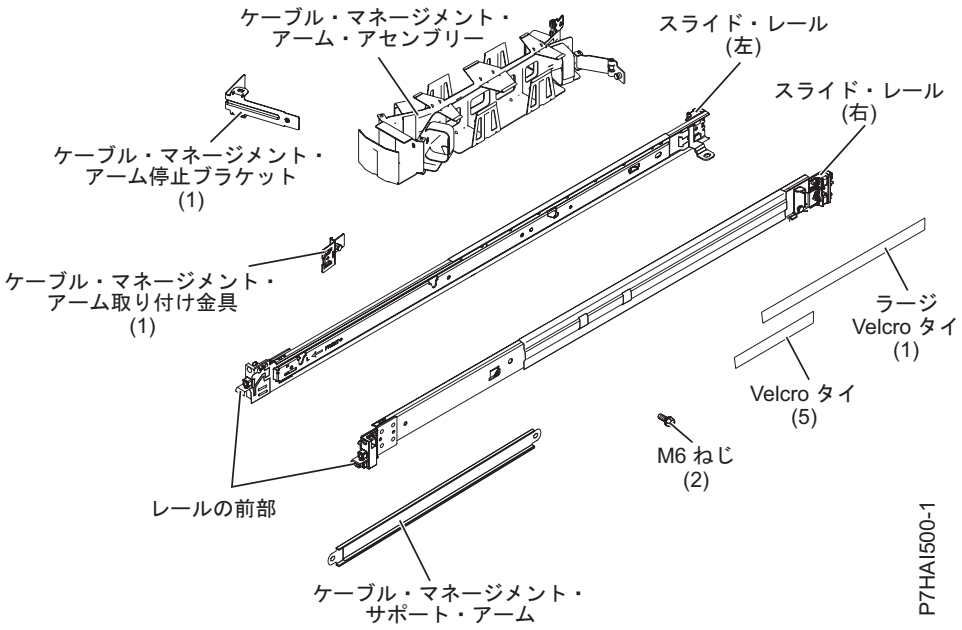


図 14. 部品目録

注: ねじは、配送時や、振動が大きな区域で安定度を強化するために使用できます。

7042-CR5、7042-CR6、または 7042-CR7 HMC をラックに取り付けるには、次のステップを実行します。

1. 各スライド・レールには、R (右) または L (左) のマークが付いています。スライド・レールのいずれか 1 つを選択して、前面の可動式タブ **(1)** を押し上げます。次に、前面ラッチ **(2)** を引き出して、前面のレールをスライドさせて出します。つまみねじがスライド・レール **(3)** に取り付けられている場合は、取り外します。

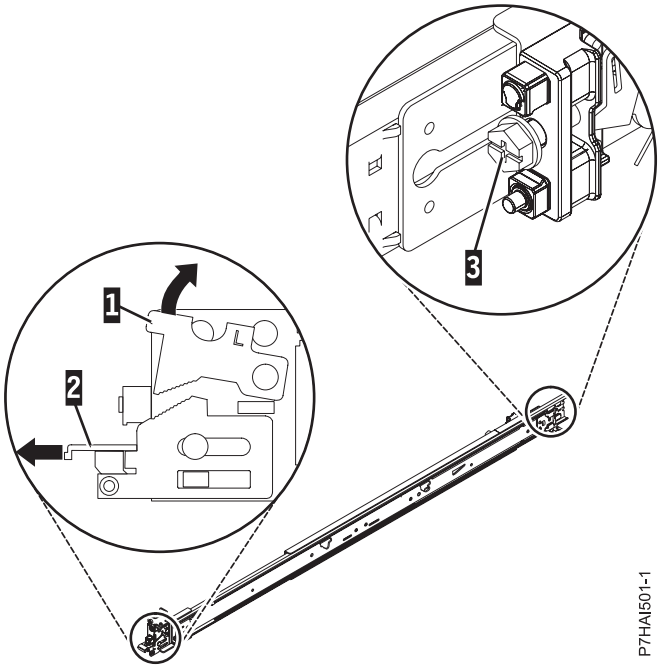


図 15. スライド・レールと可動式タブ

注: 可動式タブが押し上げられたままで元の位置に戻っていないことを確認してください。

2. スライド・レールの後部にある 3 つのピンの位置を、ラック後部の選択した U の 3 つの穴に合わせます。レールを押してピンが穴 **(1)** に入るようにしてから、スライド・レールを所定の位置に掛かるまで下に **(2)** 落とします。

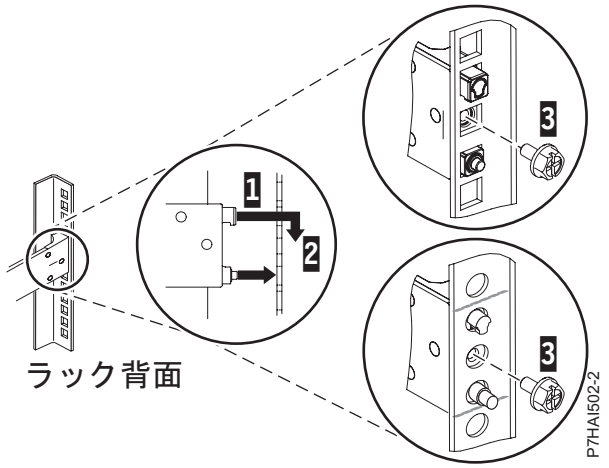


図 16. ピンとラック後部の穴の位置合わせ

3. スライド・レールを前方に引き、レール前部の 2 本のピン **(1)** を、ラック前面にある U の下側の 2 つの穴に挿入します。カチッと音がする位置までレールを落とします。前部ラッチ **(2)** を完全に押し込みます。ステップ 1 から 3 を繰り返し、もう一方のレールをラックに取り付けます。それぞれの前部ラッチが完全に収まっていることを確認します。

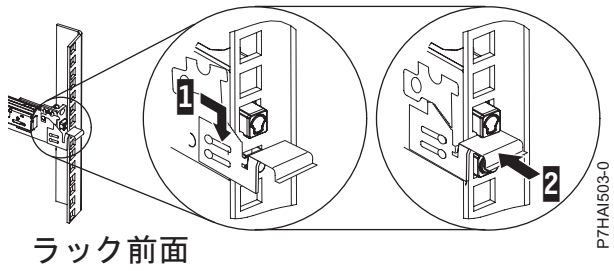


図 17. ラック前部のレールとピン

4. 2 回カチッと音がする位置までスライド・レールを前方に **(1)** 引きます。サーバーを慎重に持ち上げたら、スライド・レールの上でサーバーを傾けて位置合わせし、サーバー背面のくぎの頭 **(2)** がスライド・レールの後部スロット **(3)** と揃うようにします。後部のくぎの頭が 2 つの後部スロットに入るまでサーバーをスライドさせます。次に、残りのくぎの頭がスライド・レールの他のスロットにはまるまで、サーバーの前部 **(4)** をゆっくりと下ろします。前面ラッチ **(5)** が、くぎの頭の上をスライドすることを確認します。

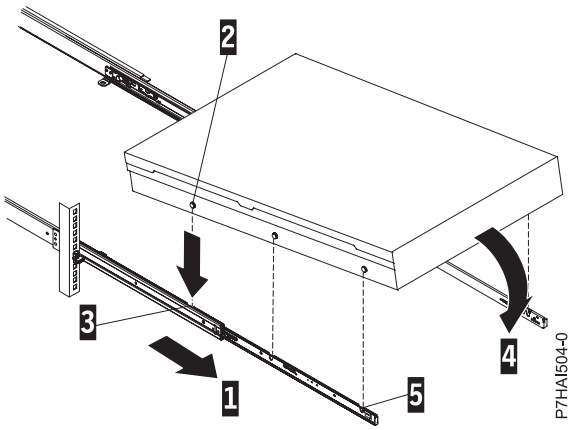


図 18. 引き出したスライド・レールと、レールのスロットと位置合わせしたサーバーのくぎの頭

5. スライド・レールにある青色のリリース・ラッチ **(1)** を引き上げ、サーバー **(2)** を所定の位置に収まるまでラックの中に押し込みます。

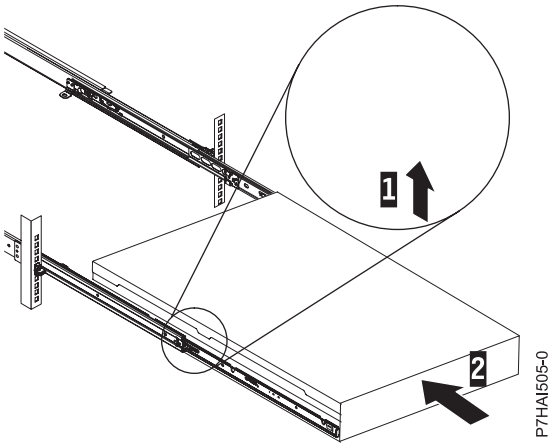


図 19. リリース・ラッチとサーバー

6. ケーブル・マネージメント・アームは、サーバーのどちら側にも取り付けることができます。次の図は、左側に取り付けた例を示しています。ケーブル・マネージメント・アームを右側に取り付けるには、説明に従ってハードウェアを反対側に取り付けます。サポート・アームの一方の端 **(1)** を、ケーブル・マネージメント・アームを取り付けようとしているスライド・レールに接続し、サポート・アームのもう一方の端 **(2)** をラックに向かって回せるようにします。

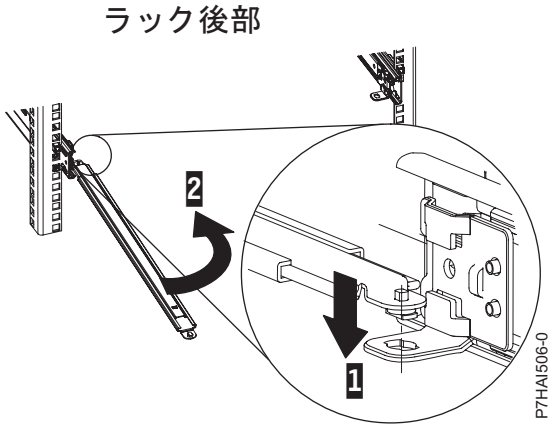


図 20. サポート・アームの接続

7. L 字型のケーブル・マネージメント停止ブラケット **(1)** をサポート・アームの接続していない方の端に取り付けます。ブラケット **(2)** を回して、サポート・アームに固定します。

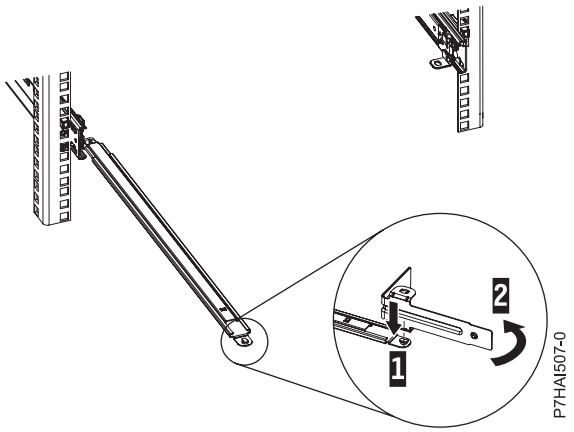


図 21. サポート・アームに固定されたケーブル・マネージメント停止ブラケット

8. サポート・アームの反対側をスライド・レールの後部に取り付けるには、ピンを引き出してから **(1)**、ブラケット **(2)** をスライド・レールに滑り込ませます。

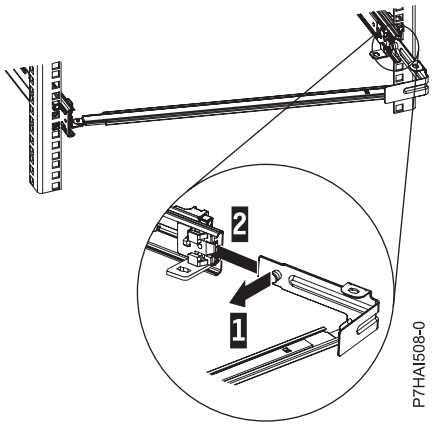


図 22. 引き出したピンと、スライド・レールに取り付けたブラケット

9. 取り付け金具のピン **(1)** を引き出して、ケーブル・マネージメント・アームを取り付けているスライド・レールに取り付け金具 **(2)** を滑り込ませます。バネ式のピンが所定の位置に収まるまで、ブラケットをスライド・レールに押し込みます。

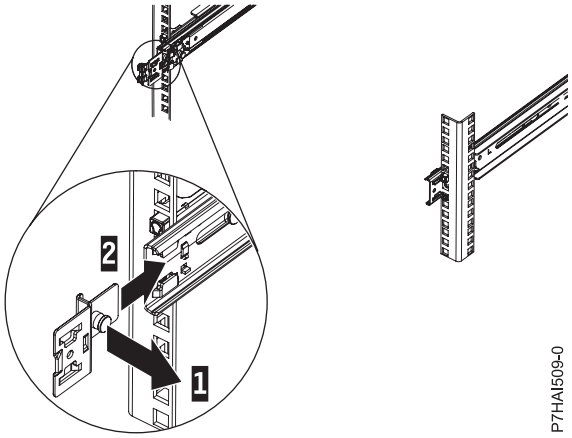


図 23. 引き出した取り付け金具のピンと、スライド・レールに取り付けた取り付け金具

10. ケーブル・マネージメント・アームをサポート・アームに乗せます。ケーブル・マネージメント・アームのピン **(1)** を引き出して、ケーブル・マネージメント・アームのタブ **(2)** をスライド・レールの内側のスロットに滑り込ませます。タブを所定の位置に収まるまで押します。もう一方のケーブル・マネージメント・アームのピン **(3)** を引き出して、そのケーブル・マネージメント・アームのタブをスライド・レールの外側のスロット **(4)** に滑り込ませます。タブを所定の位置に収まるまで押します。

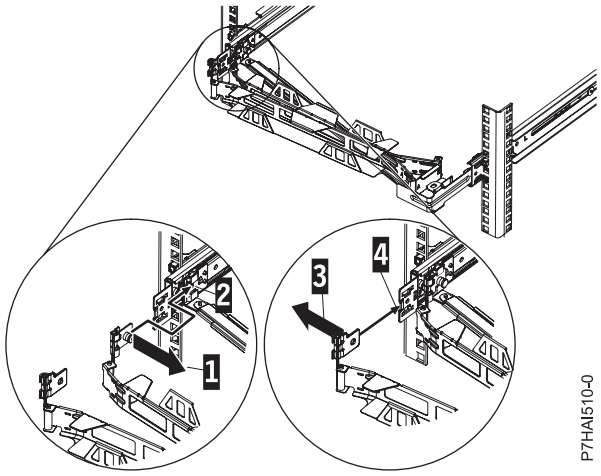


図 24. ケーブル・マネージメント・アームの接続

11. 電源コードおよびその他のケーブル (必要な場合はキーボード、モニター、およびマウス・ケーブルも含む) をサーバーの背面に取り付けます。ケーブルおよび電源コードをケーブル・マネージメント・アーム **(1)** 上に配線して、ケーブル・タイまたは面ファスナーで固定します。

    注: ケーブル・マネージメント・アームが動いたときにケーブルが張りすぎないよう、すべてのケーブルに遊びを持たせます。

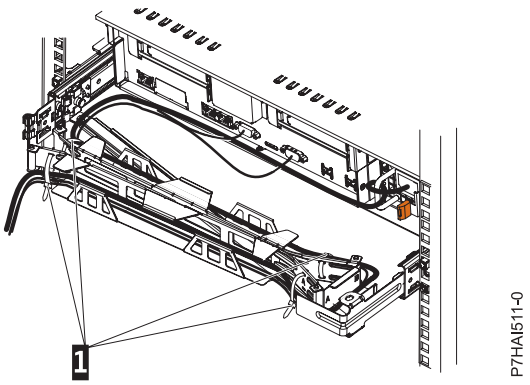


図 25. 電源コードの接続と配線

12. 所定の位置に収まるまで、サーバーをラックの中に滑り込ませます。

モニターおよびキーボードの取り付け

7042-CR6 HMC に付属のモニターおよびキーボードをラックに取り付ける方法について説明します。この作業はお客様が行う作業です。

POWER7 プロセッサー・ベースのシステムの管理に HMC が使用される場合、HMC は CR3 以降であるか、またはラック・マウント HMC モデルでなければなりません。 IBM eServer 7316-TF3 は 17 インチ、フラット・パネル、ラック・マウント型のモニターおよびキーボード・トレイです。さまざまな言語に使用できる特殊なキーボードが、キーボード・トレイ前部の内側に収まります。モニターおよびキーボード・トレイは、ラック・キャビネットで、EIA (Electronics Industries Association) 装置 1 の 1 台分のスペースを使用します。コンソール・スイッチをトレイの後ろに取り付けて、フラット・パネル・モニターおよびキーボードに複数のサーバーを接続することができます。

7042-CR6 HMC をラックに取り付けるには、次のステップを実行します。

重要: ラックにレールを取り付ける手順は複雑です。レールを正しく取り付けるには、各作業を必ず次の順序で行います。

1. 部品目録を確認します。詳しくは、『部品目録の確認』を参照してください。
2. システム装置に組み込まれているラック取り付けハードウェア・キットとシステム・レール・アセンブリーを探します。

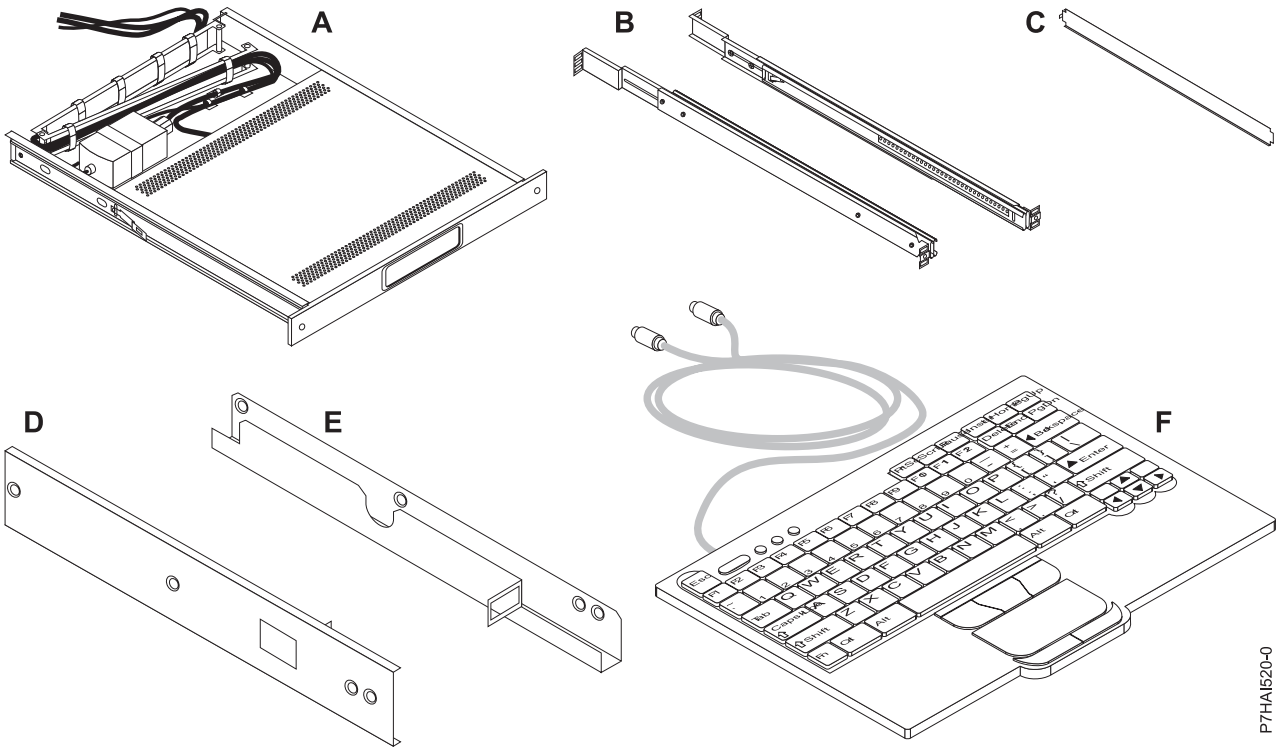


図 26. インストール・キット部品

A キーボード・トレイ (組み込みのフラット・パネル・モニター付き) (1)

B 外部レール (2)

C レール位置合わせスペーサー (1)

D コンソール・スイッチの右サイド取り付け金具 (1)

E コンソール・スイッチの左サイド取り付け金具 (1)

F キーボード (組み込みポインティング・デバイス付き) (1)

G 各種ハードウェアキット: ケージ・ナット 12 個、クリップ・ナット 12 個、プラスねじ 10 個、ねじ (8-32) 4 個、つまみねじ 2 個

H 1.8 m の電源コード (1)

I 2.4 m の国際電気標準会議 (IEC) コネクターの電源ケーブル (1)

J キーボード延長ケーブル (1)

K マウス延長ケーブル (1)

L Windows キーボードおよびマウスのドライバーを含む CD (Eserver pSeries システム、または AIX、Linux、あるいは OS/400 ベースの各システムでは使用できません)

重要: フラット・パネルのラック・マウント型モニターおよびキーボードを取り付けるには、以下のツールを使用します。

- はさみ
- プラス・ドライバー
- マイナス・ドライバー

部品目録の確認

部品目録を確認することが必要な場合があります。

部品目録をまだ確認していない場合は、取り付けを始める前に確認してください。

1. アクセサリー・ボックスにあるキット一式のレポートを確認します。
2. オーダーしたすべての部品を受け取ったか確認します。

部品の間違い、欠落、または損傷がある場合は、IBM 販売店またはIBM 営業およびサポートにご連絡ください。

ラック・マウント・テンプレートを使用せずに位置にマークを付ける

テンプレートを使用せずに、位置にマークを付けることができます。

このシステムには、ラック取り付けテンプレートは組み込まれていません。これらのシステムの高さは、1 EIA 単位です。

取り付け位置を決定するには、以下のステップを完了します。

1. ラック内にシステムを設置する場所を決定します。 EIA 位置を記録します。

   注: ラック上の EIA 装置は 3 つの穴のグループから構成されます。
2. ラックの前面に向き、右側から作業しながら、提供された接着ドットを EIA 装置の上部の穴の隣に付けます。

   注: この接着ドットは、ラック上での位置の識別をしやすくするために使用します。 手持ちのドットがない場合は、他のマーキング用具 (テープ、マーカー、鉛筆など) を、穴の位置の識別のために使用してください。スライド・レールを取り付ける場合は、各 EIA 装置の低い、中央の穴にマークまたは接着ドットを付けます。
3. もう 1 つの接着ドットをその上の EIA 単位の下部の穴の横に貼ります。

   注: 穴を数える場合、最初のドットで印された穴から数え始め、2 つ上の穴を数えます。 2 番目のドットを 3 番目の穴の隣に付けます。
4. ラック左側の対応する穴に対してもステップ 1 (30 ページ) を繰り返します。
5. ラックの背面に回ります。
6. 右側で、ラック前面のマークを付けた下部 EIA 装置に対応する EIA 装置を見つけます。
7. 下部の EIA 装置に接着ドットを付けます。
8. EIA 装置の上部の穴に接着ドットを付けます。
9. ラックの左側で対応する穴にマークを付けます。

モニターおよびキーボードのラックへの取り付け

7042-CR6 HMC に付属しているモニターおよびキーボードをラックに取り付ける方法について説明します。

IBM 7316-TF3 17 インチ、フラット・パネル、ラック・マウント型のモニターおよびキーボードを取り付けるには、ラック・キャビネットで、1.75 インチ (1 EIA) のラック取り付けスペースが必要です。このキットに付属のブラケットを使用して、モニター・コンソール・キットと同じラック取り付けスペースに、オプションのコンソール・スイッチを取り付けることができます。

7042-CR6 HMC のモニターおよびキーボードをラックに取り付けるには、次のステップを実行します。

重要: 取り付け作業が容易になるように、ラック・ドアおよびサイド・パネルを取り外します。

モニターおよびキーボードをラックに取り付けるには、次のステップを実行します。

1. ラックにモニターおよびキーボード・トレイを取り付けるための位置を選択します。詳しくは、『位置のマーク付け』を参照してください。
2. 4 個のケージ・ナット (四角穴のラック・フランジに取り付け) または 4 個のクリップ・ナット (丸穴のラック・フランジに取り付け) を、ラックの前部および後部にある同じ EIA 位置に取り付けます。

   注: オプションのコンソール・スイッチを取り付ける予定である場合は、以下の図に示すように、ケージ・ナットまたはクリップ・ナットを中心後部の位置に取り付けます。

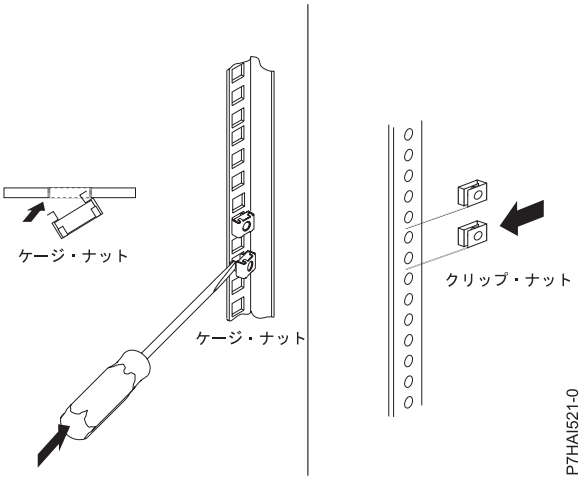


図 27. ケージ・ナットの取り付け

3. 外部スライド・レールにそれぞれ付いている 2 個のレール調整ねじを緩めます。レールを、外側に最大限に引き出します。
4. ラック・キャビネットの奥行きに応じて、外部スライド・レール・ブラケットを調整します。次に、各種ハードウェア・キットの 4 個のねじを使用して、ラック・キャビネットの奥行きに応じてスライド・レール・ブラケットの前部を取り付けます。レールが調整できるように、ねじは指で締めてください。

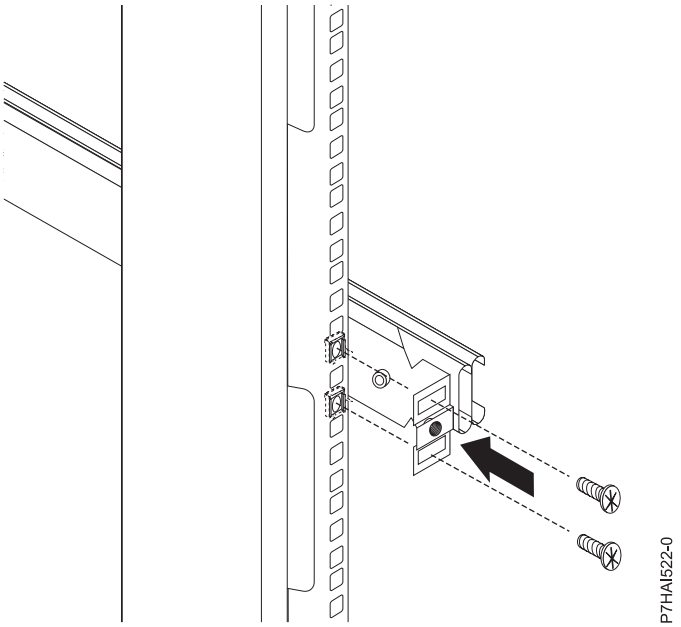


図 28. スライド・レール・ブラケットの調整

注: スライド・レールのブラケットがラック・キャビネット・マウント・フランジの外側になるようにします。スライド・レール・ブラケットの前部または後部にある中央の穴には、ねじを取り付けないでください。これらの穴は、この手順で後からつまみねじまたはオプションのコンソール・スイッチ取り付けブラケットをそれぞれ取り付けるのに使用します。

5. 各種ハードウェア・キットの 4 個のねじを使用し、これらのねじをスライド・レール・ブラケット後部から指で締めて、ラック・キャビネットに固定します。スライド・レールのブラケットがラック・キャビネット・マウント・フランジの外側になるようにします。
6. ステップ 5 でねじを緩めた場合は、各外部スライド・レールの 2 本のレール調整ねじを締めます。
7. レール位置決めスペーサーを、スライド・レールの真ん中の穴に挿入します。レール位置決めスペーサーが、レールに巻きついた状態であることを確認します。前部の 4 本のねじを締め付けて、スペーサーを取り外します。

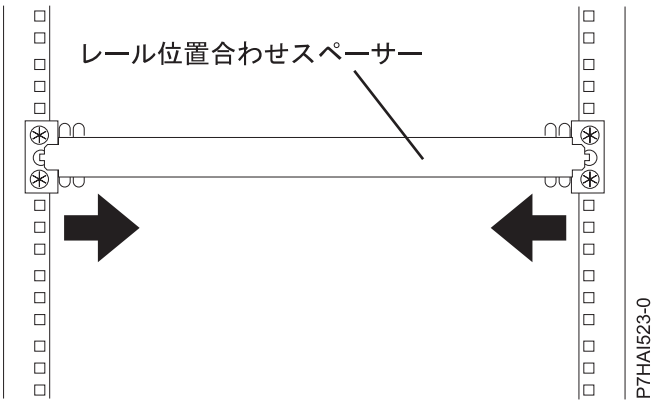


図 29. レール位置決めスペーサーの挿入

8. ラックに取り付けられているレールの内部の部品を引き出してから、ボールベアリング・アセンブリーをレール前部に向かってスライドさせます。

9. フラット・パネル・モニターおよびキーボード・トレイをスライドさせて、レールのボールベアリング・アセンブリーに挿入します。

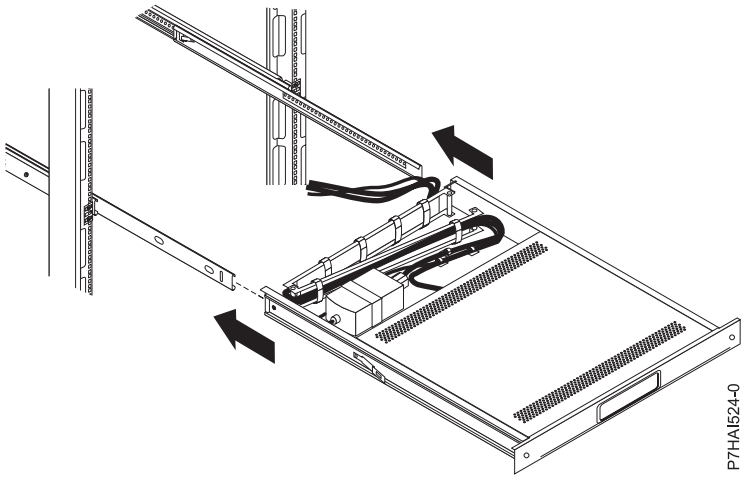


図 30. モニターおよびキーボードをスライドさせる

10. リリース・ラッチを押して、フラット・パネル・モニターおよびキーボード・トレイをラックに完全に押し込みます。ボールベアリング・アセンブリーの位置が内部レールと外部レールの間で調整されるため、始めは少し抵抗を感じる場合もあります。トレイを半分だけ引き出してから押し戻し、トレイをレールに収めます。トレイがレールの中でスムーズに動くように、この動きを何度か繰り返してください。

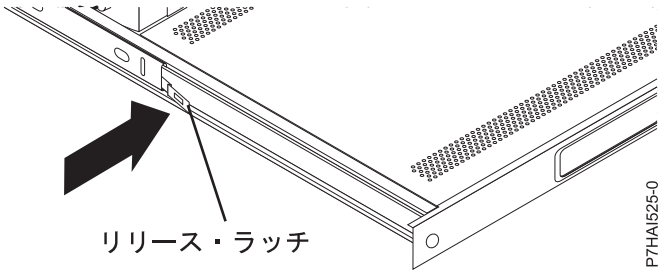


図 31. リリース・ラッチの使用

注:
ビデオ・ケーブルはフラット・パネル・モニターに接続されています。トレイをラック・キャビネットに取り付ける場合は、ビデオ・ケーブルを挟み込んだり切断したりしないようにしてください。

11. トレイをラック内に押し入れて、後部スライド・レール・ブラケットの 4 本のねじを締めます。
12. 安定した平らな面にキーボードを置き、その新しいキーボードの下部の両端に貼り付けられている 2 つのゴム製パッドをはがします。このゴム製パッドは、トレイの下のスペースにまで伸びてしまう可能性があるため、キーボードに貼ったままにしないでください。

注:
キーボード・フットは伸ばしたままにしないでください。フットを出したままにすると、モニターを閉じる時にフラット・パネル・モニター画面が損傷することがあります。

13. トレイをラックから引き出し、レール上に完全に引き出します。

14. フラット・パネル・モニターの前部を持ち上げて、完全に直立した位置に立てます。

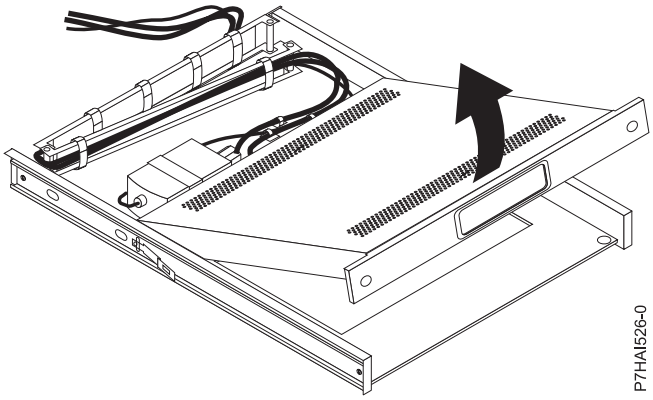


図 32. モニターを直立位置に立てる

15. キーボードをトレイに挿入します。次に、キーボードおよびマウスのケーブルを、トレイ下部のコード・クリップを通してからトレイ右サイドの開口部を通し、さらにケーブル・マネジメント・アームに向けて配線します。ケーブルのたるみを取るように開口部のケーブルを引っぱります。
16. キーボードおよびマウスのケーブルを、モニターの後ろのトレイに配置します。トレイを押し込んで元の位置に戻したときに、ケーブルがラック内にある装置の障害にならないようにしてください。以下のステップでは、ケーブル・マネジメント・アームを使用してケーブルを配線します。
17. モニターを低位置に下げてから、トレイをラックの中に完全に押し込みます。つまみねじを使用して、トレイの前部をラックに固定します。
18. ケーブル・マネジメント・アームをトレイに固定している配送用ストラップを、ラック後部から取り外します。
19. キーボードおよびマウスのケーブルを、ケーブル・マネジメント・アームを通して配線します。既存のケーブル・ストラップを使用して、ケーブルを固定します。
20. ラックの後部に近い方にあるレール調整ねじを、左サイドのレールから取り外します。ねじを使用して、ケーブル・マネジメント・アームをレールに取り付けます。

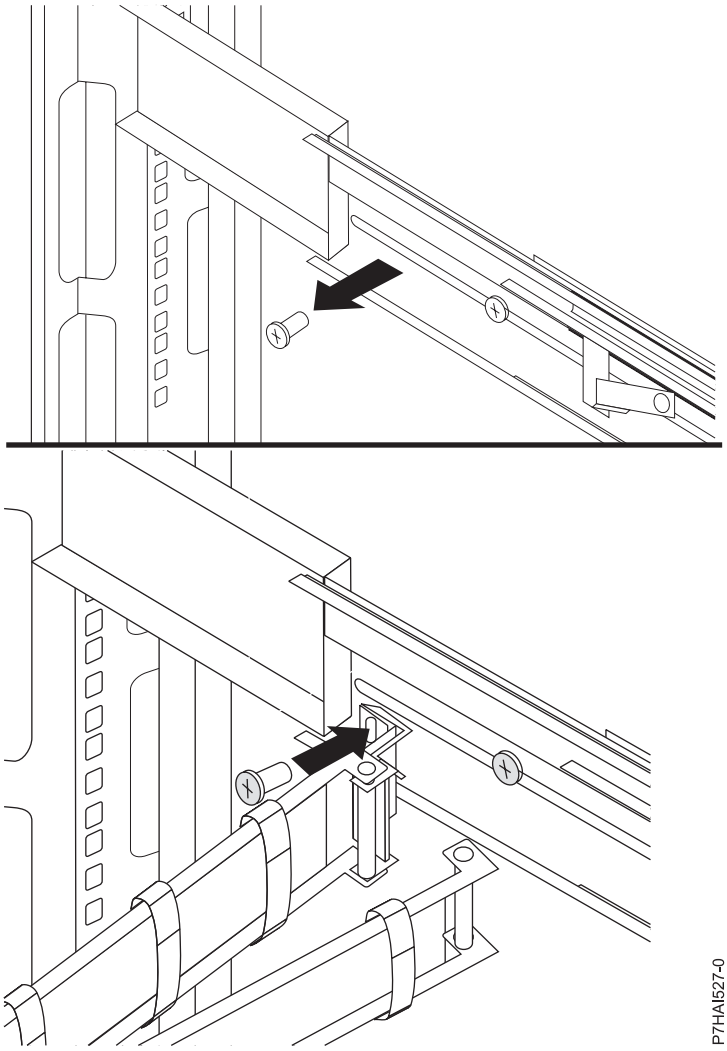


図 33. ケーブル・マネジメント・アームの取り付け

21. ビデオ、キーボード、およびマウスの各コネクターを、ラック・キャビネット内のサーバーあるいはオプションのコンソール・スイッチに接続します。オプションのコンソール・スイッチを取り付ける場合は、『オプションのコンソール・スイッチの取り付け』を参照して、記載されているステップを実行してください。オプションのコンソール・スイッチを取り付けない場合は、ステップ 21 の手順に従って、モニターおよびキーボード・トレイの取り付けを実行します。
22. ケーブル・マネジメント・アーム上のショート・ジャンパー・コードに電源コードを接続します。
23. すべてのケーブルおよび信号コネクターを、適切な装置またはコネクターに接続します。
24. すべての電源スイッチがオフになっていることを確認します。電源コードを、接地済みのコンセントまたは電力配分装置 (PDU) に接続します。

    注: AC 電源コードを DC アダプターのコンセントに接続する場合は、その前に、ローカルの電源供給の電圧が 100 から 240 ボルト AC の範囲であることを確認します。
25. ラック・キャビネットの前部から、トレイを引き出します。ラック・キャビネット内でケーブルを配線し、それらのケーブルをケーブル・ストラップで固定します。

コンソール・スイッチの取り付け (オプション)

オプションのコンソール・スイッチを取り付ける方法について説明します。

コンソール・スイッチを使用すると、単一のモニターとキーボードを複数のサーバーに接続することができます。コンソール・スイッチ・オプションは別個に入手することができますが、スイッチの取り付け金具はインストール・キットに含まれています。

コンソール・スイッチをモニターおよびキーボード・トレイの後ろに取り付けることにより、モニターとキーボード・トレイをラック内の同じスペースに設置することができます。コンソール・スイッチをトレイの後ろに取り付けるには、インストール・キットに付属のブラケットを使用します。

コンソール・スイッチをトレイの後ろに取り付けるには、以下のステップを実行します。

1. 8-32 ねじを 2 本使用して、右サイドおよび左サイドのブラケットを、コンソール・スイッチの右サイドと左サイドにそれぞれ取り付けます。

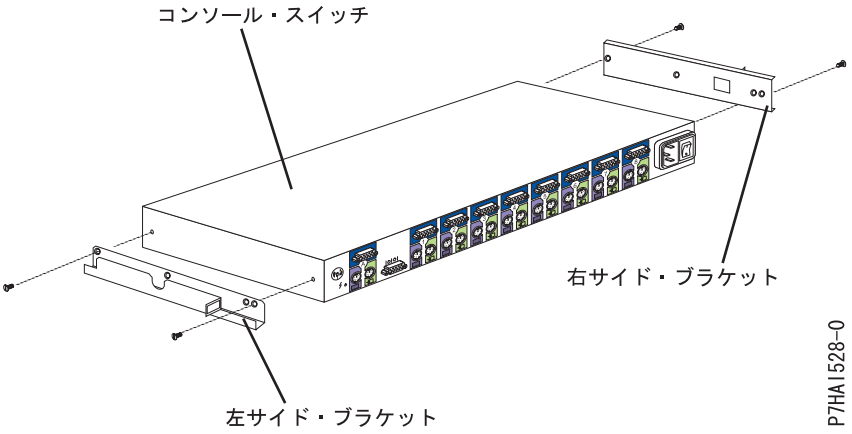


図 34. コンソール・スイッチの取り付け

注: 左サイドのブラケットには、電源、ビデオ、キーボード、およびマウスの各ケーブルを配線するための溝があります。コンソール・スイッチに取り付けた左側ブラケットの溝が、上を向くように取り付けられていることを確認してください。

2. 各種ハードウェア・キットに付属の 4 本のプラスねじ (各サイドに 2 つずつ) を使用して、コンソール・スイッチをフラット・パネルのモニターおよびキーボード・トレイの後ろに取り付けます。
3. 電源、ビデオ、キーボード、およびマウスの各ケーブルを、コンソール・スイッチの左サイド・ブラケットにある溝を通して配線します。次に、ビデオ、キーボード、およびマウスの各コネクターをコンソール・スイッチに接続します。

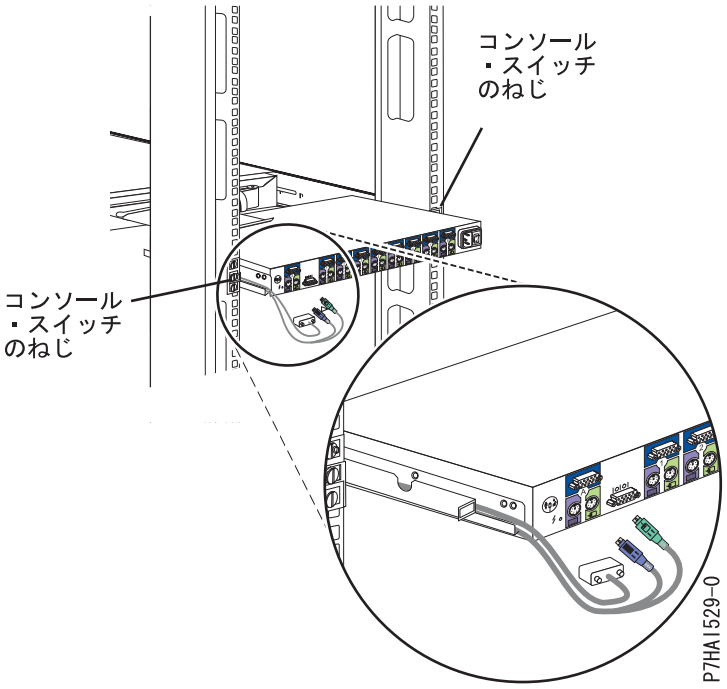


図 35. ケーブル配線

4. 電源コード、ルーティング・ケーブル、およびケーブル・ストラップを接続します。手順については、『ケーブル・マネジメント・アーム上のショート・ジャンパー・コードに電源コードを接続する』を参照してください。

HMC の構成

ネットワーク接続、セキュリティー、サービス・アプリケーション、およびいくつかのユーザー設定を構成します。

HMC 構成に適用するカスタマイズのレベルに応じて、ご使用の HMC を要件に合わせるためのセットアップのオプションがいくつかあります。ガイド付きセットアップ・ウィザードは、HMC のセットアップを容易に行うことができるように設計された HMC のツールです。推奨の HMC 環境を迅速に生成するウィザードを使用する高速パスを選択すること、または、ウィザードのガイドに沿って使用可能な設定をすべて検討することも選択できます。また、HMC メニューを使用した HMC の構成により、ウィザードの支援なしで構成ステップを実行することもできます。

開始する前に、ステップを正常に完了するために必要な構成情報を収集しておく必要があります。必要な情報のリストについては、 18 ページの『HMC 構成の準備』を参照してください。準備が済んだら、 19 ページの『HMC 用のプリインストール構成ワークシート』の作業を完了してから、このセクションに戻ってください。

ガイド付きセットアップ・ウィザードによる高速パスを使用した HMC の構成

ほとんどの場合、HMC は、デフォルト設定値の多くを使用すれば効率的に作動するようにセットアップできます。この高速パスのチェックリストを使用して、サービスを提供できるように HMC を準備してください。各ステップを完了すると、ご使用の HMC はプライベート (直接接続) ネットワーク内の動的ホスト構成プロトコル (DHCP) サーバーとして構成されます。

HMC メニューを使用した HMC の構成

このセクションでは、すべての HMC の構成タスクについての全リストを提示して、HMC の構成プロセスを完了できるようにガイドします。ガイド付きセットアップ・ウィザードを使用したくない場合は、このオプションを選択してください。

構成の設定を有効にするために、HMC を再始動する必要があるので、このチェックリストを印刷して、HMC を構成するときに使用することもできます。

前提条件

HMC メニューを使用した HMC の構成を始める前に、18 ページの『HMC 構成の準備』に説明されている構成の準備作業が完了していることを確認してください。

HMC の始動

HMC にログインして、このインターフェースで表示する言語を選択できます。初めて HMC にログオンするときは、デフォルトのユーザー ID `hscroot` およびパスワード `abc123` を使用します。

HMC を始動するには、次のようにします。

1. 電源ボタンを押して HMC をオンにします。
2. 言語設定として英語を選択する場合は、ステップ 4 から続行します。

   言語設定が英語以外の言語の場合は、ロケール変更のプロンプトが出たら、番号 **2** を入力します。

   注: 処置をとらないと、このプロンプトは、30 秒でタイムアウトになります。
3. 「ロケール選択 (Locale Selection)」ウィンドウで、リストから表示したいロケールを選択して、「**了解**」をクリックします。ロケールは、HMC インターフェースが使用する言語を判別します。
4. 「**ハードウェア管理コンソール Web アプリケーションのログオンと起動**」をクリックします。
5. 以下のデフォルトのユーザー ID およびパスワードを用いて HMC にログインします。

   ID: `hscroot`

   パスワード: `abc123`
6. Enter キーを押します。

日時の変更

バッテリー作動刻時機構で HMC の日付と時刻が保持されます。バッテリーを取り替えた場合、あるいは異なるタイム・ゾーンにシステムを物理的に移動した場合は、コンソールの日付と時刻のリセットが必要になることもあります。 HMC の日付と時刻を変更する方法を理解します。

日付と時刻の情報を変更しても、HMC が管理するシステムと論理区画に影響はありません。

HMC の日付と時刻を変更するには、次のようにします。

1. 以下のいずれかの役割のメンバーであることを確認します。
   - スーパー管理者
   - サービス担当者
   - オペレーター
   - ビューアー
2. ナビゲーション領域で「**HMC管理**」をクリックします。
3. 「コンテンツ」ペインで、「**日付/時刻の変更**」をクリックします。

4. 「**UTC**」を「**クロック (Clock)**」フィールドで選択すると、選択したタイム・ゾーンで夏時間調整が行われている場合、時刻設定は自動的に調整されます。日付、時刻、およびタイム・ゾーンを入力して、「**了解**」をクリックします。

HMC ネットワーク・タイプの構成

管理対象システム、論理区画、リモート・ユーザー、ならびにサービスおよびサポートと通信できるように、ご使用の HMC を構成します。

オープン・ネットワークを使用して管理対象システムに接続するための HMC 設定の構成:

オープン・ネットワークを使用して管理対象システムに接続して管理できるように、HMC を構成します。

オープン・ネットワークを使用して管理対象システムに接続できるように、HMC ネットワーク設定を構成するには、次のようにします。

表 7. オープン・ネットワークを使用して管理対象システムに接続するための HMC 設定の構成

作業	関連情報の入手先
1. 管理対象システムに使用するインターフェースを決定します。**eth0** を使用することをお勧めします。	19 ページの『HMC 用のプリインストール構成ワークシート』
2. ご使用の HMC のイーサネット・ポートを識別します。	58 ページの『eth0 として定義されたイーサネット・ポートの識別』
3. 以下のタスクを実行してイーサネット・アダプターを構成します。	
a. メディア速度を設定します。	60 ページの『メディア速度の設定』
b. オープン・ネットワーク・タイプを選択します。	60 ページの『プライベート・ネットワークまたはオープン・ネットワークの選択』
c. 静的アドレスを設定します。	61 ページの『IPv4 アドレスの設定』
d. ファイアウォールを設定します。	62 ページの『HMC ファイアウォール設定の変更』
e. デフォルト・ゲートウェイを構成します。	63 ページの『デフォルト・ゲートウェイとしての経路指定エントリーの構成』
f. DNS を構成します。	63 ページの『ドメイン名サービスの構成』
4. 追加のアダプターがある場合は、それを構成します。	
5. 管理対象サーバーと HMC との間の接続をテストします。	72 ページの『HMC と管理対象システム間の接続のテスト』

プライベート・ネットワークを使用して管理対象システムに接続するための HMC 設定の構成:

プライベート・ネットワークを使用して管理対象システムに接続して管理できるように、HMC を構成します。

プライベート・ネットワークを使用して管理対象システムに接続できるように、HMC ネットワーク設定を構成するには、次のようにします。

表 8. プライベート・ネットワークを使用して管理対象システムに接続するための HMC 設定の構成

作業	関連情報の入手先
1. 管理対象システムに使用するインターフェースを決定します。	19 ページの『HMC 用のプリインストール構成ワークシート』

表 8. プライベート・ネットワークを使用して管理対象システムに接続するための HMC 設定の構成 (続き)

作業	関連情報の入手先
2. ご使用の HMC のイーサネット・ポートを識別します。	58 ページの『eth0 として定義されたイーサネット・ポートの識別』
3. DHCP サーバーとしてこの HMC を構成します。	60 ページの『DHCP サーバーとしての HMC の構成』
4. 管理対象サーバーと HMC との間の接続をテストします。	72 ページの『HMC と管理対象システム間の接続のテスト』

オープン・ネットワークを使用して論理区画に接続するための HMC 設定の構成:
オープン・ネットワークを使用して論理区画に接続できるように、HMC ネットワーク設定を構成するには、次のようにします。

表 9. オープン・ネットワークを使用して論理区画に接続するための HMC 設定の構成

作業	関連情報の入手先
1. 管理対象システムに使用するインターフェースを決定します。	19 ページの『HMC 用のプリインストール構成ワークシート』
2. ご使用の HMC のイーサネット・ポートを識別します。	58 ページの『eth0 として定義されたイーサネット・ポートの識別』
3. 以下のタスクを実行してイーサネット・アダプターを構成します。	
a. メディア速度を設定します。	60 ページの『メディア速度の設定』
b. オープン・ネットワーク・タイプを選択します。	60 ページの『プライベート・ネットワークまたはオープン・ネットワークの選択』
c. 静的アドレスを設定します。	61 ページの『IPv4 アドレスの設定』
d. ファイアウォールを設定します。	62 ページの『HMC ファイアウォール設定の変更』
e. デフォルト・ゲートウェイを構成します。	63 ページの『デフォルト・ゲートウェイとしての経路指定エントリーの構成』
f. DNS を構成します。	63 ページの『ドメイン名サービスの構成』
4. 追加のアダプターがある場合は、それを構成します。	
5. 管理対象サーバーと HMC との間の接続をテストします。	72 ページの『HMC と管理対象システム間の接続のテスト』

オープン・ネットワークを使用してリモート・ユーザーに接続するための HMC 設定の構成:
オープン・ネットワークを使用してリモート・ユーザーに接続できるように、HMC ネットワーク設定を構成するには、次のようにします。

表 10. オープン・ネットワークを使用してリモート・ユーザーに接続するための HMC 設定の構成

作業	関連情報の入手先
1. 管理対象システムに使用するインターフェースを決定します。	19 ページの『HMC 用のプリインストール構成ワークシート』
2. ご使用の HMC のイーサネット・ポートを識別します。	58 ページの『eth0 として定義されたイーサネット・ポートの識別』
3. 以下のタスクを実行してイーサネット・アダプターを構成します。	
a. メディア速度を設定します。	60 ページの『メディア速度の設定』

表 10. オープン・ネットワークを使用してリモート・ユーザーに接続するための HMC 設定の構成 (続き)

作業	関連情報の入手先
b. オープン・ネットワーク・タイプを選択します。	60 ページの『プライベート・ネットワークまたはオープン・ネットワークの選択』
c. 静的アドレスを設定します。	61 ページの『IPv4 アドレスの設定』
d. ファイアウォールを設定します。	62 ページの『HMC ファイアウォール設定の変更』
e. デフォルト・ゲートウェイを構成します。	63 ページの『デフォルト・ゲートウェイとしての経路指定エントリーの構成』
f. DNS を構成します。	63 ページの『ドメイン名サービスの構成』
g. サフィックスを構成します。	64 ページの『ドメイン・サフィックスの構成』
4. 追加のアダプターがある場合は、それを構成します。	

HMC コール・ホーム・サーバー設定の構成:
HMC コール・ホーム・サーバー設定を構成して問題が報告されるようにするには、以下のようにします。

表 11. HMC コール・ホーム・サーバー設定の構成

タスク	関連情報の入手先
1. 必要なすべてのカスタマー情報が準備されていることを確認します。	19 ページの『HMC 用のプリインストール構成ワークシート』
2. エラーの報告用にこの HMC を構成するか、またはエラーの報告用に既存のコール・ホーム・サーバーを選択します。	66 ページの『ローカル・コンソールを構成してサービス・プロバイダーへエラーを報告する方法』 70 ページの『既存のコール・ホーム・サーバーを選択して、この HMC 用のサービスおよびサポートに接続する方法』
3. コール・ホーム構成が機能しているかどうかを検証します。	70 ページの『サービス・プロバイダーへの接続が機能しているかどうかの検証』
4. 収集されたシステム・データを表示するには、ユーザーに許可を与えます。	70 ページの『収集されたシステム・データを表示するためのユーザーの許可』
5. システム・データの伝送をスケジュールします。	71 ページの『サービス情報の送信』

eth0 として定義されたイーサネット・ポートの識別:

管理対象サーバーとのイーサネット接続は、HMC 上で `eth0` として定義されたイーサネット・ポートを使用して行う必要があります。

HMC をご使用の管理システムの DHCP サーバーとして使用する予定の場合で、HMC の PCI スロットに追加のイーサネット・アダプターを取り付けていない場合は、常に、1 次内蔵イーサネット・ポートがご使用の HMC の `eth0` または `eth1` として定義されます。

PCI スロットに追加のイーサネット・アダプターを取り付けてある場合、`eth0` として定義されるポートは、取り付けているイーサネット・アダプターの位置およびタイプによって異なります。

注: 次に示すのは一般的な規則であり、すべての構成に適用されるわけではありません。

次の表は、HMC タイプごとのイーサネット配置の規則を示したものです。

表 12. HMC タイプおよびイーサネット配置の関連規則

HMC タイプ	イーサネット配置の規則
ラック・マウント HMC、2 つの内蔵イーサネット・ポート付き	HMC は、追加のイーサネット・アダプターを 1 つのみサポートします。 • 追加のイーサネット・アダプターが取り付けられた場合、そのポートは eth0 として定義されます。この場合、1 次内蔵イーサネット・ポートは eth1 として定義され、2 次内蔵イーサネット・ポートは eth2 として定義されます。 • イーサネット・アダプターがデュアル・ポート・イーサネット・アダプターの場合、Act/Link A のラベルが付いたポートは通常 eth0 となります。 Act/link B のラベルが付いたポートは eth1 となります。この場合、1 次内蔵イーサネット・ポートは eth2 として定義され、2 次内蔵イーサネット・ポートは eth3 として定義されます。 • アダプターが取り付けられていない場合は、1 次内蔵イーサネット・ポートが eth0 として定義されます。
スタンドアロン・モデル、単一の内蔵イーサネット・ポート付き	定義は、取り付けたイーサネット・アダプターのタイプによって異なります。 • イーサネット・アダプターが 1 つだけ取り付けられている場合、そのアダプターは eth0 として定義されます。 • イーサネット・アダプターがデュアル・ポート・イーサネット・アダプターの場合、Act/link A のラベルが付いたポートは eth0 となります。 Act/link B のラベルが付いたポートは eth1 となります。この場合は、1 次内蔵イーサネット・ポートが eth2 として定義されます。 • アダプターが取り付けられていない場合は、内蔵イーサネット・ポートが eth0 として定義されます。 • 複数のイーサネット・アダプターが取り付けられている場合は、『イーサネット・アダプターのインターフェース名の判別』を参照してください。

イーサネット・アダプターのインターフェース名の判別:

HMC を DHCP サーバーとして構成する場合、そのサーバーは、HMC が eth0 および eth1 として識別する NIC (ネットワーク・インターフェース・カード) コネクターでのみ作動可能です。イーサネット・ケーブルを接続する必要がある NIC コネクターを判別する必要がある場合があります。ここでは、HMC が eth0 および eth1 として識別する NIC コネクターの判別方法について説明します。

HMC がイーサネット・アダプターに割り当てた名前を判別するには、次のようにします。

1. 制限付きシェル端末を開きます。「**HMC 管理**」 > 「**制限付きシェル端末を開く (Open Restricted Shell Terminal)**」を選択します。
2. コマンド行に tail -f /var/log/messages と入力します。 このメッセージ・ログは、新規イベントが発生するとスクロールします。

3. ご使用のイーサネット・ケーブルを接続します。ケーブルが既に接続されている場合は、プラグを抜き、5 秒待ってから再度接続してください。ケーブルを接続すると、制限付きシェルは、メッセージを表示するためにスクロールします。次の例のエントリーは、このイーサネット・ポートが eth0 として識別されることを示しています: `Aug 28 12:41:20 termite kernel: e1000: eth0: e1000_watchdog: NIC Link is Up 100`.
4. 他のすべてのイーサネット・ポートについてこの手順を繰り返し、その結果を記録してください。
5. Ctrl+C と入力して、**tail** コマンドを停止させます。

メディア速度の設定:

ここでは、イーサネット・アダプターの速度および二重モードなどのメディア速度を指定する方法について説明します。

1. ナビゲーション領域で「**HMC管理**」をクリックします。
2. 「**ネットワーク設定の変更**」をクリックします。
3. 「**LAN アダプター**」タブをクリックします。
4. 処理したい LAN アダプターを選択し、「**詳細**」をクリックします。
5. ローカル・エリア・ネットワークの情報セクションで、「**自動検出 (Autodetection)**」を選択するか、適切なメディア速度と二重モードの組み合わせを選択します。
6. 「**OK**」をクリックします。

プライベート・ネットワークまたはオープン・ネットワークの選択:

プライベート・サービス・ネットワーク は、HMC および管理対象システムで構成されています。プライベート・サービス・ネットワークは、コンソールやそれが管理するシステムに限定されており、貴社のネットワークとは別のものです。オープン・ネットワーク は、ご使用のプライベート・サービス・ネットワークと貴社のネットワークで構成されます。オープン・ネットワークは、コンソールおよび管理対象システムの他にネットワークのエンドポイントを含むことも、複数のサブネットとネットワーク・デバイスにまたがることもできます。

プライベート・ネットワークまたはパブリック・ネットワークを選択するには、次のようにします。

1. ナビゲーション領域で「**HMC管理**」をクリックします。
2. 「**ネットワーク設定の変更**」をクリックします。
3. 「**LAN アダプター**」タブをクリックします。
4. 処理したい LAN アダプターを選択し、「**詳細**」をクリックします。
5. 「**LAN アダプター**」タブをクリックします。
6. 「ローカル・エリア・ネットワーク情報」ページで、「**プライベート**」または「**オープン**」を選択します。
7. 「**OK**」をクリックします。

DHCP サーバーとしての HMC の構成:

動的ホスト構成プロトコル (Dynamic Host Configuration Protocol (DHCP)) は、動的なクライアント構成をするための自動化された方式です。

HMC を DHCP サーバーとして構成するには、次のようにします。

1. ナビゲーション領域で「**HMC管理**」をクリックします。

2. 作業領域で、「**ネットワーク設定の変更**」をクリックします。「ネットワーク設定のカスタマイズ」ウィンドウが開きます。
3. 処理したい LAN アダプターを選択し、「**詳細**」をクリックします。
4. 「**プライベート**」を選択してから、ネットワーク・タイプを選択します。
5. DHCP サーバー・セクションで、「**DHCP サーバーの使用可能化**」を選択し、HMC を DHCP サーバーとして使用可能にします。

   注: HMC を DHCP サーバーとして構成できるのは、プライベート・ネットワーク上のみです。オープン・ネットワークを使用する場合は、「**DHCP を有効にする (Enable DHCP)**」を選択するためのオプションはありません。
6. DHCP サーバーのアドレス範囲を入力します。
7. 「**OK**」をクリックします。

HMC をプライベート・ネットワーク上の DHCP サーバーとして構成した場合、ご使用の HMC DHCP プライベート・ネットワークが正しく構成されているか検証する必要があります。HMC をプライベート・ネットワークに接続する方法については、60 ページの『プライベート・ネットワークまたはオープン・ネットワークの選択』を参照してください。

詳しくは、6 ページの『DHCP サーバーとしての HMC』を参照してください。

IPv4 アドレスの設定:

ここでは、HMC で IPv4 アドレスを設定する方法について説明します。

1. ナビゲーション領域で「**HMC管理**」をクリックします。
2. 「**ネットワーク設定の変更**」をクリックします。
3. 「**LAN アダプター**」タブをクリックします。
4. 処理したい LAN アダプターを選択し、「**詳細**」をクリックします。
5. 「**基本設定**」タブをクリックします。
6. IPv4 アドレスを選択します。
7. 「IP アドレスの指定」を選択した場合は、TCP/IP インターフェース・アドレスおよび TCP/IP インターフェース・ネットワーク・マスクを入力します。
8. 「**OK**」をクリックします。

IPv6 アドレスの設定:

ここでは、HMC で IPv6 アドレスを設定する方法について説明します。

1. ナビゲーション領域で「**HMC管理**」をクリックします。
2. 「**ネットワーク設定の変更**」をクリックします。
3. 「**LAN アダプター**」タブをクリックします。
4. 処理したい LAN アダプターを選択し、「**詳細**」をクリックします。
5. 「**IPv6 設定**」タブをクリックします。
6. 「自動構成」オプションを選択するか、静的 IP アドレスを追加します。
7. IP アドレスを追加した場合は、IPv6 アドレスおよび接頭部長さを入力して「**OK**」をクリックします。
8. 「**OK**」をクリックします。

IPv6 アドレスのみの使用:

HMC が IPv6 アドレスのみを使用するように構成する方法について説明します。

1. ナビゲーション領域で「**HMC管理**」をクリックします。
2. 「**ネットワーク設定の変更**」をクリックします。
3. 「**LAN アダプター**」タブをクリックします。
4. 処理したい LAN アダプターを選択し、「**詳細**」をクリックします。
5. 「**IPv4 アドレスなし (No IPv4 address)**」を選択します。
6. 「**IPv6 設定**」タブをクリックします。
7. 「**DHCPv6 を使用して IP 設定を構成**」を選択するか、静的 IP アドレスを追加します。次に、「**OK**」をクリックします。

「OK」をクリックしたら HMC をリブートして、これらの変更を有効にする必要があります。

HMC ファイアウォール設定の変更

オープン・ネットワークでは、ファイアウォールを使用して、外部から貴社のネットワークへのアクセスを制御します。HMC も、その各々のイーサネット・アダプターにファイアウォールを持っています。 HMC をリモート側で制御するか、またはリモート・アクセスを他に渡す場合は、ご使用のオープン・ネットワークに接続されている HMC 上のイーサネット・アダプターのファイアウォール設定を変更します。

ファイアウォールを構成するために、以下のステップを実行してください。

1. ナビゲーション領域で「**HMC管理**」をクリックします。
2. 「**ネットワーク設定の変更**」をクリックします。
3. 「**LAN アダプター**」タブをクリックします。
4. 処理したい LAN アダプターを選択し、「**詳細**」をクリックします。
5. 「**ファイアウォール**」タブをクリックします。
6. 以下のいずれかの方法を使用すれば、ある特定のアプリケーションを使用する任意の IP アドレスが、ファイアウォールを通れるようにできます。あるいは、1 つ以上の IP アドレスを指定することができます。
   - ある特定のアプリケーションを使用している IP アドレスは、ファイアウォールを通ることができます。
     a. 上部ボックスで、該当のアプリケーションを強調表示します。
     b. 「**着信の許可**」をクリックします。そのアプリケーションが選択されたことを示すために、該当の下部ボックスに表示されます。
   - ファイアウォールを通ることができる IP アドレスを指定します。
     a. 上部ボックスで、アプリケーションを強調表示します。
     b. 「**IP アドレス別の着信許可**」をクリックします。
     c. 「許可されるホスト」ウィンドウで、IP アドレスとネットワーク・マスクを入力します。
     d. 「**追加**」をクリックし、「**了解**」をクリックします。
7. 「**OK**」をクリックします。

制限付きリモート・シェル・アクセスの使用可能化:

ファイアウォールの構成時に、制限付きリモート・シェル・アクセスを使用可能にできます。

制限付きリモート・シェル・アクセスを使用可能にするには、次のようにします。

1. ナビゲーション領域で、「**HMC 管理**」をクリックします。
2. 「**リモート・コマンド実行 (Remote Command Execution)**」をクリックします。
3. 「**ssh 機能を使用してリモート・コマンド実行を可能にする (Enable remote command execution using the ssh facility)**」を選択して、「**OK**」をクリックします。

これで制限付きリモート・シェル・アクセスが使用可能になります。

リモート Web アクセスの使用可能化:

HMC へのリモート Web アクセスを使用可能にできます。

リモート Web アクセスを使用可能にするには、次のようにします。

1. ナビゲーション領域で、「**HMC 管理**」をクリックします。
2. 「**リモート操作 (Remote Operation)**」をクリックします。
3. 「**使用可能**」を選択してから「**OK**」をクリックします。

これでリモート Web アクセスが使用可能になります。

デフォルト・ゲートウェイとしての経路指定エントリーの構成

ここでは、経路指定エントリーをデフォルト・ゲートウェイとして構成する方法について説明します。このタスクは、オープン・ネットワークを用いたものに使用できます。

デフォルト・ゲートウェイとして経路指定エントリーを構成するには、次のようにします。

1. 作業領域で、「**ネットワーク設定の変更**」をクリックします。「ネットワーク設定のカスタマイズ」ウィンドウが開きます。
2. 「**経路指定**」タブをクリックします。
3. 「デフォルト・ゲートウェイ情報」セクションで、デフォルト・ゲートウェイとして設定したい経路指定エントリーのゲートウェイ・アドレスおよびゲートウェイ・デバイスを入力します。
4. 「**OK**」をクリックします。

ドメイン名サービスの構成

オープン・ネットワークをセットアップする予定の場合は、ドメイン名サービスを構成してください。

ドメイン名システム (DNS) は、ホスト名およびそれらに関連するインターネット・プロトコル (IP) アドレスを管理するための分散データベース・システムです。ドメイン名サービスの構成には、DNS の使用可能化、およびドメイン・サフィックスのサーチ順序の指定が含まれます。

1. 作業領域で、「**ネットワーク設定の変更**」をクリックします。「ネットワーク設定の変更」ウィンドウが開きます。
2. 「**ネーム・サービス**」タブをクリックします。
3. 「**DNS 使用可能**」を選択して DNS を使用可能にします。
4. DNS サーバーおよびドメイン・サフィックス・サーチ・オーダーを指定して、「**追加**」をクリックします。

5. 「**OK**」をクリックします。

ドメイン・サフィックスの構成

ドメイン・サフィックスのリストは、リスト内の最初のエントリーで始まる IP アドレスを判別するのに使用されます。

ドメイン・サフィックスは、その IP アドレスを判別するのに役立つように、ホスト名に付加された文字列です。例えば、myname のホスト名が識別できないことがあります。しかし、文字列 myloc.mycompany.com がドメイン・サフィックス・テーブル内のエレメントであれば、 myname.mloc.mycompany.com と識別できる可能性があります。

ドメイン・サフィックス・エントリーを構成するために、以下のステップを実行してください。

1. ナビゲーション領域で、「**HMC 管理**」をクリックします。
2. 作業領域で、「**ネットワーク設定の変更**」をクリックします。「ネットワーク設定のカスタマイズ」ウィンドウが開きます。
3. 「**ネーム・サービス**」タブをクリックします。
4. ドメイン・サフィックス・エントリーとして使用する文字列を入力します。
5. 「**追加**」をクリックして、リストに文字列を追加します。

HMC を構成して、LDAP リモート認証が使用されるようにする方法

ご使用の HMC を構成して、LDAP (Lightweight Directory Access Protocol) リモート認証が使用されるようにすることができます。

ユーザーが HMC にログインすると、最初にローカルのパスワード・ファイルに対して認証が実行されます。ローカルのパスワード・ファイルが検出されない場合、HMC はリモートの LDAP サーバーに接続して認証を行うことができます。LDAP リモート認証が使用されるように、HMC を構成する必要があります。

注: HMC を構成し、LDAP 認証が使用されるようにする場合、その前に HMC と LDAP サーバーの間に正常に機能するネットワーク接続が存在することを確認してください。 HMC ネットワーク接続の構成に関する詳細は、 56 ページの『HMC ネットワーク・タイプの構成』を参照してください。

LDAP 認証が使用されるようにご使用の HMC を構成するには、次を実行してください。

1. ナビゲーション領域で、「**HMC 管理**」をクリックします。
2. コンテンツ領域で、「**LDAP 構成 (LDAP Configuration)**」をクリックします。「LDAP サーバー定義」ウィンドウが開きます。
3. 「**LDAP を使用可能にする (Enable LDAP)**」を選択します。
4. 認証に使用するために、LDAP サーバーを定義します。
5. 認証の対象になるユーザーを識別するのに使用される LDAP 属性を定義します。デフォルトは **uid** ですが、独自の属性を使用することができます。
6. 識別名のツリー (検索ベースとも呼ばれる) を LDAP サーバーに対して定義します。
7. 「**OK**」をクリックします。
8. あるユーザーが LDAP 認証を使用する場合、そのユーザーは自身のプロファイルを構成して、ローカル認証ではなく LDAP リモート認証が使用されるようにする必要があります。

HMC を構成して、Kerberos リモート認証用に鍵配布センター・サーバーが使用されるようにする方法

HMC を構成して、Kerberos リモート認証用に鍵配布センター (KDC) サーバーが使用されるようにすることができます。

ユーザーが HMC にログインすると、最初にローカルのパスワード・ファイルに対して認証が実行されます。ローカルのパスワード・ファイルが検出されない場合、HMC はリモートの Kerberos サーバーに接続して認証を行うことができます。Kerberos リモート認証が使用されるように、HMC を構成する必要があります。

注: HMC を構成し、KDC サーバーを使用して Kerberos リモート認証が行われるようにする場合、その前に HMC と KDC サーバーの間に正常に機能するネットワーク接続が存在することを確認してください。HMC ネットワーク接続の構成に関する詳細は、56 ページの『HMC ネットワーク・タイプの構成』を参照してください。

HMC を構成し、KDC サーバーを使用して Kerberos リモート認証が行われるようにする場合、以下のようにします。

1. HMC の Network Time Protocol (NTP) サービスを使用可能に設定し、同じ NTP サーバーを使用して HMC と KDC サーバーの時間を同期させます。 HMC 上で NTP サービスを使用可能にするには、以下のようにします。
   a. ナビゲーション領域で、「**HMC 管理**」を選択する。
   b. コンテンツ領域で、「**日付/時刻の変更**」を選択する。
   c. 「**NTP 構成 (NTP Configuration)**」タブを選択する。
   d. 「**この HMC で NTP サービスを使用可能にする (Enable NTP service on this HMC)**」を選択する。
   e. 「**OK**」をクリックします。
2. リモートの各 HMC ユーザーのプロファイルを構成し、ローカル認証ではなく Kerberos リモート認証が使用されるようにします。
3. オプション: サービス・キー・ファイルをこの HMC にインポートできます。サービス・キー・ファイルには、KDC サーバーに対して HMC を識別するホスト・プリンシパルが含まれています。サービス・キー・ファイルは、*keytabs* としても知られています。サービス・キー・ファイルをこの HMC にインポートするには、以下のようにします。
   a. ナビゲーション領域で、「**HMC 管理**」を選択する。
   b. コンテンツ領域で、「**KDC の構成 (Configure KDC)**」を選択する。「鍵配布センターの構成 (Key Distribution Center Configuration)」ウィンドウが開きます。
   c. 「**アクション (Actions)**」>「**サービス・キーのインポート (Import Service Key)**」の順に選択する。「サービス・キーのインポート (Import Service Key)」ウィンドウが開きます。
   d. サービス・キー・ファイルの場所を入力する。
   e. 「**OK**」をクリックします。
4. 新規 KDC サーバーをこの HMC に追加する。新規 KDC サーバーをこの HMC に追加するには、以下のようにします。
   a. ナビゲーション領域で、「**HMC 管理**」を選択する。
   b. コンテンツ領域で、「**KDC の構成 (Configure KDC)**」を選択する。「鍵配布センターの構成 (Key Distribution Center Configuration)」ウィンドウが開きます。

c. 「**アクション (Actions)**」>「**KDC サーバーの追加 (Add KDC Server)**」の順に選択する。「サービス・キーのインポート (Import Service Key)」ウィンドウが開きます。
d. KDC サーバーのレルムと、ホスト名または IP アドレスを入力する。
e. 「**OK**」をクリックします。

HMC を構成してサービスおよびサポートに連絡できるようにする方法

HMC を構成して、問題が発生した際に通知を受けるようにすることができます。

HMC を構成し、コール・ホーム・セットアップ・ウィザードを使用してサービス・プロバイダーへ接続できるようにする方法:

HMC を構成し、コール・ホーム・ウィザードを使用してその HMC がコール・ホーム・サーバーとして機能できるようにします。

ここでは、直接 (LAN ベース) および間接 (SSL) のインターネット接続を使用して、HMC をコール・ホーム・サーバーとして構成する際の手順を説明します。

この作業を開始する前に、以下のことを確認してください。

- ネットワーク管理者が、ネットワーク接続が可能であることを検証済みであるかどうか。詳しくは、 18 ページの『HMC 構成の準備』を参照してください。
- プロキシー・サーバー経由のインターネット・サポートを構成する場合は、以下の項目が存在しているかどうか。
  - プロキシー・サーバーの IP アドレスとポート
  - プロキシー認証情報
- **eth1** として指定されたアダプター (オープン・ネットワークとして指定されるもの) が使用されます。詳しくは、 11 ページの『HMC に関するネットワーク設定の選択』を参照してください。
- イーサネット・ケーブルにより HMC が LAN に物理的に接続されているかどうか。

HMC を構成し、コール・ホーム・ウィザードを使用してその HMC がコール・ホーム・サーバーとして機能できるようにするには、以下のようにします。

1. ナビゲーション領域で、「**サービス・マネジメント**」を選択します。
2. コンテンツ領域で、「**コール・ホーム・セットアップ・ウィザード (Call-Home Setup Wizard)**」を選択します。接続およびコール・ホーム・サーバー・ウィザードが開きます。ウィザードの指示に従い、コール・ホームを構成します。

ローカル・コンソールを構成してサービス・プロバイダーへエラーを報告する方法:

この HMC を構成して、LAN 接続、電話またはモデム、あるいは VPN を使用して、エラーをコール・ホーム機能で報告することができます。

HMC を構成し、LAN ベースのインターネットおよび SSL を使用してサービスおよびサポートに連絡する方法:

ここでは、直接 (LAN ベース) および間接 (SSL) のインターネット接続を使用して、HMC をコール・ホーム・サーバーとして構成する方法を説明します。

この作業を開始する前に、以下のことを確認してください。

- ネットワーク管理者が、ネットワーク接続が可能であることを検証済みであるかどうか。詳しくは、 18 ページの『HMC 構成の準備』を参照してください。

- お客様連絡先情報を構成済みであるかどうか。このことを検証するには、HMC インターフェースにアクセスして、「**サービス管理**」>「**お客様情報の管理 (Manage Customer Information)**」をクリックします。
- プロキシー・サーバー経由のインターネット・サポートを構成しようとしている場合は、以下の項目が存在しているかどうか。
  - プロキシー・サーバーの IP アドレスとポート
  - プロキシー認証情報
- 少なくとも 1 つのオープン・ネットワーク・インターフェースが構成されているかどうか。詳しくは、5 ページの『HMC 環境でのプライベート・ネットワークおよびオープン・ネットワーク』を参照してください。
- イーサネット・ケーブルにより HMC が LAN に物理的に接続されているかどうか。

LAN ベースのインターネットと SSL を使用してコール・ホーム・サーバーとして HMC を構成するには、以下を行います。

1. ナビゲーション領域で、「**サービス管理**」をクリックします。
2. 「接続 (Connectivity)」セクションで、「**アウトバウンド接続の管理 (Manage Outbound Connectivity)**」をクリックします。「コール・ホーム・サーバー・コンソール (Call-Home Server Consoles)」ウィンドウが開きます。
3. 「**構成...**」をクリックします。
4. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**ローカル・システムをコール・ホーム・サーバーとして使用可能にする (Enable local system as call-home server)**」にチェック・マークを付けます。
5. 同意内容を受諾します。
6. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**インターネット (Internet)**」タブを選択します。
7. 「**既存インターネット接続をサービス用に許可にする (Allow an existing internet connections for service)**」ボックスにチェック・マークを付けます。
8. SSL プロキシーを使おうとしている場合、「**SSL プロキシーの使用 (Use SSL proxy)**」ボックスにチェック・マークを付けます。
9. SSL プロキシーを使おうとしている場合、プロキシーのアドレスとポートを入力します。この情報はネットワーク管理者から入手してください。
10. 「**SSL プロキシーの使用 (Use SSL proxy)**」にチェック・マークを付けていた場合で、かつ、このプロキシーではユーザー ID とパスワードの認証が必要となる場合は、「**SSL プロキシーを使用した認証 (Authenticate with the SSL proxy)**」ボックスにチェック・マークを付けます。ユーザー ID とパスワードを入力します。ユーザー ID およびパスワードは、ネットワーク管理者から入手してください。
11. 使用する「**インターネットに対するプロトコル (Protocol to Internet)**」を選択します。
12. 「**インターネット (Internet)**」タブで、「**テスト... (Test...)**」をクリックします。
13. 「インターネットのテスト (Test Internet)」ウィンドウで「**開始 (Start)**」をクリックします。
14. テストが正常に完了するか確認します。
15. 「インターネットのテスト (Test Internet)」ウィンドウで「**取消**」をクリックします。
16. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**OK**」をクリックします。

電話とモデムを使用してサービス・プロバイダーに接続する方法:

IBM サポートへのモデム・アクセスを使用して、コール・ホーム・サーバーとして HMC を構成する方法を説明します。

この作業を開始する前に、以下のことを確認してください。

- 専用のアナログ電話回線が使用可能かどうか。
- モデムの構成に必要な情報を持っているかどうか。詳しくは、18 ページの『HMC 構成の準備』を参照してください。
- お客様連絡先情報を構成済みであるかどうか。このことを検証するには、HMC インターフェースにアクセスして、「**サービス管理**」>「**お客様情報の管理 (Manage Customer Information)**」をクリックします。
- 以下の情報が使用可能かどうかを確認します。
  - アナログ回線のタイプ (トーンまたはパルスのどちらか)。大部分の回線はトーンですが、昔の回転式のタイプまたはパルス・タイプがまだ一部使用されている場合があります。
  - その受話器を持ち上げた時に、その回線がダイヤル音を発するかどうか。大部分の回線はダイヤル音を発しますが、そうでない回線がまだ一部使用されている場合があります。
  - アクセス番号文字列が必要かどうか。アクセス番号文字列は 1 つの数字または一連の数字であり、外線にアクセス可能にします。

IBM サポートへのモデム・アクセスを使用してコール・ホーム・サーバーとして HMC を構成するには、以下を行います。

1. ナビゲーション領域で、「**サービス管理**」をクリックします。
2. 「接続 (Connectivity)」セクションで、「**アウトバウンド接続の管理 (Manage Outbound Connectivity)**」をクリックします。
3. 「**構成**」をクリックします。
4. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**ローカル・システムをコール・ホーム・サーバーとして使用可能にする (Enable local system as call-home server)**」を選択します。
5. 同意内容を受諾します。
6. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**ローカル・モデム (Local Modem)**」タブをクリックします。
7. 「ローカル・モデム (Local Modem)」ページで、「**サービス用にローカル・モデム・ダイヤルを許可する (Allow local modem dial for service)**」チェック・ボックスを選択します。
8. 「ローカル・モデム (Local Modem)」ページで、「**モデムの構成 (Modem Configuration)**」チェック・ボックスを選択します。
9. 「モデム設定のカスタマイズ (Customize Modem Settings)」ウィンドウで、「**ダイヤル・タイプ、トーンまたはパルス (Dial type, Tone or Pulse)**」をクリックします。その受話器を持ち上げた時に、その回線がダイヤル音を発した場合は、「**ダイヤル音を待つ (Wait for dial tone)**」チェック・ボックスを選択します。外線のアクセスに必要なすべてのアクセス番号文字列を入力します。
10. 「**OK**」をクリックします。
11. 「ローカル・モデム (Local Modem)」ページで「**追加 (Add)**」をクリックします。
12. リストから番号を選択します。
13. これがローカル番号の場合は、「**電話番号 (Telephone number)**」フィールドから市外局番を除去します。

14. 「電話番号の追加 (Add Telephone Number)」パネルで、「**追加 (Add)**」をクリックします。
15. 「モデム設定のカスタマイズ (Customize Modem Settings)」パネルで、「**テスト (Test)**」をクリックします。
16. 「電話番号のテスト (Test Telephone Number)」パネルで、「**開始 (Start)**」をクリックします。
17. テストが正常に完了するか確認します。
18. 「電話番号のテスト (Test Telephone Number)」ウィンドウで「**取消**」をクリックします。
19. 最大 5 つの電話番号を構成可能です。最低でも 2 つの電話番号 (プライマリーとバックアップ) を構成してください。これらの番号は、それを構成した順序で使用されることになります。呼び出し可能リストに番号を追加するには、この手順にある各ステップを繰り返します。
20. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**OK**」をクリックします。

LAN ベースの VPN を使用してサービス・プロバイダーへ接続する方法:

VPN を使用してコール・ホーム・サーバーを構成します。

この作業を開始する前に、以下のことを確認してください。

- ネットワーク管理者が、ネットワーク接続が可能であることを検証済みであるかどうか。詳しくは、 18 ページの『HMC 構成の準備』を参照してください。
- **eth1** として指定されたアダプター (オープン・ネットワークとして指定されるもの) が使用されます。詳しくは、 11 ページの『HMC に関するネットワーク設定の選択』を参照してください。
- イーサネット・ケーブルにより HMC が LAN に物理的に接続されているかどうか。
- お客様連絡先情報を構成済みであるかどうか。この状態を検証するには、HMC インターフェースで、「**サービス管理**」>「**お客様情報の管理 (Manage Customer Information)**」をクリックします。

VPN を使用してコール・ホーム・サーバーを構成するには、以下を行います。

1. ナビゲーション領域で、「**サービス管理**」をクリックします。
2. 「接続 (Connectivity)」セクションで、「**アウトバウンド接続の管理 (Manage Outbound Connectivity)**」をクリックします。
3. 「**構成**」をクリックします。
4. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**ローカル・システムをコール・ホーム・サーバーとして使用可能にする (Enable local system as call-home server)**」を選択します。
5. 同意内容を受諾します。
6. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**インターネット VPN (Internet VPN)**」タブをクリックします。
7. 「インターネット VPN (Internet VPN)」ページで、「**VPN と既存インターネット接続をサービス用に許可する (Allow A VPN and an existing Internet connections for service)**」を選択します。
8. 「インターネット VPN (Internet VPN)」ページで、「**テスト (Test)**」チェック・ボックスをクリックします。
9. 「インターネット VPN のテスト (Test Internet VPN)」ウィンドウで「**開始 (Start)**」をクリックします。
10. テストが正常に完了するか確認します。
11. 「インターネット VPN のテスト (Test Internet VPN)」ウィンドウで「**取消**」をクリックします。

12. 「アウトバウンド接続の設定 (Outbound Connectivity Settings)」ウィンドウで、「**OK**」をクリックします。

既存のコール・ホーム・サーバーを選択して、この HMC 用のサービスおよびサポートに接続する方法:

エラーを報告するために既存の HMC コール・ホーム・サーバーを選択する際には、この HMC が認識済み、または検出済みのものを選択します。

検出済みの HMC とは、コール・ホーム・サーバーとして使用可能な HMC と、この HMC と同じサブネット上にあるか、同じ管理対象システムを管理するか、いずれかの HMC のことです。

検出済みの HMC を選択して、この HMC がエラーを報告する際にコール・ホーム機能を使用するには、以下のようにします。

1. ナビゲーション領域で、「**サービス管理**」をクリックします。
2. コンテンツ領域で、「**アウトバウンド接続の管理 (Manage Outbound Connectivity)**」をクリックします。「コール・ホーム・サーバー・コンソール (Call-Home Server Consoles)」ウィンドウが開きます。
3. 「**検出済みコール・ホーム・サーバー・コンソールを使用する (Use discovered call-home server consoles)**」をクリックします。 HMC によって、コール・ホーム用に構成された HMC の IP アドレスまたはホスト名が表示されます。
4. 「**OK**」をクリックします。

注: バージョン 7.1.0 未満の HMC は、バージョン 7.1.0 以上の HMC でコール・ホーム・プロキシー・サーバーとして追加することはできません。

別のサブネット上にある既存の HMC コール・ホーム・サーバーを、手動で追加することもできます。コール・ホーム用に構成された HMC の IP アドレスまたはホスト名を選択し、「**追加**」をクリックします。次に、「**OK**」をクリックします。

サービス・プロバイダーへの接続が機能しているかどうかの検証:

サービスおよびサポートへの接続が機能していることを確認するために問題報告機能をテストします。

コール・ホーム構成が機能しているかどうかを検証するには、以下を行います。

1. ナビゲーション領域で、「**サービス管理**」をクリックします。
2. 作業領域で、「**イベントの作成 (Create Event)**」をクリックします。
3. 「**自動的な問題報告のテスト (Test Automatic problem Reporting)**」を選択し、コメントを入力します。
4. 「**サービスの要求**」をクリックします。その要求が送信されるのを数分待ちます。
5. 「サービス管理」ウィンドウで、「**イベントの管理**」を選択します。
6. 「**すべてのオープン状態の問題 (All open problems)**」を選択します。
7. オープン状態だった問題番号に割り当てられた、PMH イベントと PMH 番号があるかどうかをチェックします。
8. そのイベントを選択し、「**クローズ (Close)**」を選択します。
9. 「クローズ (Close)」ウィンドウで、氏名と短いコメントを入力します。

収集されたシステム・データを表示するためのユーザーの許可:

ご使用のシステムに関するデータを表示するには、ユーザーに許可を与える必要があります。

収集されたシステム・データを表示するためにユーザーに許可を与えるには、その前に IBM ID を取得する必要があります。 IBM ID の取得について、詳しくは 19 ページの『HMC 用のプリインストール構成ワークシート』を参照してください。

収集されたシステム・データを表示するためにユーザーに許可を与えるには、以下のようにします。

1. ナビゲーション領域で、「**サービス管理**」を選択します。
2. コンテンツ領域で、「**ユーザーの許可 (Authorize User)**」を選択します。
3. IBM ID を入力します。
4. 「**OK**」をクリックします。

サービス情報の送信:

サービス・プロバイダーに直接情報を送信すること、および情報が定期的に送信されるようにスケジュールすることが可能です。

IBM はパーソナライズされた Web 機能を提供して、その機能で、IBM エレクトロニック・サービス・エージェントが収集した情報を使用します。これらの機能を使用するには、まず最初に、IBM 登録 Web サイト (http://www.ibm.com/account/profile) で登録を行う必要があります。ユーザーによるエレクトロニック・サービス・エージェント情報の使用を許可して Web 機能をパーソナライズするには、 70 ページの『収集されたシステム・データを表示するためのユーザーの許可』を参照してください。IBM ID をご使用のシステムに登録する利点に関して、詳細は http://www.ibm.com/support/electronicを参照してください。

注: サービス・プロバイダー情報は、HMC を使用するためインストールおよび構成したら直ちに送信する必要があります。

サービス情報を送信するには、以下のようにします。

1. ナビゲーション領域で、「**サービス管理**」をクリックします。
2. コンテンツ領域で、「**サービス情報の送信 (Transmit Service Information)**」をクリックします。
3. 「サービス情報の送信 (Transmit Service Information)」ウィンドウのタスクを完了し、「**OK**」をクリックします。

管理対象システムに対するパスワードの設定

ご使用のサーバーおよび拡張システム管理 (ASM) の両方にパスワードを設定する必要があります。ここでは、HMC インターフェースの使用方法および上記パスワードの設定方法について説明します。

「認証は保留中です」のメッセージを受け取った場合は、管理対象システムのパスワードを設定するよう、HMC からプロンプトが出されます。

「認証は保留中です」のメッセージを受け取らなかった場合は、管理対象システムのパスワードを設定するために以下のステップを完了してください。

サーバー・パスワードの更新:

サーバー・パスワードを更新するには、次のようにします。

1. ナビゲーション領域で、管理対象システムを選択します。
2. 「タスク」領域で、「**操作**」をクリックします。
3. 「**パスワードの変更**」をクリックします。「パスワードの更新 (Update Password)」ウィンドウが表示されます。
4. 必要な情報を入力し、「**了解**」をクリックします。

拡張システム管理 (ASM) の汎用パスワードの更新:

注: 一般ユーザー ID 用のデフォルトのパスワードは `general` で、管理者 ID 用のデフォルトのパスワードは `admin` です。

ASM の汎用パスワードを更新するには、次のようにします。

1. HMC のナビゲーション領域で、管理対象システムを選択します。
2. 「タスク」領域で、「**操作**」をクリックします。
3. 「**拡張システム管理 (ASM)**」をクリックします。「ASM インターフェースの起動 (Launch ASM Interface)」ウィンドウが開きます。
4. 「サービス・プロセッサー IP アドレスの選択 (Select a Service Processor IP Address)」を選択して、「**OK**」をクリックします。ASM インターフェースが表示されます。
5. 「ASMI へようこそ」ペインで、ご使用のユーザー ID とパスワードを入力して、「**ログイン**」をクリックします。
6. ナビゲーション領域で、「**ログイン・プロファイル**」を展開します。
7. 「**パスワードの変更**」を選択します。
8. 必要な情報を指定して、「**続行**」をクリックします。

拡張システム管理 (ASM) 管理者パスワードの再設定:
管理者パスワードを再設定するには、認定サービス・プロバイダーに連絡してください。

HMC と管理対象システム間の接続のテスト

このオプションで、ネットワークに適切に接続されているかどうかを検証できます。

ネットワーク接続をテストするには、以下のいずれかの役割のメンバーでなければなりません。

- スーパー管理者
- サービス担当者

HMC と管理システム間の接続をテストするには、次のようにします。

1. ナビゲーション領域で「**HMC管理**」をクリックします。
2. 「**ネットワーク接続性のテスト**」をクリックします。
3. 「Ping」タブには、接続対象の全システムのホスト名または IP アドレスを入力します。オープン・ネットワークをテストするには、ゲートウェイを入力します。「**Ping**」をクリックします。

まだ論理区画を作成していない場合は、アドレスを ping することはできません。サーバーに論理区画を作成するために HMC を使用することができます。「論理区画化」の PDF ファイル (サイズは約 1 MB) を表示するには、http://publib.boulder.ibm.com/infocenter/systems/scope/hw/topic/p7hat/p7hat.pdf を参照してください。.

ネットワーク内で HMC をどのように使用できるかを理解するには、3 ページの『HMC ネットワーク接続』を参照してください。

HMC をネットワークに接続できるように構成することについて詳しくは、55 ページの『HMC メニューを使用した HMC の構成』を参照してください。

構成完了後のステップ

HMC を取り付けて構成したら、必要に応じて HMC データをバックアップしてください。

重要な HMC データのバックアップ

重要なコンソール情報は、USB フラッシュ・メモリー・デバイス、DVD にバックアップ、FTP を介してバックアップ、あるいはネットワークを使用してバックアップできます。

HMC を使用して、次のようなすべての重要なデータをバックアップできます。

- ユーザー設定ファイル
- ユーザー情報
- HMC プラットフォーム構成ファイル
- HMC ログ・ファイル
- 修正サービスのインストールによる HMC 更新

バックアップ機能では、 HMC ハード・ディスク上に格納された HMC データを以下に保存します。

- DVD メディア
- USB フラッシュ・メモリー・デバイス
- HMC ファイル・システム (NFS など) にマウントされたリモート・システム
- FTP を介したリモート・サイト

HMC または論理区画に関連した情報に変更を加えた後で HMC をバックアップします。

注: データを取り外し可能メディアに保管するためには、メディアがフォーマット済みでなければなりません。メディアをフォーマットするには、「**HMC 管理**」>「**メディアのフォーマット**」をクリックし、手順に従ってください。

HMC をバックアップするには、次のいずれかの役割のメンバーである必要があります。

- スーパー管理者
- オペレーター
- サービス担当者

重要な HMC データをバックアップするには、以下のようにします。

1. ナビゲーション領域で、「**HMC 管理**」をクリックします。
2. 「**HMC データのバックアップ**」を選択する。
3. アーカイブ・オプションを選択する。 ローカル・システム上のメディアへのバックアップ、マウントされたリモート・システムへのバックアップ、またはバックアップ・データのリモート・サイトへの送信が可能です。
4. データをバックアップするには、ウィンドウ上の指示に従ってください。

HMC ハード・ディスク全体のリモート・システムへのバックアップ

HMC を使用して、HMC のハード・ディスク全体をリモート・システムにバックアップすることができます。

ご使用のリモート・システムには、ネットワーク・ファイルシステム (NFS) またはセキュア・シェル (ssh) を構成しておく必要があり、このネットワークは HMC からアクセス可能でなければなりません。このタスクを完了するには、HMC をシャットダウンして、リブートする必要があります。 HMC のみを使用してこれらのタスクを実行してください。

HMC ハード・ディスクをリモート・システムにバックアップするには、次のいずれかの役割のメンバーである必要があります。

- スーパー管理者
- オペレーター
- サービス担当者

HMC ハード・ディスクをリモート・システムにバックアップするには、次のようにします。

1. HMC 上の各ネットワーク・アダプターのインターフェース番号 (例えば eth0、eth1 など)、MAC アドレス、および IP アドレスを記録します。この作業を行うには、「**HMC 管理**」>「**ネットワーク設定の変更**」>「**LAN アダプター**」の順にクリックします。
2. HMC をシャットダウンして、電源オフします。
3. DVD ドライブに HMC リカバリー・メディア を入れた状態で、HMC コンソールを電源オンします。HMC インターフェースを構成済みのネットワーク・ブート・サーバーから始動させたい場合は、ネットワーク・インターフェースが起動順序にあるデバイスの 1 つであることを確認してください。起動デバイスのリストを表示するには、HMC を電源オンするときに F12 を押し、ブートしたいネットワーク・インターフェースを選択します。
4. バックアップ・オプションを選択して、「**次へ**」をクリックします。
5. リモート・サーバーと通信するために使用するネットワーク・インターフェースを選択します。ネットワーク・ブート・サーバーにコンタクトすることにより HMC を始動しており、このサーバーがデータのバックアップ先のリモート・サーバーでもある場合は、デフォルト設定を選択します。次に「**次へ**」をクリックしてステップ 7 に進みます。デフォルト設定を選択しない場合は、次のステップを続行します。

   注: インターフェース番号 (eth0、eth1) は、ステップ 1 で記録した番号と異なる場合があります。リストされた MAC アドレスを使用して、目的のインターフェースを識別できます。詳しくは、 58 ページの『eth0 として定義されたイーサネット・ポートの識別』を参照してください。
6. デフォルト設定を選択しない場合は、選択済みのインターフェースを用いて、使用するネットワーク・プロトコルを選択する必要があります。ご使用のネットワーク内の DHCP サーバーから IP アドレスを取得するか、選択済みのネットワーク・インターフェースに静的 IP アドレスを割り当てるよう選択できます。選択を行い、「**次へ**」をクリックします。
7. デフォルト設定を選択しなかった場合は、リモート・サーバーの IP アドレスまたはホスト名を入力します。gzip 圧縮ユーティリティーおよび **tar** コマンドを使用して、バックアップ・ファイルが作成されます。「**リモート・ホスト上のファイル (File on remote host)**」フィールドで .tgz 拡張子を持つファイルを指定してください。デフォルトのネットワーク設定を選択した場合は、ネットワーク・ブート構成にあるディレクトリー・セットアップを使用する必要があります。この情報は、「**リモート・ホスト上のファイル (File on remote host)**」フィールドに表示されます。必要な情報をすべて完了したら、「**次へ**」をクリックします。
8. HMC からリモート・サーバーにデータを転送するのに使用する方法を選択します。データの暗号化を選択する場合は、リモート・ホストでセキュア・シェル (SSH) サーバーが実行中である必要があります。暗号化を使用せずにデータを転送することを選択する場合は、リモート・ホストでネットワーク・ファイル・サーバー (NFS) が実行中である必要があり、データのバックアップ先のディレクトリーが、書き込みアクセスのためにエクスポートされる必要があります。選択を行い、「**次へ**」をクリックします。
9. 暗号化を使用してデータを転送することを選択する場合は、リモート・サーバーのユーザー ID およびパスワードを入力する必要があります。

10. 入力した情報が正しいことを確認し、「**完了**」をクリックします。バックアップが完了すると、HMC インターフェースが表示されます。

HMC を電源オンしたときに F1 を押して起動順序を変更した場合は、HMC をリブートして、設定を再び変更する必要があります。起動順序を変更する際、起動順序でハード・ディスクがネットワーク・インターフェースの前にリストされることを確認してください。

HMC マシン・コードの更新、アップグレード、および移行

HMC に対する更新およびアップグレードは、新機能の追加や既存機能の改良のために、定期的にリリースされます。HMC マシン・コードの更新、アップグレード、および移行の間の相違点について詳しく説明します。また、HMC マシン・コードを更新、アップグレード、または移行する方法についても説明します。

これらの各タスクの終了時には、HMC はリブートされますが、区画はリブートされません。

HMC コードの更新
既存の HMC レベルに対して保守を適用します。

「**アップグレード・データの保管**」タスクを実行する必要はありません。

HMC コードのアップグレード
HMC ソフトウェアを同じプログラムの新規リリース・レベルまたは修正レベルに置き換えます。

リカバリー・メディアからブートする必要があります。

HMC コードの移行
ある HMC バージョンから別の HMC バージョンに HMC データを移します。

移行はアップグレードの一種です。

HMC マシン・コードのバージョンおよびリリースの判別

HMC マシン・コードのバージョンおよびリリースを表示する方法を説明します。

HMC マシン・コードのレベルによって、並行サーバー・ファームウェア保守や、新規リリースへのアップグレードの機能拡張など、使用できる機能が異なります。

HMC マシン・コードのバージョンおよびリリースを表示するには、次のようにします。

1. ナビゲーション領域で「**更新**」をクリックします。
2. 作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に表示される情報を見て記録します。この情報には、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが含まれています。

インターネット接続を使用した HMC のマシン・コードの更新の入手および適用

インターネット接続が可能な HMC の場合に、その HMC 用のマシン・コードの更新を入手する方法を説明します。

HMC 用のマシン・コードの更新を入手するには、ステップ 1 から 5 を実行します。

ステップ 1. インターネットに接続していることを確認する

サービスおよびサポートのシステムまたは Web サイトから、ご使用の HMC またはサーバーに更新をダウンロードするには、以下のいずれかが必要です。

- SSL プロキシーを使用している、または使用していない SSL 接続
- インターネット VPN

インターネットに接続していることを確認して、次のようにします。

1. ナビゲーション領域で、「**サービス管理**」をクリックします。
2. 「**アウトバウンド接続の管理**」を選択する。
3. HMC 用に選択したアウトバウンド接続タイプに対するタブを選択する (インターネット VPN、または SSL 接続)。

   注: サービスおよびサポートへの接続が存在しない場合、この手順を進める前にサービス接続をセットアップします。サービスおよびサポートへの接続をセットアップする方法の説明は、「IBM サービスおよびサポートに接続するためのサーバーのセットアップ」を参照してください。
4. 「**テスト**」をクリックする。
5. テストが正常に完了するか確認します。 テストが正常でない場合、この手順を進める前に、接続のトラブルシューティングを行い、問題を修復します。代替方法として、更新を DVD で入手することもできます。
6. 『ステップ 2. 既存の HMC マシン・コード・レベルを表示する』から続行する。

ステップ 2. 既存の HMC マシン・コード・レベルを表示する

既存の HMC マシン・コード・レベルを表示するには、次のようにします。

1. ナビゲーション領域で「**更新**」をクリックします。
2. 作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に表示される情報を見て記録する。この情報には、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが含まれています。
3. 『ステップ 3. 使用可能な HMC マシン・コード・レベルを表示する』から続行する。

ステップ 3. 使用可能な HMC マシン・コード・レベルを表示する

使用可能な HMC マシン・コード・レベルを表示するには、次のようにします。

1. インターネットに接続したコンピューターまたはサーバーから、http://www.ibm.com/eserver/support/fixes にアクセスする。
2. 「プロダクト・ファミリー (Product family)」リストで、該当するファミリーを選択する。
3. 「製品またはフィックス・タイプ (Product or fix type)」リストで、「**ハードウェア管理コンソール (Hardware Management Console)**」を選択する。
4. 「**続行**」をクリックします。 「ハードウェア管理コンソール」サイトが表示されます。
5. ご使用の HMC バージョン・レベルが表示されるまでスクロールダウンして、使用可能な HMC レベルを表示する。

   注: あるいは、サービスおよびサポートにお問い合わせいただくこともできます。
6. 『ステップ 4. HMC マシン・コードの更新を適用する』から続行する。

ステップ 4. HMC マシン・コードの更新を適用する

HMC マシン・コードの更新を適用するには、次のようにします。

1. HMC マシン・コードの更新をインストールする前に、ご使用の HMC 上の重要なコンソール情報のバックアップを取る。 手順については、 73 ページの『重要な HMC データのバックアップ』を参照してください。その後に、次のステップから続行します。

2. ナビゲーション領域で「**更新**」をクリックします。
3. 「**HMC の更新**」をクリックする。「修正サービスのインストール」ウィザードが開きます。
4. ウィザードの指示に従って、更新をインストールする。
5. HMC をシャットダウンしてから再始動して、更新を有効にする。
6. 「**ハードウェア管理コンソール Web アプリケーションのログオンと起動**」をクリックします。
7. HMC インターフェースにログインします。

ステップ 5. HMC マシン・コードの更新が正常にインストールされたことを確認する

HMC マシン・コードの更新が正常にインストールされたことを確認するには、次のようにします。

1. ナビゲーション領域で「**更新**」をクリックします。
2. 作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが表示されます。
3. バージョンおよびリリースが、インストールした更新と一致することを確認します。
4. 表示されているコードのレベルがインストールしたレベルでない場合は、次のステップを実行する。
   a. HMC 上のネットワーク接続を選択する。
   b. 別のリポジトリーを使用してファームウェア更新を再試行する。
   c. 問題が解決しない場合は、次のレベルのサポートに連絡する。

DVD または FTP サーバーを使用した HMC 用マシン・コードの更新の入手および適用

DVD または FTP サーバーを使用して HMC 用マシン・コード更新を入手する方法を説明します。

HMC マシン・コード更新を入手するには、ステップ 1 から 5 を実行します。

ステップ 1. 既存の HMC マシン・コード・レベルを表示する

既存の HMC マシン・コード・レベルを表示するには、次のようにします。

1. ナビゲーション領域で「**更新**」をクリックします。
2. 作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に表示される情報を見て記録する。この情報には、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが含まれています。
3. 『ステップ 2. 使用可能な HMC マシン・コード・レベルを表示する』から続行する。

ステップ 2. 使用可能な HMC マシン・コード・レベルを表示する

使用可能な HMC マシン・コード・レベルを表示するには、次のようにします。

1. インターネットに接続したコンピューターまたはサーバーから、ハードウェア管理コンソール Web サイト (http://www-933.ibm.com/support/fixcentral/) にアクセスする。
2. ご使用の HMC バージョン・レベルが表示されるまでスクロールダウンして、使用可能な HMC レベルを表示する。

   注: あるいは、IBM サービスおよびサポートにお問い合わせいただくこともできます。
3. 『ステップ 3. HMC マシン・コードの更新を入手する』から続行する。

ステップ 3. HMC マシン・コードの更新を入手する

HMC マシン・コードの更新を入手するには、次のようにします。

フィックス・セントラル (Fix Central) Web サイトから HMC マシン・コードの更新を注文できます。サービスおよびサポートに連絡するか、あるいは FTP サーバーにダウンロードすることができます。

フィックス・セントラル (Fix Central) Web サイトから HMC マシン・コードの更新を注文する方法

1. インターネットに接続したコンピューターまたはサーバーから、ハードウェア管理コンソール Web サイト (http://www-933.ibm.com/support/fixcentral/) にアクセスする。
2. 「サポートされる HMC プロダクト (Supported HMC products)」の下で、HMC の最新レベルを選択する。
3. ファイル名/パッケージ領域までスクロールダウンして、注文したい更新を検索する。
4. 「注文 (Order)」列で、「**実行 (Go)**」を選択する。
5. 「**続行 (Continue)**」をクリックして、ご使用の IBM ID を指定してサインインする。
6. 表示されるプロンプトのとおりに行って、注文を送信する。

取り外し可能メディアへ HMC マシン・コード更新をダウンロードする方法

1. インターネットに接続したコンピューターまたはサーバーから、ハードウェア管理コンソール Web サイト (http://www-933.ibm.com/support/fixcentral/) にアクセスする。
2. 「サポートされる HMC プロダクト (Supported HMC products)」の下で、HMC の最新レベルを選択する。
3. ファイル名/パッケージ領域までスクロールダウンして、ダウンロードしたい更新を検索する。
4. ダウンロード対象の更新情報をクリックする。
5. ご使用条件を受諾して、取り外し可能メディアに更新情報を保存する。

完了したら、『ステップ 4. HMC マシン・コードの更新を適用する』から続行する。

ステップ 4. HMC マシン・コードの更新を適用する

HMC マシン・コードの更新を適用するには、次のようにします。

1. HMC マシン・コードの更新をインストールする前に、HMC データのバックアップを取る。詳しくは、73 ページの『重要な HMC データのバックアップ』を参照してください。
2. 更新を収めた DVD-RAM を入手または作成した場合は、HMC の DVD ドライブにその DVD-RAM を挿入する。更新を収めた USB メモリー・デバイスを入手または作成した場合は、そのメモリー・デバイスを挿入する。
3. ナビゲーション領域で「**更新**」をクリックします。
4. 「**HMC の更新**」をクリックする。「HMC 修正サービスのインストール」ウィザードが開きます。
5. ウィザードの指示に従って、更新をインストールする。
6. シャットダウン、再始動、および HMC へ再ログインして、更新を有効にする。
7. 『ステップ 5. HMC マシン・コードの更新が正常にインストールされたことを確認する』から続行する。

ステップ 5. HMC マシン・コードの更新が正常にインストールされたことを確認する

HMC マシン・コードの更新が正常にインストールされたことを確認するには、次のようにします。

1. ナビゲーション領域で、「**更新**」をクリックする。作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが表示されます。
2. バージョンおよびリリースが、インストールした更新と一致することを確認します。
3. 表示されているコードのレベルがインストールしたレベルでない場合は、次のステップを実行します。

a. マシン・コードの更新を再試行する。この手順用に DVD を作成した場合、新しいメディアを使用します。
b. 問題が解決しない場合は、次のレベルのサポートに連絡する。

HMC ソフトウェアのアップグレード

HMC 構成データを維持したまま、HMC のソフトウェアをあるリリースから次のリリースへアップグレードする方法を説明します。

HMC マシン・コードをアップグレードするには、ステップ 1 から 9 を実行します。

注: バージョン 6 の HMC からバージョン 7 の HMC にアップグレードする場合は、82 ページの『HMC のマシン・コードをバージョン 6 からバージョン 7 に移行する』を参照してください。

ステップ 1. アップグレードの入手

HMC マシン・コード・アップグレードはフィックス・セントラル (Fix Central) Web サイトから注文することができます。

フィックス・セントラル (Fix Central) Web サイトからアップグレードを入手するには、次のようにします。

1. インターネットに接続したコンピューターまたはサーバーから、ハードウェア管理コンソール Web サイト (http://www-933.ibm.com/support/fixcentral/) にアクセスする。
2. 「**続行**」をクリックします。 「ハードウェア管理コンソール」サイトが表示されます。
3. アップグレードする HMC バージョンへナビゲートする。
4. ダウンロードおよび注文のセクションを見つける。

   注: インターネットにアクセスできない場合、IBM サービスおよびサポートに連絡して、アップグレードを収めた DVD を注文してください。
5. 表示されるプロンプトのとおりに行って、注文を送信する。
6. アップグレードを入手したら、『ステップ 2. 既存の HMC マシン・コード・レベルを表示する』から続行する。

ステップ 2. 既存の HMC マシン・コード・レベルを表示する

既存の HMC マシン・コードのレベルを判別するには、以下のステップを実行します。

1. ナビゲーション領域で、「**更新**」をクリックする。
2. 作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に表示される情報を見て記録する。この情報には、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが含まれています。
3. 『ステップ 3. 管理対象システムのプロファイル・データのバックアップ』から続行する。

ステップ 3. 管理対象システムのプロファイル・データのバックアップ

管理システムのプロファイル・データをバックアップするには、次のようにします。

1. ナビゲーション領域で、「**システム管理**」を選択する。
2. 「**サーバー**」を選択する。
3. サーバーを選択し、その状態が「*稼働中*」または「*スタンバイ*」であることを確認する。
4. 「タスク」の下で、「**構成**」 > 「**パーティション・データの管理**」 > 「**バックアップ**」を選択する。
5. バックアップ・ファイル名を入力し、その情報を記録しておく。

6. 「**OK**」をクリックします。
7. 各管理対象システムごとに、これらのステップを繰り返す。
8. 『ステップ 4. HMC データのバックアップ』から続行する。

ステップ 4. HMC データのバックアップ

新規バージョンの HMC ソフトウェアをインストールする前に、HMC データのバックアップをとり、ソフトウェアのアップグレード中に、問題のあるイベントが発生した場合に、前のレベルを復元できるようにしておきます。新規バージョンの HMC ソフトウェアへのアップグレードが正常に完了したら、この重要なコンソール・データは使用しないでください。

注: 取り外し可能メディアにバックアップするように選択する場合は、そのメディアを使用可能にしておく必要があります。

HMC データをバックアップするには、以下のようにします:

1. 取り外し可能メディアにバックアップする予定であれば、メディアのフォーマットを行うための以下のステップを実行する。
   a. メディアをドライブに挿入する。
   b. ナビゲーション領域で、「**サービス管理**」を選択する。
   c. 「**メディアのフォーマット**」を選択する。
   d. メディア・タイプを選択する。
   e. フォーマット・タイプを選択する。
   f. 「**OK**」をクリックします。
2. ナビゲーション領域で、「**HMC 管理**」を選択する。
3. 「**HMC データのバックアップ**」を選択します。 「HMC データのバックアップ」ウィンドウが開きます。
4. アーカイブ・オプションを選択する。 ローカル・システムのメディアにバックアップしたり、HMC ファイル・システム (例えば NFS) にマウントされているリモート・システムにバックアップしたり、ファイル転送プロトコル (FTP) を使用してバックアップをリモート・サイトに送信したりできます。
   - ローカル・システムにバックアップするには、「**ローカル・システムのメディアへのバックアップ (Back up to media on local system)**」を選択して、指示に従う。
   - マウントされているリモート・システムにバックアップするには、「**マウントされたリモート・システムへのバックアップ (Back up to mounted remote system)**」を選択して、指示に従う。
   - リモート FTP サイトにバックアップするには、「**重要データのバックアップをリモート・サイトに送信 (Send back up critical data to remote site)**」を選択し、指示に従う。
5. 『ステップ 5. 現行 HMC 構成情報の記録』から続行してください。

ステップ 5. 現行 HMC 構成情報の記録

新規バージョンの HMC ソフトウェアにアップグレードする前に、予防措置として、HMC 構成情報を記録しておきます。

現行 HMC 構成を記録するには、次のようにします。

1. ある管理対象システムまたはその論理区画に対してスケジュールされた操作を表示するには、「**システム管理**」を開く。HMC 自体に対してスケジュールされた操作を記録するには、「**HMC 管理**」を選択し、ステップ 3 までスキップします。
2. 管理対象システム、および HMC 構成情報を記録する区画があればその区画を選択する。

3. タスク・リストから、「**操作のスケジュール**」を選択する。 選択されたターゲット用にスケジュールされたすべての操作が表示されます。
4. 「**ソート**」 > 「**オブジェクト別**」を選択する。
5. 各オブジェクトを選択し、以下の詳細情報を記録する。
   - オブジェクト名
   - スケジュール日
   - 操作時刻 (24 時形式で表示される)
   - 繰り返し (「はい」の場合は、以下のステップを実行します)。
     a. 「**表示**」 > 「**スケジュールの詳細**」を選択する。
     b. 間隔情報を記録する。
     c. 「スケジュール済み操作」ウィンドウを閉じる
     d. スケジュール済み操作ごとに繰り返す。
6. 「スケジュール済み操作のカスタマイズ」ウィンドウを閉じる。
7. 『ステップ 6. リモート・コマンドの状況を記録する』から続行する。

ステップ 6. リモート・コマンドの状況を記録する

リモート・コマンドの状況を記録するには、次のようにします。

1. ナビゲーション領域で、「**HMC 管理**」を選択する。
2. タスク・リストから、「**リモート・コマンド実行 (Remote Command Execution)**」をクリックする。
3. 「**ssh 機能を使用してリモート・コマンド実行を可能にする (Enable remote command execution using the ssh facility)**」チェック・ボックスが選択されたかどうかを記録する。
4. 「**取消**」をクリックする。
5. 『ステップ 7. アップグレード・データの保管』から続行する。

ステップ 7. アップグレード・データの保管

現行の HMC 構成を HMC 上の指定したディスク区画またはローカル・メディアに保管できます。ご使用の HMC ソフトウェアを新規リリースにアップグレードする直前のアップグレード・データのみを保管します。この処置によって、アップグレード後に HMC 構成の設定値を復元することができます。

注: 復元できるバックアップ・データのレベルは 1 つだけです。アップグレード・データを保管するたびに、前のレベルのデータは上書きされます。

アップグレード・データを保管するには、次のようにします。

1. ナビゲーション領域で、「**HMC 管理**」を選択する。
2. コンテンツ領域の「操作」の下で「**アップグレード・データの保管**」を選択する。「アップグレード・データの保管」ウィザードが開きます。
3. アップグレード・データの保管先のメディアを選択する。取り外し可能メディアへの保管を選択する場合は、ここでそのメディアを挿入します。「**次へ**」をクリックします。
4. 「**完了**」をクリックする。
5. タスクが完了するのを待つ。 「アップグレード・データの保管」タスクが失敗した場合は、先へ進む前に、次のレベルのサポートに連絡します。

   注: 「アップグレード・データの保管」タスクが失敗した場合は、アップグレード・プロセスを続行しないでください。

6. 「**OK**」をクリックします。
7. 『ステップ 8. HMC ソフトウェアのアップグレード』から続行する。

ステップ 8. HMC ソフトウェアのアップグレード

HMC ソフトウェアをアップグレードするには、DVD ドライブに挿入した取り外し可能メディアでシステムを再始動します。

1. HMC プロダクト・インストール用メディアを DVD ドライブに挿入する。
2. ナビゲーション・バーで、「**HMC 管理**」を選択する。
3. コンテンツ領域で、「**HMC のシャットダウンまたは再始動 (Shutdown or Restart HMC)**」を選択する。
4. 必ず、「**HMC の再始動 (Restart the HMC)**」を選択する。
5. 「**OK**」をクリックします。 HMC が再始動し、システム情報がウィンドウ上でスクロールされます。
6. 「**アップグレード**」を選択し、「**次へ**」をクリックする。
7. 以下のオプションから選択してください。
   - 前のタスクでアップグレード・データを保管した場合は、次のステップから続行する。
   - この手順の前で、アップグレード・データを保管していなかった場合は、続行する前に、ここでアップグレード・データを保管する必要がある。
8. 「**メディアからアップグレード (Upgrade from media)**」を選択して、「**次へ**」をクリックする。
9. 設定を確認して、「**完了**」をクリックする。
10. プロンプトのとおりに行う。

    注:
    - 画面がブランクになったら、スペース・バーを押して、情報を表示してください。
    - 最初の DVD はインストールに約 20 分かかります。
11. ログイン・プロンプトが出されたら、ユーザー ID とパスワードを使用してログインする。 HMC コードのインストールが完了します。
12. 『ステップ 9. HMC マシン・コード・アップグレードが正常にインストールされたことを確認する』から続行する。

ステップ 9. HMC マシン・コード・アップグレードが正常にインストールされたことを確認する

HMC のアップグレードが正常にインストールされたことを確認するには、次の手順で行います。

1. ナビゲーション領域で、「**更新**」をクリックする。作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが表示されます。
2. バージョンおよびリリースが、インストールした更新と一致することを確認します。
3. 表示されているコードのレベルがインストールしたレベルでない場合は、新しい DVD を使用してアップグレード・タスクを再試行します。問題が解決しない場合は、次のレベルのサポートに連絡する。

HMC のマシン・コードをバージョン 6 からバージョン 7 に移行する

HMC 構成データを維持したまま、HMC のマシン・コードをバージョン 6 からバージョン 7 に移行する方法を説明します。

HMC マシン・コードをバージョン 6 からバージョン 7 に移行するには、ステップ 1 から 9 を実行します。

重要: バージョン 7 リリース 0 に移行するには、現在、HMC マシン・コードは最低でもバージョン 6 リリース 1.2 になっている必要があります。

最小必要要件を満たしているか確認する

HMC のマシン・コードをバージョン 6 からバージョン 7 に移行するには、まず、以下の最小必要要件を満たしていることを確認する必要があります。

- ご使用の HMC がレベル 6.12 以降である。ご使用の HMC コードのレベルおよびリリースの検査の詳細については、75 ページの『HMC マシン・コードのバージョンおよびリリースの判別』を参照してください。
- ご使用のシステム・ファームウェアが最新のレベルである。
- ネットワーク保全性検査が済んでいる。
- ご使用の HMC ハードウェアがこのアップグレードをサポートしている。

ステップ 1. アップグレードの入手

アップグレードを入手するには、次のようにします。

HMC マシン・コード・アップグレードは、フィックス・セントラル (Fix Central) Web サイトから注文できます。この Web サイトから、サービスおよびサポートに連絡するか、アップグレードを FTP サーバーにダウンロードします。

1. インターネットに接続したコンピューターまたはサーバーから、http://www.ibm.com/eserver/support/fixes にアクセスする。
2. 「プロダクト・ファミリー (Product family)」リストで、該当するファミリーを選択する。
3. 「製品またはフィックス・タイプ (Product or fix type)」リストで、「**ハードウェア管理コンソール (Hardware Management Console)**」を選択する。
4. 「**続行**」をクリックします。 「ハードウェア管理コンソール」サイトが表示されます。
5. 必要な HMC バージョンへナビゲートする。
6. ダウンロードおよび注文のセクションを見つける。

   注: インターネットにアクセスできない場合、サービスおよびサポートに連絡して、アップグレードを収めた DVD を注文してください。
7. プロンプトのとおりに行って、注文を送信する。
8. アップグレードを入手したら、『ステップ 2. 既存の HMC マシン・コード・レベルを表示する』から続行する。

ステップ 2. 既存の HMC マシン・コード・レベルを表示する

既存の HMC マシン・コードのレベルを判別するには、以下のステップを実行します。

1. ナビゲーション領域で、「**ライセンス内部コード保守**」フォルダーをクリックする。
2. 「**HMC コードの更新**」を選択する。
3. 「状況」領域で、ご使用の HMC マシン・コードのバージョンおよびリリースを探す。
4. 現行のバージョンおよびリリースを記録する。

   重要: HMC マシン・コード 6.1.3 から 7.3.4.0 にアップグレードするには、最初に修正を適用する必要があります。詳しくは、http://www.ibm.com/eserver/support/fixes を参照してください。

5. 『ステップ 3. 管理対象システムのプロファイル・データのバックアップ』から続行する。

ステップ 3. 管理対象システムのプロファイル・データのバックアップ

管理システムのプロファイル・データをバックアップするには、次のようにします。

1. コンテンツ領域で、管理対象システムを選択する。
2. メニューで、「**選択済み**」>「**プロファイル・データ**」>「**バックアップ**」をクリックする。
3. バックアップ・ファイル名を入力し、その情報を記録しておく。
4. 「**OK**」をクリックします。
5. 各管理対象システムごとに、ステップ 1 から 4 を繰り返す。

ステップ 4. 重大なコンソール情報のバックアップ

新規バージョンの HMC ソフトウェアをインストールする前に、重要なコンソール情報のバックアップをとり、ソフトウェアのアップグレード中に、問題のあるイベントが発生した場合に、前のレベルを復元できるようにしておきます。新規バージョンの HMC ソフトウェアへのアップグレードが正常に完了したら、この重要なコンソール・データは使用しないでください。

注: コンソール・データを取り外し可能メディアにバックアップするように選択する場合は、そのメディアを使用可能にしておく必要があります。

重要なコンソール情報をバックアップするには、次のようにします。

1. 以下のオプションから選択してください。
   - DVD-RAM にバックアップする予定がない 場合は、後続ステップに進む。
   - DVD-RAM にバックアップする予定であれば、以下のステップを実行する。
     a. DVD-RAM をドライブに挿入する。
     b. ナビゲーション領域で、「**ライセンス内部コード保守**」をクリックする。
     c. 「**HMC コードの更新**」を選択する。
     d. 「**取り外し可能メディアのフォーマット**」を選択する。
     e. 「**DVD-RAM のフォーマット**」を選択する。
     f. 「**OK**」をクリックします。
     g. 次のステップを引き続き実行します。
2. 「**重要なコンソール・データのバックアップ**」を選択する。
3. アーカイブ・オプションを選択する。 HMC 内の DVD または HMC ファイルシステムにマウントされているリモート・システム (例えば NFS) にバックアップしたり、ファイル転送プロトコル (FTP) を使用して、バックアップをリモート・サイトに送信したりできます。
   - DVD にバックアップするには、「**ローカル・システムの DVD へのバックアップ (Back up to DVD on local system)**」を選択して、次の手順に従う。
   - マウントされているリモート・システムにバックアップするには、「**マウントされたリモート・システムへのバックアップ (Backup to mounted remote system)**」を選択して、次の手順に従う。
   - リモート FTP サイトにバックアップするには、「**重要データのバックアップをリモート・サイトへ送信 (Send backup critical data to remote site)**」を選択して、次の手順に従う。
4. 85 ページの『ステップ 5. 現行 HMC 構成情報の記録』から続行してください。

ステップ 5. 現行 HMC 構成情報の記録

新規バージョンの HMC ソフトウェアにアップグレードする前に、予防措置として、HMC 構成情報を記録しておきます。

HMC 構成情報を記録するには、以下のステップを行ってください。

1. ある管理対象システムまたはその論理区画に対してスケジュールされた操作を表示するには、「**システム管理**」を開く。HMC 自体に対してスケジュールされた操作を記録するには、「**HMC 管理**」を選択し、ステップ 3 までスキップします。
2. 管理対象システム、および HMC 構成情報を記録する区画があればその区画を選択する。
3. タスク・リストから、「**操作のスケジュール**」を選択する。 選択されたターゲット用にスケジュールされたすべての操作が表示されます。
4. 「**ソート**」 > 「**オブジェクト別**」を選択する。
5. 各オブジェクトを選択し、以下の詳細情報を記録する。
   - オブジェクト名
   - スケジュール日
   - 操作時刻 (24 時形式で表示される)
   - 繰り返し (「はい」の場合は、以下のステップを実行します)。
     a. 「**表示**」 > 「**スケジュールの詳細**」を選択する。
     b. 間隔情報を記録する。
     c. 「スケジュール済み操作」ウィンドウを閉じる
     d. スケジュール済み操作ごとに繰り返す。
6. 「スケジュール済み操作のカスタマイズ」ウィンドウを閉じる。
7. 『ステップ 6. リモート・コマンドの状況を記録する』から続行する。

ステップ 6. リモート・コマンドの状況を記録する

1. ナビゲーション領域で、「**HMC 管理**」を選択する。
2. 「**HMC 構成**」を選択する。
3. タスク・リストから、「**リモート・コマンド実行の使用可能または使用不可 (Enable/Disable Remote Command Execution)**」をクリックする。
4. 「**ssh 機能を使用してリモート・コマンド実行を可能にする (Enable remote command execution using the ssh facility)**」チェック・ボックスが選択されたかどうかを記録する。
5. 「**取消**」をクリックする。
6. 『ステップ 7. アップグレード・データの保管』から続行する。

ステップ 7. アップグレード・データの保管

現行の HMC 構成を HMC 上の指定したディスク区画に保管できます。 ご使用の HMC ソフトウェアを新規リリースにアップグレードする直前のアップグレード・データのみを保管します。この処置によって、アップグレード後に HMC 構成の設定値を復元することができます。

アップグレードされたデータは、インストール処理時に自動的に復元されます。

注: 復元できるバックアップ・データのレベルは 1 つだけです。 アップグレード・データを保管するたびに、前のレベルのデータは上書きされます。

1. ナビゲーション領域で、「**ライセンス内部コード**」フォルダーを開く。

2. 「**HMC コードの更新**」を選択する。
3. 「**アップグレード・データの保管**」を選択する。
4. 「**DVD**」を選択し、「**続行**」をクリックする。
5. DVD メディアをドライブに挿入する。
6. 「**続行**」をクリックして、タスクを開始する。
7. タスクが完了するのを待つ。 「アップグレード・データの保管」タスクが失敗した場合は、先へ進む前に、次のレベルのサポートに連絡します。

   注: 「アップグレード・データの保管」タスクが失敗した場合は、アップグレード・プロセスを続行しないでください。
8. 「**OK**」をクリックします。
9. 「**取消**」をクリックする。
10. 『ステップ 8. バージョン 6 からバージョン 7 への HMC ソフトウェアのアップグレード』から続行する。

ステップ 8. バージョン 6 からバージョン 7 への HMC ソフトウェアのアップグレード

重要: HMC マシン・コード 6.1.3 から 7.3.4.0 にアップグレードするには、最初に PTF を適用する必要があります。詳しくは、http://www.ibm.com/eserver/support/fixes を参照してください。

HMC ソフトウェアをアップグレードするには、DVD-RAM ドライブに挿入した DVD でシステムを再始動します。

1. HMC プロダクト・インストール用メディアを挿入する。
2. 以下のステップを実行します。
   a. HMC のメニュー・バーから「**コンソール**」 > 「**終了**」を選択する。
   b. 「**今すぐ終了**」を選択する。
   c. ログアウト・リストから、「**コンソールのリブート**」、次に「**了解**」を選択する。 HMC が再始動し、システム情報がウィンドウ上でスクロールされます。
3. 「**アップグレード**」を選択し、「**次へ**」をクリックする。
4. 警告が表示されたときは、以下のオプションから選択する。
   - 前のタスクでアップグレード・データを保管した場合は、次のステップから続行する。
   - この手順の前で、アップグレード・データを保管していなかった場合は、続行する前に、ここでアップグレード・データを保管する必要がある。
5. 「**メディアからアップグレード (Upgrade from media)**」を選択して、「**次へ**」をクリックする。
6. 設定を確認して、「**完了**」をクリックする。
7. プロンプトのとおりに行う。

   注:
   - 画面がブランクになったら、スペース・バーを押して、情報を表示してください。
   - 最初の DVD はインストールに約 20 分かかります。
8. プロンプトが出されたら、最初のメディアを取り外してから、2 番目のメディアを挿入する。

9. 「**1.メディアから追加のソフトウェアをインストールする (1. Install additional software from media)**」を選択し、Enter を押す。 任意のキーを押してインストールを確認します。 HMC は、パッケージをインストールするときに、状況メッセージを表示します。
10. 「**ハードウェア管理コンソール Web アプリケーションのログオンと起動**」をクリックします。
11. HMC インターフェースにログインします。
12. 『ステップ 9. HMC マシン・コード・アップグレードが正常にインストールされたことを確認する』から続行する。

ステップ 9. HMC マシン・コード・アップグレードが正常にインストールされたことを確認する

1. ナビゲーション領域で、「**更新**」をクリックする。作業領域の「HMC コード・レベル (HMC Code Level)」見出しの下に、HMC のバージョン、リリース、保守レベル、ビルド・レベル、および基本バージョンが表示されます。
2. バージョンおよびリリースが、インストールした更新と一致することを確認します。
3. 表示されているコードのレベルがインストールしたレベルでない場合は、新しい DVD を使用してアップグレード・タスクを再試行します。問題が解決しない場合は、次のレベルのサポートに連絡する。

ステップ 10. 更新パッケージの入手

HMC 更新パッケージは、フィックス・セントラル (Fix Central) Web サイトから注文できます。この Web サイトから、サービスおよびサポートに連絡するか、更新パッケージを FTP サーバーにダウンロードします。

1. インターネットに接続したコンピューターまたはサーバーから、http://www.ibm.com/eserver/support/fixes にアクセスする。
2. 「プロダクト・ファミリー (Product family)」リストで、該当するファミリーを選択する。
3. 「製品またはフィックス・タイプ (Product or fix type)」リストで、「**ハードウェア管理コンソール (Hardware Management Console)**」を選択する。
4. 「**続行**」をクリックします。 「ハードウェア管理コンソール」サイトが表示されます。
5. 必要な HMC バージョンへナビゲートする。
6. ダウンロードおよび注文のセクションを見つける。

   注: インターネットにアクセスできない場合、サービスおよびサポートに連絡して、アップグレードを収めた DVD を注文してください。
7. プロンプトに従って、取り外し可能メディアに更新パッケージをダウンロードするか、または注文を送信する。

ステップ 11. この HMC 用操作の再スケジュール

HMC をアップグレードした場合、旧 HMC バージョンを使ってスケジュールしていた各操作を手動で再スケジュールする必要があります。

1. ナビゲーション領域で、「**HMC 管理**」をクリックします。
2. 作業領域で、「**操作のスケジュール**」をクリックします。

ネットワーク・アップグレード・イメージを使用したリモート・ロケーションからの HMC のアップグレード

ネットワーク・アップグレード・イメージを使用して、リモート・ロケーションから HMC のソフトウェアをアップグレードする方法を説明します。

ネットワーク・アップグレード・イメージを使用して、リモート・ロケーションから HMC のソフトウェアをアップグレードする方法を説明します。レベル V6R1.2 以上の HMC (HMC の V7 レベルをすべて含む) をアップグレードするには、以下の手順を使用します。

1. インターネットに接続したコンピューターまたはサーバーから、ハードウェア管理コンソール Web サイト (http://www14.software.ibm.com/webapp/set2/sas/f/netinstall/v7770network.html) にアクセスします。
2. 該当する HMC V7 ネットワーク・イメージをダウンロードし、それを FTP サーバーに保存します。これらのファイルは、HMC に直接ダウンロードすることはできません。イメージ・ファイルは、FTP 要求を受け入れるサーバーにダウンロードしてください。
3. 以下のファイルをダウンロードしたことを確認します。
   - initrd.gz
   - bzImage
   - disk1.img
   - disk2.img
   - disk3.img
   - hmcnetworkfiles.sum
4. アップグレード・データを HMC に保存します。アップグレード・データを保存するには、次のコマンド行を実行します。
   - データを DVD と HDD の両方に保存するには、次のコマンドを実行します。

     ```
     mount /media/cdrom

     saveupgdata -r diskdvd
     ```
   - データを HDD に保存するには、次のコマンドを実行します。

     ```
     saveupgdata -r disk
     ```
5. アップグレード・ファイルを、HMC のブート可能ディスク区画にコピーします。ファイルをコピーするには、**getupgfiles** コマンドを実行します。

   例: **getupgfiles -h <ftp server> -u <user id> -d <remote directory>**

   値の説明:
   - **ftp server** は、HMC ネットワーク・イメージをダウンロードした FTP サーバーのホスト名または IP アドレスです。
   - **user id** は、FTP サーバーの有効なユーザー ID です。 --passwd 引数を使用してパスワードを指定しないと、パスワードを求めるプロンプトが出されます。
   - **remote directory** は、HMC ネットワーク・イメージが保存される FTP サーバーのディレクトリーです。
6. HMC をリブートして、ブート可能ディスク区画にコピーしたコードをアップグレードします。 HMC をリブートするには、**chhmc -c altdiskboot -s enable --mode upgrade** を実行します。

7. HMC をリブートし、アップグレードを開始します。アップグレードを開始するには、**hmcshutdown -r -t now** コマンドを実行します。

HMC ポートの位置

ロケーション・コードを使用して、部品の位置を見つけることができます。サーバー上の HMC ポートの位置に対してロケーション・コードを対応させるには、以下の HMC ポートの位置を示す図を使用します。

8202-E4B または 8205-E6B HMC ポートの位置

以下の図と表を使用して、8202-E4B または 8205-E6B 上の HMC ポートの位置を対応させます。

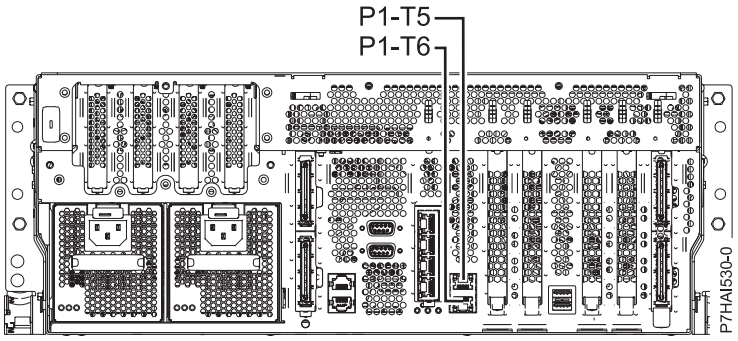


図 36. 8202-E4B または 8205-E6B HMC ポートの位置

表 13. 8202-E4B または 8205-E6B HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-T5	いいえ
HMC ポート 2	Un-P1-T6	いいえ
8202-E4B または 8205-E6B 上の HMC ポートの位置について詳しくは、『Part location and location codes for 8202-E4B or 8205-E6B』を参照してください。		

8202-E4C または 8205-E6C HMC ポートの位置

以下の図と表を使用して、8202-E4C または 8205-E6C 上の HMC ポートの位置を対応させます。

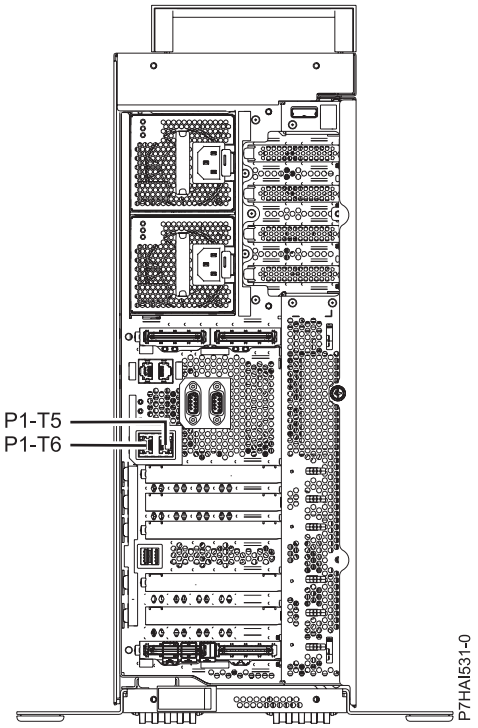


図 37. 8202-E4C または 8205-E6C HMC ポートの位置

表 14. 8202-E4C または 8205-E6C HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-T5	いいえ
HMC ポート 2	Un-P1-T6	いいえ
8202-E4C または 8205-E6C 上の HMC ポートの位置について詳しくは、『Part location and location codes for 8202-E4C or 8205-E6C.』を参照してください。		

8231-E2B HMC ポートの位置

以下の図と表を使用して、8231-E2B 上の HMCポートの位置を対応させます。

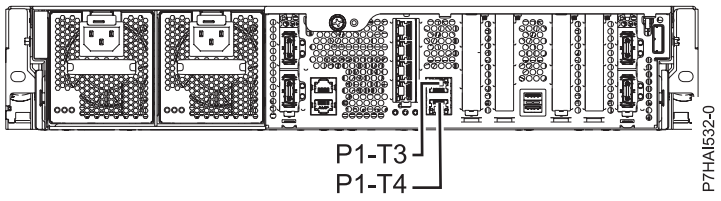


図 38. 8231-E2B HMC ポートの位置

表 15. 8231-E2B HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-T3	いいえ
HMC ポート 2	Un-P1-T4	いいえ

表 15. 8231-E2B HMC ポートの位置 (続き)

ポート	物理ロケーション・コード	識別 LED
8231-E2B 上の HMC ポートの位置について詳しくは、『Part location and location codes for 8231-E2B』を参照してください。		

8231-E1C または 8231-E2C HMC ポートの位置

以下の図と表を使用して、8231-E1C または 8231-E2C 上の HMC ポートの位置を対応させます。

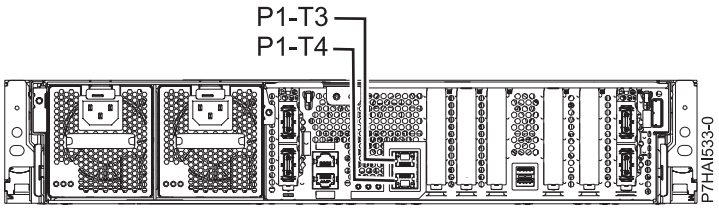


図 39. 8231-E1C または 8231-E2C HMC ポートの位置

表 16. 8231-E1C または 8231-E2C HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-T3	いいえ
HMC ポート 2	Un-P1-T4	いいえ
8231-E1C または 8231-E2C 上の HMC ポートの位置について詳しくは、『Part location and location codes for 8231-E1C or 8231-E2C』を参照してください。		

8233-E8B または 8236-E8C HMC ポートの位置

以下の図と表を使用して、8233-E8B または 8236-E8C 上の HMC ポートの位置を対応させます。

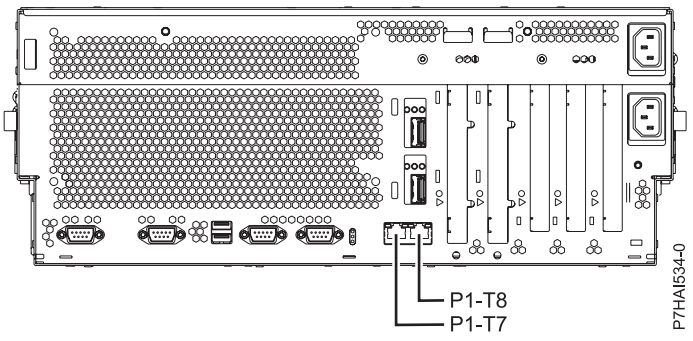


図 40. 8233-E8B または 8236-E8C HMC ポートの位置

表 17. 8233-E8B または 8236-E8C HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-T7	いいえ
HMC ポート 2	Un-P1-T8	いいえ

表 17. 8233-E8B または 8236-E8C HMC ポートの位置 (続き)

ポート	物理ロケーション・コード	識別 LED
8233-E8B または 8236-E8C 上の HMC ポートの位置について詳しくは、『Part location and location codes for 8233-E8B or 8236-E8C』を参照してください。		

8408-E8D 8248-L4T または 9109-RMD HMC ポートの位置

以下の図と表を使用して、8408-E8D 8248-L4T または 9109-RMD 上の HMC ポートの位置を対応させます。

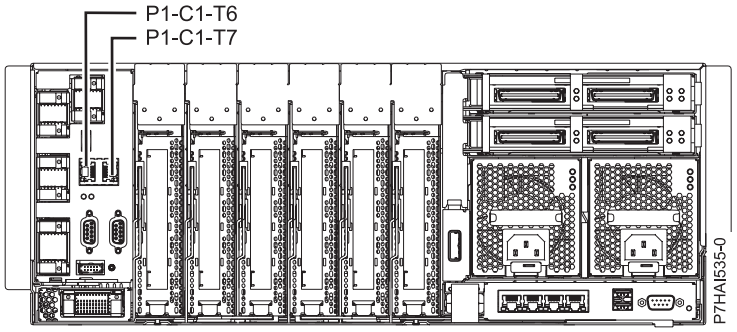


図 41. 8408-E8D 8248-L4T または 9109-RMD HMC ポートの位置

表 18. 8408-E8D 8248-L4T または 9109-RMD HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-C1-T6	はい
HMC ポート 2	Un-P1-C1-T7	はい
8408-E8D または 9109-RMD 上の HMC ポートの位置について詳しくは、『Part location and location codes for 8408-E8D or 9109-RMD』を参照してください。		

9117-MMB または 9179-MHB HMC ポートの位置

以下の図と表を使用して、9117-MMB または 9179-MHB 上の HMC ポートの位置を対応させます。

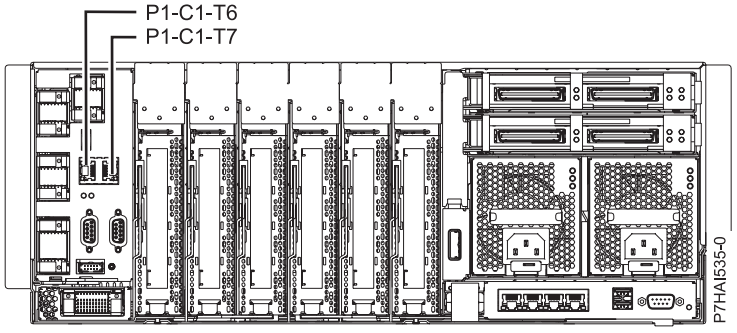


図 42. 9117-MMB または 9179-MHB HMC ポートの位置

表 19. 9117-MMB または 9179-MHB HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-C1-T6	はい
HMC ポート 2	Un-P1-C1-T7	はい
9117-MMB または 9179-MHB 上の HMC ポートの位置について詳しくは、『Part location and location codes for 9117-MMB or 9179-HMC』を参照してください。		

9117-MMC、9117-MMD、9179-MHC、9179-MHD、または の HMC ポートの位置

以下の図と表を使用して、9117-MMC、9117-MMD、9179-MHC, 9179-MHD、または 上の HMC ポートの位置を対応させます。

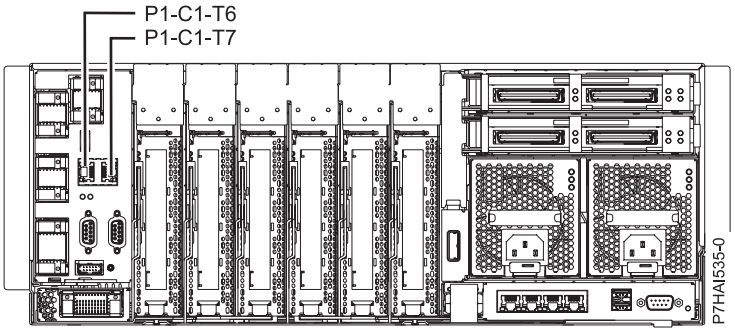


図 43. 9117-MMC、9117-MMD、9179-MHC、9179-MHD、または の HMC ポートの位置

表 20. 9117-MMC、9117-MMD、9179-MHC、9179-MHD、または の HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-C1-T6	はい
HMC ポート 2	Un-P1-C1-T7	はい
9117-MMC、9117-MMD、9179-MHC、または 9179-MHD 上の HMC ポートの位置について詳しくは、『Part location and location codes for 9117-MMC, 9117-MMD, 9179-MHC, or 9179-MHD』を参照してください。		

9119-FHB HMC ポートの位置

以下の図と表を使用して、9119-FHB 上の HMCポートの位置を対応させます。

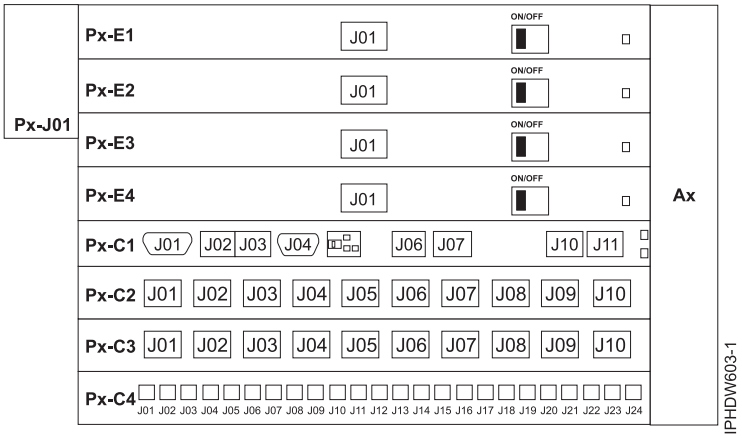


図 44. 9119-FHB HMC ポートの位置

表 21. 9119-FHB HMC ポートの位置

ポート	物理ロケーション・コード	識別 LED
HMC (コネクター J02、イーサネットからバルク電力ハブ BPH)	Un-Px-C1–J02	いいえ
HMC (コネクター J03、イーサネットからバルク電力ハブ BPH)	Un-Px-C1–J03	いいえ
9119-FHB 上の HMC ポートの位置について詳しくは、『Part location and location codes for 9119-FHB』を参照してください。		

特記事項

本書は米国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す。

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、製造元の担当者にお尋ねください。 本書で、製造元の製品、プログラム、またはサービスに言及している部分があっても、このことは当該製品、プログラム、またはサービスだけが使用可能であることを意味するものではありません。これらの製品、プログラム、またはサービスに代えて、製造元の有効な知的所有権またはその他の法的に保護された権利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、製造元によって明示的に指定されたものを除き、他社の製品、プログラムまたはサービスを使用した場合の評価と検証はお客様の責任で行っていただきます。

製造元は、本書で解説されている主題について特許権 (特許出願を含む) を所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、使用権等の許諾については、製造元に書面にてご照会ください。

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。本書は特定物として「現存するまま」の状態で提供され、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。 製造元は予告なしに、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。

本書において製造元所有以外の 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、お客様自身の責任でご使用ください。

製造元は、お客様が提供するいかなる情報も、お客様になんら義務も負わせない適切な方法で、使用もしくは配布することがあります。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。 そのため、他の操作環境で得られた結果は、異なる可能性があります。 一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

製造元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。 製造元は、それらの製品のテストを行っておりません。したがって、製造元以外の他社の製品に関する実行性、互換性、またはその他の損害賠償請求については確証できません。 製造元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にお願いします。

製造元の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている製造元の価格は製造元が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。 卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。 記述内容は製品が使用可能になる前に変更になる場合があります。

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。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

本書に示されている図や仕様は、製造元の書面による許可を得ずにその一部または全部を複製してはいけません。

製造元は、指定された特定のマシンを対象として本書を作成しています。 その他の使用および使用結果については、製造元は何ら保証責任を負いません。

製造元のコンピューター・システムには、破壊または損失したデータが検出されない危険性を減少するために設計されたメカニズムが含まれています。 しかし、この危険をゼロにすることはできません。 不意の停電によるシステムの休止やシステム障害、電力の変動または停電、もしくはコンポーネント障害を経験するユーザーは、停電または障害が起きた時刻もしくはその近辺で行われたシステム操作とセーブまたは転送されたデータの正確性を検証する必要があります。 さらに、ユーザーはそのような不安定で危機的な状況で操作されたデータを信頼する前に、独自のデータ検証手順を確立する必要があります。 ユーザーはシステムおよび関連ソフトウェアに適用できる更新情報または修正がないか、定期的に製造元の Web サイトをチェックする必要があります。

認定ステートメント

本製品は、お客様の国で、いかなる方法においても公共通信ネットワークのインターフェースへの接続について認定されていない可能性があります。そのような接続を行うには、事前に法律によるさらなる認定が必要です。ご不明な点がある場合は、IBM 担当員または販売店にお問い合わせください。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。 他の製品名およびサービス名は、IBM または各社の商標です。 現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml の「Copyright and trademark information」をご覧ください。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社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 は、Microsoft Corporation の米国およびその他の国における商標です。

電波障害自主規制特記事項

VCCI クラス A 情報技術装置

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

VCCI クラス B 情報技術装置

この装置は，クラスB情報技術装置です。この装置は，家庭環境で使用
することを目的としていますが，この装置がラジオやテレビジョン受信機に
近接して使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 ＶＣＣＩ－Ｂ

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

適用可能性: これらの条件は、IBM Web サイトのすべてのご利用条件に追加されるものです。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。 ただし、IBM の明示的な承諾を得ずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾を得ずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示したりすることはできません。

権利: ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。 これらの資料は、特定物として現存するままの状態で提供され、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なしで提供されます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21