

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』、 193 ページの『特記事項』、「*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。本体機器提供後に、追加で電源コード・セットが必要となった場合は、補修用の取扱いとなります。

本書は、IBM ハードウェア管理コンソールのバージョン 8 リリース 8.7.0 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

© Copyright IBM Corporation 2014, 2017.

目次

安全上の注意	vii
ハードウェア管理コンソールの取り付けおよび構成	1
HMC の取り付けおよび構成での新機能	1
取り付けおよび構成のタスク	2
新しいサーバーを用いた新規 HMC の取り付けおよび構成	2
HMC コードの更新およびアップグレード	3
既存の取り付け環境への 2 番目の HMC の追加	3
HMC のセットアップ	4
スタンドアロン HMC の配線	4
7310-CR4 HMC のラックへの取り付け	6
部品目録の確認	7
位置の決定	7
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	8
スライド・レールのラックへの取り付け	9
スライド・レールへの HMC の取り付け	12
ケーブル・マネジメント・アームの取り付け	14
ラック・マウント HMC の配線	15
HMC ポートの位置	16
7042-CR5 および 7042-CR6 のラックへの取り付け	20
ラックへの 7042-CR7 および 7042-CR8 の取り付け	26
7042-CR9 HMC のラックへの取り付け	36
ラックへの 7063-CR1 の取り付け	46
ラック・マウント型 7063-CR1 システムの設置の前提条件	46
ご使用のシステム用の部品の用意	47
7063-CR1 システムを搭載するラック内の位置の決定とマーク付け	47
固定レールを使用してのラックへの HMC の設置	48
システム・シャーシおよびラックへの固定レールの取り付け	49
ラックへのシステムの設置と電源ケーブルの接続および配線	50
スライド・レールを使用してのラックへの HMC の設置	52
システムおよびラックへのスライド・レールの取り付け	52
ラックへのシステムの設置と電源ケーブルの接続および配線	55
ラック・マウント型 7063-CR1 HMC のケーブル接続	56
7063-CR1 HMC の構成	57
HMC 仮想アプライアンスの取り付け	58
x86 での HMC 仮想アプライアンスのインストール	59
KVM ハイパーバイザーを使用した HMC 仮想アプライアンスのインストール	59
Xen ハイパーバイザーを使用した HMC 仮想アプライアンスのインストール	60
VMware ESXi を使用した HMC 仮想アプライアンスのインストール	61
PowerVM (論理区画) での HMC 仮想アプライアンスのインストール	61
HMC 仮想アプライアンスに対する Activation Engine の使用	62
Activation Engine 用の構成プロファイルのセットアップ	63
モニターおよびキーボードの取り付け	69
部品目録の確認	71
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	71
モニターおよびキーボードのラックへの取り付け	72
コンソール・スイッチの取り付け (オプション)	76
HMC Classic または HMC Enhanced インターフェースを使用した HMC の構成	78
HMC に関するネットワーク設定の選択	79
HMC ネットワーク接続	79

HMC ネットワーク接続のタイプ	79
コール・ホーム・サーバーに使用する接続方式の決定	83
単純化された接続	85
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	86
インターネット・プロトコルの選択	86
インターネット SSL アドレス・リスト	86
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	87
VPN サーバー・アドレス・リスト	88
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	88
複数のコール・ホーム・サーバーの使用	88
HMC 構成の準備	89
HMC 用のプリインストール構成ワークシート	90
HMC の構成	98
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	98
HMC の始動、およびガイド付きセットアップ・ウィザードにある各ステップを完了	98
構成の確認	99
HMC メニューを使用した HMC の構成	99
HMC の始動	101
日時の変更	102
HMC ネットワーク・タイプの構成	102
HMC ファイアウォール設定の変更	108
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	109
ドメイン名サービスの構成	110
ドメイン・サフィックスの構成	110
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	110
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	111
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	112
「コール・ホーム用イベント・マネージャー」の構成	118
管理対象システムに対するパスワードの設定	119
HMC と管理対象システム間の接続のテスト	120
構成完了後のステップ	120
重要な HMC データのバックアップ	120
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	121
HMC マシン・コードの更新、アップグレード、および移行	123
HMC マシン・コードのバージョンおよびリリースの判別	123
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	123
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	123
ステップ 2. 既存の HMC マシン・コード・レベルを表示する	124
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	124
ステップ 4. HMC マシン・コードの更新を適用する	124
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	124
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	125
ステップ 1. 既存の HMC マシン・コード・レベルを表示する	125
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	125
ステップ 3. HMC マシン・コードの更新を入手する	125
ステップ 4. HMC マシン・コードの更新を適用する	126
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	126
HMC ソフトウェアのアップグレード	126
ステップ 1. アップグレードの入手	126
ステップ 2. 既存の HMC マシン・コード・レベルを表示する	127
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	127
ステップ 4. HMC データのバックアップ	127
ステップ 5. 現行 HMC 構成情報の記録	128
ステップ 6. リモート・コマンドの状況を記録する	129
ステップ 7. アップグレード・データの保管	129
ステップ 8. HMC ソフトウェアのアップグレード	129

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	130
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	130
HMC Enhanced+ インターフェースを使用した HMC の構成	131
HMC に関するネットワーク設定の選択	131
HMC ネットワーク接続.	131
HMC ネットワーク接続のタイプ.	131
コール・ホーム・サーバーに使用する接続方式の決定.	136
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.	137
インターネット・プロトコルの選択.	138
インターネット SSL アドレス・リスト.	138
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.	139
VPN サーバー・アドレス・リスト	139
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.	140
複数のコール・ホーム・サーバーの使用	140
HMC 構成の準備.	141
HMC 用のプリインストール構成ワークシート	142
HMC の構成	150
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	150
HMC の始動、およびガイド付きセットアップ・ウィザードにある各ステップを完了	150
構成の確認	151
HMC メニューを使用した HMC の構成	151
HMC の始動	152
日時の変更	153
HMC ネットワーク・タイプの構成	154
HMC ファイアウォール設定の変更	161
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	162
ドメイン名サービスの構成	162
ドメイン・サフィックスの構成	163
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	163
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	164
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	165
「コール・ホーム用イベント・マネージャー」の構成	172
管理対象システムに対するパスワードの設定	173
HMC と管理対象システム間の接続のテスト	174
構成完了後のステップ	175
重要な HMC データのバックアップ	175
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.	176
HMC マシン・コードの更新、アップグレード、および移行.	177
HMC マシン・コードのバージョンおよびリリースの判別	178
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	178
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.	178
ステップ 2. 既存の HMC マシン・コード・レベルを表示する.	179
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	179
ステップ 4. HMC マシン・コードの更新を適用する	179
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.	180
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	180
ステップ 1. 既存の HMC マシン・コード・レベルを表示する.	180
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	180
ステップ 3. HMC マシン・コードの更新を入手する	181
ステップ 4. HMC マシン・コードの更新を適用する	181
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.	182
HMC ソフトウェアのアップグレード	182
ステップ 1. アップグレードの入手	182
ステップ 2. 既存の HMC マシン・コード・レベルを表示する.	182
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	183

ステップ 4. HMC データのバックアップ	183
ステップ 5. 現行 HMC 構成情報の記録	184
ステップ 6. リモート・コマンドの状況を記録する	184
ステップ 7. アップグレード・データの保管	185
ステップ 8. HMC ソフトウェアのアップグレード	185
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	186
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	186
HMC ポートの位置	187
特記事項	193
IBM Power Systems サーバーのアクセシビリティ機能	194
プライバシー・ポリシーに関する考慮事項	196
商標	196
電波障害規制特記事項	196
クラス A 表示	196
クラス B 表示	201
使用条件	204

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。
- 重要な注記は、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 カードまたはファイ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。

- IBM から電源コードが供給されている場合は、その電源コードのみを使用して当装置を電源に接続します。IBM から供給された電源コードは、他の製品には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。
 - AC 電源では、すべての電源コードをそれぞれの AC 給電部から切り離します。
 - DC 電力配分パネル (PDP) 付きのラックでは、PDP へのお客様の DC 電源を切断してください。
- 製品に電源を接続する際には、すべての電源ケーブルが適切に接続されていることを確認します。
 - AC 電源付きのラックでは、すべての電源コードを正しく配線され接地されたコンセントに接続します。電源コンセントから供給される電圧と相回転がシステムの定格銘板に従っていることを確認します。

- DC 電力配分パネル (PDP) 付きのラックでは、お客様の DC 電源を PDP へ接続します。DC 電源および DC 電源帰線を接続する際に、必ず、適切な極性が使用され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。
- 考えられる危険な状態がすべて修正されるまで、マシンへの電力をオンに切り替えようとししないでください。
- 電気に関する安全上の問題が存在することを前提としてください。サブシステムの取り付け手順時に指定された導通、接地、および電源のチェックをすべて実行して、そのマシンが安全要件を満たしていることを確認してください。
- なんらかの危険な状態が存在する場合は、検査を続行しないでください。
- 装置のカバーを開ける前に、取り付けおよび構成の手順で別途指示されている場合を除き、接続されている AC 電源コードを切り離し、ラック電力配分パネル (PDP) 内の該当する回路ブレーカーの電源をオフにして、すべての通信システム、ネットワーク、およびモデムを切り離します。

危険:

- 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. AC 電源では、コンセントから電源コードを取り外します。
3. DC 電力配分パネル (PDP) 付きのラックでは、PDP 内の回路ブレーカーの電源をオフにして、お客様の DC 電源から電力を除去します。
4. シグナル・ケーブルをコネクタから取り外します。
5. 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に接続します。
4. AC 電源では、電源コードをコンセントに接続します。
5. DC 電力配分パネル (PDP) 付きのラックでは、お客様の DC 電源からの電力を回復し、PDP 内の回路ブレーカーの電源をオンにします。
6. デバイスの電源をオンにします。

鋭利な先端の部品やジョイントがシステムの中や周囲に存在している可能性があります。機器を取り扱う際には、指を切ったり、こすったり、挟んだりしないように注意してください。(D005)

(R001 パート 2 の 1):

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ください。
- 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。ラックに搭載された装置の上にものを載せないでください。また、ラックに取り付けられた装置に寄りかかったり、身体を安定させるため (はしごから作業を行うときなど) にそれらの装置を使用したりしないでください。



- 各ラック・キャビネットには複数の電源コードが付属していることがあります。
 - AC 電源付きのラックでは、保守作業中に電源を切り離す指示がある場合は、ラック・キャビネット内のすべての電源コードを必ず取り外してください。
 - DC 電力配分パネル (PDP) 付きのラックでは、保守作業中に電源を切断するよう指示された場合、システム装置 (単数または複数) への電力を制御する回路ブレーカーをオフにするか、またはお客様の DC 電源を切断してください。
- 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。

(R001 パート 2 の 2):

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、装置を取り付けしないでください。
- 空気の流れが妨げられているラック内には、装置を取り付けしないでください。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。

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 (コンプライアンス ID RACK-001)** または **22U (コンプライアンス ID RR001)** 以上にあらゆ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 (コンプライアンス ID RACK-001)** または **22U (コンプライアンス ID RR001)** の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** がほとんど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。
- 再配置するラック・キャビネットに取り外し可能なアウトリガーが取り付けられている場合は、アウトリガーを再配置してから、キャビネットを再配置する必要があります。
- 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)



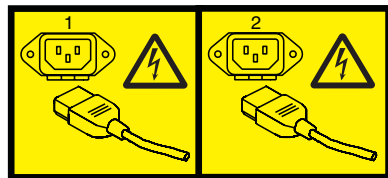
危険: このラベルが貼られているコンポーネントの内部には、危険な電圧、強い電流が流れています。このラベルが付いているカバーまたはバリアは開けないでください。(L001)

(L002)

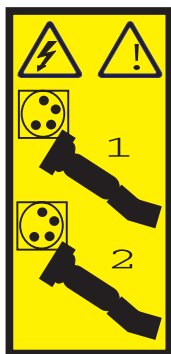


危険: ラック・マウント型デバイスを棚やワークスペースとして使用しないでください。(L002)

(L003)



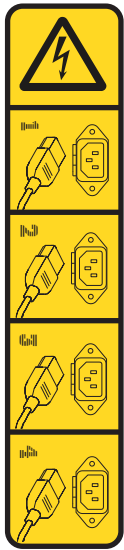
または



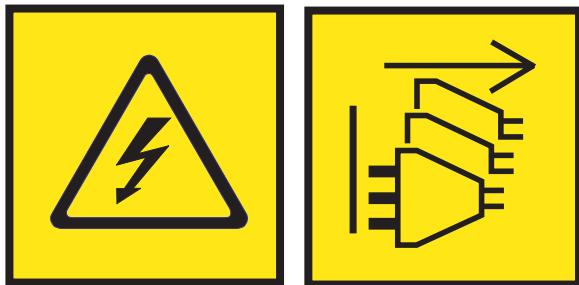
または



または



または



危険: 複数の電源コード。この製品は複数の AC 電源コードや複数の DC 電源ケーブル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ために、すべての電源コードと電源ケーブルを切り離してください。(L003)

(L007)



注意: 近くに高温になる部品が存在します。(L007)

(L008)



注意: 近くに危険な可動部品があります。(L008)

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。光ファイバーの導通を確認するために、切断された光ファイバーの一方の端に明るい光を入れ、もう一方の端を覗き込んでも目に損傷を与えない可能性はありますが、このやり方は潜在的に危険です。そのため、一方の端に明るい光を入れ、もう一方の端を覗き込んで光ファイバーの導通を確認することはお勧めしません。光ファイバー・ケーブルの導通を検査するには、光学式光源および電力メーターを使用してください。(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°C (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)**

注意:

IBM 提供のベンダー・リフト・ツールに関する注意:

- リフト・ツールの作業は、許可された担当者のみが行ってください。
- リフト・ツールは、ラックの高い位置での装置 (荷物) の補助、引き上げ、取り付け、取り外しに使用するためのものです。これは、装置を装着して大きなスロープを移送するために使用したり、パレット・ジャック、ウォーカー、フォーク・トラックなどの指定ツールや関連の再配置実施の代替として使用したりするためのものではありません。このような作業を実行できない場合は、特別な訓練を受けた担当員またはサービスを使用する必要があります (例えば、整備業者や運送業者など)。
- リフト・ツールを使用する前に、作業用者の資料を読んで完全に理解してください。よく読んで理解し、安全の規則に従い、手順に従って作業しないと、資産が損傷したり、作業者が負傷したりする可能性があります。質問がある場合は、ベンダーのサービスおよびサポートにお問い合わせください。ご使用の地域用の紙の資料は、マシンの近くの保管場所に保存しておく必要があります。最新リビジョンの資料は、ベンダーの **Web** サイトから入手可能です。
- 使用前には、毎回スタビライザーのブレーキ機能をテストして確認してください。スタビライザーのブレーキを固定した状態で、過剰な力でリフト・ツールを動かしたり回転させたりしてはなりません。
- わずかな位置決めを除き、プラットフォームが上がっている状態でリフト・ツールを移動させてはなりません。
- 定められた積載能力を超えてはなりません。引き伸ばされたプラットフォームの中央と端における最大積載量については、積載能力チャートを参照してください。
- 積載量が増加するのは、プラットフォームの中央に適切に配置されている場合のみです。スライドさせたプラットフォームの柵の端には、**91 kg** を超える装置を置いてはなりません。また、装置の重心も考慮する必要があります。
- プラットフォーム傾斜ライザー・アクセサリ・オプションの隅に荷重をかけないでください。使用する前に、プラットフォーム・ライザー傾斜オプションは、提供されたハードウェアのみを使用して、メインの柵の **4 (4x)** カ所すべてに固定してください。積載オブジェクトは、大きな力を加えなくてもプラットフォーム上で簡単にスライドするように設計されているため、押したり寄り掛かったりしないように注意してください。ライザー傾斜オプションは、最終的な微調整 (必要な場合) を除き、常に平行な状態を維持してください。
- 突き出した積載の下には立たないでください。
- 表面に段差がある場所や傾斜 (大きなスロープ) では使用しないでください。
- 装置を積み重ねないでください。
- 薬物やアルコールの影響がある状態で操作を行ってはなりません。
- リフト・ツールに対して踏み台で支えてはなりません。
- 倒れる危険があります。プラットフォームが上がった状態で装置を押したり寄り掛かったりしてはなりません。
- 人を持ち上げるためのプラットフォームや階段として使用してはなりません。人を乗せるためのものではありません。
- リフトのどの部分にも立ってはなりません。階段ではありません。
- マストに登ってはなりません。
- 損傷あるいは誤動作しているリフト・ツール・マシンを操作してはなりません。
- プラットフォームの下には、押し潰されたり挟まったりする危険な場所があります。装置を下ろす場合は、必ず人や障害物がない場所で行ってください。作業中は、手足に十分に注意してください。
- フォークではありません。パレット・トラック、ジャック、あるいはフォーク・リフトを使用して、むき出しのリフト・ツール・マシンを持ち上げたり移動したりしてはなりません。
- マストはプラットフォームより高い位置まで伸びます。天井の高さ、ケーブル・トレイ、スプリングラー、電灯、およびその他の頭上にある物に注意してください。
- 装置を上げた状態でリフト・ツール・マシンから離れないでください。
- 装置が動作しているときは、手、指、衣類に十分に注意してください。

- ウィンチは、手の力のみで回転させてください。ウィンチ・ハンドルを片手で回すのが困難である場合は、荷重が大きすぎる可能性が高いです。プラットフォーム・トラベルの最上部または最下部を超えてウィンチを回さないでください。過度に巻き戻すと、ハンドルが外れてケーブルが損傷します。下げたり巻き戻したりする場合は、常にハンドルを保持してください。ウィンチ・ハンドルを離す前に、ウィンチが装置を保持していることを必ず確認してください。
- ウィンチの事故は、重傷の原因となる可能性があります。人を動かすためのものではありません。装置を引き上げる際には、クリック音が聞こえることを確認してください。ハンドルを離す前に、ウィンチが所定の位置にロックされていることを確認してください。このウィンチで作業する前に、手順を示すページをお読みください。絶対にウィンチが勝手に巻き戻ることがないようにしてください。ウィンチが勝手に回転すると、ケーブルが不規則にウィンチ・ドラムの周囲に巻かれたり、ケーブルが損傷したり、重傷の原因となる可能性があります。(C048)

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。

DC 電源システムは、GR-1089-CORE に記載されているとおり、Common Bonding Network (CBN (共通ボンディング・ネットワーク)) に設置されることを意図したものです。

ハードウェア管理コンソールの取り付けおよび構成

ハードウェア管理コンソール (HMC) ハードウェアの取り付け方法、その管理対象システムへの接続方法、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。

注: IBM Power® System S824L (8247-42L) サーバーでは仮想化はサポートされていません。

HMC の取り付けおよび構成での新機能

HMC の取り付けおよび構成に関して、このトピックをまとめた前回の更新以降の、新機能および大きな変更情報をお読みください、

2017 年 8 月

- HMC Classic インターフェースは、ハードウェア管理コンソール (HMC) バージョン 8.7.0 以降ではサポートされなくなりました。以前に HMC Classic インターフェースで使用可能だった機能は、HMC Enhanced+ インターフェースで使えるようになりました。
- 以下のトピックが追加されました。
 - 46 ページの『ラックへの 7063-CR1 の取り付け』
 - 159 ページの『BMC 接続の構成』
- 46 ページの『ラックへの 7063-CR1 の取り付け』のトピックが追加されました。

2016 年 10 月

- 16 ページの『HMC ポートの位置』のトピックが更新されました。

2016 年 5 月

- 36 ページの『7042-CR9 HMC のラックへの取り付け』のトピックが追加されました。

2015 年 10 月

- 58 ページの『HMC 仮想アプライアンスの取り付け』のトピックが追加されました。
- 以下のトピックが更新されました。
 - 86 ページの『インターネット SSL アドレス・リスト』
 - 89 ページの『HMC 構成の準備』

2015 年 6 月

- HMC バージョン 8.2.0 に付属のオプションだった HMC Enhanced + Tech Preview (Pre-GA) インターフェースの手順および機能は、HMC バージョン 8.3.0 に付属の HMC Enhanced+ インターフェースと同じです。資料で言及しているのは HMC Enhanced+ についてのみですが、内容は HMC Enhanced + Tech Preview (Pre-GA) インターフェースにも当てはまります。
- HMC バージョン 8.2.0 に付属のオプションだった HMC Enhanced インターフェースの手順および機能は、HMC バージョン 8.3.0 に付属の HMC Enhanced+ インターフェースの一部になりました。
- 131 ページの『HMC Enhanced+ インターフェースを使用した HMC の構成』のセクションが追加されました。

- 118 ページの『「コール・ホーム用イベント・マネージャー」の構成』のトピックが更新されました。

2014 年 10 月

- 以下のトピックが追加されました。
 - 26 ページの『ラックへの 7042-CR7 および 7042-CR8 の取り付け』
 - 118 ページの『「コール・ホーム用イベント・マネージャー」の構成』
- 101 ページの『HMC の始動』のトピックが更新されました。

2014 年 6 月

- POWER8 プロセッサを搭載した IBM Power Systems サーバーに関する情報を追加しました。

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タスクの概要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: POWER8® プロセッサ・ベースのサーバーを管理する場合、HMC はバージョン 8.1.0 でなければなりません。詳しくは、123 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。	90 ページの『HMC 用のプリインストール構成ワークシート』 89 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。	4 ページの『スタンドアロン HMC の配線』 15 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。	98 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』 99 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。	126 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。	

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 3. 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。	90 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。	4 ページの『スタンドアロン HMC の配線』 15 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。	123 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』 126 ページの『HMC ソフトウェアのアップグレード』

表 3. 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 (続き)

作業	関連情報の入手先
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。	99 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。	112 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 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。

スタンドアロン HMC を管理対象システムにケーブル接続することができます。

1. HMC は、必ず正しい位置に置くようにしてください。
2. モニター・コネクタにモニター・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、電源コネクタのそばにあります。スイッチを動かして、お客様の地域で使用する電圧が表示されるようにしてください。
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・プロシーチ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。



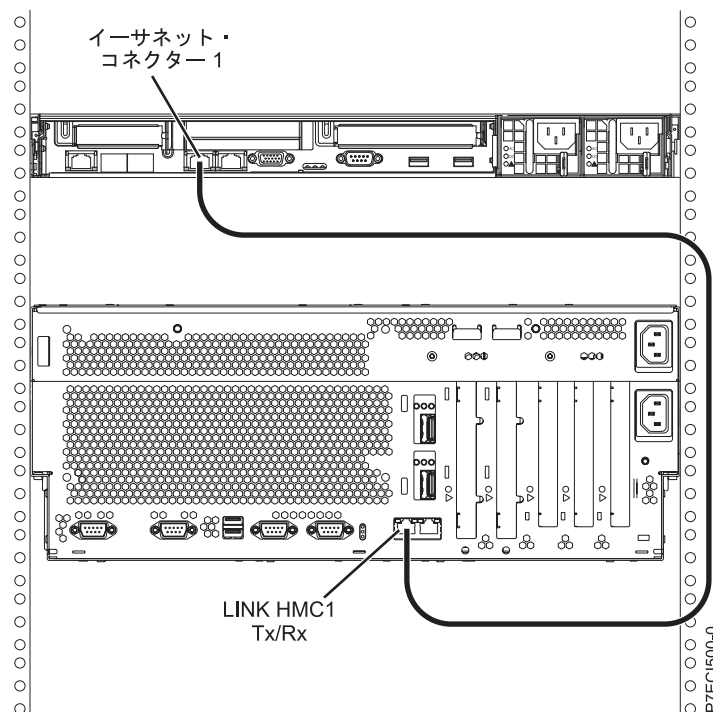
IPHA1522-0

- 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取り付け済みの場合は、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 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。98 ページの『HMC の構成』から続行します。

関連概念:

83 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。

79 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・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。

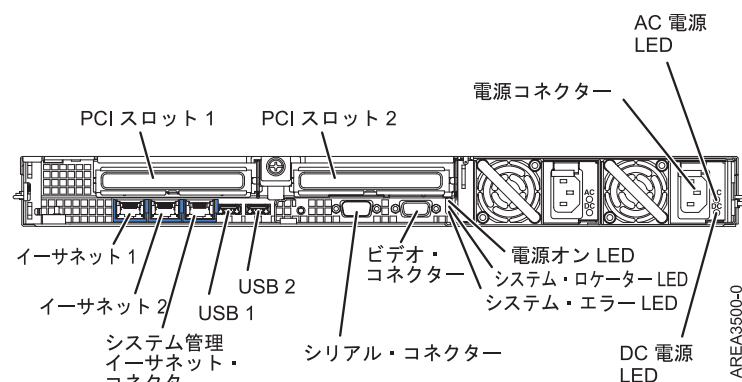


図 1. 7310-CR4 の背面図

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。

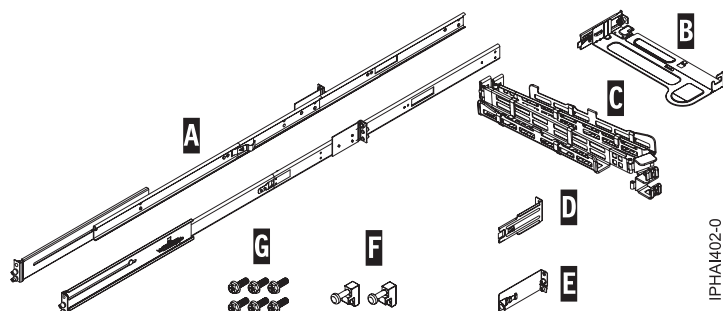


図 2. レール・キット

表 4. 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・ストライク (2)
- G ねじ (6)

重要: このシステム装置は 1 つの EIA 単位の高さです。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。

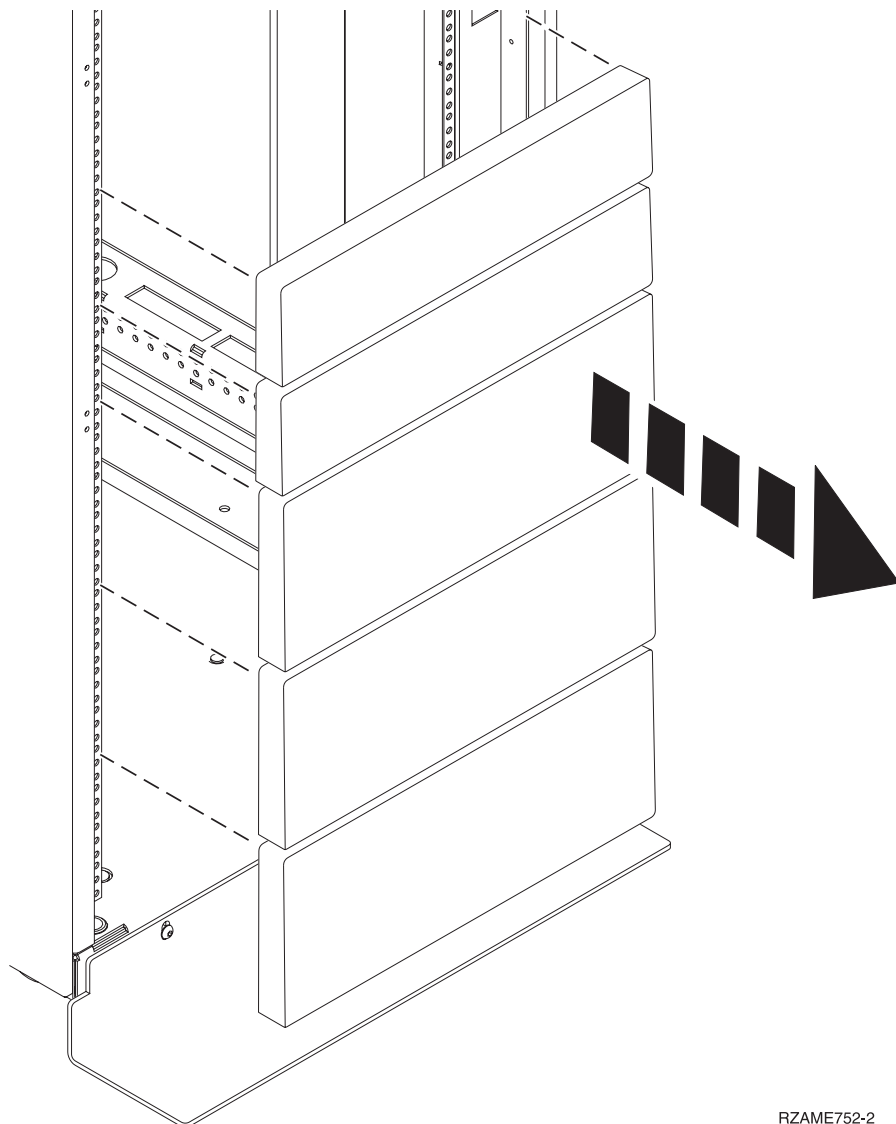
部品の間違い、欠落、または損傷がある場合は、IBM 販売店またはIBM 営業およびサポートにご連絡ください。

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. システムをラックに取り付けることにします。EIA の位置を記録します。

注: ご使用のラックでの 1 EIA 単位は、3 つの穴のグループで構成されています。

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 単位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 単位の下部の穴と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 (8 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、ラックの前面でマークを付けた最下段の EIA 単位に対応する EIA 単位を見つけます。
7. 最下段の EIA 単位に接着ドットを貼り付けます。
8. EIA 単位の上部の穴に接着ドットを付けます。
9. ラック左側の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方法について説明します。

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、ラックの背面右側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 単位の下部および中央の穴 **(B)** から突き出ます。

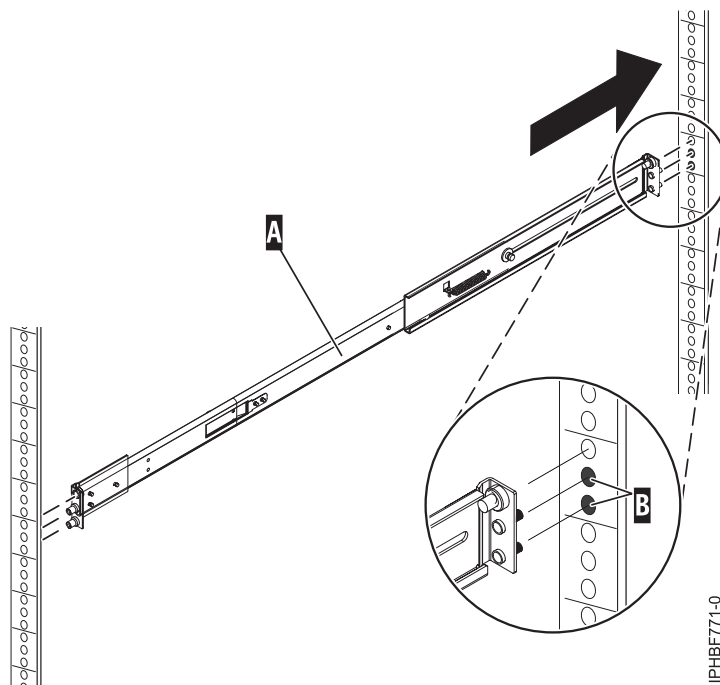


図 4. 右スライド・レールのラック背面への取り付け

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 単位の下部および中央の穴 **(B)** から突き出ます。

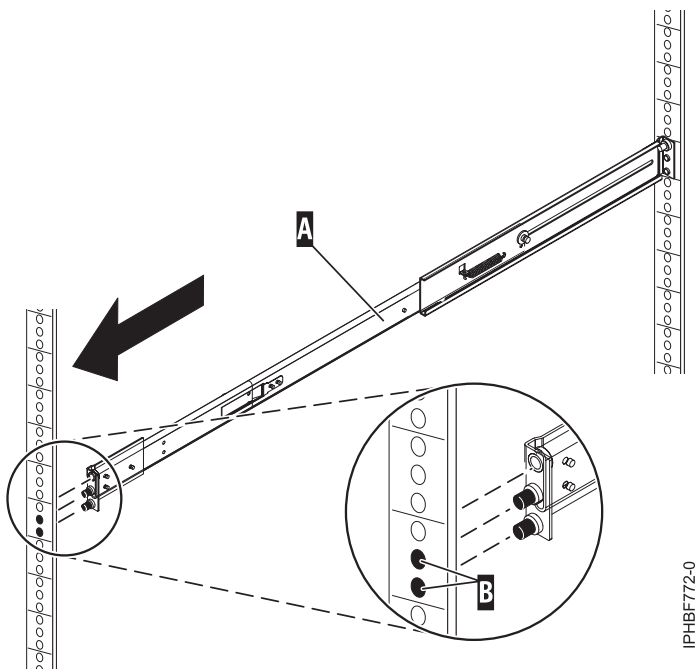


図 5. 右スライド・レールのラック前面への取り付け

3. ステップ 1 (9 ページ) から 2 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・ストライク **(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。

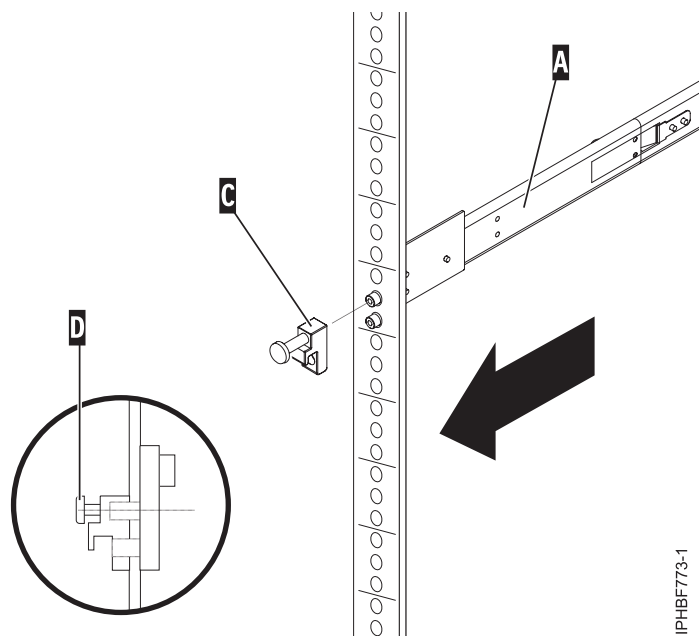


図 6. ラッチ・ストライクのレールの前面への取り付け

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。

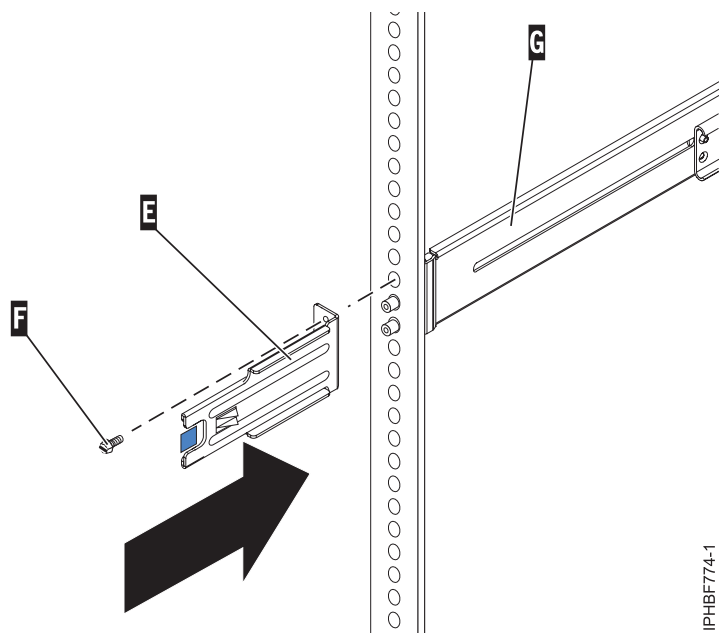


図 7. ケーブル・マネージメント・ブラケットの左背面レールへの取り付け

7. このシステムを輸送する計画がない場合は、『スライド・レールへの HMC 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)** の背面右側に取り付けます。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。

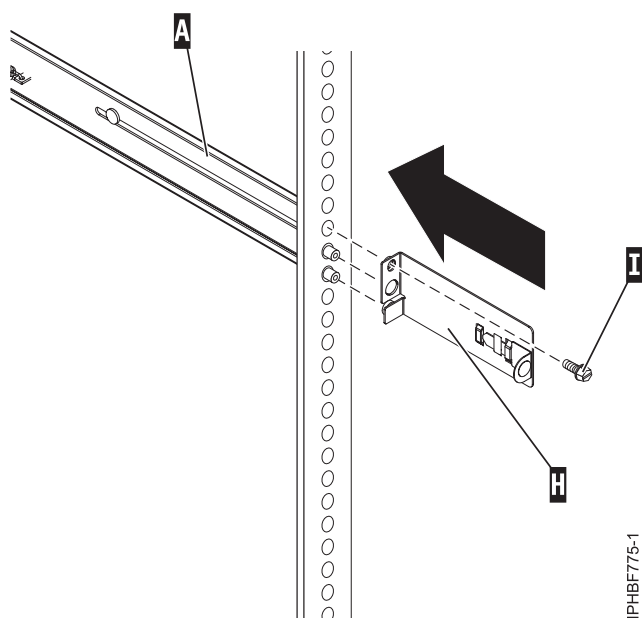


図 8. 右背面レールへのケーブル・マネージメント・サポート・ブラケットの取り付け。

スライド・レールへの HMC の取り付け

スライド・レールへの HMC 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 を取り付けの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。

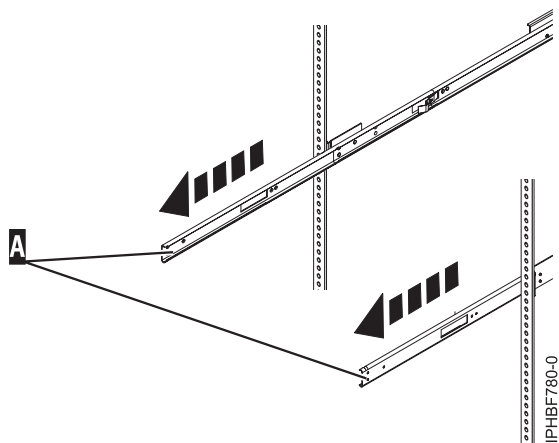


図 9. スライド・レールの延長

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 をレールの高さを持ち上げ、ホイールのセット **(B)** が HMC の背面のレール・ガイド間にくるようにします。

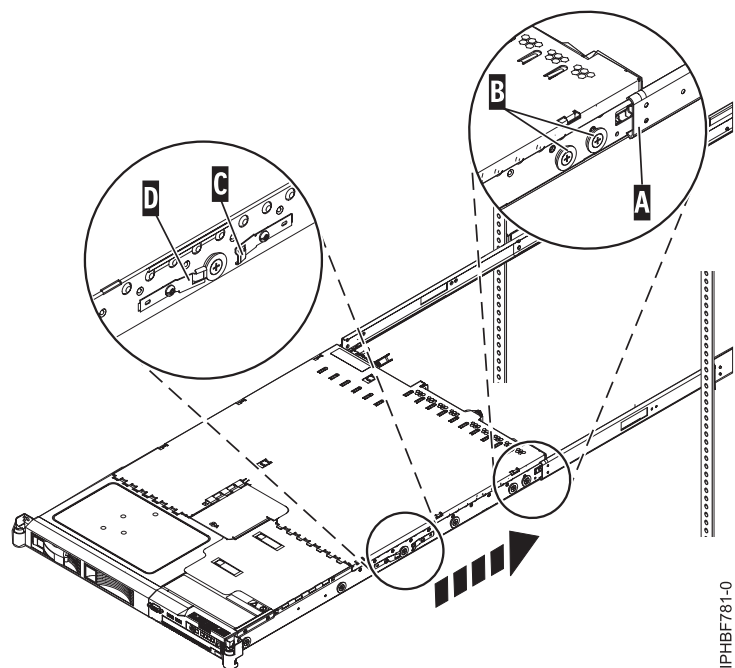


図 10. スライド・レールへの HMC の取り付け

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稼働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。

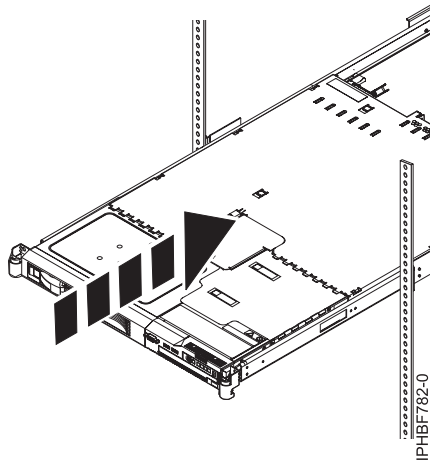


図 11. HMC のラック内へのスライド

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。

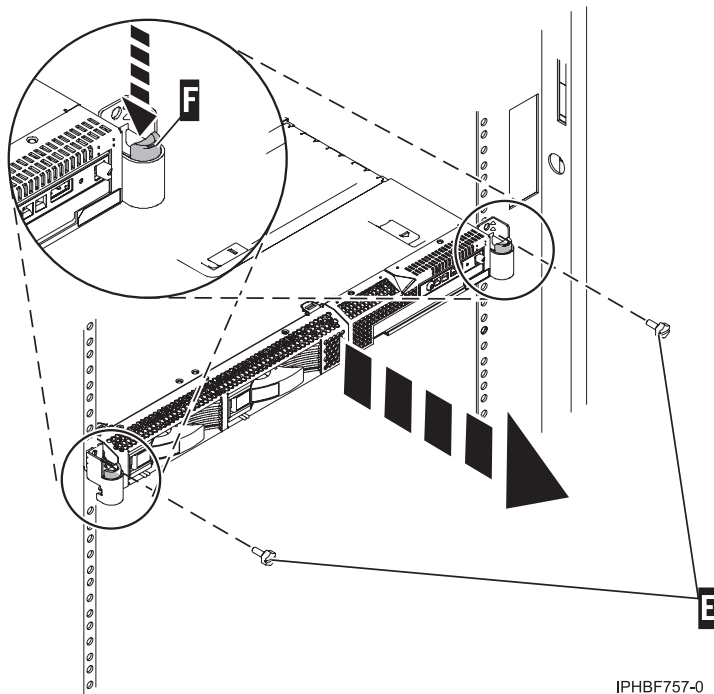


図 12. ラック・ラッチとねじ

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、(ラックの背面から見て) 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・マネジメント・アーム・フランジ **(A)** を見つけます。
2. ケーブル・マネジメント・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。

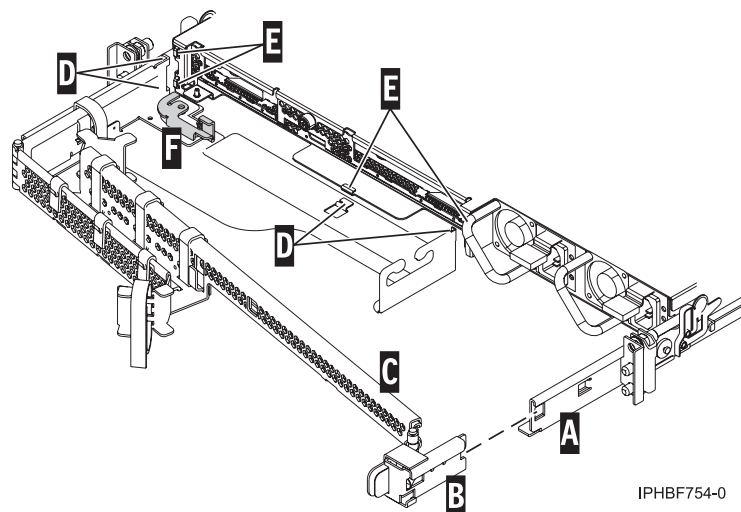


図 13. ケーブル・マネジメント・アームおよびシステム装置。

3. ケーブル・マネジメント・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

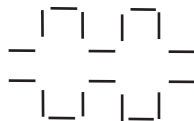
ラック・マウント HMC を物理的に取り付ける方法について説明します。

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、6 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、83 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。



IPHA1522-0

- 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、83 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、79 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取り付け済みの場合は、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。98 ページの『HMC の構成』から続行します。

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。

モデル 8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置

以下の図と表を使用して、8247-21L、8247-22L、8284-21A、または 8284-22A 上の HMC ポートを対応させます。

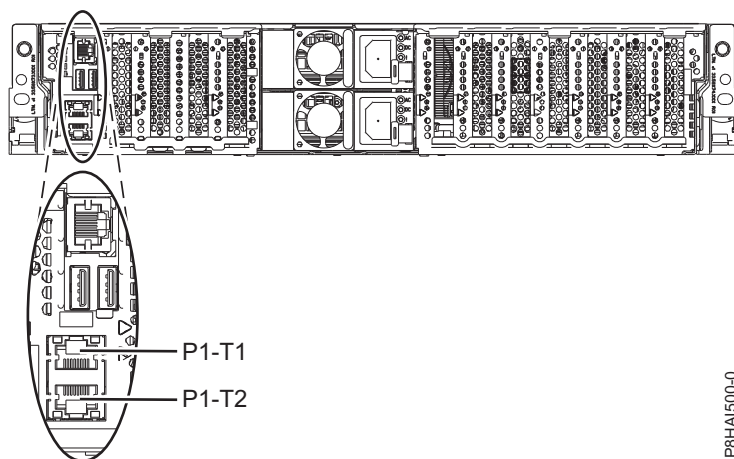


図 14. 8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置

表 5. 8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-T1	いいえ
HMC ポート 2	Un-P1-T2	いいえ

8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置について詳しくは、n and location codes for 8247-21L、8247-22L、または 8284-22A の部品の位置およびロケーション・コードを参照してください。

モデル **8247-42L**、**8286-41A**、または **8286-42A** の HMC ポート位置

以下の図と表を使用して、8247-42L、8286-41A、または 8286-42A 上の HMC ポートの位置を対応させます。

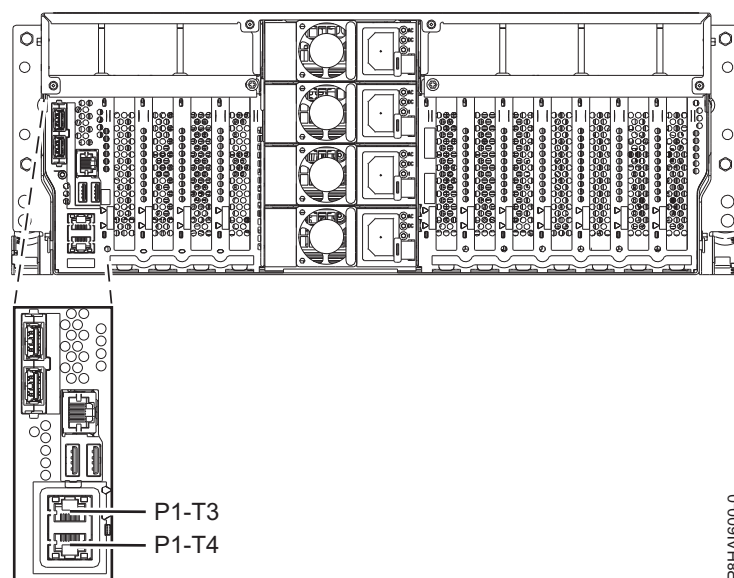


図 15. ラック図 - 8247-42L、8286-41A、または 8286-42A の HMC ポート位置

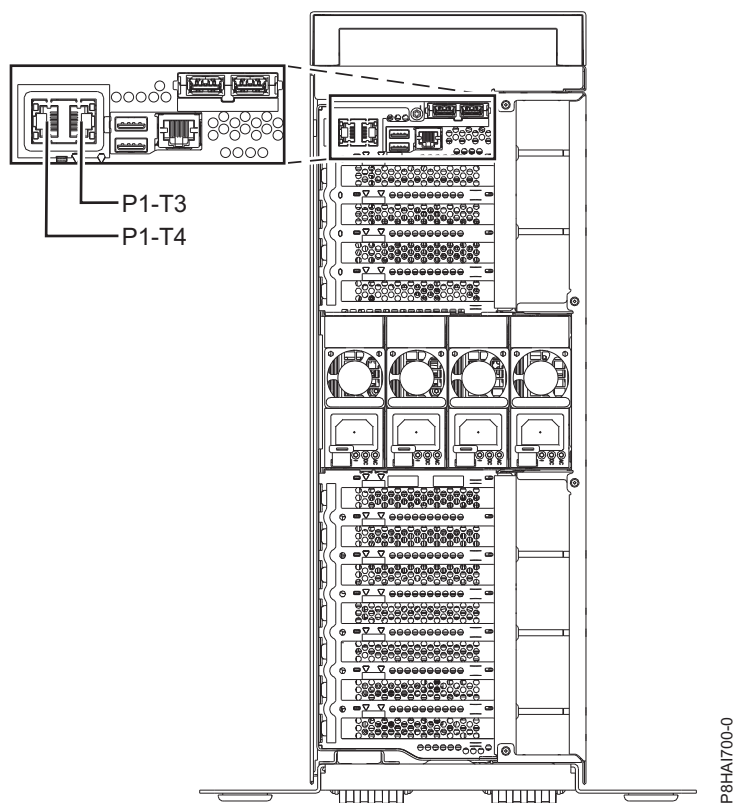


図 16. タワー図の 8286-41A HMC ポート位置

表 6. 8247-42L、8286-41A、または 8286-42A の HMC ポート位置

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
8247-42L、8286-41A、または 8286-42A 上の HMC ポート位置について詳しくは、『Part location and location codes for 8247-42L, 8286-41A, or 8286-42A』を参照してください。		

モデル 9080-MHE、9080-MME、9119-MHE、および 9119-MME の HMC ポート位置

以下の図と表を使用して、9080-MHE、9080-MME、9119-MHE、および 9119-MME 上に HMC ポートをマップします。

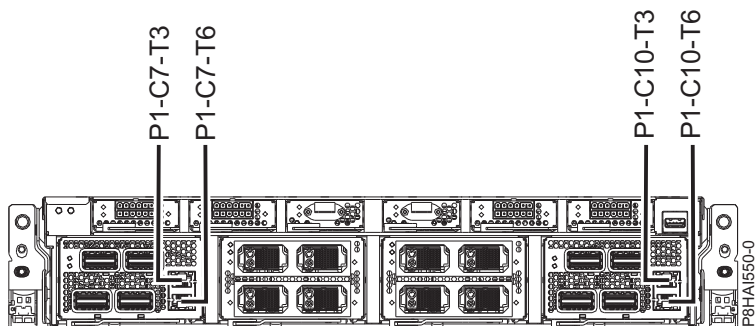


図 17. 9080-MHE、9080-MME、9119-MHE、および 9119-MME の HMC ポート位置

表 7. 9080-MHE、9080-MME、9119-MHE、および 9119-MME の HMC ポート位置

ポート	物理ロケーション・コード	識別 LED
サービス・プロセッサ・カード 1 - HMC ポート 1	Un-P1-C7-T3	いいえ
サービス・プロセッサ・カード 1 - HMC ポート 2	Un-P1-C7-T6	いいえ
サービス・プロセッサ・カード 2 - HMC ポート 1	Un-P1-C10-T3	いいえ
サービス・プロセッサ・カード 2 - HMC ポート 2	Un-P1-C10-T6	いいえ
9080-MHE、9080-MME、9119-MHE、および 9119-MME 上の HMC ポート位置について詳しくは、『部品の位置と、9080-MHE、9080-MME、9119-MHE、または 9119-MME の位置のロケーション・コード』を参照してください。		

モデル 8408-44E および 8408-E8E の HMC ポート位置

以下の図と表を使用して、8408-44E および 8408-E8E 上の HMC ポートを対応させます。

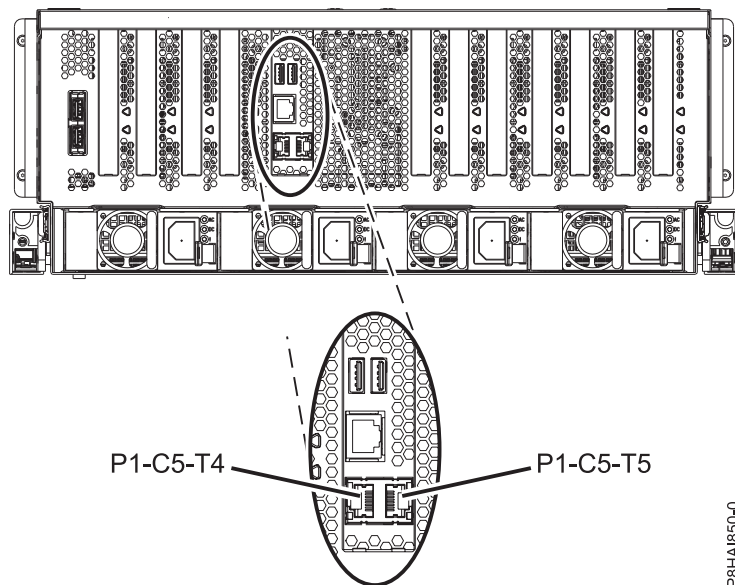


図 18. 8408-44E および 8408-E8E の HMC ポート位置

表 8. 8408-44E および 8408-E8E の HMC ポート位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-C5-T4	いいえ
HMC ポート 2	Un-P1-C5-T5	いいえ
8408-44E および 8408-E8E 上の HMC ポート位置について詳しくは、部品の位置と、8404-44E および 8408-E8E の位置のロケーション・コード (Part location and location codes for 8408-44E and 8408-E8E location)を参照してください。		

7042-CR5 および 7042-CR6 のラックへの取り付け

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

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。

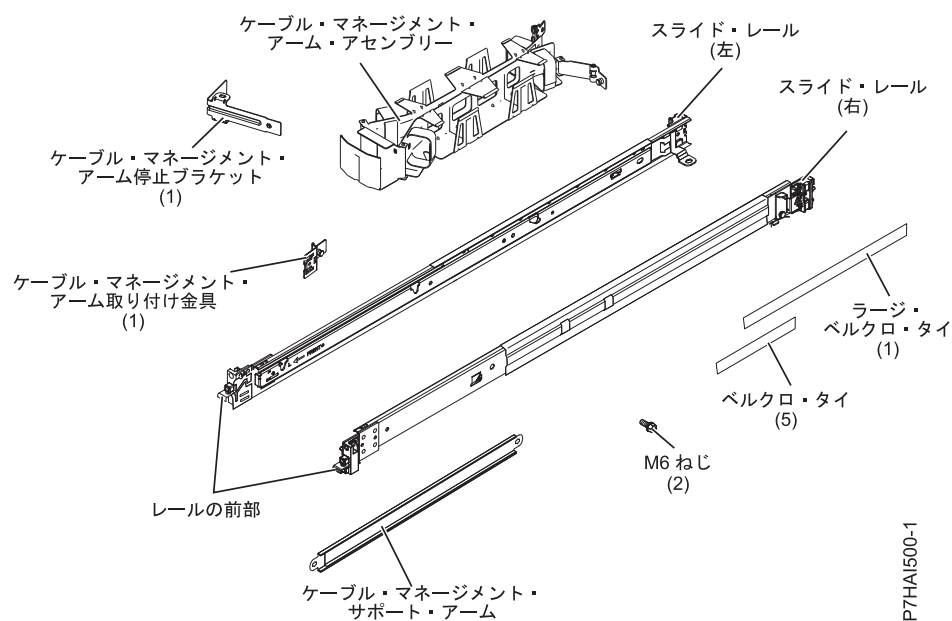


図 19. 部品目録

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 HMC または 7042-CR6 HMC をラックに取り付けるには、次の手順を実行します。

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。

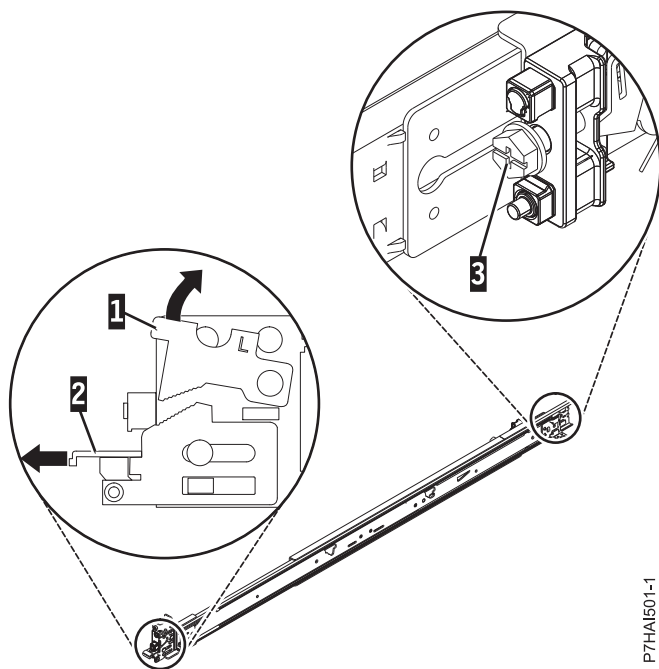


図 20. スライド・レールと可動式タブ

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。

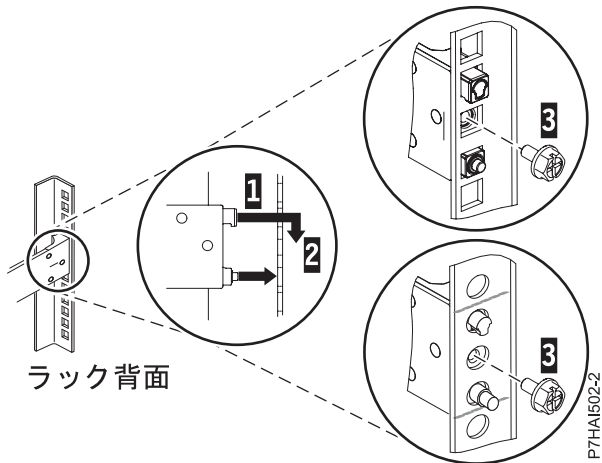


図 21. ピンとラック後部の穴の位置合わせ

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 を繰り返して、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。

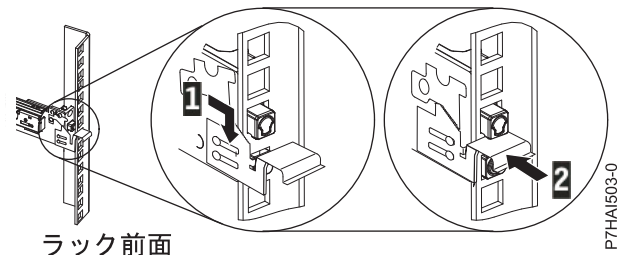


図 22. ラック前部のレールとピン

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。

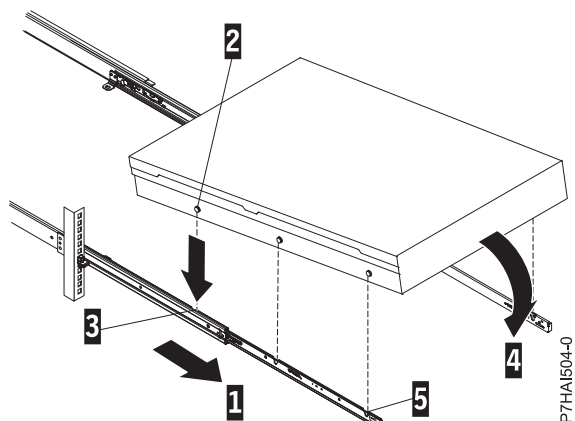


図 23. 引き出したスライド・レールと、レールのスロットと位置合わせしたサーバーのくぎの頭

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。

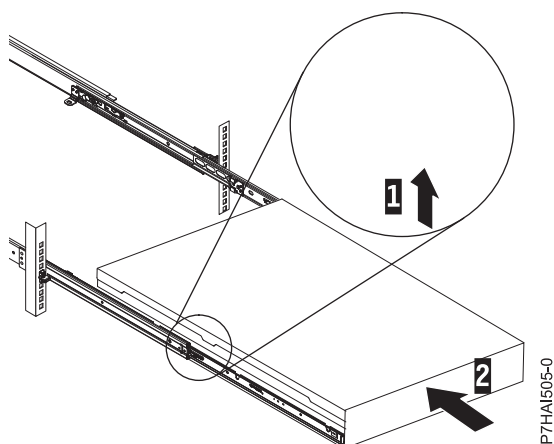


図 24. リリース・ラッチとサーバー

6. ケーブル・マネジメント・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。

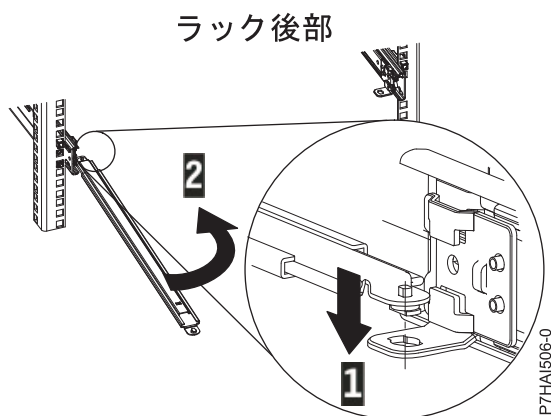


図 25. サポート・アームの接続

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。

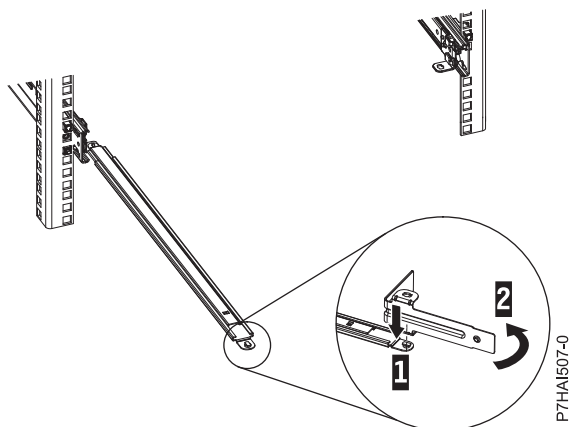


図 26. サポート・アームに固定されたケーブル・マネージメント停止ブラケット

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。

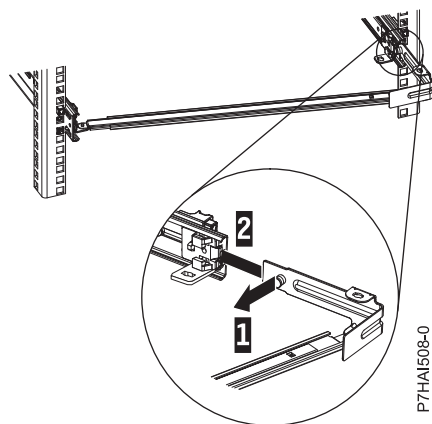


図 27. 引き出したピンと、スライド・レールに取り付けたブラケット

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。

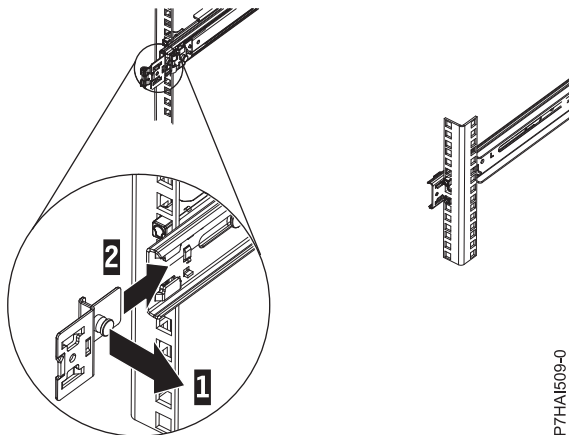


図 28. 引き出した取り付け金具のピンと、スライド・レールに取り付けた取り付け金具

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。

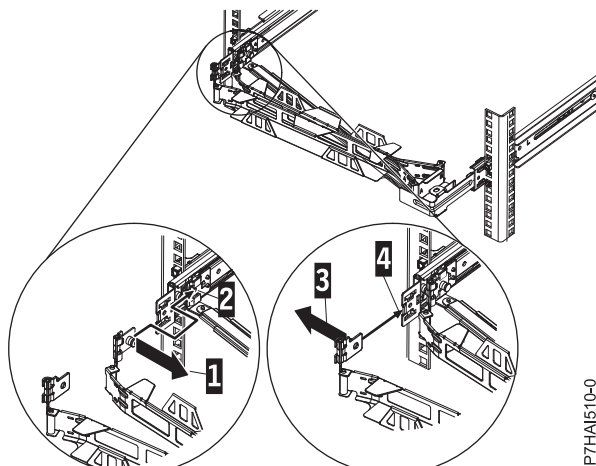


図 29. ケーブル・マネージメント・アームの接続

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に、すべてのケーブルに遊びを持たせます。

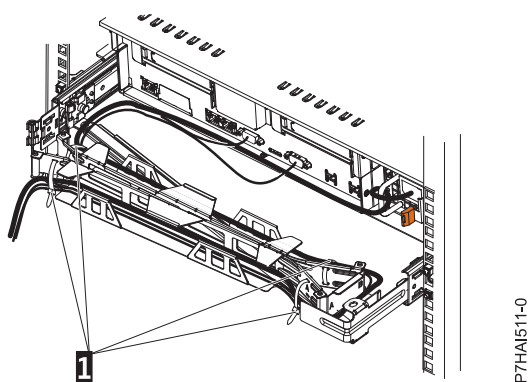


図 30. 電源コードの接続と配線

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。

ラックへの 7042-CR7 および 7042-CR8 の取り付け

7042-CR7 および 7042-CR8 のハードウェア管理コンソール (HMC) をラックに取り付ける方法について説明します。

部品目録を確認します。次の図は、サーバーをラック・キャビネットに取り付けるの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。

ケーブル・マネージメント・アーム・ボックスの内容

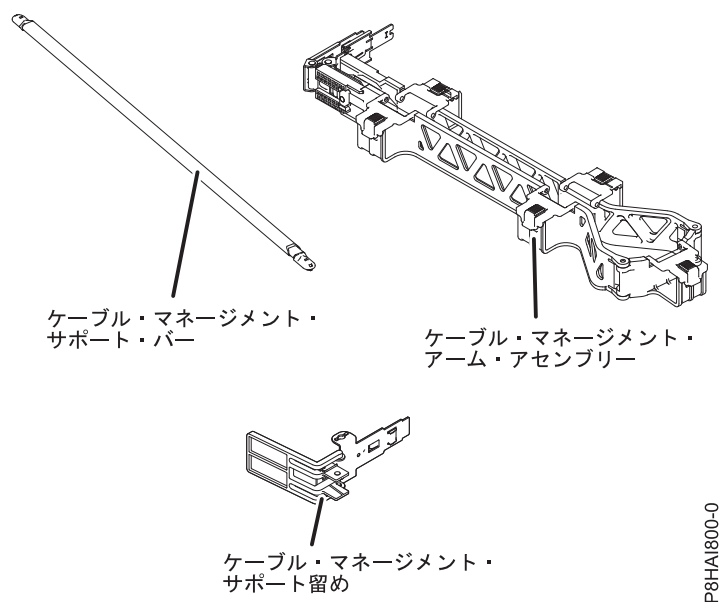
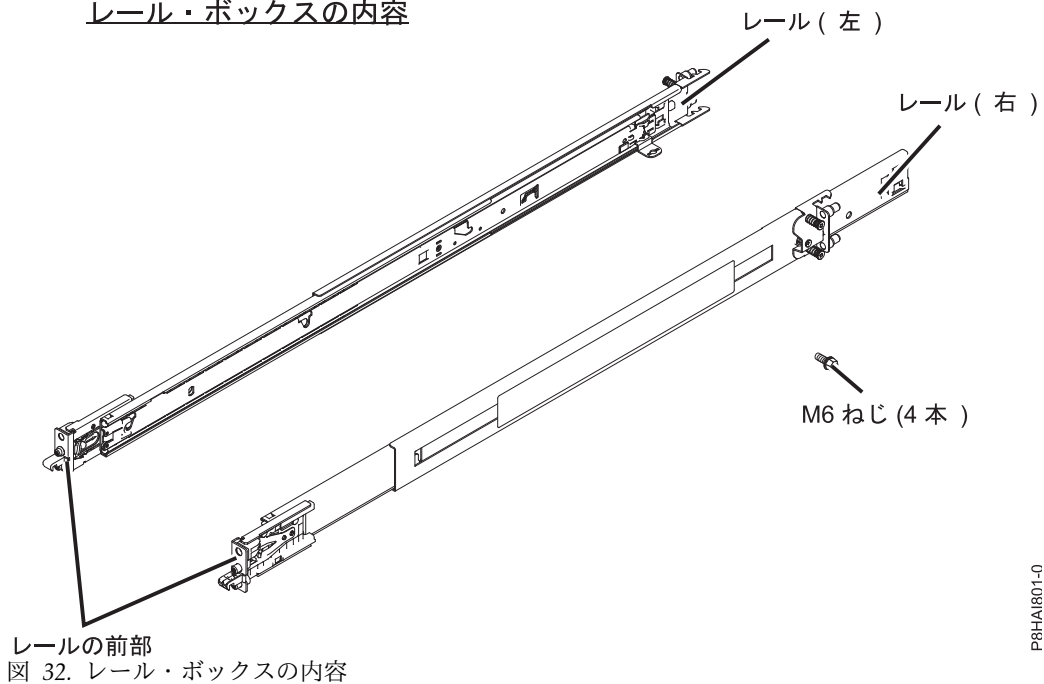


図 31. ケーブル・マネージメント・アーム・ボックスの内容

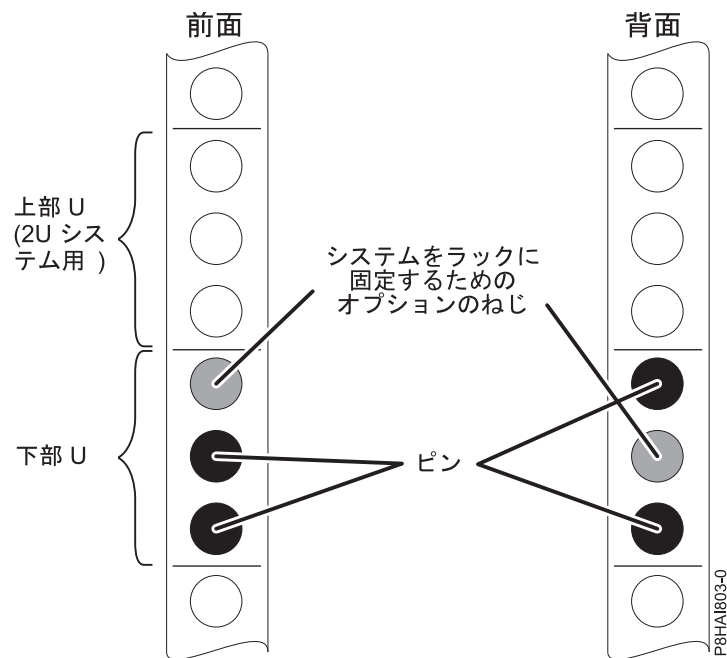
レール・ボックスの内容



注: この取り付けのためには、スライド・レール・ボックスとケーブル・マネージメント・アーム・ボックスの両方が必要です。

7042-CR7 HMC または 7042-CR8 HMC をラックに取り付けるには、以下の手順を実行します。

1. サーバーを取り付けるラック内の使用可能な 1U スペースまたは 2U スペース (取り付けるサーバーによって異なります) を選択します。



注: 2U スペース・サーバーを取り付ける場合は、必ず、スライド・レールをラックの 2U の領域の下部 U に取り付けてください。

2. 各スライド・レールの端には、「左前/後 (Left Front/Rear)」または「右前/後 (Right Front/Rear)」のマークが付いています。スライド・レールの 1 つを選択し、カチッと音がして所定の位置に収まるまで後部ブラケットを最後まで引きます。

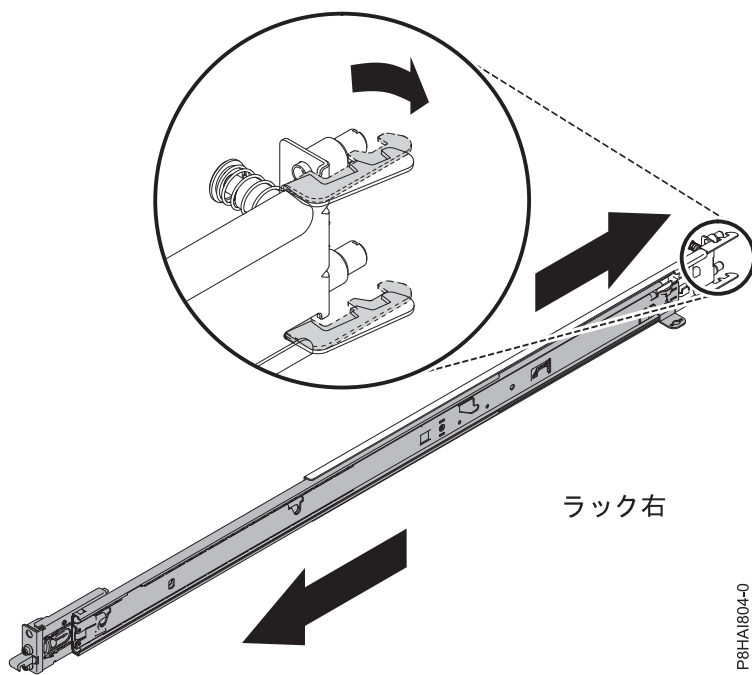


図 34. スライド・レールと可動式タブ

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。

3. ラックの前面から、ラックの後部にある、選択した U のスライド・レールの後部で 2 本のピンを揃えます。ピンが穴に入るようにレールを押し、スライド・レールの後部がラックにロックされるまで、レールをスライドさせてラックに入れます。

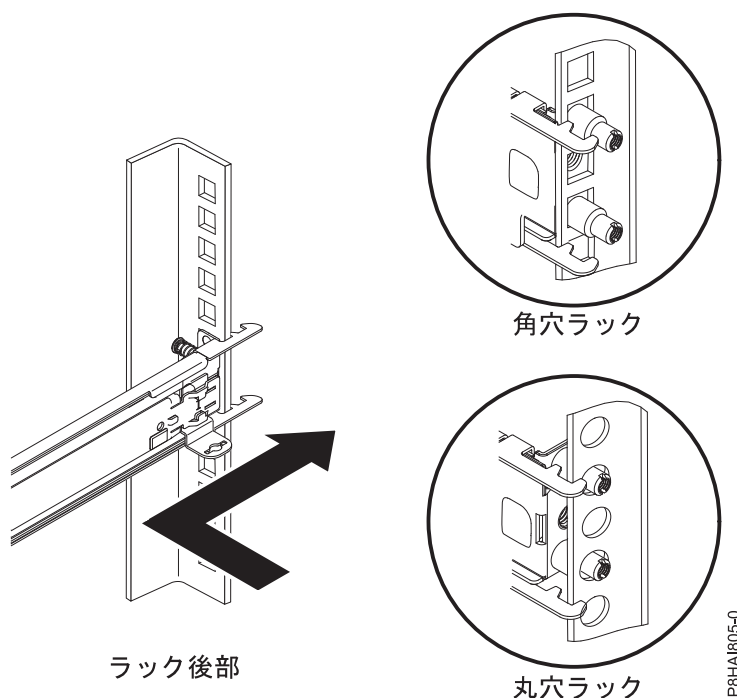


図 35. ピンとラック後部の穴の位置合わせ

注: スライド・レールを 1U スペースに取り付ける場合、装置が既にこの 1U スペースの真上および真下に取り付けられているのであれば、レールを伸ばして、スライド・レールの後部をラックの後部までスライドさせる必要があります。

4. 前部スライド・レール・ラッチを開きます。このラッチを受け取ったときに閉じていた場合は、青いボタンを中に押し、ラッチを元に戻して開いてください。

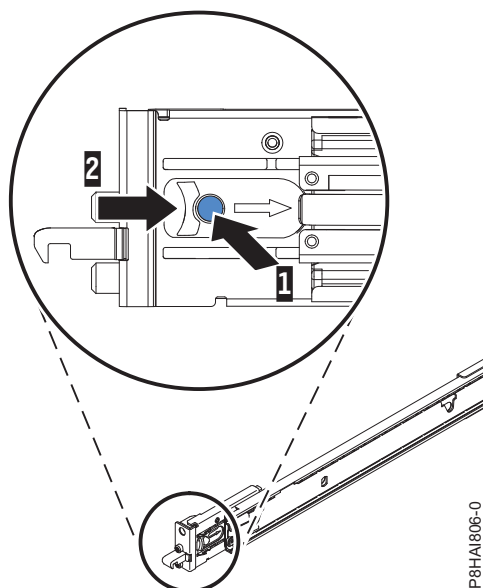


図 36. 前部スライド・レール・ラッチ

5. スライド・レールを前方に押し、前部ラッチをラック EIA レールの前にある該当する U スペースに固定します。レールの長さを調整してください。前部ラッチをラックの EIA レールの前に置いた状態で、前部の端が回転して位置に入っていくことを確認します。

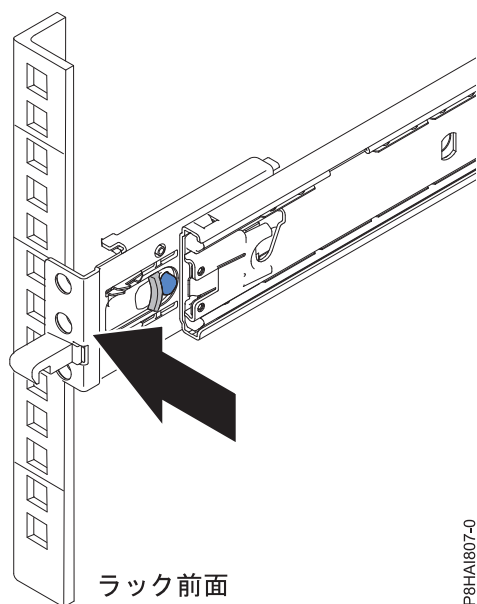


図 37. ラック前面のレールとピン

6. 青いボタンを押して、ブラケットをピンで閉じます。スライド・レールを上下に動かして、レールを完全にかみ合わせます。ステップ 1 から 5 を繰り返して、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かみ合っていることを確認します。

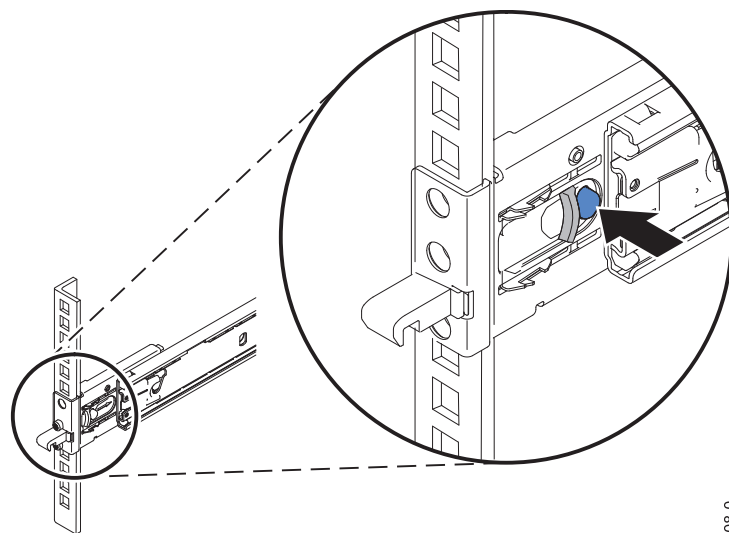


図 38. ラック前面のレールとピン

7. 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下ろします。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 (カチッという音が 2 回聞こえます) まで、サーバーの前部 **(3)** をゆっくりと下ろします。システムがスライド・レールに固定されるように、前部ラッチが前部のくぎの頭に被さっていることを確認します。

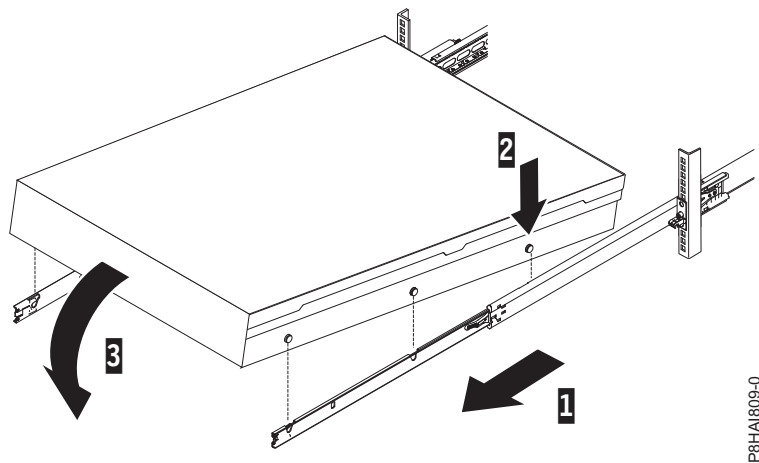


図 39. 引き出したスライド・レールと、レールのスロットと位置合わせしたサーバーのくぎの頭

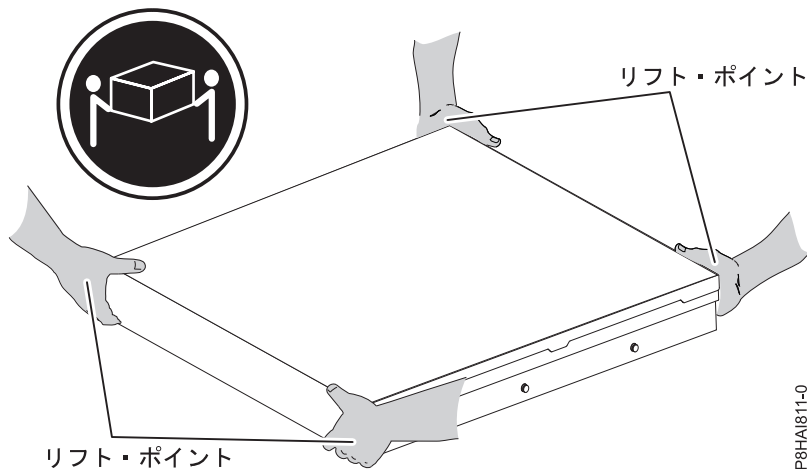


図 40. リフト・ポイント

注: 装置を持ち上げる場合には、安全に持ち上げる方法に従ってください。2U サーバーを取り付ける場合は、必ず 2 人でサーバーを持ち上げてください。持ち上げる人の手の位置は、図 40 に図示されているとおりにする必要があります。

8. スライド・レールのロック・レバー (1) を持ち上げ、カチッと音がしてサーバー (2) が所定の位置に収まるまでラックの中に押し込みます。

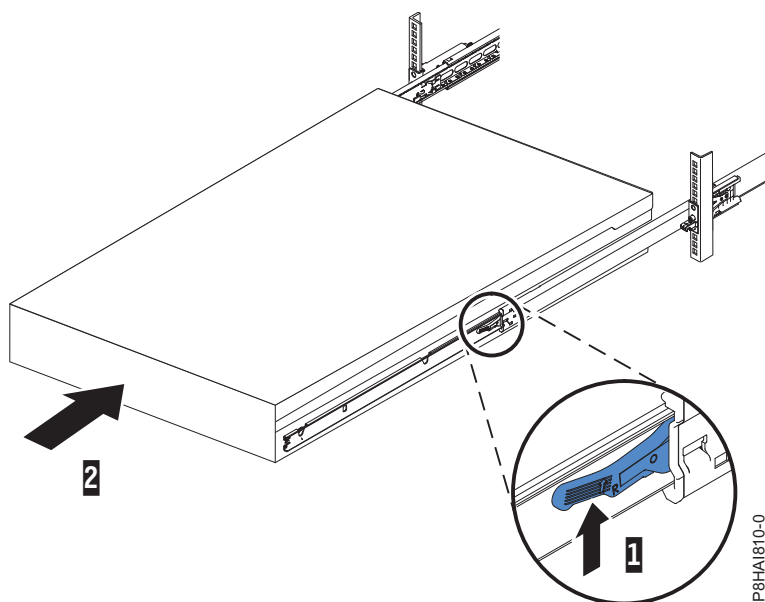
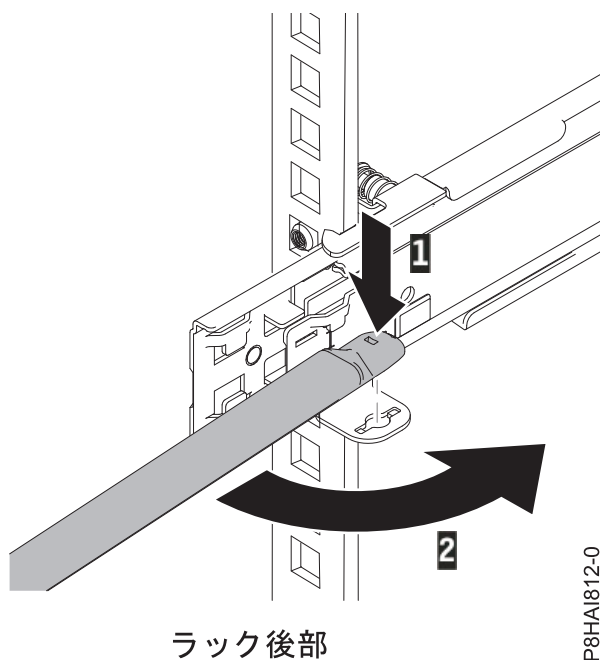


図 41. リリース・ラッチとサーバー

9. 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。



ラック後部

図 42. サポート・アームの接続

10. サポート・アームのもう一方の端をケーブル・マネージメント停止ブラケット **(1)** に接続します。ブラケット **(2)** を回して、サポート・アームに固定します。

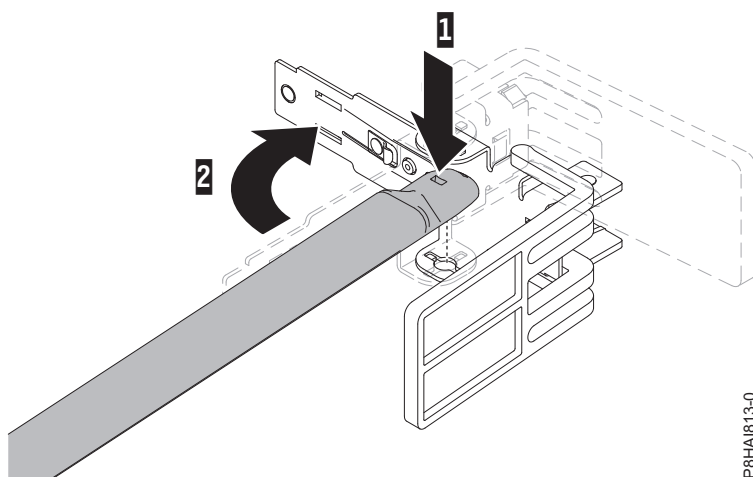


図 43. サポート・アームに固定されたケーブル・マネージメント停止ブラケット

11. 外側ピンと内側ピンを識別するために、ケーブル・マネージメント・アームのピンに大文字 **I** および **O** が印字されています。ケーブル・マネージメント停止ブラケット (大文字 **O** が付いているもの) を、サポート・アームの接続されていない方の端に取り付けます。サポート・アームがしっかり取り付けられていることを確認してください。

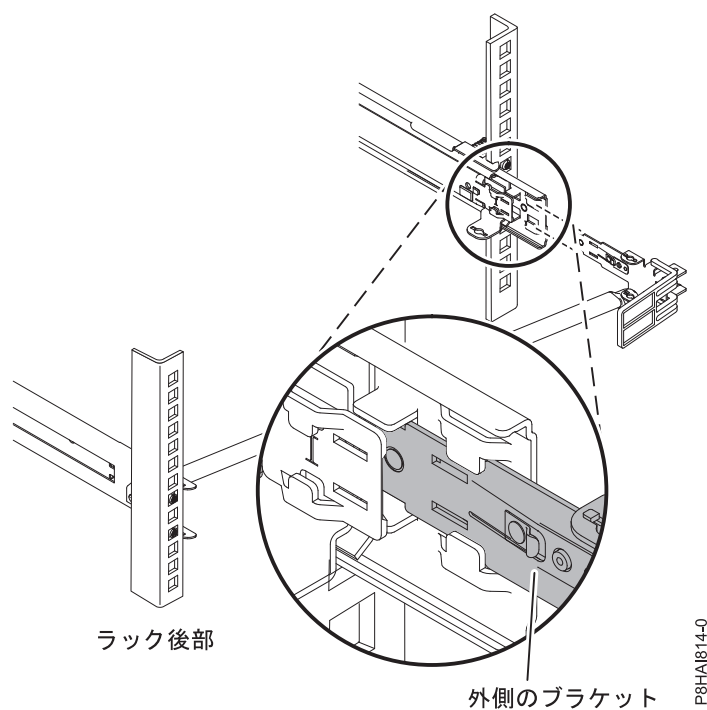
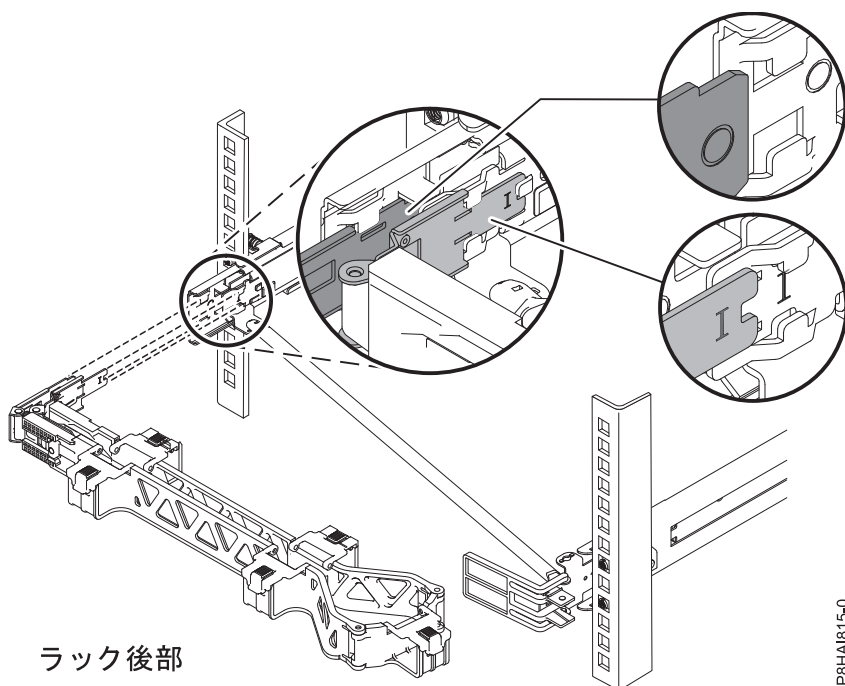


図 44. スライド・レールへの停止ブラケットの接続

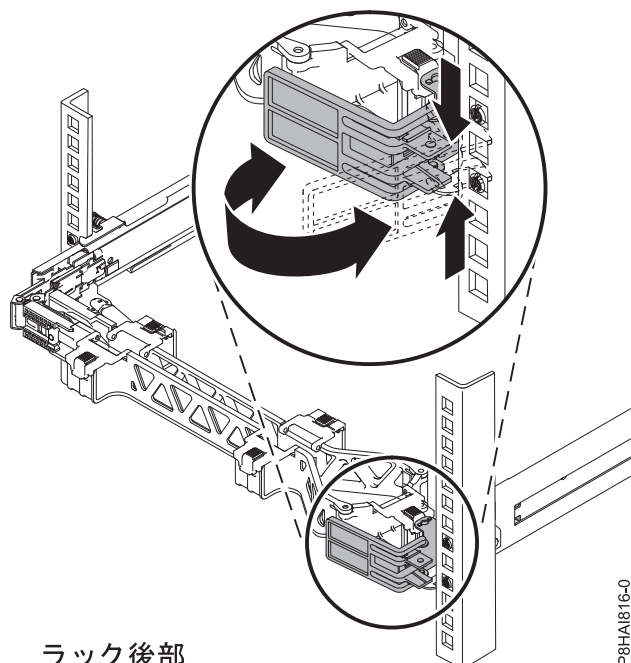
12. ケーブル・マネージメント・アームをサポート・アームに乗せます。ケーブル・マネージメント・アームの内側と外側の両方のピンを引き出し、次にケーブル・マネージメント・アーム・タブをスライドさせて、スライド・レールの内側と外側の両方のスロット内に入れます。タブが所定の位置に収まるまで押し込みます。



ラック後部

図 45. ケーブル・マネージメント・アームの接続

13. ケーブル・マネージメント・アームを容易に回転させてケーブル・マネージメント・サポート・アームに取り付けたり、アームから取り外したりできるように、停止ブラケットを閉じるための上下のタブを押して停止ブラケットを開くことができます。



ラック後部

図 46. ケーブル・マネージメント・サポート留めブラケット

14. 電源コードおよびその他のケーブル (必要の場合はキーボード、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・ストラップの位置は、システムによって若干異なる場合があります。システムの背面に備わっているケーブル・ストラップを使用して、ケーブルを保持し、ケーブルがたるまないようにします。

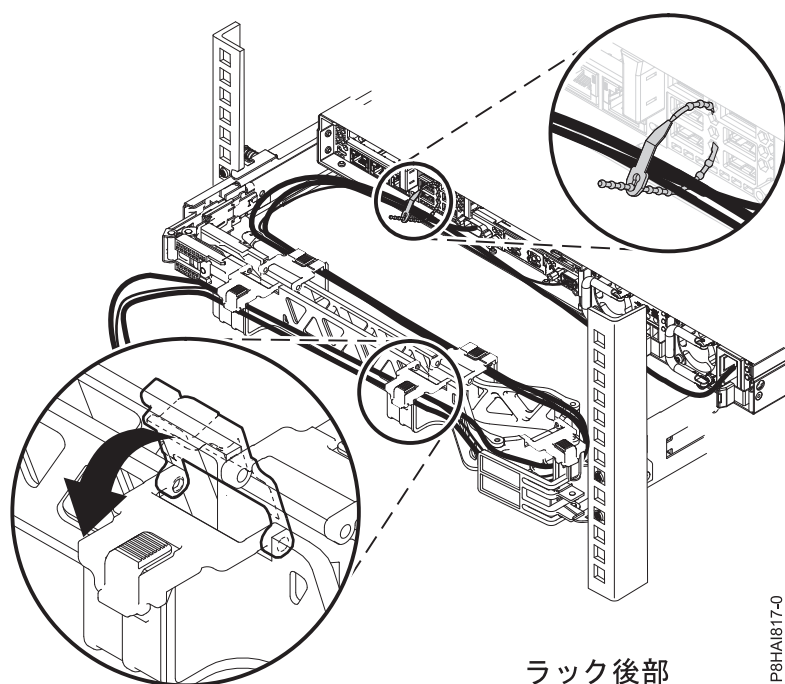


図 47. 電源コードの接続とケーブル配線

15. ケーブルは、ケーブル・マネージメント・アームが適切に動くように、面ファスナーで束ねる必要があります。

注: ケーブルが U スペースの下にたるんで下段のシステムに引っ掛からないようにしてください。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に、すべてのケーブルに遊びを持たせます。

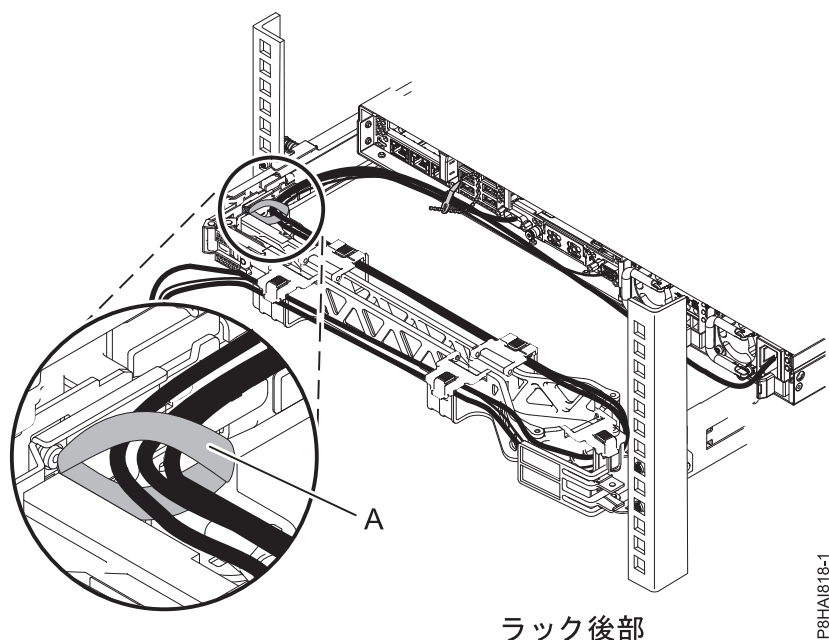


図 48. 面ファスナー

16. システムが取り付けられた状態でラックを配送する場合、または振動しやすい区域にラックがある場合は、スライドの後部に M6 ねじを挿入します。必要に応じて、ケーブル・タイを使用して、ケーブル・マネジメント・アームの固定されていない方の端をラックに固定します。

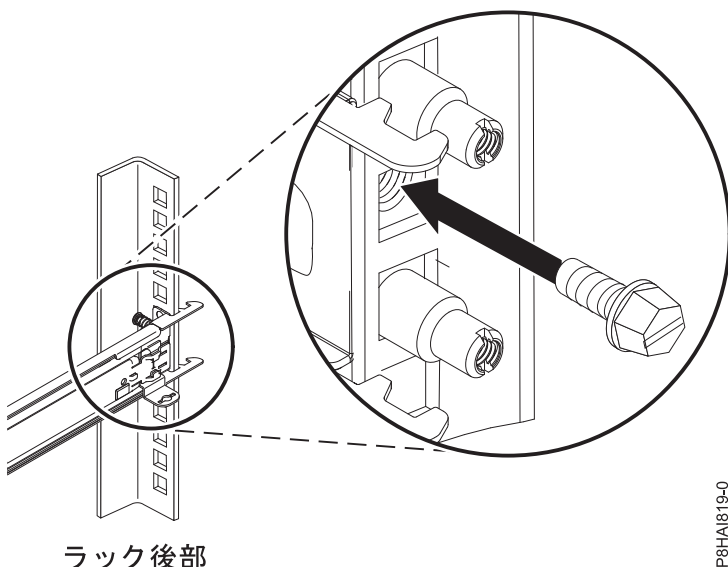


図 49. 配送のためのサーバーの固定

7042-CR9 HMC のラックへの取り付け

7042-CR9 ハードウェア管理コンソール (HMC) をラックに取り付ける方法について説明します。

部品目録を確認します。次の図は、サーバーをラック・キャビネットに取り付けるの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。

ケーブル・マネージメント・アーム・ボックスの内容

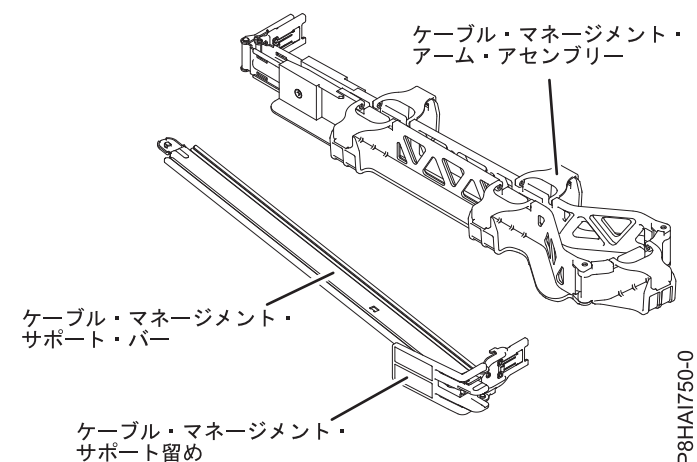


図 50. ケーブル・マネージメント・アーム・ボックスの内容

レール・ボックスの内容

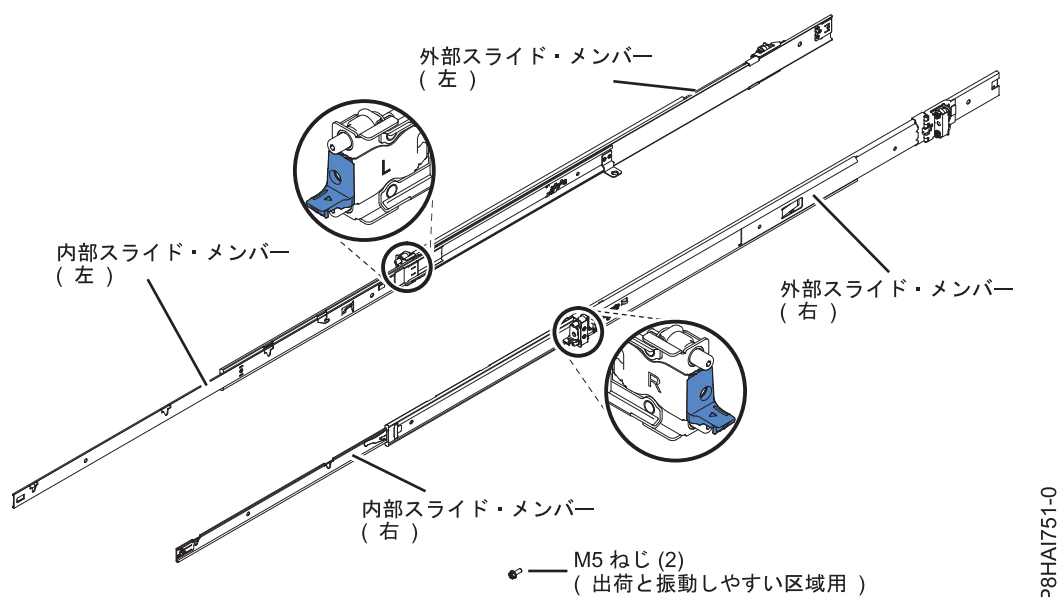


図 51. レール・ボックスの内容

注: この取り付けには、スライド・レール・ボックスとケーブル・マネージメント・アーム・ボックスの両方が必要です。

7042-CR9 HMC をラックに取り付けるには、以下のステップを実行します。

1. サーバーを取り付けるラック内の使用可能なスペース (取り付けるサーバーによって異なります) を選択します。

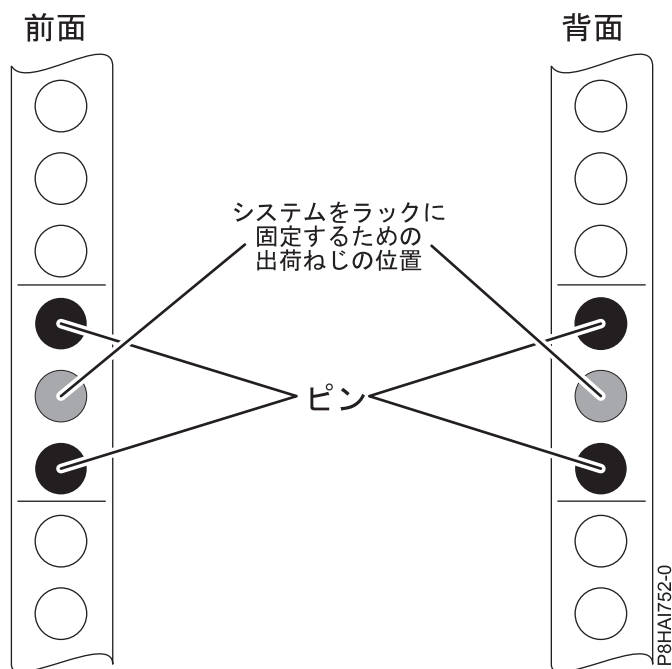


図 52. ラック・スペースの識別

注: 1 ユニット (1 U) のスペースが必要であり、スライド・レールは、最下部ユニット (U) の 1 ユニットのスペースに取り付けられます。

2. カチッと音がするまで、外部スライド・メンバーを完全に伸ばします。これで、後部ラック・マウント・ブラケットが回転して、ロック解除位置になります。

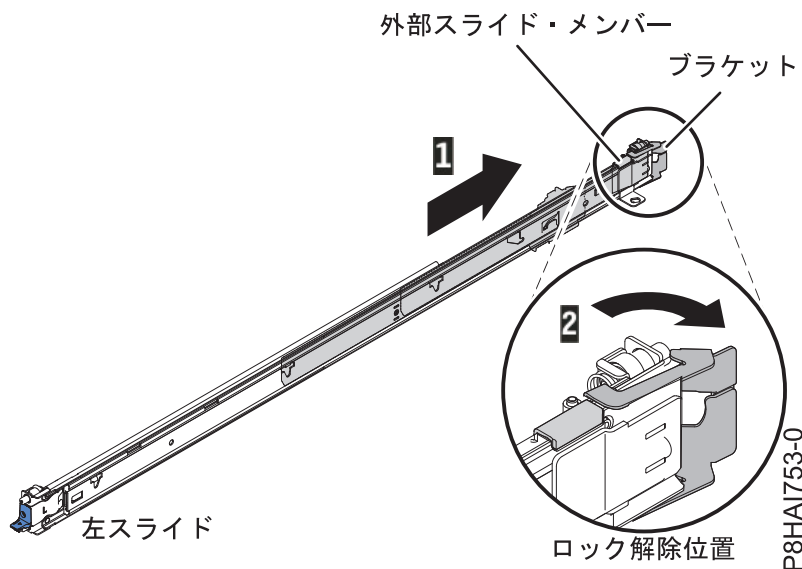


図 53. スライド・レールと外部スライド・メンバー

注: 各スライド・レールの端には、**R** (右) または **L** (左) のマークが付いています。

3. 外部スライド・メンバーの後部端を、ラック後部の穴に位置合わせします。ピンが穴に入るように、ピンの位置を合わせてスライドを押し込みます。2 つのスライド・ピンが、EIA フランジの上段および下段の穴から突き出ます。後部ラック・マウント・ブラケットが所定の位置にロックされるまで、スライドをラック後部の方向へ押しします。

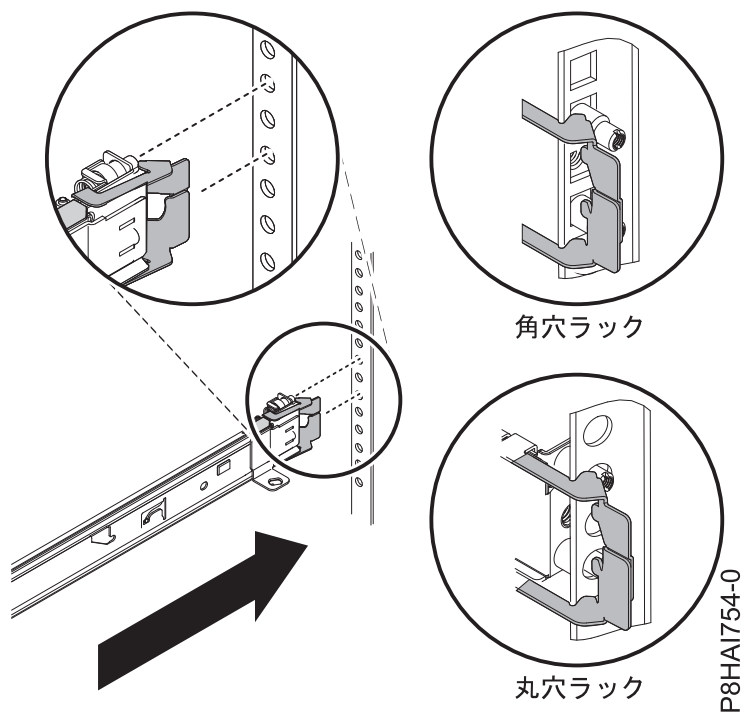


図 54. ピンとラック後部の穴の位置合わせ

4. 前部ラッチを回転させてオープン位置にし、外部スライド・メンバーの前部端をラック前部の穴に位置合わせします。ピンを EIA フランジの穴に揃えて、ピンが穴から突き出るようにスライドを前方に押します。前部ラッチをクローズ位置まで回転させることによって、スライドの前部をロックします。他の外部スライド・メンバーについて、ステップ 2 から 4 を繰り返します。

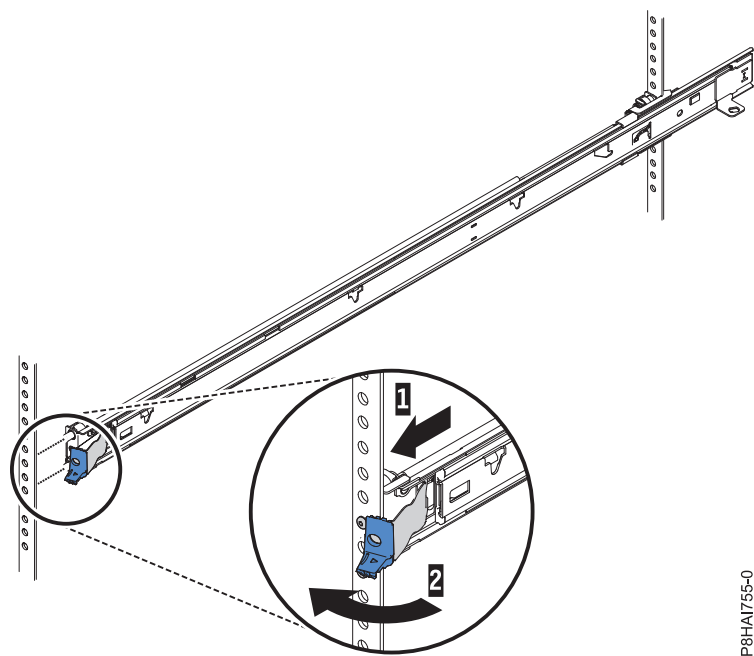


図 55. 前部スライド・レール・ラッチ

5. リリース・ラッチ **(1)** を押します。ラック・キャビネットを移動する場合、あるいはラック・キャビネットを振動しやすい区域に取り付ける場合は、サーバーの前部の拘束 M5 ねじ **(2)** を締めます。

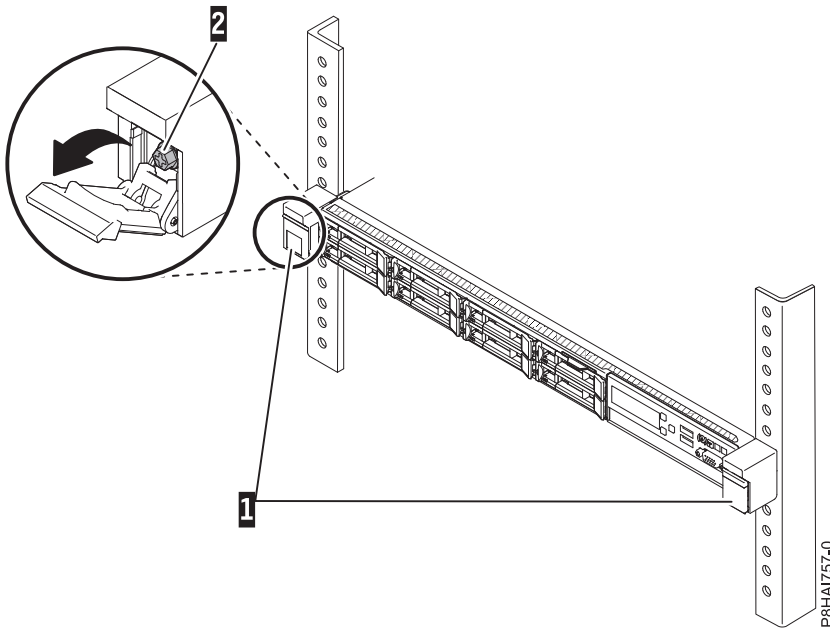


図 56. ラック前部のレールとピン

6. 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、サーバー後部のくぎの頭 **(2)** がスライド・レールのスロット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下ろします。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 **(3)** をゆっくりと下ろします。システムがスライド・レールに固定されるように、前部ラッチが前部のくぎの頭に被さっていることを確認します。

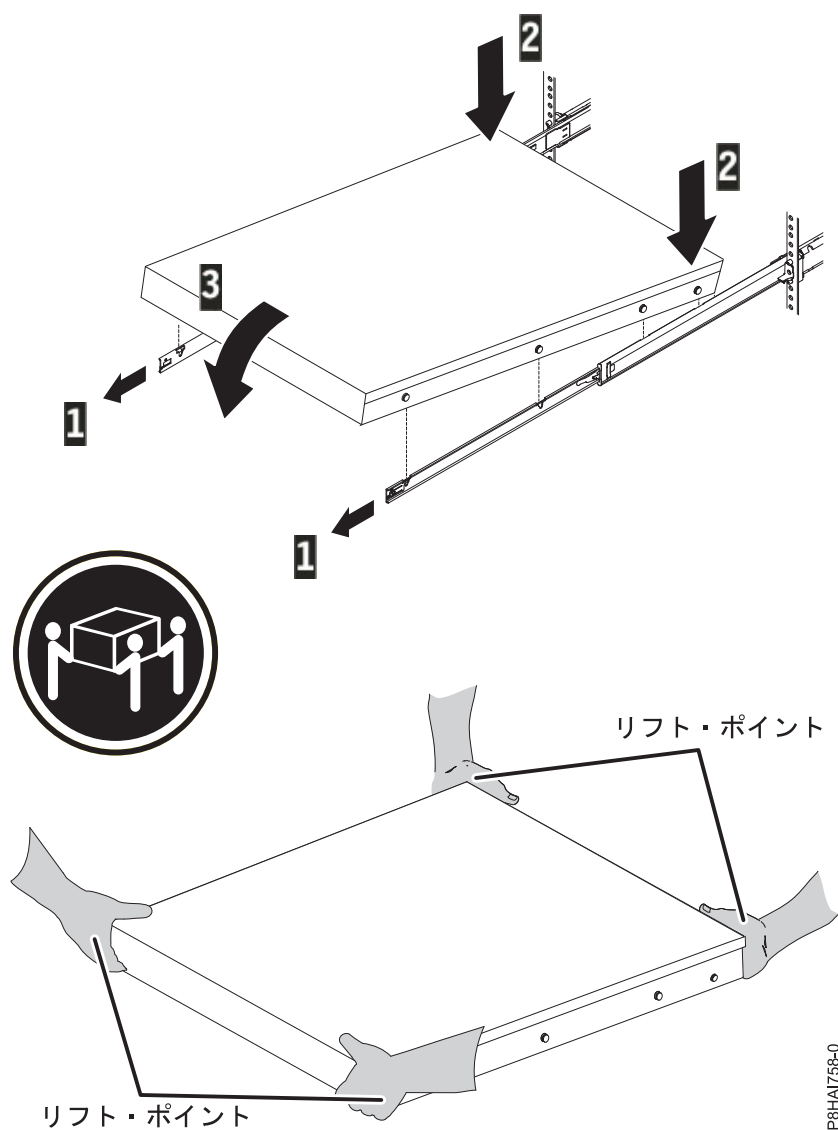


図 57. 引き出したスライド・レール、レールのスロットと位置合わせしたサーバーのくぎの頭、およびリフト・ポイント

注: 装置を持ち上げる場合には、安全に持ち上げる方法に従ってください。1 U サーバーを取り付ける場合は、必ず 2 人でサーバーを持ち上げてください。持ち上げる人の手の位置は、図 57 に図示されているとおりにする必要があります。

7. スライド・レールのロック・レバー **(1)** を持ち上げ、カチッと音がしてサーバー **(2)** が所定の位置に収まるまでラックの中に押し込みます。

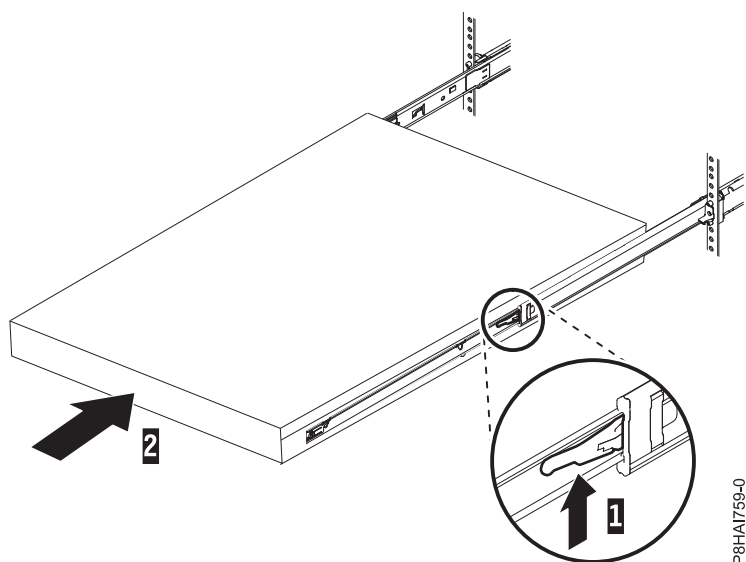


図 58. リリース・ラッチとサーバー

8. 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。図 59 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・アームは、電源装置にアクセスできるように、電源装置の反対側にちょうつがいで留めて取り付けることをお勧めします。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。ピンを下に向けて (1)、スライド・レールの後部にある水平スロットに入れます。次に、バーの他方の端をラックの方向 (2) に向けて回転します。

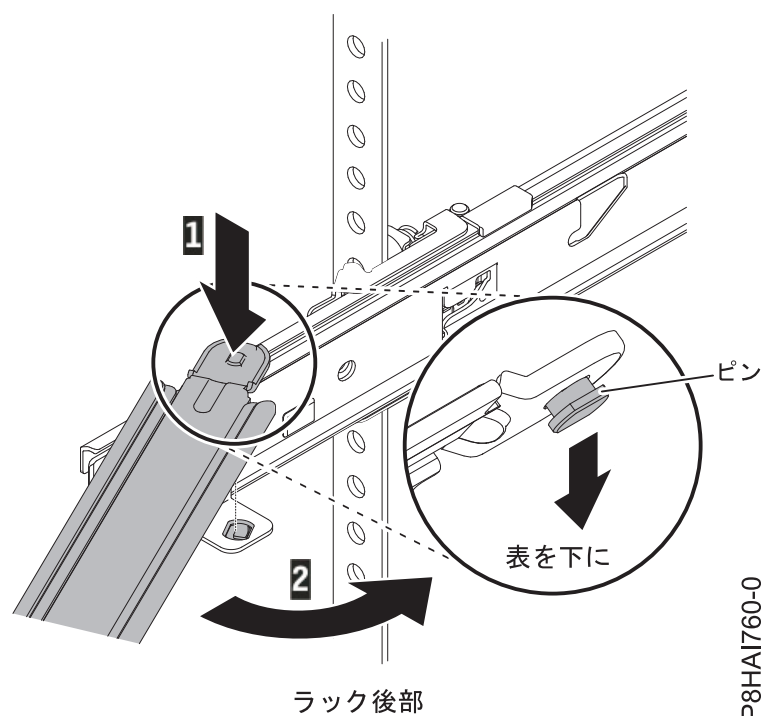


図 59. サポート・アームの接続

注: 正常に作動するためには、ケーブル・マネジメント・サポート・バーがスライド・タブの上部になければなりません。

9. ケーブル・マネジメント停止ブラケット (大文字 **O** が付いているもの) を、サポート・アームの接続されていない方の端に取り付けます。サポート・アームがしっかり取り付けられていることを確認してください。

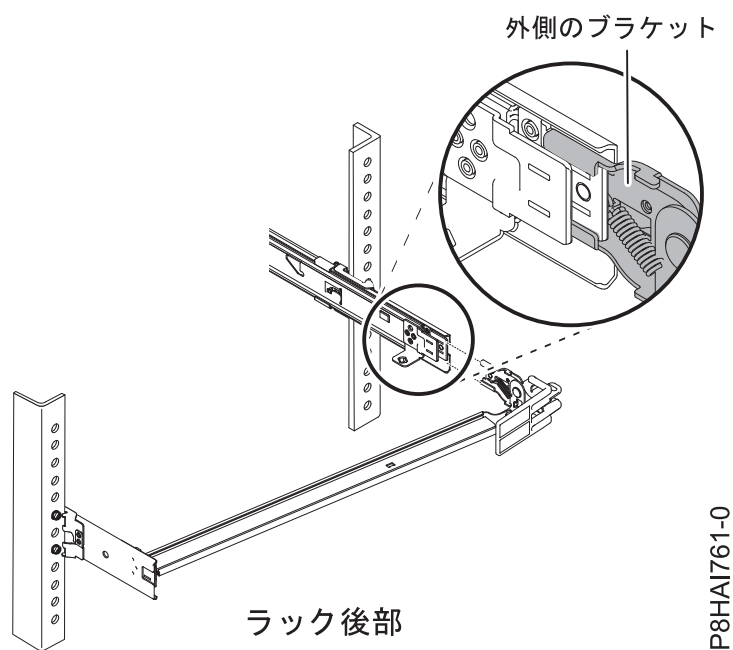


図 60. スライド・レールへの停止ブラケットの接続

注: 外側のピンを識別できるように、ケーブル・マネジメント・アームに大文字 **O** がマークされています。

10. ケーブル・マネジメント・アームをサポート・アームに乗せます。ケーブル・マネジメント・アームのタブを、スライド・レールの内側と外側の両方のスロットの中にスライドさせて入れます。タブが所定の位置に収まるまで押し込みます。

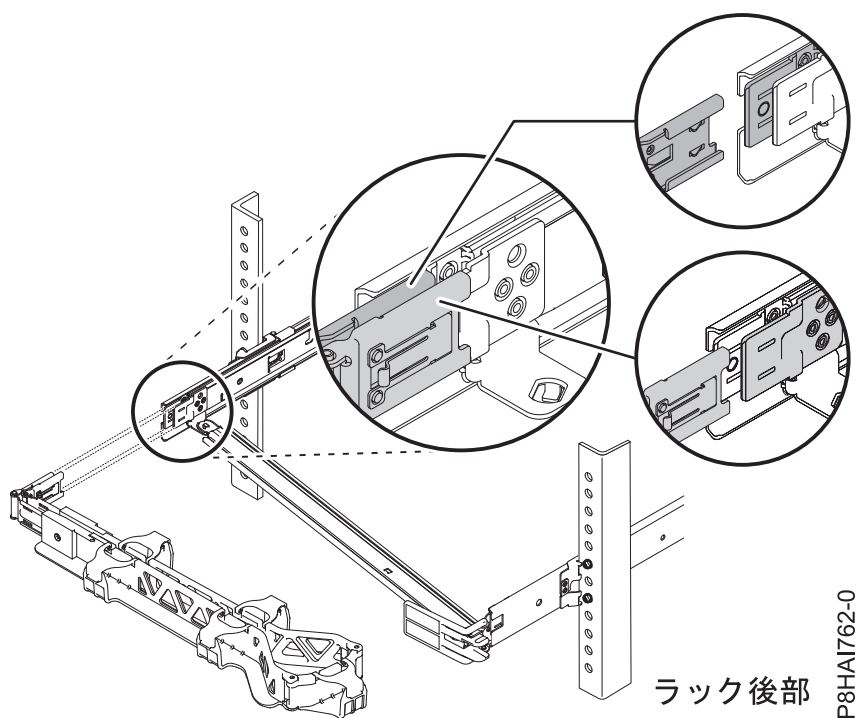


図 61. ケーブル・マネージメント・アームの接続

11. ケーブル・マネージメント・アームを容易に回転させてケーブル・マネージメント・サポート・アームに取り付けたり、アームから取り外したりできるように、ケーブル・マネージメント・サポートの上下のタブを押して停止ブラケットを開くことができます。

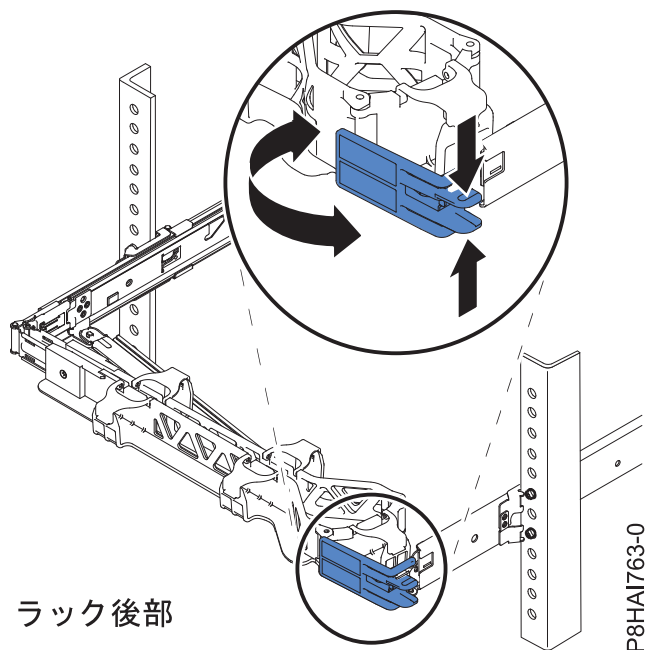


図 62. ケーブル・マネージメント・サポート留めブラケット

12. 電源コードおよびその他のケーブル (必要の場合はキーボード、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・ストラップの位置は、システムによって若干異なる場合があります。システムの背面に備わっているケーブル・ストラップを使用して、ケーブルを保持し、ケーブルがたるまないようにします。

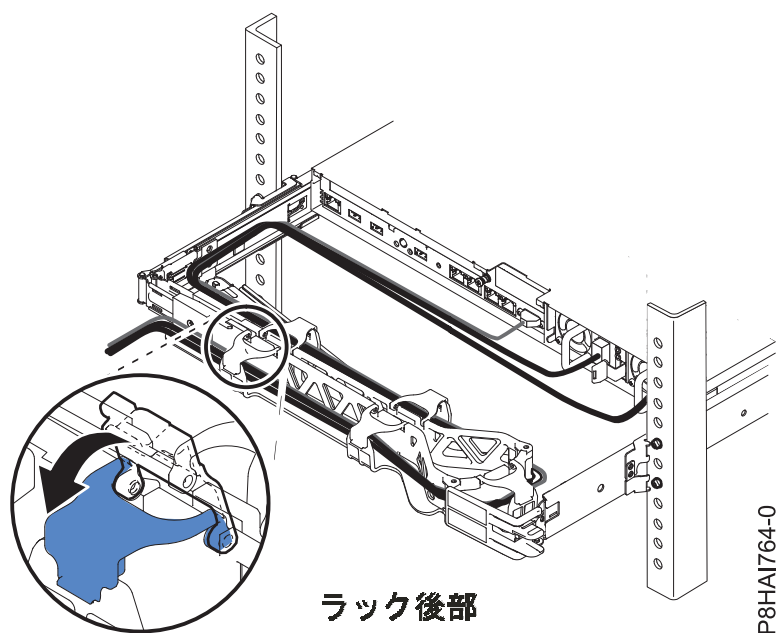


図 63. 電源コードの取り付けとケーブルの配線

13. ケーブル・マネージメント・アームが適切に動作できるように、ケーブルをケーブル・ストラップで束ねる必要があります。

注: ケーブルが U スペースの下にたんで下段のシステムに引っ掛からないようにしてください。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に、すべてのケーブルに遊びを持たせます。

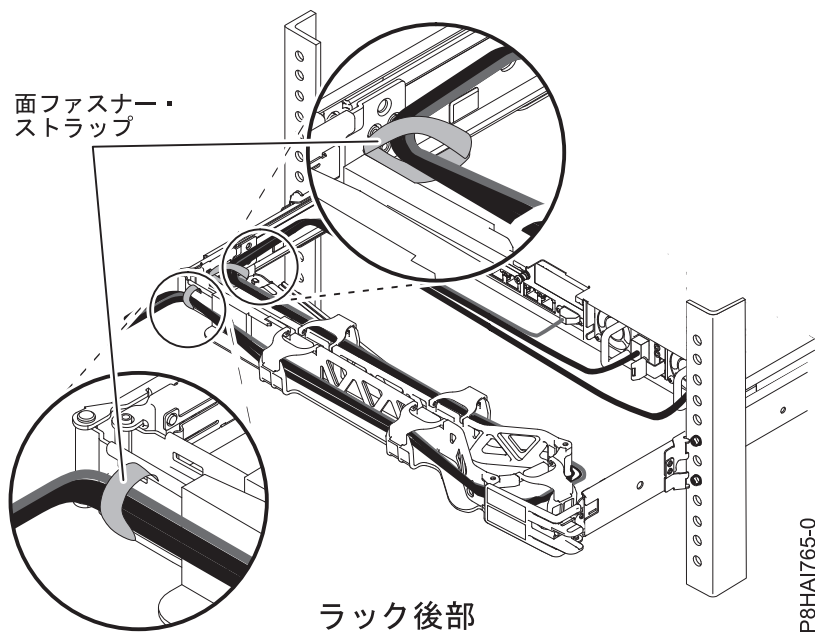


図 64. 面ファスナー

14. システムが取り付けられた状態でラックを配送する場合、あるいは振動しやすい区域にラックがある場合は、スライドの後部に M5 ねじを挿入します。必要に応じて、ケーブル・タイを使用して、ケーブル・マネージメント・アームの固定されていない方の端をラックに固定します。

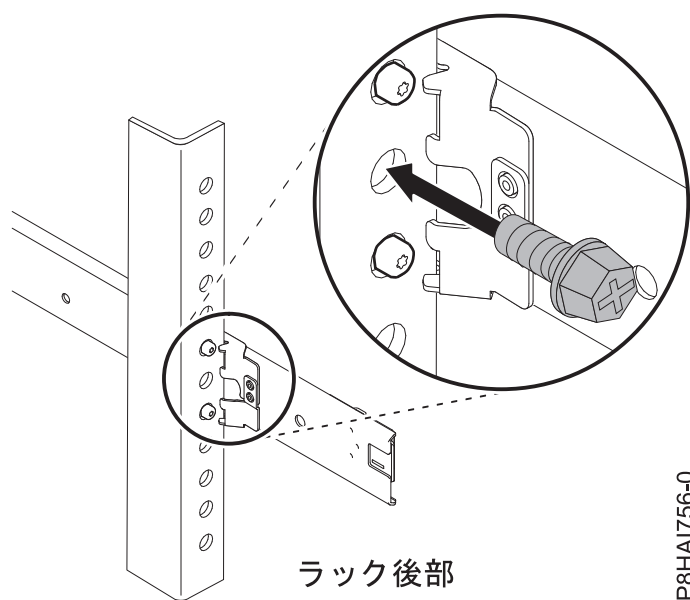


図 65. 配送のためのサーバーの固定

ラックへの 7063-CR1 の取り付け

7063-CR1 ハードウェア管理コンソール (HMC) をラックに取り付ける方法について説明します。

ラック・マウント型 7063-CR1 システムの設置の前提条件

ここでは、システムの設置に必要な前提条件について説明します。

サーバーを設置する前に、以下の資料を読むことが必要な場合があります。

- この資料の最新版は、オンラインで維持されています。Installing the 7063-CR1 into a rack (ラックへの 7063-CR1 の設置) (http://www.ibm.com/support/knowledgecenter/POWER8/p8hai/p8hai_install7063_kickoff.htm)を参照してください。
- サーバーの設置を計画するには、システムの計画 (http://www.ibm.com/support/knowledgecenter/POWER8/p8had/p8had_8xx_kickoff.htm)を参照してください。

設置を開始する前に、次の品目が揃っていることを確認してください。

- プラス・ドライバー
- マイナス・ドライバー
- カッター・ナイフ
- 静電気放電 (ESD) リスト・ストラップ
- 2 EIA (米国電子工業会) 単位 (2U) のスペースを備えたラック

注: ラックをまだ設置していない場合は、ラックを設置します。手順については、ラックおよびラック・フイーチャー (http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/p8hbf_8xx_kickoff.htm) を参照してください。

ご使用のシステム用の部品の用意

以下の情報を使用して、ご使用のシステム用の部品を用意します。

1. 注文したすべてのボックスを受け取ったことを確認します。
2. 必要に応じて、サーバー・コンポーネントを取り出します。
3. 各サーバー・コンポーネントを取り付ける前に、以下のステップに従って、部品が揃っていることを確認します。
 - a. サーバーのインベントリー・リストを見つけます。
 - b. 注文したすべての部品を受け取ったことを確認します。

注: 注文情報は、製品に付属しています。営業担当員または IBM ビジネス・パートナーからも注文情報を入手できます。

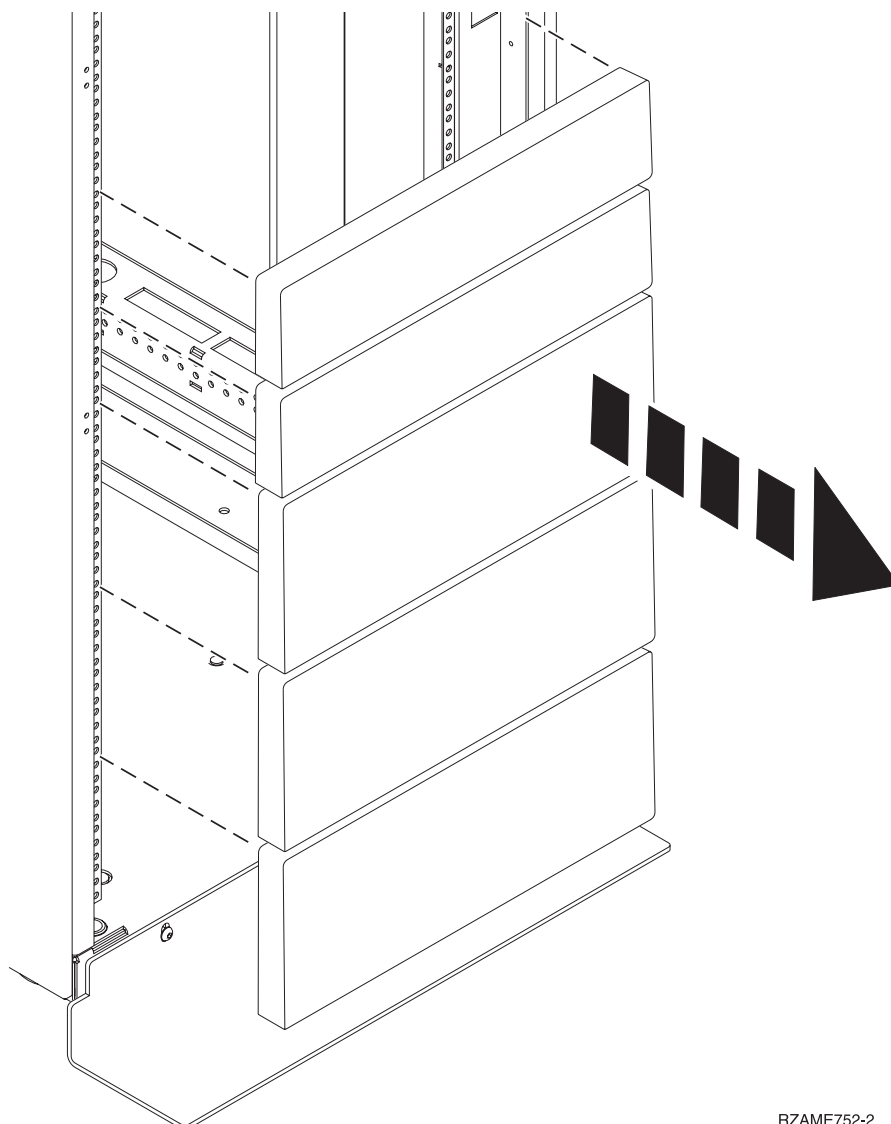
部品が間違っていたり、欠落または損傷があった場合は、以下のいずれかに連絡してください。

- お客様の IBM 販売店。
- IBM Rochester manufacturing automated information line: 1-800-300-8751 (米国のみ)。
- Directory of worldwide contacts Web サイト (<http://www.ibm.com/planetwide>)。地域を選択して、サービスおよびサポート窓口の情報を表示してください。

7063-CR1 システムを搭載するラック内の位置の決定とマーク付け

システム装置をラックに取り付ける場所を決定することが必要になる場合があります。

1. ラックの安全上の注意 (Rack safety notices) (<http://www.ibm.com/support/knowledgecenter/POWER8/p8hbf/racksafety.htm>) をお読みください。
2. システム装置をラック内のどこに取り付けるかを決定します。システム装置をラック内に取り付けるための計画を立てる際に、以下の情報について検討してください。
 - 大きくて重いシステム装置を、ラックの下段に設置します。
 - 装置を、最初にラックの下段に設置するよう計画します。
 - 計画に EIA (Electronic Industries Alliance (米国電子工業会)) の位置を記録します。
3. 必要であれば、装置を配置する計画のラック・エンクロージャーの内側にアクセスできるよう、フィルター・パネルを取り外します。 48 ページの図 66



RZAME752-2

図 66. フィラー・パネルの取り外し

4. システムを取り付けラック内のどこに取り付けるかを決定します。EIA の位置を記録します。
5. ラックの前面に向かって右側から作業を行い、各 EIA 単位の下段の穴にテープ、マーカ、または鉛筆を使用してマークを付けます。
6. ラック左側の対応する穴に対してもステップ 5 を繰り返します。
7. ラックの背面に回ります。
8. ラックの右側で、ラックの前面でマークを付けた最下部 EIA 単位に対応する EIA 単位を見つけます。
9. 最下段の EIA 単位にマークを付けます。
10. ラック左側の対応する穴にマークを付けます。

固定レールを使用してのラックへの HMC の設置

固定レールを使用して 7063-CR1 HMC をラックに設置する場合は、以下の作業を実行します。

システム・シャーシおよびラックへの固定レールの取り付け:

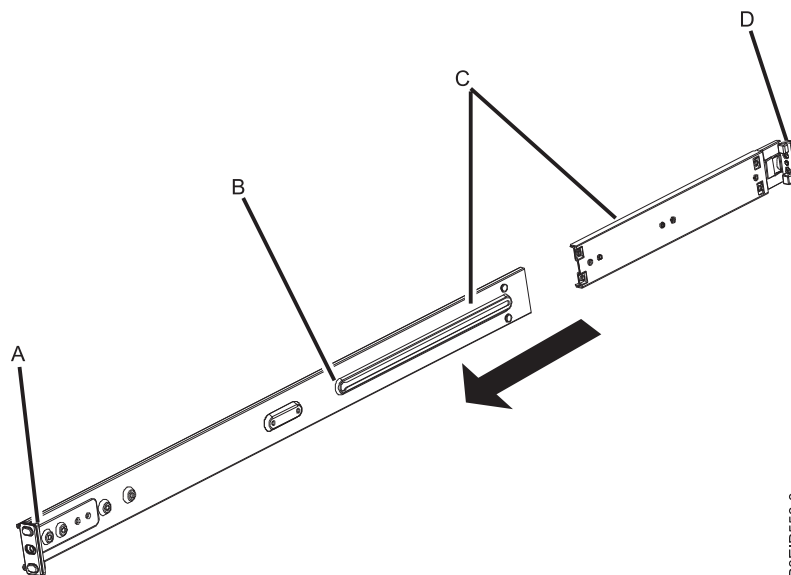
レールをシャーシおよびラックに取り付ける必要があります。この作業を実行するには、以下の手順を使用します。

重要: レールに不具合が生じたり、ご自身とシステム装置に危険が生じるのを避けるために、ご使用のラック用の適切なレールと取り付け具を使用していることを確認してください。ご使用のラックに支持フランジ用の四角い穴または支持フランジ用のねじ穴がある場合、レールと取り付け具が、ラックで使われている支持フランジ用の穴に一致することを確認してください。一致しないハードウェアを、ワッシャーやスペーサーを使用して取り付けしないでください。ご使用のラックに適合したレールと取り付け具が装備されていない場合は、お客様の IBM 販売店にお問い合わせください。

注: システムには、1 EIA ラック単位 (1U) のスペースが必要です。

レールを取り付けるために、必要な部品が揃っていることを確認します。レール・キットには、以下の部品が含まれています。

- スライド・レールねじ (各スライド・レールの 2 つの部分を取り付けるために使用)
 - スライド・レール・ラックねじ (レールをラックに固定するために使用)
 - レール
 - 10 個から 32 個の 0.635 cm (0.25 インチ) ねじ (レールをシステム・シャーシに取り付けるために使用)。
1. パッケージからレールの各部分を取り外して、作業面に置きます。
 2. 各ラック・スライド・レールの 2 つの部分を接続します。ラック・スライド・レールの 2 つの部分を接続するには、以下の作業を実行します。
 - a. 左ラック・スライド・レールの 2 つの部分を識別します。短い部分と長い部分 **(C)** を位置合わせします。ラック・レール・ピンが同じ方向 **(A)** および **(D)** を指していることを確認します。



- b. ラック・スライド・レールの短い方の部分に金属のピンが付いています。このピンを、ラック・スライド・レールの長い方の部分の穴 **(B)** に差し込みます。ラック・レールの短い方の部分をスライドさせて、ラック・レールの長い方に組み入れます。

- c. ラック・スライド・レールの 2 つの部分の穴を位置合わせします。プラスのドライバーを使用して、2 本のレールねじをラック・スライド・レールの穴に通して緩くねじり、2 つの部分を接続します。

注: ラック・スライド・レールのねじを締め付けないでください。

- d. 上記ステップを右スライド・レールに対して繰り返します。
3. シャーシ・レールをシステム・シャーシに取り付けます。シャーシ・レールをシステム・シャーシに取り付けるには、以下の作業を実行します。
 - a. システムの左側で、システム・シャーシの左側の金属製つまみを、左シャーシ・スライド・レールの四角い孔の位置に合わせます。シャーシ・スライド・レールが音を立てて所定の場所に収まるまで、ラックの前面方向へシャーシ・スライド・レールをスライドさせます。
 - b. レール・キットに含まれていた 2 本のねじを使用して、システム・シャーシ・スライド・レールをシステム・シャーシに取り付けます。
 - c. システムの右側のシャーシ・スライド・レールに対して繰り返します。
4. ラック・スライド・レールをラックに取り付けます。
 - a. ラックの前面に移動します。
 - b. 左ラック・スライド・レールを選択し、以前にマークを付けた EIA 単位の位置を確認します。ラックの背面を示すために、各スライド・レールにも「**Back**」というマークが付いています。必ず、ラック・スライド・レールの前端を持ってください。
 - c. ラックの前面からラックの背面までレールを延ばし、ラック・スライド・レール・ピンを、以前にマークを付けたラック・フランジの穴の位置に合わせます。
 - d. 背面ラック・レール・ラッチが音を立てて所定の場所に収まるまで、ラック・レール・ピンを背面ラック・フランジに押し込みます。
 - e. ラック・レールの前面をラック・レール・フランジの前面方向へ引っ張ります。スライド・レール・ピンを、レール・フランジの穴の位置に合わせ、レール・ラッチが音を立てて所定の場所に収まるまで引っ張ります。
 - f. ドライバーを使用して、ステップ 2 で取り付けたレールねじを締めます。
 - g. 右側のスライド・レールに対してステップ 4a から 4f を繰り返します。
5. レールをラックに固定します。
 - a. ラックの背面に移動します。
 - b. 各ワッシャーを、レール・キットに含まれている長い方のねじに沿ってそれぞれスライドさせます。
 - c. ねじとワッシャーを、ラックの背面の両側で各レールの中央の穴に通して締め付けます。

ラックへのシステムの設置と電源ケーブルの接続および配線:

システムをラック内のレール上に設置した後、電源ケーブルを接続して配線します。

注: このシステムをラックに設置するには、2 人必要です。

1. システム・シャーシの上面から保護プラスチック・フィルムを取り外します。
2. ラックの前面に移動します。
3. 2 人でシステムを持ち上げ、シャーシの両側にあるシステム・シャーシ・レールをラック・スライド・レールと位置合わせします。
4. 1 人がシステムの重量を支えている間に、2 人目は各スライド・レールが音を立てて所定の位置に収まるまで、システムをラック内に慎重に押し込みます。

- システムが音を立てて所定の場所に収まるまで、ラックの背面方向へ押します。
- システム・シャーシの両側にあるハンドルにねじを差し込んで回し、システムをラックに固定します。
- 電源コードのプラグを電源装置に差し込みます。

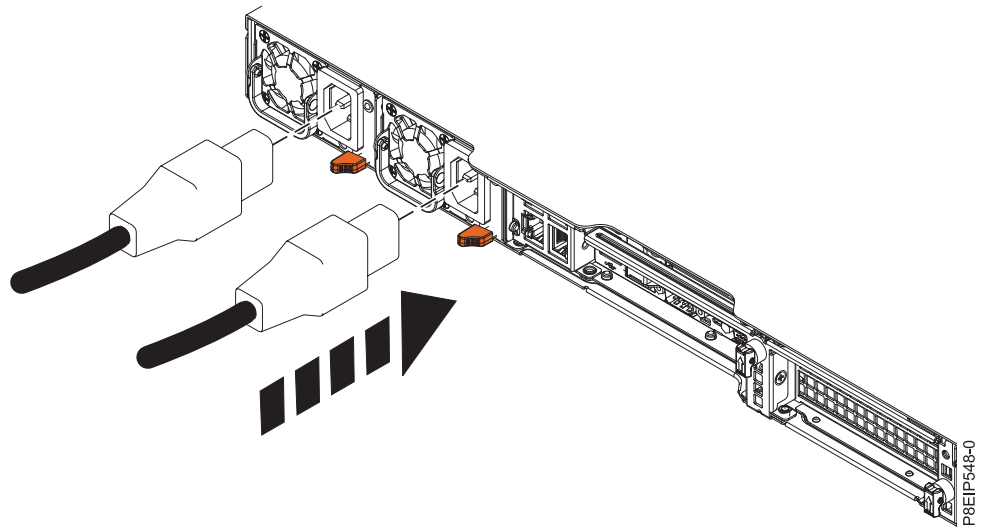


図 67. 電源装置への電源コードのプラグの差し込み

- すべてのケーブルをサーバーの背面に接続します。

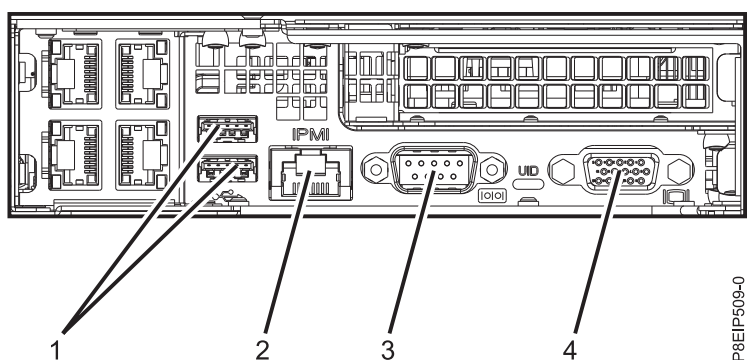


図 68. 背面ポート

表 9. 入出力ポート

ID	説明
1	USB 2.0 (キーボードとマウスに使用)
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Serial IPMI
4	Video Graphics Array (VGA) (モニターに使用)。1024 x 768、60 Hz VGA 設定のみがサポートされます。最大 3 メートルのケーブルのみがサポートされます。現時点でサポートされているのは、テキスト・ベース機能のみです。

9. システムの電源コード、および他のすべての接続デバイスの電源コードを交流 (AC) 電源に差し込みます。
10. 131 ページの『HMC Enhanced+ インターフェースを使用した HMC の構成』に進みます。

スライド・レールを使用してのラックへの HMC の設置

スライド・レールを使用して HMC をラックに設置する場合は、以下の作業を実行します。

システムおよびラックへのスライド・レールの取り付け:

スライド・レールをシステムに取り付けてから、ラックに取り付けます。

重要: レールに不具合が生じたり、ご自身とシステム装置に危険が生じるのを避けるために、ご使用のラック用の適切なレールと取り付け具を使用していることを確認してください。ご使用のラックに支持フランジ用の四角い穴または支持フランジ用のねじ穴がある場合、レールと取り付け具が、ラックで使われている支持フランジ用の穴に一致することを確認してください。一致しないハードウェアを、ワッシャーやスペーサーを使用して取り付けしないでください。ご使用のラックに適合したレールと取り付け具が装備されていない場合は、お客様の IBM 販売店にお問い合わせください。

スライド・レールは、完全に組み立てられた状態で到着します。スライド・レールをラックに取り付けるには、レールを 4 つの部分に分解する必要があります。

1. 後日システムをラックから取り外さずにバックプレーンの保守が行えるように、下部 DASD (仮想直接アクセス・ストレージ・デバイス) バックプレーンの両側のねじを取り外します。

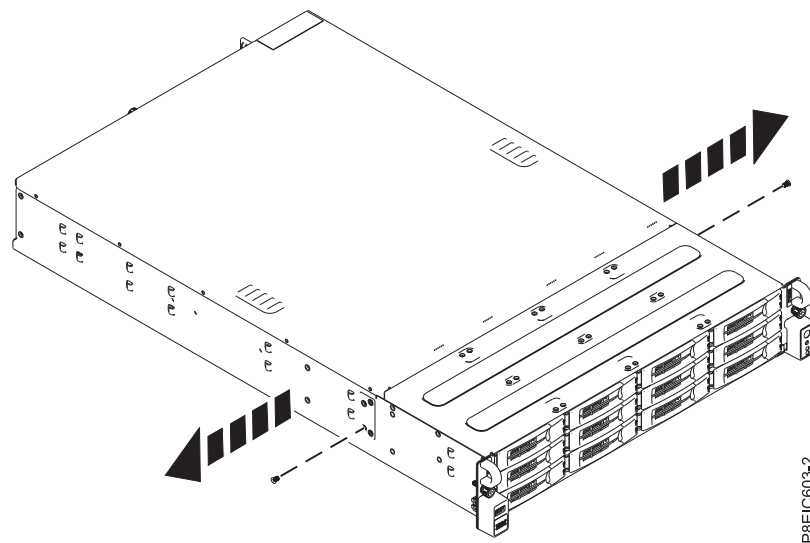


図 69. DASD バックプレーンのねじの取り外し

2. システム・シャーシの各側面に、システム・シャーシのスライド・レールを取り付けます。システム・シャーシの背面で、システム・シャーシのタブ (B) をスライド・レールのスロット (A) に位置合わせします。シャーシのスライド・レールを前方に押して、スラム・ラッチが所定の位置に収まるようにします。

注: システム・レールには、システムの前面から見て左側のシステム・レールを示す **L** と、右側のシステム・レールを示す **R** のマークが付けられています。

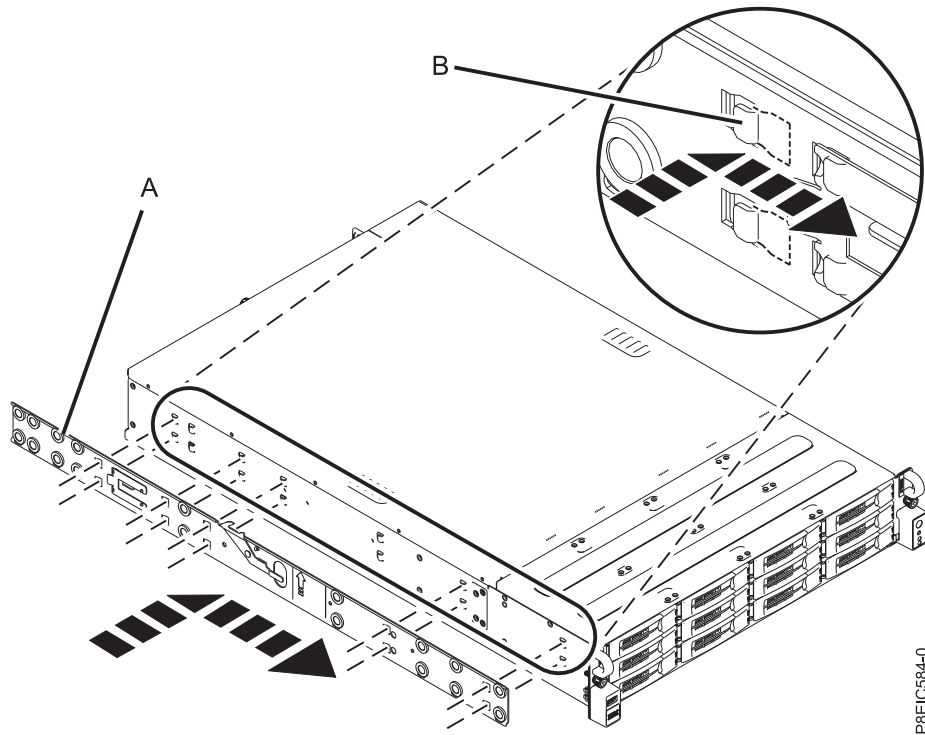


図 70. システムの左側のシャーシへのシャーシ・スライド・レールの取り付け

3. 各システム・シャーシ・スライド・レールに保持ねじを取り付けて、システム・シャーシにスライド・レールをさらに固定します。

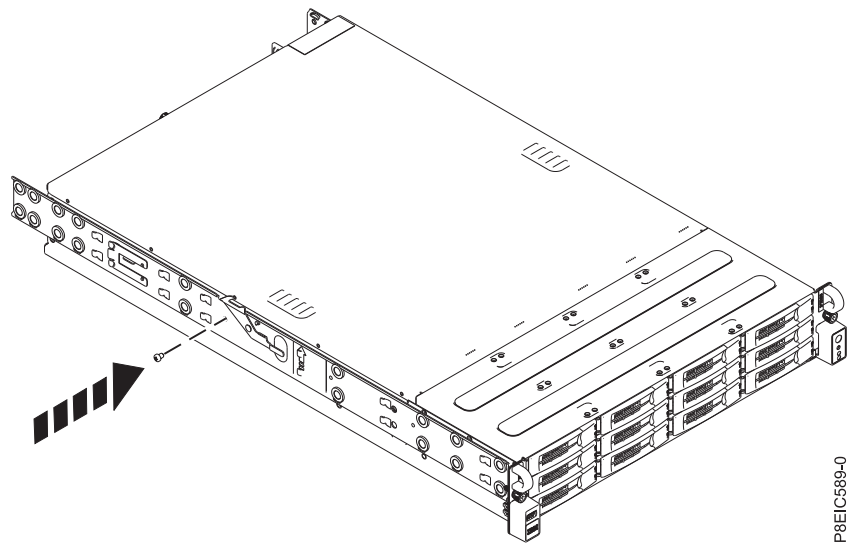


図 71. システムの左側のシャーシへのシャーシ・レール保持ねじの取り付け

4. 次に、ラックにラック・スライド・レールを取り付けます。それぞれのラック・スライド・レールには、前面から見た場合に **R** (右) または **L** (左) とマークが付けられています。右のスライド・レールを選択してラックの前面に持って行き、選択済みの EIA 単位を見つけます。
5. ラックの前面から、スライド・レールの前部にあるピン **(1)** を、事前にマークを付けたラックの前面の穴 **(2)** に挿入します。レールを前方に引いて、レールのばねクリップ **(3)** がレール・フランジに掛かり、所定に位置に収まるようにします。

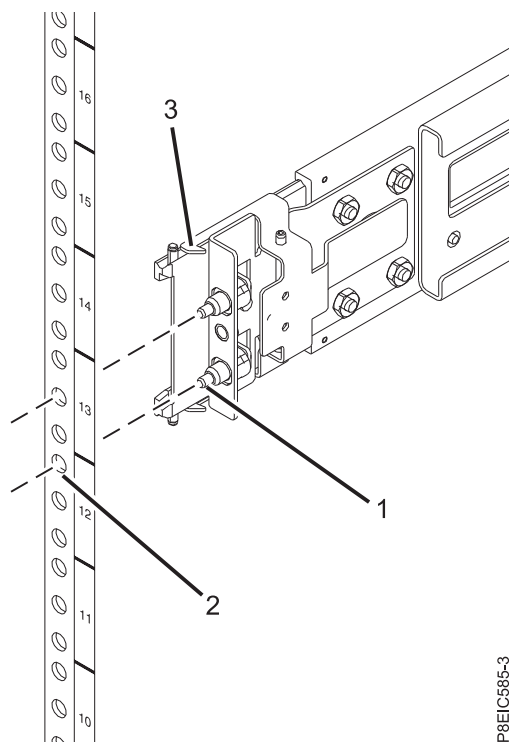


図 72. ラック前面からのスライド・レールの取り付け

6. 左側のレールについて、ステップ 3 と 4 を繰り返します。
7. ラックの背面に移動します。スライド・レールを手前に引いて、2 つのピン **(1)** をラックの穴 **(2)** に挿入します。レールのばねクリップ **(3)** が所定の位置に収まるまで、レールを引きます。ねじ **(4)** を取り付けて、スライド・レールをラックに固定します。

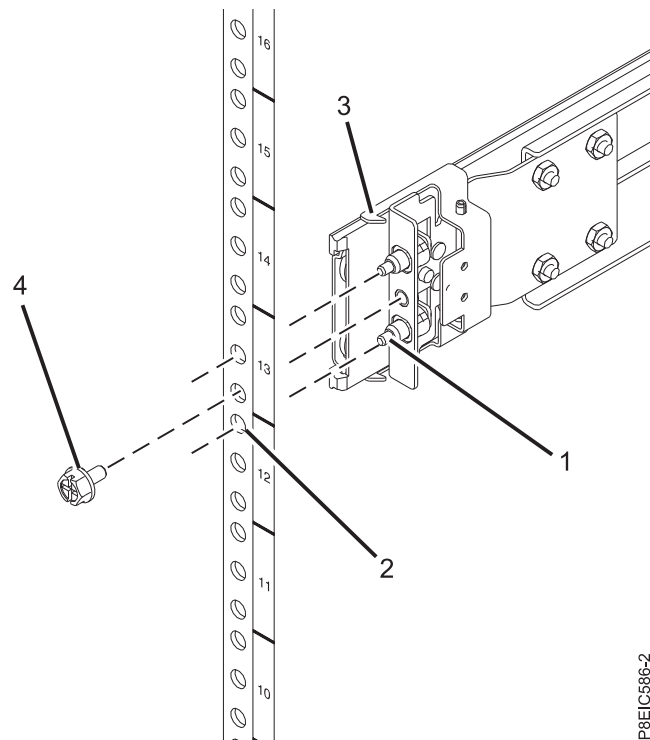


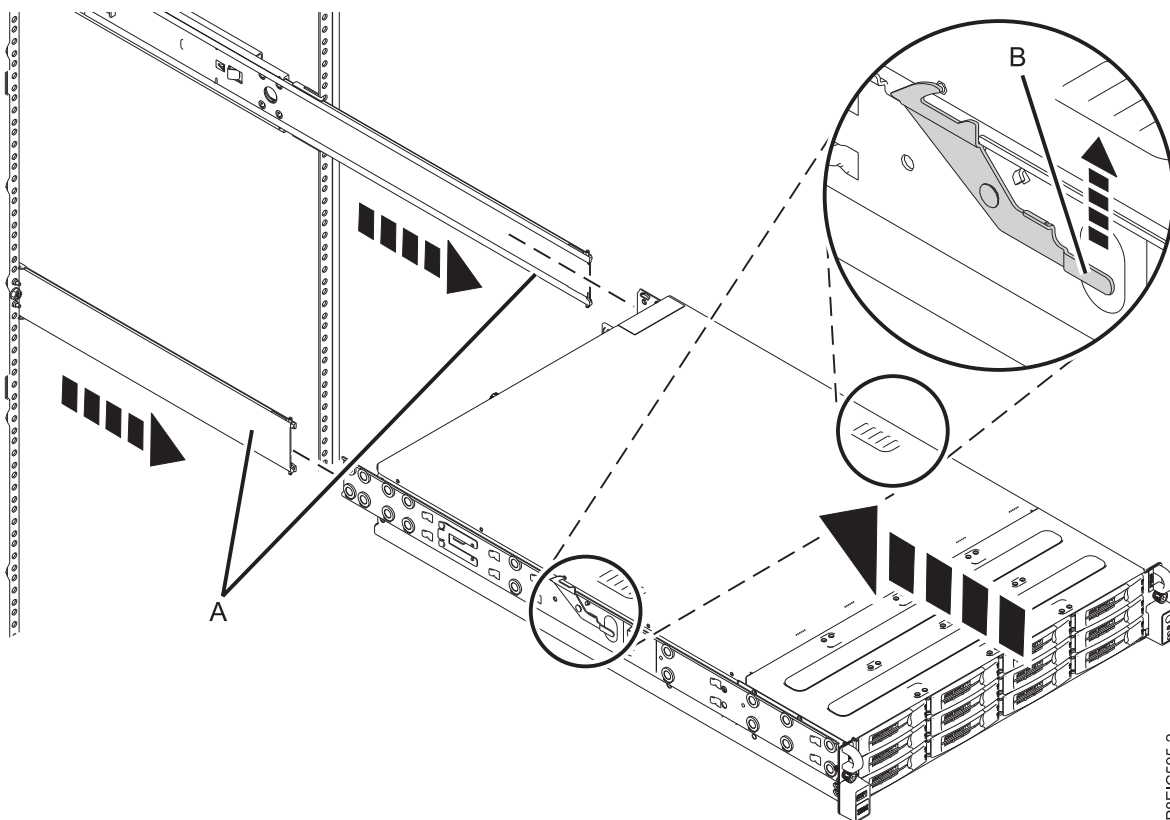
図 73. ラックの背面でのスライド・レールの取り付け

ラックへのシステムの設置と電源ケーブルの接続および配線:

システムをラック内のレール上に設置した後、電源ケーブルを接続して配線します。

注: このシステムをラックに設置するには、2 人必要です。

1. スライド・レールを、レールがクリック音とともに保守位置に収まるまで完全に伸ばします **(A)**。
2. 2 人でシステムを持ち上げ、シャーシ・レールの下部ローラー・ピンを両側のラック・スライド・レールの溝に合わせます。



P8E1C595-2

図 74. シャーシ・レールの下部ローラー・ピンとラック・スライド・レールの溝の位置合わせ

3. ラックの両側にある、緑の矢印のマークが付いたラッチ (B) を同時に持ち上げます。
4. システムをラックに押し込みます。
5. システムの両側のつまみねじを締めて、システムをラックに固定します。

ラック・マウント型 7063-CR1 HMC のケーブル接続

ラック・マウント型ハードウェア管理コンソール (HMC) を物理的に設置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、46 ページの『ラックへの 7063-CR1 の取り付け』を参照してください。HMC をラックに取り付けたら、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、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、79 ページの『HMC ネットワーク接続』を参照してください。

6. 管理対象システムが既に取り付け済みの場合は、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。
7. ネットワークへのイーサネット Intelligent Platform Management Interface (IPMI) ポートの接続

注: この接続は、HMC 上のベースボード管理コントローラー (BMC) にアクセスするために必要です。BMC へのアクセスは、保守作業に必要であり、HMC ファームウェアを保守するためにも必要です。詳しくは、79 ページの『HMC ネットワーク接続のタイプ』を参照してください。

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、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、ご使用の HMC のソフトウェアをインストールして構成する必要があります。『7063-CR1 HMC の構成』に進みます。

7063-CR1 HMC の構成

ハードウェア管理コンソール (HMC) をインストールおよび構成する方法について説明します。

Fix Central Web サイトから必要な HMC バージョンをダウンロードできます。取り外し可能メディア (DVD または USB など) を使用して、HMC パッケージからブート可能 ISO ファイル (ISO イメージ) を作成します。

注: 以下のインストールは、例として示されています。

USB フラッシュ・ドライブを使用した HMC のインストール

USB フラッシュ・ドライブを使用して HMC をインストールするには、Linux システムの場合の以下の手順を実行します。

1. Fix Central Web サイトから必要な HMC バージョンをダウンロードします。
2. 次のコマンドを実行します。`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync` (ここで、**sdx** は USB ドライブの名前です)

注: USB ドライブは、少なくとも 4 GB でなければなりません。

3. USB ドライブを挿入して、システムの電源をオンにします。

コンソール・ビューアーからリモート・メディアを使用時の HMC のインストール

コンソール・ビューアーからリモート・メディアを使用して HMC をインストールするには、以下の手順を実行します。

1. BMC Web インターフェース (<http://<bmc-ip>>) にログインします。
2. 「リモート制御」を選択します。
3. 「コンソールの指定変更 (**Console Redirection**)」を選択します。
4. 「コンソールの起動 (**Launch Console**)」をクリックします。
5. Java™ iKVM Viewer で、「**Virtual Media**」 > 「**Virtual Storage**」を選択します。
6. 「**Logical Drive Type**」の下で、「**ISO File**」を選択します。
7. 「**Open Image**」をクリックして、ご使用のシステム上の ISO ファイルの位置を確認します。
8. 「**Plugin**」を押して、その ISO ファイルをマウントします。

9. システムの電源をオンにします。

BMC Web インターフェースからリモート・メディアを使用しての HMC のインストール

BMC Web インターフェースからリモート・メディアを使用して HMC をインストールするには、以下の手順を実行します。

1. BMC Web インターフェース (<http://<bmc-ip>>) にログインします。
2. 「仮想メディア (Virtual Media)」を選択します。
3. 「CD-ROM イメージ (CD-ROM Image)」を選択します。
4. 以下の情報を入力します。

共有ホスト

Server Message Block (SMB) ホストの IP。ホスト名を使用している場合は、BMC 上のドメイン名システム (DNS) が正しく構成されていることを確認します。

イメージへのパス

システムへの SMB パス。例: /<share name>/<rest of path>/<name of iso>.iso

ユーザー (オプション)

SMB ホストへのログインに使用されるユーザー名。

パスワード (オプション)

ユーザーのパスワード。

5. 「保管」をクリックします。
6. 「マウント」をクリックします。
7. Device 1 に以下のメッセージが表示されます。「**There is an iso file mounted.**」

注: このメッセージが表示されない場合は、入力した情報を再度確認し、ステップ 5 からステップ 7 を繰り返します。

8. システムの電源をオンにします。

注: Server Message Block バージョン 3 (SMBv3) はサポートされません。

次に、HMC ソフトウェアの構成が必要です。手順については、131 ページの『HMC Enhanced+ インターフェースを使用した HMC の構成』を参照してください。

関連概念:

159 ページの『BMC 接続の構成』

管理コンソール用の BMC 上のネットワーク設定を構成したり表示したりすることができます。

HMC 仮想アプライアンスの取り付け

ハードウェア管理コンソール (HMC) 仮想アプライアンスを取り付ける方法について説明します。

HMC 仮想アプライアンス は、既存の x86 または POWER® 仮想化インフラストラクチャーにインストールすることができます。HMC 仮想アプライアンス では、以下の x86 仮想化ハイパーバイザーをサポートします。

- カーネル・ベース仮想マシン (KVM)
- Xen
- VMware

HMC 仮想アプライアンスを稼働するための最小要件:

- 8 GB のメモリー
- 4 個のプロセッサ
- ネットワーク・インターフェース 1 つ (最大 4 個可能)
- 160 GB のディスク・スペース (推奨: 十分なパフォーマンスおよびキャパシティーのモニター (PCM) データを取得するためには 700 GB)

注:

1. HMC 仮想アプライアンスをホスティングするシステム上のプロセッサは、Intel VT-x または AMD-V ハードウェア仮想化対応プロセッサでなければなりません。
2. 受け取る HMC 仮想アプライアンス DVD は、ブート可能ではありません。最初にメディアをマウントし、次に、メディアから .tgz ファイルをコピーします。DVD をマウントする方式は、ご使用になるオペレーティング・システムにより異なる場合があります。
3. 次の例で使用されているコマンド構文は、ご使用になるオペレーティング・システムにより異なる場合があります。

関連情報:

HMC V8 ネットワークのインストール・イメージおよびインストール手順

x86 での HMC 仮想アプライアンスのインストール

x86 環境での ハードウェア管理コンソール (HMC) 仮想アプライアンスのインストール方法について説明します。

KVM ハイパーバイザーを使用した **HMC** 仮想アプライアンスのインストール:

カーネル・ベース仮想マシン (KVM) ハイパーバイザーを使用したハードウェア管理コンソール (HMC) 仮想アプライアンス のインストール方法について説明します。

HMC 仮想アプライアンス を KVM にインストールするには、以下の手順を実行します、

注: 以下のステップでは、コマンド行インターフェースを使用するため、root ユーザー権限が必要です。コマンド構文は、オペレーティング・システムにより異なる場合があります。

1. 仮想化パッケージが Red Hat Enterprise Linux (RHEL) バージョン 6.7 以降のシステムにインストールされていることを確認します。
2. <KVM vHMC インストール・ファイル名>.tar.gz ファイルをホスト・システムにダウンロードします。
3. コマンド `mkdir -p /var/lib/libvirt/images/vHMC` を実行します。
4. コマンド `cd /var/lib/libvirt/images/vHMC` を実行します。
5. 仮想ディスク・イメージを抽出するために、コマンド `tar -zxvf <KVM vHMC インストール・ファイル名>.tgz` を実行します。

注: このコマンドでは、ご使用の HMC 仮想アプライアンス .tar ファイルの絶対パスを指定してください。

6. **domain.xml** ファイルが <KVM vHMC インストール・ファイル名>.tar.gz ファイルに付属しています。以下のステップを実行します。
 - a. **domain.xml** ファイルを編集して、ご使用のディスクへのパスが正しいことを確認します。このファイルには、文字列 **DISK_PATH** が含まれています。
 - b. **virtio** がご使用のディスク・デバイスのバス値に使用されていることを確認します。

- c. ご使用の VM に別の名前を付けるよう選択することができます。**domain.xml** ファイルでのデフォルト名は、**vHMC** です。
- d. メディア・アクセス制御 (MAC) アドレスが **domain.xml** ファイルに設定されていることを確認します。このファイルには、文字列 **MAC_ADDRESS** が含まれています。

注: MAC アドレスが自動的に生成されるようにする場合には、この行を削除してください。

- e. ご使用のブリッジがイーサネット・デバイスに一致することを確認します。デフォルトの **domain.xml** ファイルには、1 つのイーサネットが指定されています。
7. VM を定義するために、コマンド `virsh define <domain>.xml` を実行します。
8. VM を始動するために、コマンド `virsh start vHMC` を実行します。
9. ご使用のコンソールの仮想ネットワーク・コンピューティング (VNC) ディスプレイ番号を判別するために、コマンド `virsh vncdisplay vHMC` を実行します。
10. ご使用のコンソールに VNC ビューアーを使用して接続するために、コマンド `vncviewer HOSTNAME:ID` を実行します (ここで、ID はディスプレイ番号 (例えば 0) です)。

注: リモート・アクセスが必要な場合は、ポート 5900 へのアクセスを許可するようにファイアウォールをドロップまたは構成する必要があります。

Xen ハイパーバイザーを使用した **HMC** 仮想アプライアンスのインストール:

Xen ハイパーバイザーを使用したハードウェア管理コンソール (HMC) 仮想アプライアンスのインストール方法を説明します。

HMC 仮想アプライアンスは、Xen バージョン 4.2 以降をサポートしています。

Xen ハイパーバイザーを使用して HMC 仮想アプライアンスをインストールするには、以下のステップを実行します。

注: 以下のステップでは、コマンド行インターフェースを使用するため、**root** ユーザー権限が必要です。コマンド構文は、オペレーティング・システムにより異なる場合があります。

1. 仮想化パッケージが Red Hat Enterprise Linux (RHEL) バージョン 6.4 以降のシステムにインストールされていることを確認します。
2. `<XEN vHMC インストール・ファイル名>.tar.gz` ファイルをホスト・システムにダウンロードします。
3. コマンド `mkdir -p /var/lib/libvirt/images/vHMC` を実行します。
4. コマンド `cd /var/lib/libvirt/images/vHMC` を実行します。
5. 仮想ディスク・イメージを抽出するために、コマンド `tar -zxvf <XEN vHMC インストール・ファイル名>.tgz` を実行します。

注: このコマンドでは、ご使用の HMC 仮想アプライアンス `.tar` ファイルの絶対パスを指定してください。

6. **vhmc.cfg** ファイルが `<XEN vHMC インストール・ファイル名>.tar.gz` ファイルに付属しています。**vhmc.cfg** ファイルをテキスト・エディターで開いて、以下の値を編集します。
 - a. 仮想 HMC の名前を変更する (オプション): **vhmc.cfg** ファイルを編集して、ご使用のディスクへのパスが正しいことを確認します。このファイルには、文字列 **DISK_PATH** が含まれています。
 - b. **DISK_PATH** を `disk1.img` のパスに置き換える:

```
disk = [ 'file:DISKPATH,hda,w' ]
```
 - c. イーサネット・アダプターを置き換えて、MAC アドレスを追加する (オプション):

```
vif = [ 'type=virtio, model=e1000, bridge=eth0' ]
```

オプションの MAC アドレス

```
vif = [ 'type=virtio, mac=MACADDRESS, model=e1000, bridge=eth0' ]
```

注: 仮想 HMC がリブートされるたびに、Xen ハイパーバイザーは MAC アドレスを自動的に再生成します。この問題は、オプションの MAC アドレスを追加することで解決されます。

- d. **FLOPPYPATH** を置き換える (アクティベーション・エンジンを使用している場合):

```
device_model_args = [ "-fda", "FLOPPYPATH" ]
```

7. VM を作成して始動するために、コマンド `xl create vHMC.cfg` を実行する。
8. 定義済み仮想マシンのリストに VM が追加されたことを確認するために、コマンド `xl list` を実行する。
9. VM ローカル・コンソールにアクセスするために、コマンド `vncviewer localhost 0` を実行する。

VMware ESXi を使用した HMC 仮想アプライアンスのインストール:

VMware ESXi を使用したハードウェア管理コンソール (HMC) 仮想アプライアンスを取り付ける方法について説明します。

vSphere クライアント上でグラフィカル・ユーザー・インターフェースを使用して HMC 仮想アプライアンスを VMware ESXi にインストールし、Open Virtualization Format (OVF) テンプレートをデプロイすることができます。

注: HMC 仮想アプライアンスは、VMware ESXi バージョン 5.5 以降にインストールできます。

vSphere クライアントを使用して HMC 仮想アプライアンスを VMware ESXi にインストールするには、以下の手順を実行します。

注: コマンド構文は、オペレーティング・システムにより異なる場合があります。

1. Tar アーカイブ・ファイル <VMware vHMC インストール・ファイル名>.tgz を取得します。
2. tar コマンドを使用して、Tar アーカイブ・ファイルから OVA ファイルを抽出します。
3. vSphere クライアントを始動して、ESXi ホストにログインします。
4. 「ファイル」メニューで、「**OVF テンプレートのデプロイ (Deploy OVF template)**」を選択します。
5. 「参照 (**Browse**)」をクリックして、目的の OVA ファイルを選択します。
6. 「次へ」をクリックします。
7. デプロイメントが完了したら、「閉じる」をクリックし、HMC 仮想アプライアンスのアイコンを選択して HMC 仮想アプライアンスの電源をオンにします。

PowerVM (論理区画) での HMC 仮想アプライアンスのインストール

PowerVM® 環境での ハードウェア管理コンソール (HMC) 仮想アプライアンスのインストール方法について説明します。

注: HMC ISO イメージ・ファイルを使用して区画上に HMC 仮想アプライアンスをインストールする際に、Web ユーザー・インターフェースへのローカル・グラフィカル・コンソール・アクセスはありません。

HMC 仮想アプライアンスを PowerVM にインストールするには、以下のステップを実行します。

1. ISO イメージを PowerVM にインストールするための通常の手順に従います。詳しくは、VIOS メディア・リポジトリ/仮想メディア・ライブラリーの構成方法 (How to configure a VIOS Media Repository/Virtual Media Library)を参照してください。
2. インストールが完了してシステムが始動したら、「**language selection**」ダイアログ・ボックスから言語を選択する必要があります。
3. 使用条件に同意してください。

注: コマンド・コントローラーがコマンドを受け入れる準備が整っていることを確認してから、コマンドを実行します。例えば、**lshmc -V** コマンドの実行は、正常に実行されるまでです。

4. **hscroot** としてログインし、**chhmc** コマンドを使用してネットワークを構成します。

以下の例は、HMC 上でネットワークを構成し、SSH およびリモート Web アクセスを使用可能にするのに使用できる **chhmc** コマンドのシーケンスを示しています。

```
chhmc -c network -s modify -i eth0 -a <hmc ip address> -nm <hmc network mask> --lparcomm on
chhmc -c network -s modify -h <hmc hostname> -d <hmc domain name> -g <gateway ip>
chhmc -c network -s add -ns <name server> -ds <domain search>
chhmc -c ssh -s enable
chhmc -c ssh.name -s add -a <ip address>
chhmc -c SecureRemoteAccess.name -s add -a <ip address>
hmcshutdown -r -t now
```

- **hmc ip address** はご使用の HMC の IP アドレスです。
- **hmc network mask** はご使用の HMC のネットワーク・マスクです。
- **hmc hostname** はご使用の HMC のホスト名です。
- **hmc domain name** はご使用の HMC のドメイン名です。
- **gateway ip** はご使用のネットワーク上のゲートウェイの IP アドレスです。
- **name server** はご使用のネットワークのネーム・サーバー・アドレスです。
- **domain search** は HMC で検索したいドメインの名前です。
- すべての IP アドレスでのアクセスを可能にするには、**ip address** の代わりに **-a 0.0.0.0 -nm 0** を使用します。

5. システムを再始動します。

HMC 仮想アプライアンスに対する **Activation Engine** の使用

ハードウェア管理コンソール (HMC) 仮想アプライアンスに対する **Activation Engine** の使用方法について説明します。

Activation Engine は、仮想マシン内の各種コンポーネントをシステム始動中に構成できるようにするフレームワークです。**Activation Engine** は、事前取り込みディスク・イメージがないと使用できません。例えば、HMC 仮想アプライアンスが HMC リカバリー ISO ファイルを使用して作成された場合、**Activation Engine** は使用できません。**Activation Engine** を使用するためには、HMC 仮想アプライアンスが最初の始動時に管理可能状態になるように XML 構成プロファイルをセットアップする必要があります。XML 構成プロファイルの構成について詳しくは、63 ページの『**Activation Engine** 用の構成プロファイルのセットアップ』を参照してください。この構成ファイルを使用して、以下のオプションを構成することができます。

- デフォルトのキーボード (US) の設定
- デフォルト・ロケール (US)
- ご使用条件とマシン・コード条件
- セットアップ・ウィザードの使用不可設定

- コール・ホーム・ウィザードの使用不可設定
- 最大 4 つのネットワーク・インターフェース・カードの構成
- インターフェースごとのファイアウォール設定の構成

Activation Engine をセットアップするには、以下のステップを実行します。

1. テキスト・エディターを使用して、**vHMC-Conf.xml** という XML ファイルを作成するか、または **<vHMC インストール・ファイル>.tgz** パッケージ内に提供されているサンプル・ファイルを使用します。
2. ディスケット・イメージを作成します。Linux オペレーティング・システムを実行中のシステムでは、この作業は、以下のように **dd** コマンドを使用して実行できます。

```
dd if=/dev/zero of=/Floppy/Path/Floppy.img count=1440 bs=1k
```

3. 以下のように **mkfs.ext2** コマンドを使用してファイルをフォーマットします。

```
/sbin/mkfs.ext2 /Floppy/Path/Floppy.img
```

4. 以下のように、**vHMC-Conf.xml** ファイルをディスク・イメージにコピーします。

```
mkdir /Path/to/Tempfolder/Temp
mount -o loop,rw /Floppy/Path/Floppy.img /Path/to/Tempfolder/Temp
cp /Path/to/vHMC-Conf.xml /Path/to/Tempfolder/Temp
umount /Path/to/Tempfolder/Temp
```

5. カーネル・ベース仮想マシン (KVM) ハイパーバイザーの場合は、以下のように、ディスク位置を **domain.xml** ファイルに追加します。

```
<disk type='file' device='floppy'>
  <driver name='qemu' type='raw' cache='default' />
  <source file='Path/to/Floppy' />
  <target dev='fda' bus='fdc' />
  <address type='drive' controller='0' bus='0' target='0' unit='0' />
</disk>
```

6. VM を定義するために、コマンド **virsh define PATH_TO_DOMAIN_XML** を実行します。
7. VM を始動するために、コマンド **virsh start NAME_OF_VM** を実行します (NAME_OF_VM は Domain.xml ファイルに記載されています)。

Activation Engine 用の構成プロファイルのセットアップ:

XML タグを使用して Activation Engine 構成ファイルをセットアップする方法について説明します。

構成ファイル用の **XML** タグ

XML タグは、各種属性の特定の値を設定するために Activation Engine 構成ファイルで使用されます。これらの値は、Activation Engine 構成ファイルで手動で設定できます。各タグと、その許可された値の説明を表示するには、以下のセクションを使用してください。

- 64 ページの『HMC タグ』
- 64 ページの『イーサネット・タグ』
- 66 ページの『ファイアウォール・タグ』
- 67 ページの『NTPServers タグ』

注: 動的ホスト構成プロファイル・デーモン (DHCPD) サーバー設定は、Activation Engine では提供されません。

構成ファイルの構成例を表示するには、以下のセクションを使用してください。

- 68 ページの『NTPServers のない Activation Engine XML 構成ファイルの例』
- 68 ページの『NTPServers のある Activation Engine XML 構成ファイルの例』

HMC タグ

HMC タグは、HMC セットアップ構成の値を保持します。以下の例は、使用可能な HMC タグを示しています。

HMC License Agreement Tag:

```

TAG: <AcceptLicense></AcceptLicense>
Acceptable Values:
Yes -> Will Accept HMC License Agreement
No  -> Will Prompt User to Accept HMC License Agreement

```

HMC Locale Tag:

```

TAG: <Locale></Locale>
Acceptable Values:
en_US.UTF-8

```

HMC Setup Wizard Tag:

```

TAG: <SetupWizard></SetupWizard>
Acceptable Values:
Yes  -> Will Display HMC Setup Wizard
No   -> Will Disable HMC Setup Wizard

```

HMC Setup Call Home Wizard Tag:

```

TAG: <SetupCallHomeWizard></SetupCallHomeWizard>
Acceptable Values:
Yes  -> Will Display HMC Call Home Wizard
No   -> Will Disable HMC Call Home Wizard

```

HMC Setup Keyboard Tag:

```

TAG: <SetupKeyboard></SetupKeyboard>
Acceptable Values:
Yes  -> Will Prompt User for Keyboard Configuration:wq
No   -> Will Accept Default keyboard setup (U.S.)

```

イーサネット・タグ

イーサネット・タグは、イーサネット・アダプター構成の値を保持します。Activation Engine は、最大 4 つのイーサネット・アダプターを構成することができます。以下の例は、使用可能なイーサネット・タグを示しています。

Ethernet Enable Tag:

```

TAG: <Enable></Enable>
Acceptable Values:
Yes ->   Configure this adapter
No  ->   Do not Configure this adapter

```

Ethernet MACAddr Tag:

```

TAG: <MACAddr></MACAddr>
Acceptable Values:
XX:XX:XX:XX:XX:XX -> Where X is a 0-F Value
XX-XX-XX-XX-XX-XX -> Where X is a 0-F Value

```

Ethernet IPVersion Tag:

TAG: <IPVersion></IPVersion>
Acceptable Values:
IPv4 -> Use IPv4 configuration
IPv6 -> Use IPv6 configuration
MIX -> Use Both IPv4 and IPv6 configuration

Ethernet IPv4 Network Type Tag:

TAG: <IPv4NetworkType></IPv4NetworkType>
Acceptable Values:
Static -> Configure Adapter using Static Configuration
Dhcp -> Configure Adapter using DHCP Configuration

Ethernet IPv4 Address Tag:

TAG: <IPv4Address></IPv4Address>
Acceptable Values:
Any valid IPv4 Address Value

Ethernet IPv4 Netmask Tag:

TAG: <IPv4Netmask></IPv4Netmask>
Acceptable Values:
Any valid IPv4 Netmask Value

Ethernet IPv4 Gateway Tag:

TAG: <IPv4Gateway></IPv4Gateway>
Acceptable Values:
Any valid IPv4 Address Value

Ethernet IPv6 Network Type Tag:

TAG: <IPv6NetworkType></IPv6NetworkType>
Acceptable Values:
Static -> Configure Adapter using Static Configuration
Dhcp -> Configure Adapter using DHCP Configuration

Ethernet IPv6 Address Tag:

TAG: <IPv6Address></IPv6Address>
Acceptable Values:
Any valid IPv6 Address Value

Ethernet IPv6 Gateway Tag:

TAG: <IPv6Gateway></IPv6Gateway>
Acceptable Values:
Any valid IPv6 Address Value

Ethernet Hostname Tag:

TAG: <Hostname></Hostname>
Acceptable Values:
Valid String

Ethernet Domain Tag:

TAG: <Domain></Domain>
Acceptable Values:
Any Valid Domain Value
Ex. austin.ibm.com

Ethernet DNS Servers Tag:

```

TAG:    <DNSServers></DNSServers>
Acceptable Values:
Up to 3 Valid IPV4 or IPV6 Addresses seperated by a coma
It is acceptable to have an Empty DNS Server Value.
Ex.1  IPV4:  9.3.2.1      IPV6: 2001:4860:4860::8888
Ex.2  IPV4:  9.3.2.1,9.5.4.1  IPV6: 2001:4860:4860::8888,2001:4860:4860::8844
Ex.3  IPV4:  9.3.2.1,9.5.4.1,9.4.3.2  IPV6: 2001:4860:4860::8888,2001:4860:4860::8844,
      ::ffff:903:201

```

ファイアウォール・タグ

ファイアウォール・タグは、対応するイーサネット・アダプターのそれぞれのファイアウォール値を保持します。以下の例は、使用可能な HMC タグを示しています。

注: すべてのタグに、Enabled または Disabled の値が必要です。

Firewall PEGASUS Tag:

```

TAG:    <PEGASUS></PEGASUS>
Acceptable Values:
Enabled -> Will Allow PEGASUS Ports to be open
Disabled -> Will Disable PAGASUS Ports

```

Firewall RPD Tag:

```

TAG:    <RPD></RPD>
Acceptable Values:
Enabled -> Will Allow RMC Ports to be open
Disabled -> Will Disable RMC Ports

```

Firewall FCS Tag:

```

TAG:    <FCS></FCS>
Acceptable Values:
Enabled -> Will Allow FCS Ports to be open
Disabled -> Will Disable FCS Ports

```

Firewall I5250 Tag:

```

TAG:    <I5250></I5250>
Acceptable Values:
Enabled -> Will Allow 5250 Ports to be open
Disabled -> Will Disable 5250 Ports

```

Firewall PING Tag:

```

TAG:    <PING></PING>
Acceptable Values:
Enabled -> Will Allow PING Port to be open
Disabled -> Will Disable PING Port

```

Firewall L2TP Tag:

```

TAG:    <L2TP></L2TP>
Acceptable Values:
Enabled -> Will Allow L2TP Ports to be open
Disabled -> Will Disable L2TP Ports

```

Firewall SLP Tag:

```

TAG:    <SLP></SLP>
Acceptable Values:
Enabled -> Will Allow SLP Ports to be open
Disabled -> Will Disable SLP Ports

```

Firewall RSCT Tag:

```
TAG:    <RSCT></RSCT>
Acceptable Values:
Enabled -> Will Allow RSCT Ports to be open
Disabled -> Will Disable RSCT Ports
```

Firewall SECUREREMOTEACCESS Tag:

```
TAG:    <SECUREREMOTEACCESS></SECUREREMOTEACCESS>
Acceptable Values:
Enabled -> Will Allow Secure Remote Access Ports to be open
Disabled -> Will Disable Secure Remote Access Ports
```

Firewall SSH Tag:

```
TAG:    <SSH></SSH>
Acceptable Values:
Enabled -> Will Allow SSH Port to be open
Disabled -> Will Disable SSH Port
```

Firewall VTTY Tag:

```
TAG:    <VTTY></VTTY>
Acceptable Values:
Enabled -> Will Allow VTTY Ports to be open
Disabled -> Will Disable VTTY Ports
```

Firewall NTP Tag:

```
TAG:    <NTP></NTP>
Acceptable Values:
Enabled -> Will Allow NTP Ports to be open
Disabled -> Will Disable NTP Ports
```

Firewall SNMPTraps Tag:

```
TAG:    <SNMPTraps></SNMPTraps>
Acceptable Values:
Enabled -> Will Allow SNMP Traps Ports to be open
Disabled -> Will Disable SNMP Traps Ports
```

Firewall SNMPAgents Tag:

```
TAG:    <SNMPAgents></SNMPAgents>
Acceptable Values:
Enabled -> Will Allow SNMP Agents Ports to be open
Disabled -> Will Disable SNMP Agents Ports
```

NTPServers タグ

NTPServers タグは、HMC 仮想アプライアンスで最大 5 つの NTP サーバーを構成する場合に必要です。NTP サーバーは、<ntpparam ntpserver="server" ntpversion="1-4"/> タグを使用して追加できます。server パラメーターには、IPv4 値または IPv6 値、あるいはドメイン名を指定できます。以下の例は、使用可能な NTPServers タグを示しています。

NTPServers Tag:

```
TAG: <NTPServers></NTPServers>
Accepts <ntpparam ntpserver="server" ntpversion="1-4"/>
```

```
Ex.1 <NTPServers>
      <ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
    </NTPServers>
```

```
Ex.2 <NTPServers>
```

```

<ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>
<ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
<ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>

```

ntpparam Tag

```

TAG: <ntpparam ntpserver="" ntpversion="" />
Attribute Values:

```

```

ntpserver: will accept IPv4/IPv6 values and valid hostnames
ntpversion: will accept a 1-4 numeric value

```

NTPServers のない Activation Engine XML 構成ファイルの例

以下の例は、NTPServers のない Activation Engine XML 構成ファイルを示しています。

```

<vHMC-Configuration>
  <LicenseAgreement>
  </LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
</Ethernet>
  <Enable>No</Enable>
  <MACAddr></MACAddr>
  <IPVersion></IPVersion>
  <IPv4NetworkType></IPv4NetworkType>
  <IPv4Address></IPv4Address>
  <IPv4Netmask></IPv4Netmask>
  <IPv4Gateway></IPv4Gateway>
  <IPv6NetworkType></IPv6NetworkType>
  <IPv6Address></IPv6Address>
  <IPv6Gateway></IPv6Gateway>
  <Hostname></Hostname>
  <Domain></Domain>
  <DNSServers></DNSServers>
</Firewall>
  <PEGASUS>Enabled</PEGASUS>
  <RPD>Enabled</RPD>
  <FCS>Enabled</FCS>
  <I5250>Enabled</I5250>
  <PING>Enabled</PING>
  <L2TP>Disabled</L2TP>
  <SLP>Enabled</SLP>
  <RSCT>Enabled</RSCT>
  <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
  <SSH>Enabled</SSH>
  <VTTY>Disabled</VTTY>
  <NTP>Disabled</NTP>
  <SNMPTraps>Disabled</SNMPTraps>
  <SNMPAgents>Disabled</SNMPAgents>
</Firewall>
</Ethernet>
</vHMC-Configuration>

```

NTPServers のある Activation Engine XML 構成ファイルの例

以下の例は、NTPServers のある Activation Engine XML 構成ファイルを示しています。

```

<vHMC-Configuration>
  <LicenseAgreement>
  </LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>

```

```

    <Locale>en_US.UTF-8</Locale>
    <SetupWizard>No</SetupWizard>
    <SetupCallHomeWizard>No</SetupCallHomeWizard>
    <SetupKeyboard>No</SetupKeyboard>
<Ethernet>
    <Enable>No</Enable>
    <MACAddr></MACAddr>
    <IPVersion></IPVersion>
    <IPv4NetworkType></IPv4NetworkType>
    <IPv4Address></IPv4Address>
    <IPv4Netmask></IPv4Netmask>
    <IPv4Gateway></IPv4Gateway>
    <IPv6NetworkType></IPv6NetworkType>
    <IPv6Address></IPv6Address>
    <IPv6Gateway></IPv6Gateway>
    <Hostname></Hostname>
    <Domain></Domain>
    <DNSServers></DNSServers>
<Firewall>
    <PEGASUS>Enabled</PEGASUS>
    <RPD>Enabled</RPD>
    <FCS>Enabled</FCS>
    <I5250>Enabled</I5250>
    <PING>Enabled</PING>
    <L2TP>Disabled</L2TP>
    <SLP>Enabled</SLP>
    <RSCT>Enabled</RSCT>
    <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
    <SSH>Enabled</SSH>
    <VTTY>Disabled</VTTY>
    <NTP>Disabled</NTP>
    <SNMPTraps>Disabled</SNMPTraps>
    <SNMPAgents>Disabled</SNMPAgents>
</Firewall>
</Ethernet>
<NTPServers>
    <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/>
    <ntpparam ntpserver="9.4.34.1" ntpversion="4"/>
    <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>
</NTPServers>
</vHMC-Configuration>

```

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。

POWER8 プロセッサ・ベースのシステムの管理に HMC が使用される場合、HMC は CR3 以降でなければならず、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。各種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・キャビネット内で、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。

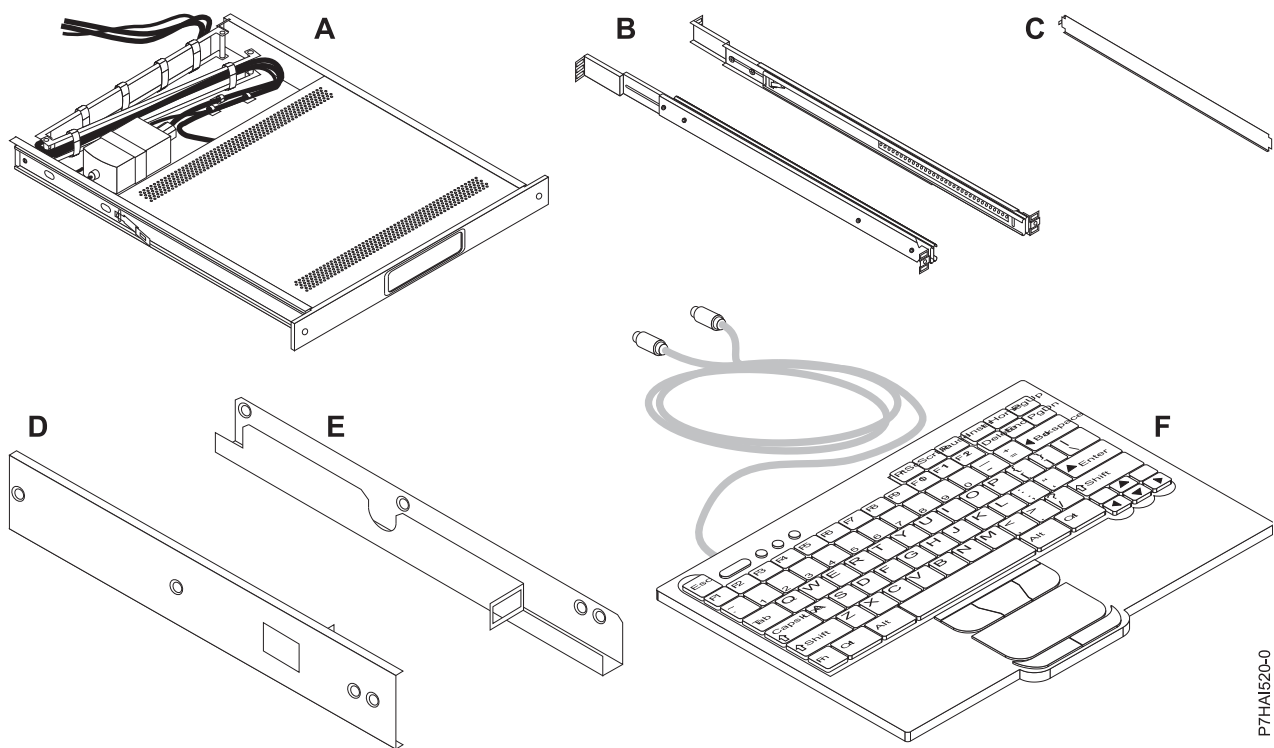


図 75. インストール・キット部品

表 10. インストール・キット部品の内容

インストール・キット	部品の内容
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)

表 10. インストール・キット部品の内容 (続き)

インストール・キット	部品の内容
	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. システムをラックに取り付けることにします。 EIA の位置を記録します。

注: ご使用のラックでの 1 EIA 単位は、3 つの穴のグループで構成されています。

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 単位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 単位の下部の穴と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 (8 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、ラックの前面でマークを付けた最下段の EIA 単位に対応する EIA 単位を見つけます。
7. 最下段の EIA 単位に接着ドットを貼り付けます。
8. EIA 単位の上部の穴に接着ドットを付けます。

9. ラック左側の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。

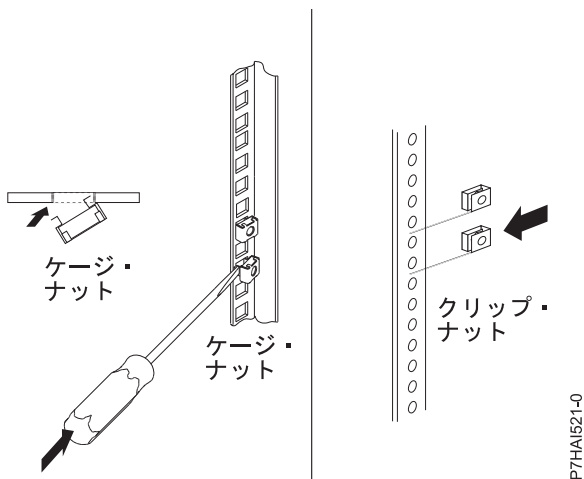


図 76. ケージ・ナットの取り付け

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。

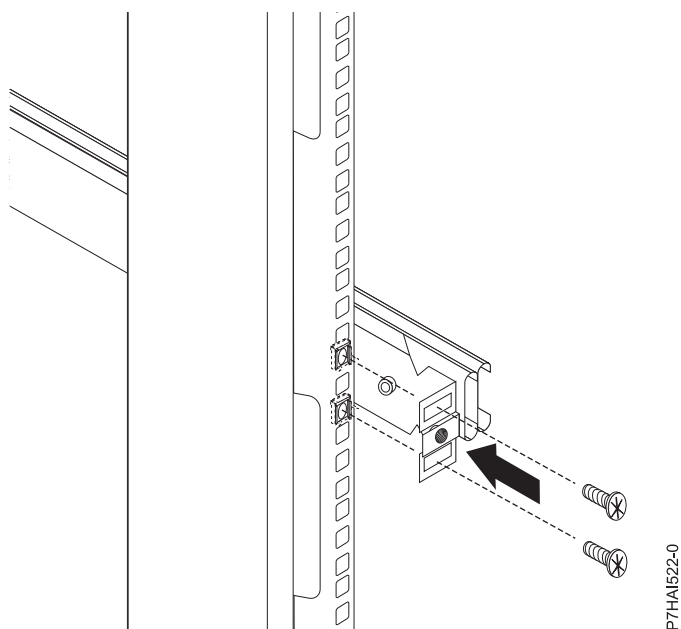


図 77. スライド・レール・ブラケットの調整

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、ねじを取り付けしないでください。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。

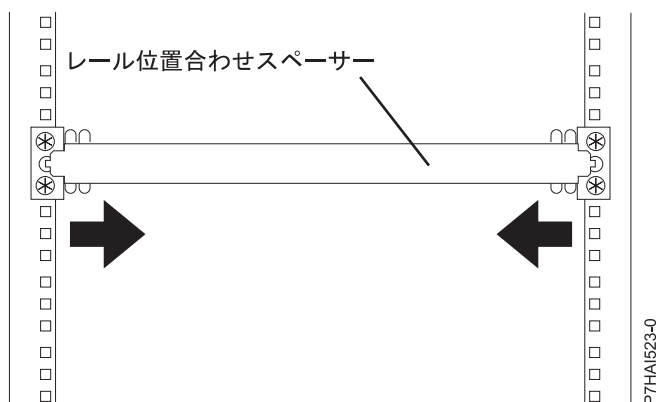


図 78. レール位置決めスペーサーの挿入

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。

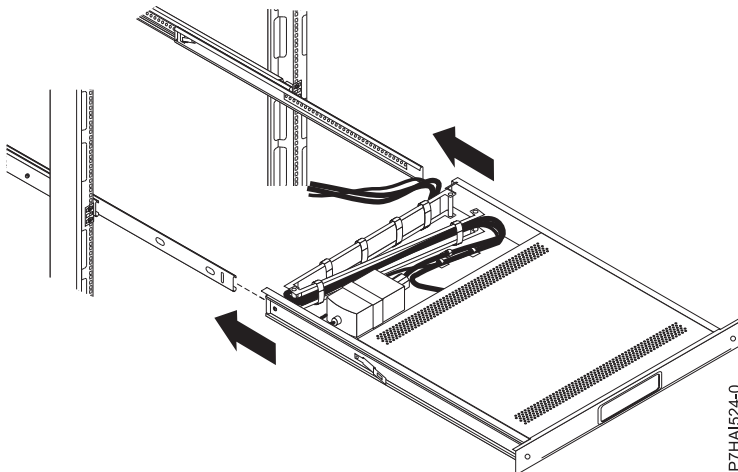


図 79. モニターおよびキーボードをスライドさせる

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。

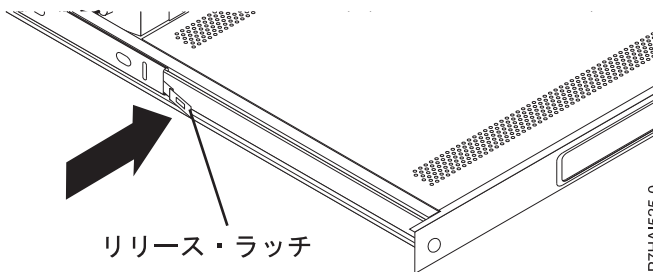


図 80. リリース・ラッチの使用

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。

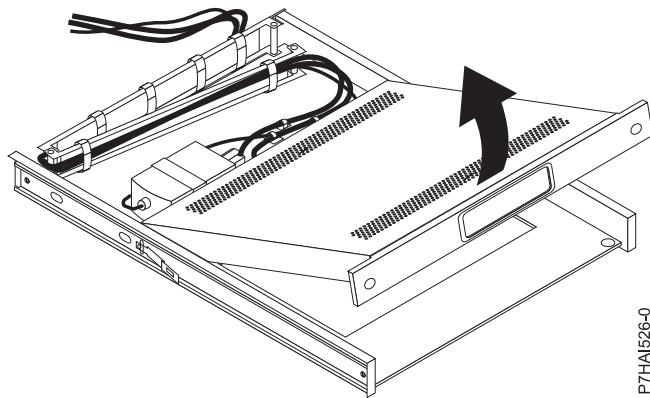


図 81. モニターを直立位置に立てる

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ばります。
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た後、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。

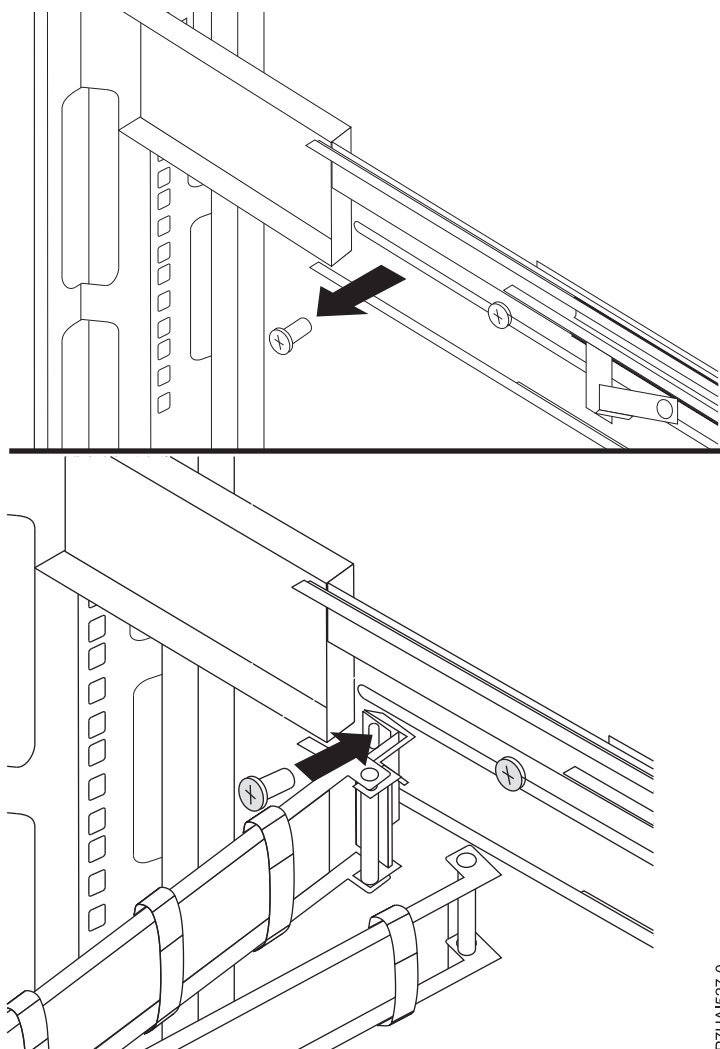


図 82. ケーブル・マネジメント・アームの取り付け

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を、適切な装置またはコネクタに接続します。
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)

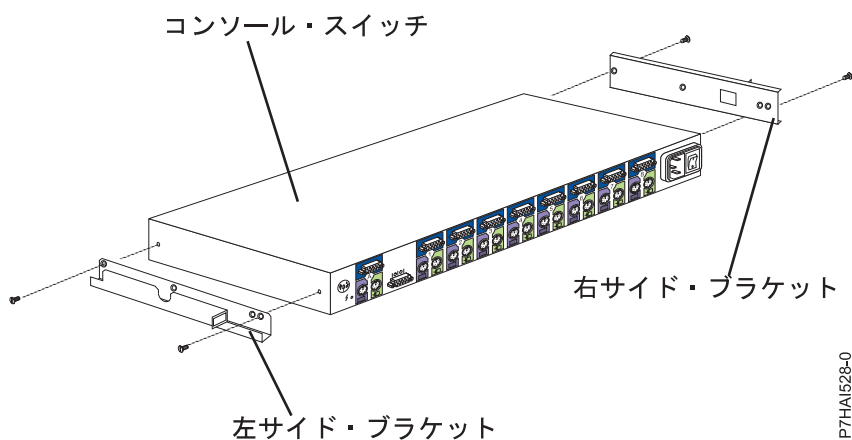
オプションのコンソール・スイッチを取り付ける方法について説明します。

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。



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をコンソール・スイッチに接続します。

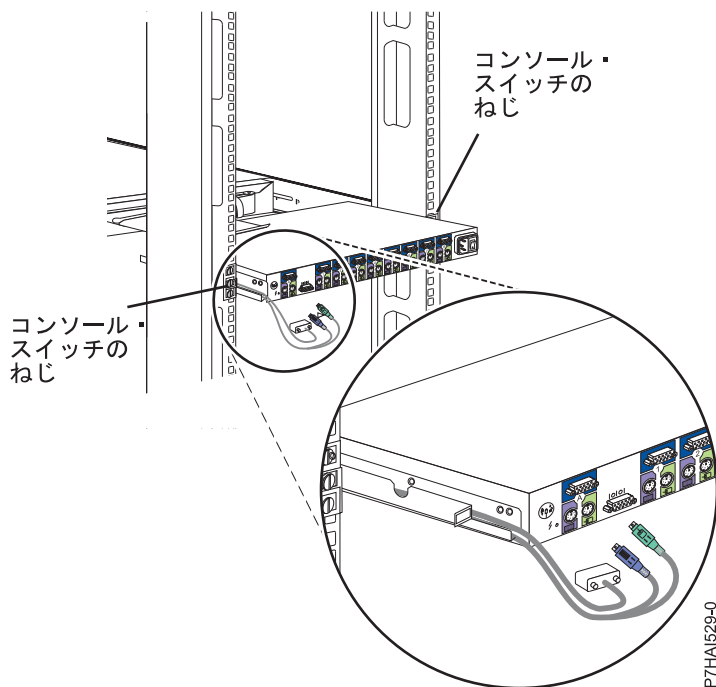


図 84. ケーブル配線

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 Classic または HMC Enhanced インターフェースを使用した HMC の構成

HMC Classic または HMC Enhanced インターフェースを使用した、ネットワーク接続のセットアップ、HMC の構成、構成完了後の手順の実行、および HMC のアップグレードと更新の方法について説明します。

注:

1. HMC Classic インターフェースは、ハードウェア管理コンソール (HMC) バージョン 8.7.0 以降では使用できなくなりました。以前に HMC Classic インターフェースで使用可能だった機能は、HMC Enhanced+ インターフェースで使用できるようになりました。
2. HMC Enhanced GUI は、HMC にログイン中に「HMC Enhanced」オプションを選択すると、HMC バージョン 8.1.0.1 または 8.2.0 で使用可能になります。HMC バージョン 8.3.0 以降では、HMC Enhanced インターフェースの手順および機能は HMC Enhanced+ インターフェースの一部になっています。
3. 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。

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、98 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) を収集したり、特定のプラットフォーム活動 (動的 LPAR、並行修復) をそれらのオペレーティング・システムに合わせ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 BMC へ

注: ベースボード管理コントローラー (BMC) 接続は、HMC モデル 7063-CR1 にのみ該当します。

保守作業の実行に使用されます。BMC 接続は、システム上に HMC ファームウェアをロードして維持するために使用されます。この接続は、HMC 上の BMC にアクセスするのに必要です。

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。

- Web ブラウザーを使用して、リモートですべての HMC GUI 機能にアクセスする。
- 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・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。

- 1 つ以上のネットワーク・インターフェースを HMC と管理対象システム間の通信に独占的に使用できます。つまり、そのネットワーク上に存在するのは、HMC および管理対象システムのサービス・プロセッサのみであることを意味します。サービス・プロセッサへのネットワーク・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・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) バージョン 8.7.0 は、Google Chrome バージョン 57、Microsoft Internet Explorer (IE) バージョン 11.0、Mozilla Firefox バージョン 45 ならびに 52 の Extended Support Release (ESR)、および Safari バージョン 10.1 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。

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・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. 「了解」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、「Options」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. 「了解」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 がい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。

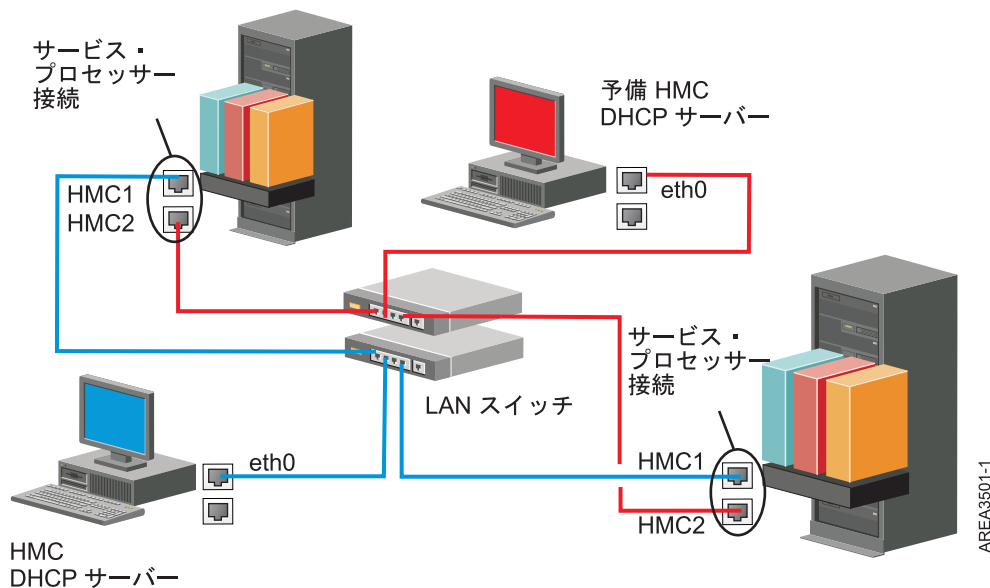
HMC 自身は、自分自身のファイアウォールをその各ネットワーク・インターフェース上で提供します。「HMC ガイド付きセットアップ・ウィザード」の実行時に基本的なファイアウォールが自動的に構成されますが、初期の HMC 取り付けと構成の完了後にファイアウォール設定をカスタマイズする必要があります。

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。

HMC を DHCP サーバーとして構成する方法については、107 ページの『DHCP サーバーとしての HMC の構成』を参照してください。

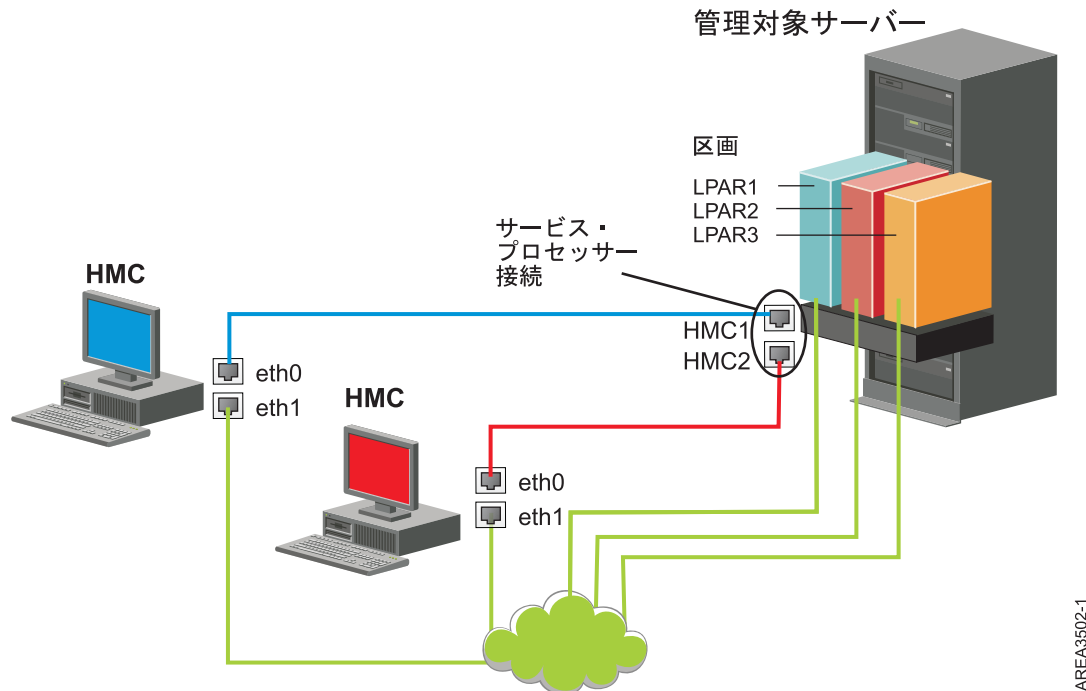


この図には、2 つの管理対象システムに接続する冗長 HMC 環境を記載してあります。最初の HMC は、各 FSP 上の最初のポートに接続され、冗長 HMC は各 HMC 上の 2 番目のポートに接続されています。各 HMC は DHCP サーバーとして構成され、異なる範囲の IP アドレスを使用しています。各接続は独立したプライベート・ネットワーク上にあります。このように、どの FSP ポートも 2 台以上の HMC に接続されていないようにすることが重要です。

ある HMC に接続される各管理対象システムの FSP ポートには、ユニークな IP アドレスが必要です。各 FSP が固有の IP アドレスを持つようにするには、HMC の組み込み DHCP サーバー機能を使用します。この FSP がアクティブなネットワーク・リンクを検出すると、FSP はブロードキャスト要求を発行して DHCP サーバーを見つけます。正しく構成されていると、HMC は、選択された範囲のアドレスのいずれかを割り当てて、その要求に応答します。

FSP が複数存在する場合、HMC と FSP 間のプライベート・ネットワーク用に、ユーザー独自の LAN スイッチまたはハブを持っている必要があります。または、このプライベート・セグメントは、より大きな管理されたスイッチ上のプライベート仮想 LAN (VLAN) 内で、複数ポートとして存在することができます。複数のプライベート VLAN がある場合、その VLAN が分離されていること、およびその VLAN を縦断するトラフィックが存在しないことを確認する必要があります。

複数の HMC がある場合、各 HMC を論理区画に、およびお互いに、同一オープン・ネットワーク上で接続する必要もあります。



この図には、プライベート・ネットワーク上で単一の管理対象サーバーに接続され、さらにパブリック・ネットワーク上で 3 つの論理区画に接続された 2 つの HMC が記載されています。この HMC 用に追加のイーサネット・アダプターを保有して、3 つのネットワーク・インターフェースを保有可能です。この 3 番目のネットワークを管理ネットワークとして使用するか、または CSM (クラスター・システム・マネージャー) の管理サーバーにこれを接続できます。

HMC を DHCP サーバーとして構成する方法について詳しくは、107 ページの『DHCP サーバーとしての HMC の構成』を参照してください。

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。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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・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、86 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。

- 伝送速度の高速化
- 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。

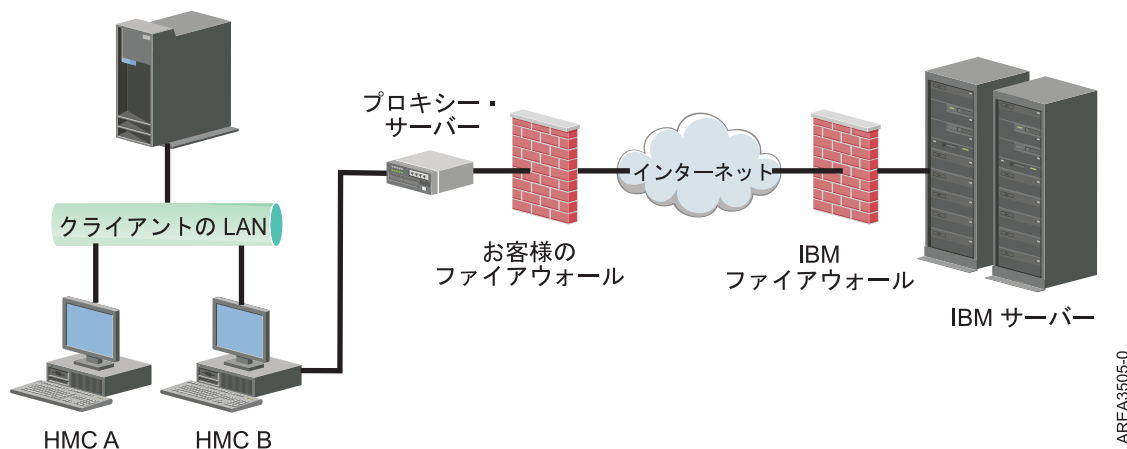
- リモート・サポート機能の要求は、常に、HMC から開始されて IBM に送信されます。インバウンド接続が、IBM Service Support System から開始されることは決してありません。
- HMC と IBM Service Support System 間で転送される全データは、高度な暗号化機能を使用して暗号化されています。データは、選択した接続方式に応じて、SSL または IPSec Encapsulating Security Payload (ESP) のいずれかを使用して暗号化されます。
- 暗号化された接続の開始時に、HMC はターゲットとなる宛先を IBM Service 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・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 プロキシを使用した場合に考えられる他の利点の 1 つは、プロキシによりロギング機能および監査機能をサポートできることです。

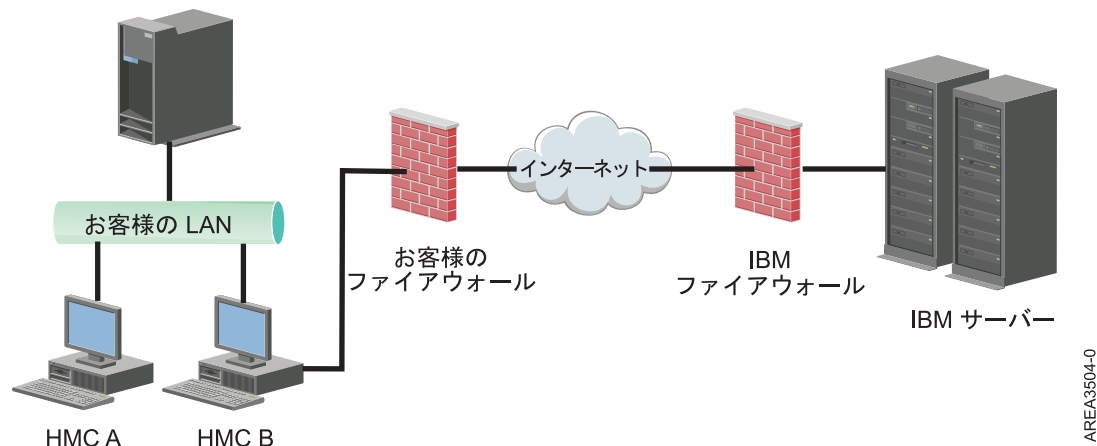
SSL ソケットをフォワードするには、そのプロキシ・サーバーは基本プロキシ・ヘッダー機能 (RFC 2616 に記載あり) と CONNECT メソッドをサポートする必要があります。オプションとして、基本プロキシ認証 (RFC 2617) を、プロキシ・サーバー経由でソケットを転送しようとする前に HMC が認証するように構成することができます。



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・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・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、86 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 86 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。



単純化された接続:

単純化された接続を使用する場合に HMC が使用する IP アドレスについて説明します。

現行のコール・ホーム・インフラストラクチャーにフロントエンド・プロキシを提供する新規のコール・ホーム・サーバー環境が使用可能になりました。この環境は、IBM サーバーの台数を削減し、IPv6 接続を使用可能にし、NIST 800-131A のサポートで機能強化されたセキュリティーを提供することにより、必要とされる情報技術を単純化します。ご使用のファイアウォールで開く IBM IP アドレスが少なくなります。すべてのコール・ホーム・インターネット・トラフィックは、コール・ホーム・プロキシを通じて伝送します。

注: 単純化された接続は、HMC バージョン 8.3.0 以降で使用可能です。

HMC は、単純化された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。

- 129.42.56.189
- 129.42.60.189
- 129.42.54.189

HMC は、単純化された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。

- 2620:0:6c0:200:129:42:56:189
- 2620:0:6c2:200:129:42:60:189
- 2620:0:6c4:200:129:42:54:189

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・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、107 ページの『IPv4 アドレスの設定』および 108 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
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216
- 170.225.15.41

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
- 207.25.252.197
- 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
- 207.25.252.197
- 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。

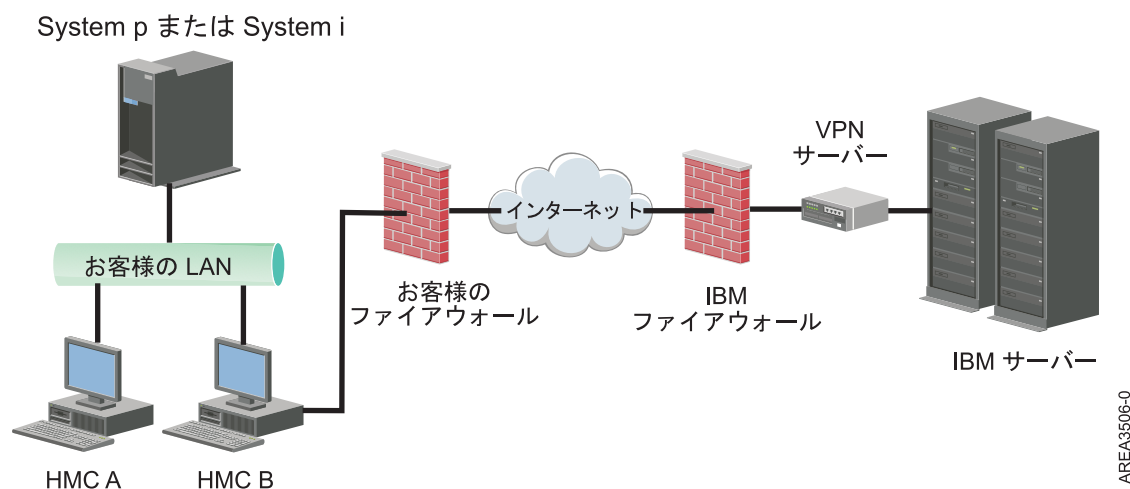
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

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を提供します。

注: この接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、88 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、102 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。

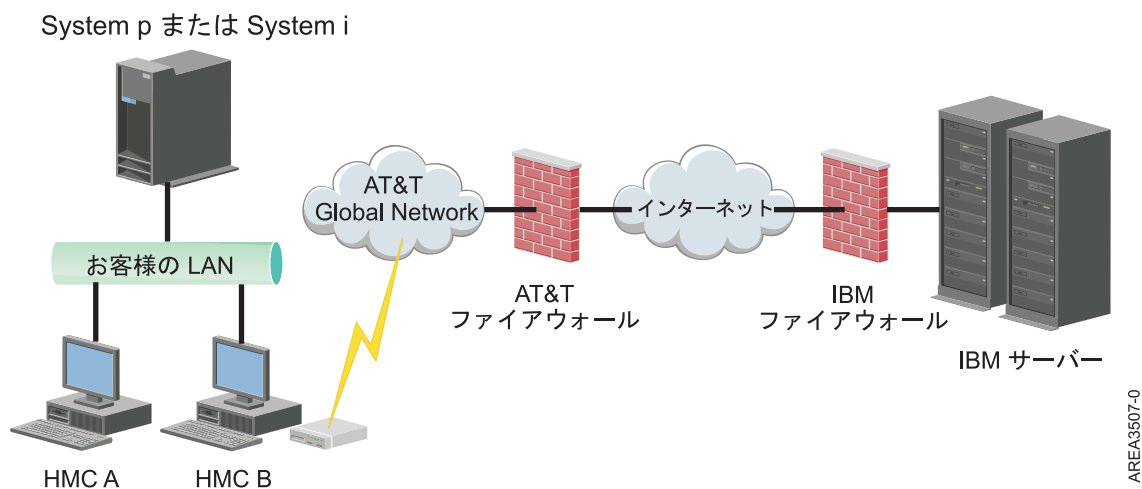
インターネット VPN 接続を使うように HMC を構成すると、HMC は以下のサーバーを使用します。ネットワーク・アドレス変換 (NAT) ファイアウォールを使おうとする時に、すべての接続が ESP、およびポート 500 とポート 4500 上の UDP を使用します。

- 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。

注: この接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。



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、102 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。

HMC を構成するためには、関連する概念を理解し、決定し、情報を準備する必要があります。

このセクションでは、ご使用の HMC を以下のものに接続するために必要な情報について説明します。

- 管理対象システム内のサービス・プロセッサ
- 管理対象システム上の論理区画
- リモート・ワークステーション
- IBM Service (「コール・ホーム」機能をインプリメントする)

注: 追加の接続およびセキュリティ情報が使用可能です。詳しくは、「**ESA for HMC Connectivity Security for IBM POWER6®, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000®**」ホワイト・ペーパーを参照してください。これは、以下で入手できます。IBM Electronic Service Agent™ (<http://www-01.ibm.com/support/esa/security.htm>)。

HMC 構成を準備するには、以下の手順を実行します。

1. インストールする HMC コードの最新レベルのバージョンを取得してインストールします。
2. HMC が管理するサーバーとの関連で、HMC の物理的な位置を決定します。HMC とその管理対象システムとの間の距離が 7.62 m を超える場合は、サービス担当員が HMC にアクセスできるように、管理対象システムの位置から HMC に Web ブラウザーによるアクセスができる必要があります。
3. HMC が管理するサーバーを識別します。
4. サーバーの管理にプライベート・ネットワークまたはオープン・ネットワークを使用するかどうかを決定します。プライベート・ネットワークを使用することに決めた場合は、Cluster Systems Management (CSM) 構成を使用しない限り、DHCP を使用します。CSM は IPv6 をサポートしません。CSM にアクセスするには、2 つのネットワークを持つ必要があります。CSM の詳細については、該当のフィーチャーに付属の資料を参照してください。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、81 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。
5. オープン・ネットワークを使用して FSP を管理する場合は、Advanced System Management Interface メニューを使用して FSP のアドレスを手動で設定する必要があります。プライベートのルーティング不可能なネットワークをお勧めします。
6. 2 台の HMC がある場合は、プライマリー HMC とセカンダリー HMC を指定します。プライマリー HMC は、物理的にこのマシンに近くて、しかもコール・ホームに構成された HMC にする必要があります。

7. HMC をリモート・ワークステーション、論理区画、およびネットワーク・デバイスに接続するために必要なネットワーク設定を決定します。
8. HMC が「コール・ホーム」する方法を定義します。コール・ホーム・オプションには、アウトバウンドのみの Secure Sockets Layer (SSL) インターネット接続、モデム、または仮想プライベート・ネットワーク (VPN) 接続のいずれかの使用が含まれます。
9. 作成する HMC ユーザーおよびそのパスワード、ならびに付与するロールを決定します。hscroot および hscpe ユーザーにパスワードを割り当てる必要があります。
10. コール・ホームの構成時に必要となる以下の会社連絡先情報を記録します。
 - 会社名
 - 管理者の連絡先
 - 電子メール・アドレス
 - 電話番号
 - FAX 番号
 - HMC の物理的な所在地住所
11. コール・ホームを介して IBM サービスに情報が送信された時の、オペレーターまたはシステム管理者への通知に電子メールを使用する計画がある場合は、Simple Mail Transfer Protocol (SMTP) サーバーおよび使用する電子メール・アドレスを確認します。
12. 以下のパスワードを定義する必要があります。
 - FSP に対して HMC を認証するために使用されるアクセス・パスワード
 - 「管理者」ユーザーに使用される ASMI パスワード
 - 「一般」ユーザーに使用される ASMI パスワード

HMC から新規サーバーに最初に接続するときのパスワードを作成します。HMC が予備または 2 番目の HMC である場合は、HMC ユーザー・パスワードを取得して、管理対象サーバーの FSP に初めて接続するときそのパスワードを入力する準備を整えます。

この準備ステップが完了したら、『HMC 用のプリインストール構成ワークシート』に進みます。

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、79 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。

表 11. イーサネット・アダプターのスピードと二重モード

	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、81 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。

表 12. プライベート・ネットワークとオープン・ネットワーク

	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。

表 13. プライベート・ネットワーク

	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)		
「はい」の場合、使用する IP アドレスの範囲を記録します。		

7063-CR1 HMC を使用している場合、HMC 上のベースボード管理コントローラー (BMC) にアクセスするためにイーサネット IPMI ポートをネットワークに接続する必要があります。詳しくは、159 ページの『BMC 接続の構成』を参照してください。ご使用の BMC 接続について以下の表を記入します。

表 14. BMC 接続

	IPMI
この接続は DHCP モードを使用して構成しますか? (はい/いいえ)	
「いいえ」の場合、以下の指定された静的アドレスをリストしてください。	
IP アドレス:	
サブネット・マスク:	
ゲートウェイ:	

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、86 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。

表 15. IPv6 の使用

	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。				

表 16. IPv6 の使用

	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)				

表 17. IPv6 の使用

	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 108 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、108 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。

表 18. IPv4 の使用

	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:				

表 18. IPv4 の使用 (続き)

	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・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。

表 19. ローカル・ホスト情報

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	

表 19. ローカル・ホスト情報 (続き)

ローカル・ホスト情報	
DNS を使用したいですか? (はい/いいえ)	
「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です。

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です。

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。

表 20. 電子メール通知

フィールド	
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:	

表 20. 電子メール通知 (続き)

フィールド	
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

表 21. サービス連絡先情報

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)	

表 21. サービス連絡先情報 (続き)

サービス連絡先情報	
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 (セキュリティ特性と構成要件を含む) は、 83 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。

表 22. 接続のタイプ

接続のタイプ	
	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 プロキシの使用 (Use SSL Proxy)**」を選択します。

表 23. インターネット経由の Secure Sockets Layer (SSL)

インターネット経由の Secure Sockets Layer (SSL)	
SSL プロキシの使用 ? (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、 86 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。

表 24. ローカル HMC からのダイヤルアップ

フィールド	
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、88 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 25. 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

表 26. サポート上のさらなる利点

フィールド	
IBM ID のリスト	
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 エレクトロニック・サービス・エージェント 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の構成方法について説明します。

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、89 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、90 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 の始動、およびガイド付きセットアップ・ウィザードにある各ステップを完了:

HMC インターフェースにログインし、ガイド付きセットアップ・ウィザードを使用して HMC を構成します。

注: これが新規インストールの場合は、管理対象システムが電源に接続されていないことを確認します。ラック・マウント型 HMC では、主電源装置に接続する前に電源分配バス (PDB) に接続されている唯一のデバイスは HMC であることを意味します。これが同じ管理対象システムに接続された 2 番目の HMC である場合、この管理対象システムを電源に接続できます。

1. 電源ボタンを押して HMC をオンにします。
2. HMC が、30 秒後に自動的にデフォルトの言語とロケール設定を選択するのを待ちます。
3. ハードウェア管理コンソールのご使用条件に同意します。ハードウェア管理コンソールのご使用条件に同意しない場合は、HMC の構成を完了することはできません。
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. HMC に以下のようにしてログインします。

注: システム管理者 (**hmcadmin**) がパスワードを変更した場合は、そのパスワードをここで入力してください。

- ID: hscroot
- パスワード: abc123

ガイド付きセットアップ・ウィザードが開きます。

6. ガイド付きセットアップのエントリー・ウィンドウで、「了解」をクリックします。

注: HMC の始動時にガイド付きセットアップ・ウィザードが表示されなかった場合は、HMC ウェルカム・ページのナビゲーション領域の「ガイド付きセットアップ・ウィザード」をクリックします。

7. 記入済みのプリインストール構成ワークシートを使用して、ガイド付きセットアップ・ウィザードにある各ステップを完了します。「はい」をクリックして、「接続およびコール・ホーム・サーバー」ウィザードの各ステップを続行して完了します。
8. 「要約」ウィンドウで、「完了」をクリックします。
9. イーサネット・クロスケーブルを管理対象システムに接続していない場合は、この時点で接続します。
10. HMC ナビゲーション領域で、「サービス管理」をクリックします。
11. コンテンツ領域で、「ユーザーの許可」をクリックします。「ユーザーの許可」ウィンドウが開きます。
12. フィールドに IBM ID を入力し、「了解」をクリックします。

構成の確認:

「状況」ウィンドウで、選択したさまざまな構成設定の進行情況をモニターします。このウィンドウでは、いくつかのタスクについて数分間、保留の状況を表示することもあります。「ログの表示」をクリックして、各タスクに関連する状況メッセージを調べます。いつでも、「閉じる」をクリックすると、ガイド付きセットアップ・ウィザードが終了します。実行中のタスクは、そのまま実行を継続します。これで HMC が構成されました。

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。

この情報には、PDF に収録されていないタスクの参照も含まれています。 HMC ウェルカム・ページの「**Additional Resources (追加のリソース)**」セクションを参照して、追加のサポート資料にアクセスできます。

前提条件

HMC メニューを使用した HMC の構成を始める前に、 89 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。

表 27. 人手による HMC 構成タスクおよび関連情報の入手先

作業	関連情報の入手先
1. HMC を開始します。	101 ページの『HMC の始動』
2. 日時を設定します。	
3. 事前定義済みのパスワードを変更します。	
4. 追加のユーザーを作成して、そのステップを終了したら、このチェックリストに戻ります。	
5. ネットワーク接続を構成します。	102 ページの『HMC ネットワーク・タイプの構成』
6. オープン・ネットワークおよび固定 IP アドレスを使用する場合は、識別情報を設定します。	
7. オープン・ネットワークおよび固定 IP アドレスを使用する場合は、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します。	109 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』
8. オープン・ネットワークおよび固定 IP アドレスを使用する場合は、ドメイン名サービスを構成します。	110 ページの『ドメイン名サービスの構成』
9. 固定 IP アドレスを使用しており、DNS が使用可能である場合は、ドメイン・サフィックスを構成します。	110 ページの『ドメイン・サフィックスの構成』
10. ご使用のサーバーを IBM サービスおよびサポートに接続するように構成し、そのステップを終了したらこのチェックリストに戻ります。	112 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』
11. 「コール・ホーム用イベント・マネージャー」を構成します。	118 ページの『「コール・ホーム用イベント・マネージャー」の構成』
12. 管理対象システムに電源を接続します。	
13. 管理対象システムのパスワード、および各 ASMI パスワード (一般および管理者) を設定します。	119 ページの『管理対象システムに対するパスワードの設定』
14. 管理対象システムの日時を設定するために ASMI にアクセスします。	
15. 管理対象システムを始動して、そのステップを終了したら、このチェックリストに戻ります。	
16. 管理対象システムに論理区画が 1 つあることを確認します。	
17. オプション: 別の管理対象システムを追加して、そのステップを終了したら、このチェックリストに戻ります。	
18. オプション: 新しいサーバーを HMC とともに取り付ける場合は、論理区画を構成して、オペレーティング・システムをインストールします。	

表 27. 人手による HMC 構成タスクおよび関連情報の入手先 (続き)

作業	関連情報の入手先
19. この時点で新しいサーバーをインストールしない場合は、ご使用の構成をさらにカスタマイズするために、構成完了後のオプション・タスクを実行します。	120 ページの『構成完了後のステップ』

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、以下の手順を実行します。

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 とパスワードを使用して、HMC にログインします。

ID: `hscroot`

パスワード: `abc123`

注: HMC バージョン 8.1.0.1 では、以下のログイン・オプションから選択できます。

ログイン: 前回のログイン、HMC Classic、または HMC Enhanced

HMC にログインするときに使用するソフトウェア・インターフェースを選択してください。HMC Classic インターフェースは、HMC の従来の機能すべてへのアクセスを可能にし、HMC Enhanced インターフェースは、仮想化タスクおよび機能の再設計されたものと新規のもの両方を提供します。

前回のログイン

以前のログイン・セッションから選択したグラフィカル・ユーザー・インターフェース (GUI) を表示します。

HMC Enhanced

拡張 PowerVM 機能を備えた、より新しい拡張 GUI を表示します。

HMC Classic

拡張 PowerVM 機能を備えていない、標準 GUI を表示します。

注: HMC は、DHCP サーバーとして機能している場合、最初にサービス・プロセッサに接続する際に、デフォルトのパスワードを使用します。

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 28. 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。	90 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。	105 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。	106 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。	106 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。	107 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。	108 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。	109 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。	110 ページの『ドメイン名サービスの構成』

表 28. 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 (続き)

作業	関連情報の入手先
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。	120 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 29. 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。	90 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。	105 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。	107 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。	120 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 30. 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。	90 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。	105 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。	106 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。	106 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。	107 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。	108 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。	109 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。	110 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。	

表 30. 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 (続き)

作業	関連情報の入手先
5. 管理対象サーバーと HMC との間の接続をテストします。	120 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 31. 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。	90 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。	105 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。	106 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。	106 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。	107 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。	108 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。	109 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。	110 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。	110 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、以下のようになります。

表 32. 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。	90 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。	113 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』 116 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。	117 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。	117 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。	117 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 33. 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、106 ページの『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。

HMC アダプター設定のデフォルトは、「自動検出 (**Autodetection**)」です。このアダプターが LAN スイッチに接続されている場合は、スイッチのポート設定を一致させる必要があります。メディア速度および二重モードを設定するには、以下のステップを実行します。

1. ナビゲーション領域で「**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. 「了解」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. 「了解」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. 「了解」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、106 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、81 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. 「了解」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「了解」をクリックします。
8. 「了解」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、「了解」をクリックします。

「了解」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なります。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. 「了解」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「了解」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. 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. 「経路指定」タブをクリックします。

4. 「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。
5. 「了解」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。

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・サフィックスの検索順序の指定が含まれます。

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変更」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. 「**DNS** 使用可能」を選択して DNS を使用可能にします。
5. DNS サーバーおよびドメイン・サフィックス・検索・オーダーを指定して、「追加」をクリックします。
6. 「了解」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」をクリックする。
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、102 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 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 の構成**」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 (例えば、Microsoft Active Directory、Tivoli®、および Open LDAP)。
5. 認証済みユーザーの識別に使用される 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。Microsoft Active Directory の場合は、属性として「**sAMAccountName**」を使用します。
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. 「**了解**」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、102 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、以下のようになります。

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、以下のようになります。
 - 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. 「**了解**」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. 「了解」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. 「了解」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、89 ページの『HMC 構成の準備』を参照してください。
- プロキシ・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・サーバーの IP アドレスとポート
 - プロキシ認証情報
- **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、79 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、「サービス管理」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:

LAN 接続を使用してエラーをコール・ホーム機能で報告できるようにこの HMC を構成します。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、89 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・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・サーバーの IP アドレスとポート
 - プロキシ認証情報
- 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、81 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**)」ページを選択します。

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 プロキシを使おうとしている場合、「**SSL プロキシの使用 (Use SSL proxy)**」ボックスにチェック・マークを付けます。
9. SSL プロキシを使おうとしている場合、プロキシ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**)」ページで、「テスト」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、「了解」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。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、89 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. 「了解」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」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、「了解」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。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、89 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、79 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」タブをクリックします。
7. 「インターネット VPN」ページで、「VPN と既存のインターネット接続をサービス用に許可する (**and an existing Internet connections for service**)」を選択します。
8. 「インターネット VPN」ページで、「テスト」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」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」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、「了解」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、以下のようになります。

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. 「検出されたコール・ホーム・サーバーの使用 (**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. 「了解」をクリックします。

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、「了解」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. 「自動問題レポート機能のテスト」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、「閉じる」を選択します。
9. 「閉じる」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 90 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、以下のようになります。

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」を選択します。
3. IBM ID を入力します。
4. 「了解」をクリックします。

サービス情報の送信:

サービス情報を送信し、その情報が問題判別に使用できるようにします。

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、『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 を取り付け、使用できるように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、以下の手順を実行します。

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」をクリックします。
3. 以下のいずれかのタブをクリックします。
 - 「送信 (Transmit)」。このページを使用して、サービス・プロバイダーにサービス・データを送信するタイミング (頻度 (日単位) および時刻を指定)、およびサービス情報およびパフォーマンス管理情報の送信方法をスケジュールします。
 - 「FTP」。このページを使用して、FTP サーバーのファイル転送プロトコル (FTP) 情報を、サービス情報のオフロード用に、ファイアウォールありまたはなしで構成します。このサービス情報は拡張エラー・データであり、ハードウェア管理コンソール (HMC) 上で開かれた HMC または管理対象システムの問題に関する問題関連データで構成されています。
 - 「サービス・データの IBM への送信 (Transmit Service Data to IBM)」。このページを使用すると、HMC ハード・ディスクに保管されている問題判別に使用できる情報を送信できます。データは、トレース、ログ、またはダンプの場合があり、データの宛先として、IBM サービス・サポート・システム、ディスクレット、USB フラッシュ・メモリー・ドライブ、または DVD-RAM が考えられます。情報を IBM サービス・サポート・システムに送信するには、事前に電話サーバーおよびリモート・サービスが使用可能になっていることが必要です。
4. 「サービス情報の送信」ウィンドウのタスクを完了し、「了解」をクリックします。

「コール・ホーム用イベント・マネージャー」の構成:

「コール・ホーム用イベント・マネージャー」タスクの構成方法について説明します。このタスクにより、HMC から IBM に転送されるすべてのデータをモニターおよび承認することができます。

「コール・ホーム用イベント・マネージャー」モードの有効化または無効化は、HMC コマンド行インターフェースを使用して設定できます。「コール・ホーム用イベント・マネージャー」タスクが使用可能に設定されると、HMC は、イベントが発生したときに自動的にそれらをコール・ホームすることができません。承認なしでコール・ホームされるイベントを回避するには、この環境で稼働するすべての HMC で、「コール・ホーム用イベント・マネージャー」が使用可能に設定されている必要があります。

「コール・ホーム用イベント・マネージャー」タスクを使用可能または使用不可に設定するには、以下のコマンドを実行してください。

```
chhmc -c emch
```

```
-s {enable | disable}
```

```
[--callhome {enable | disable}]
```

```
[--help]
```

注: 「コール・ホーム用イベント・マネージャー」タスクが使用可能にされると、コール・ホーム・イベントは、コール・ホーム・タスクに対して承認されるまで保持されます。「コール・ホーム用イベント・マネージャー」タスクを使用不可にした場合、コール・ホーム機能が自動的に使用可能になることはありません。このセットアップにより、意図せずにデータが IBM にコール・ホームされることが回避されます。以下のコマンド・オプションから選択して、必要な構成をセットアップします。

- 「コール・ホーム用イベント・マネージャー」タスクを使用可能にする場合: **chhmc -c emch -s enable**
- 「コール・ホーム用イベント・マネージャー」タスクを使用可能にし、自動的コール・ホームを再度使用可能にする場合: **chhmc -c emch -s disable --callhome enable**

- 「コール・ホーム用イベント・マネージャー」タスクを使用不可にし、自動的コール・ホームを再度使用可能にしない場合: `chhmc -c emch -s disable --callhome disable`

HMC が、この環境に配置されている他の HMC と通信できることを確認してください。「コール・ホーム用イベント・マネージャー」には、HMC の登録時のテスト接続機能が備わっています。

HMC を「コール・ホーム用イベント・マネージャー」に登録することができます。HMC を登録すると、イベント・マネージャーは、その登録された HMC に、IBM にコール・ホームされるのを待機しているイベントがないか照会します。イベント・マネージャーは、どのようなデータが IBM に送り戻されようとしているのかを示し、それらのイベントを承認します。イベント・マネージャーは、承認後、コール・ホーム操作を続行できることを、登録済み HMC に通知します。

「コール・ホーム用イベント・マネージャー」タスクは、いずれの HMC からでも、あるいは複数の HMC からでも実行することができます。管理コンソールを「コール・ホーム用イベント・マネージャー」タスクに登録するには、以下の手順を実行してください。

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、「コール・ホーム用イベント・マネージャー」を選択します。
3. 「コール・ホーム用イベント・マネージャー」ウィンドウから、「コンソールの管理」をクリックします。
4. 「登録済みコンソールの管理 (Manage Registered Consoles)」ウィンドウから、「コンソールの追加 (Add Console)」をクリックして、管理コンソールを「コール・ホーム用イベント・マネージャー」タスクに登録します。
5. 「了解」をクリックして、登録済み管理コンソールのリストへの変更をコミットします。

注: 「コール・ホーム用イベント・マネージャー」は、イベント・マネージャー・モードが使用不可に設定された状態で使用できます。引き続き、HMC を登録し、イベント・マネージャーでイベントを表示することはできますが、イベント・マネージャーは、イベントがいつコール・ホームされるかを制御しません。

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 IP アドレスの選択 (Select a Service Processor IP Address)」を選択して、「了解」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。詳しくは、論理区画化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、79 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、99 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) にマウントされたりリモート・システム
- FTP を介したりリモート・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、マウントされたりリモート・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ます、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、105 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ます。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、120 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、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、120 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。

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」を選択します。
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. 「了解」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、以下のようになります:

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. 「了解」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. 「スケジュール操作」ウィンドウを閉じる
 - d. スケジュール操作ごとに繰り返す。
6. 「スケジュール操作のカスタマイズ」ウィンドウを閉じる。
7. 129 ページの『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. 「了解」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. 「了解」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。

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。
 - img2a
 - img3a
 - base.img
 - disk1.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 Enhanced+ インターフェースを使用した HMC の構成

HMC Enhanced+インターフェースを使用した、ネットワーク接続のセットアップ、HMC の構成、構成完了後の手順の実行、および HMC のアップグレードと更新の方法について説明します。

注: HMC バージョン 8.20 にオプションで付属していた HMC Enhanced + Tech Preview (Pre-GA) インターフェースの手順および機能は、HMC バージョン 8.30 に付属の HMC Enhanced+ インターフェースと同じです。資料で言及しているのは HMC Enhanced+ についてのみですが、内容は HMC Enhanced + Tech Preview (Pre-GA) インターフェースにも当てはまります。

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、98 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）を収集したり、特定のプラットフォーム活動（動的 LPAR、並行修復）をそれらのオペレーティング・システムに合わせ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 BMC へ

注: ベースボード管理コントローラー (BMC) 接続は、HMC モデル 7063-CR1 にのみ該当します。

保守作業の実行に使用されます。BMC 接続は、システム上に HMC ファームウェアをロードして維持するために使用されます。この接続は、HMC 上の BMC にアクセスするのに必要です。

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。

- Web ブラウザーを使用して、リモートですべての HMC GUI 機能にアクセスする。
- 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・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。

- 1 つ以上のネットワーク・インターフェースを HMC と管理対象システム間の通信に独占的に使用できます。つまり、そのネットワーク上に存在するのは、HMC および管理対象システムのサービス・プロセッサのみであることを意味します。サービス・プロセッサへのネットワーク・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) バージョン 8.7.0 は、Google Chrome バージョン 57、Microsoft Internet Explorer (IE) バージョン 11.0、Mozilla Firefox バージョン 45 ならびに 52 の Extended Support Release (ESR)、および Safari バージョン 10.1 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。

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・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. 「了解」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、「Options」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. 「了解」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。

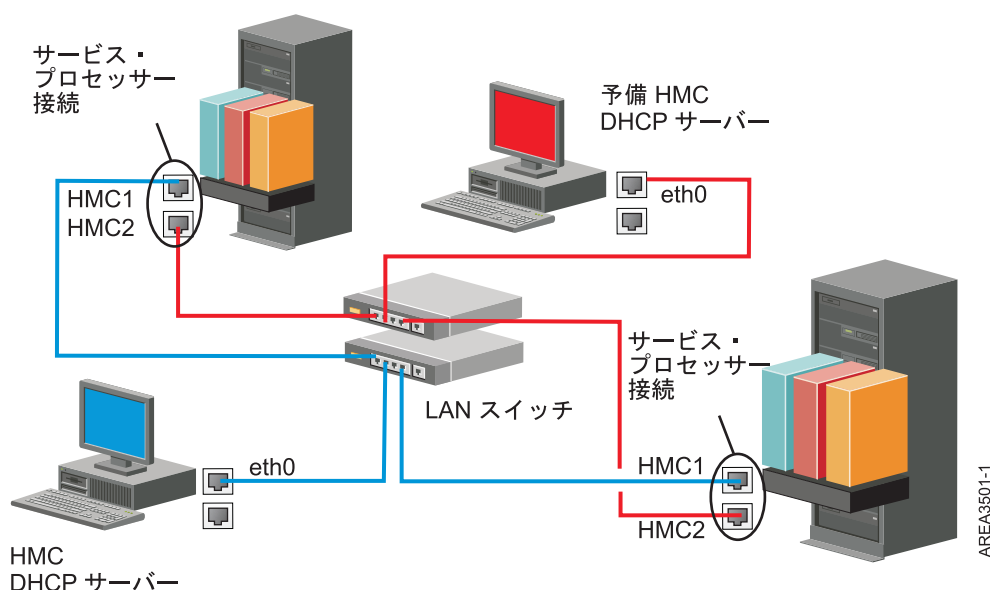
HMC 自身は、自分自身のファイアウォールをその各ネットワーク・インターフェース上で提供します。「HMC ガイド付きセットアップ・ウィザード」の実行時に基本的なファイアウォールが自動的に構成されますが、初期の HMC 取り付けと構成の完了後にファイアウォール設定をカスタマイズする必要があります。

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。

HMC を DHCP サーバーとして構成する方法については、107 ページの『DHCP サーバーとしての HMC の構成』を参照してください。

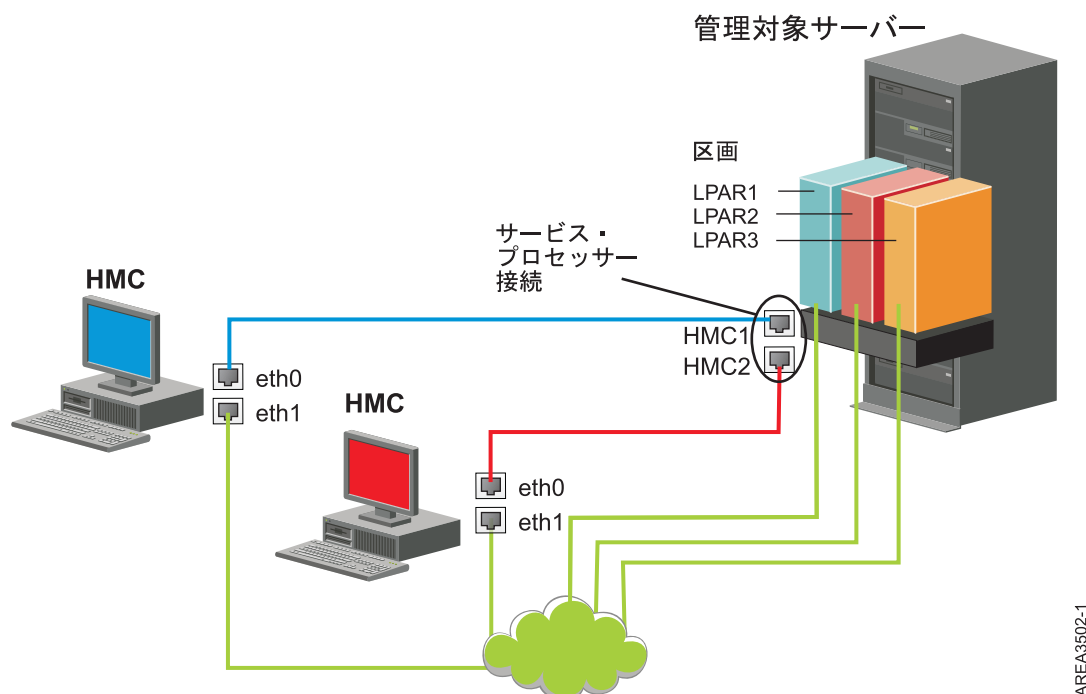


この図には、2 つの管理対象システムに接続する冗長 HMC 環境を記載してあります。最初の HMC は、各 FSP 上の最初のポートに接続され、冗長 HMC は各 HMC 上の 2 番目のポートに接続されています。各 HMC は DHCP サーバーとして構成され、異なる範囲の IP アドレスを使用しています。各接続は独立したプライベート・ネットワーク上にあります。このように、どの FSP ポートも 2 台以上の HMC に接続されていないようにすることが重要です。

ある HMC に接続される各管理対象システムの FSP ポートには、ユニークな IP アドレスが必要です。各 FSP が固有の IP アドレスを持つようにするには、HMC の組み込み DHCP サーバー機能を使用します。この FSP がアクティブなネットワーク・リンクを検出すると、FSP はブロードキャスト要求を発行して DHCP サーバーを見つけます。正しく構成されていると、HMC は、選択された範囲のアドレスのいずれかを割り当てて、その要求に応答します。

FSP が複数存在する場合、HMC と FSP 間のプライベート・ネットワーク用に、ユーザー独自の LAN スイッチまたはハブを持っている必要があります。または、このプライベート・セグメントは、より大きな管理されたスイッチ上のプライベート仮想 LAN (VLAN) 内で、複数ポートとして存在することができます。複数のプライベート VLAN がある場合、その VLAN が分離されていること、およびその VLAN を縦断するトラフィックが存在しないことを確認する必要があります。

複数の HMC がある場合、各 HMC を論理区画に、およびお互いに、同一オープン・ネットワーク上で接続する必要もあります。



この図には、プライベート・ネットワーク上で単一の管理対象サーバーに接続され、さらにパブリック・ネットワーク上で 3 つの論理区画に接続された 2 つの HMC が記載されています。この HMC 用に追加のイーサネット・アダプターを保有して、3 つのネットワーク・インターフェースを保有可能です。この 3 番目のネットワークを管理ネットワークとして使用するか、または CSM (クラスター・システム・マネージャー) の管理サーバーにこれを接続できます。

HMC を DHCP サーバーとして構成する方法については、107 ページの『DHCP サーバーとしての HMC の構成』を参照してください。

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。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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・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、86 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。

- 伝送速度の高速化
- 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。

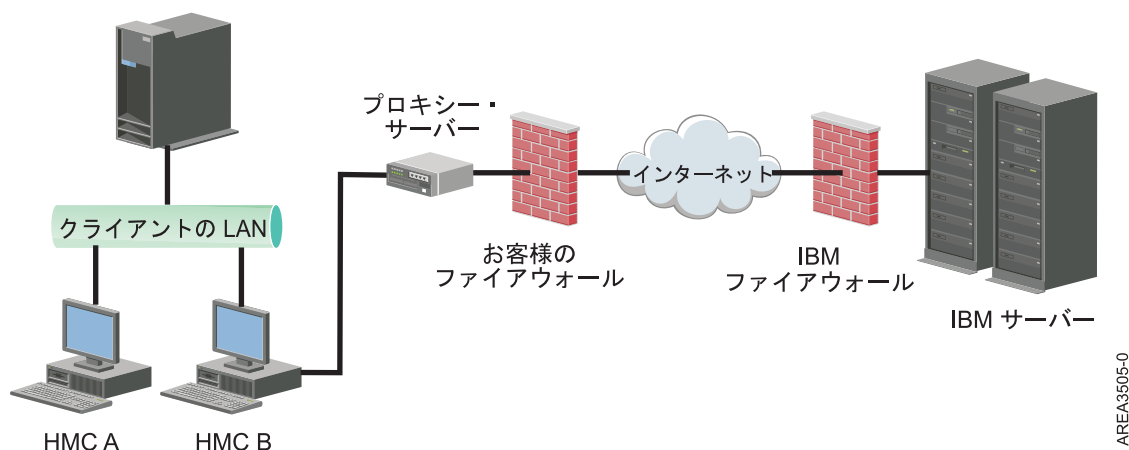
- リモート・サポート機能の要求は、常に、HMC から開始されて IBM に送信されます。インバウンド接続が、IBM Service Support System から開始されることは決してありません。
- HMC と IBM Service Support System 間で転送される全データは、高度な暗号化機能を使用して暗号化されています。データは、選択した接続方式に応じて、SSL または IPSec Encapsulating Security Payload (ESP) のいずれかを使用して暗号化されます。
- 暗号化された接続の開始時に、HMC はターゲットとなる宛先を IBM Service 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・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 プロキシを使用した場合に考えられる他の利点の 1 つは、プロキシによりロギング機能および監査機能をサポートできることです。

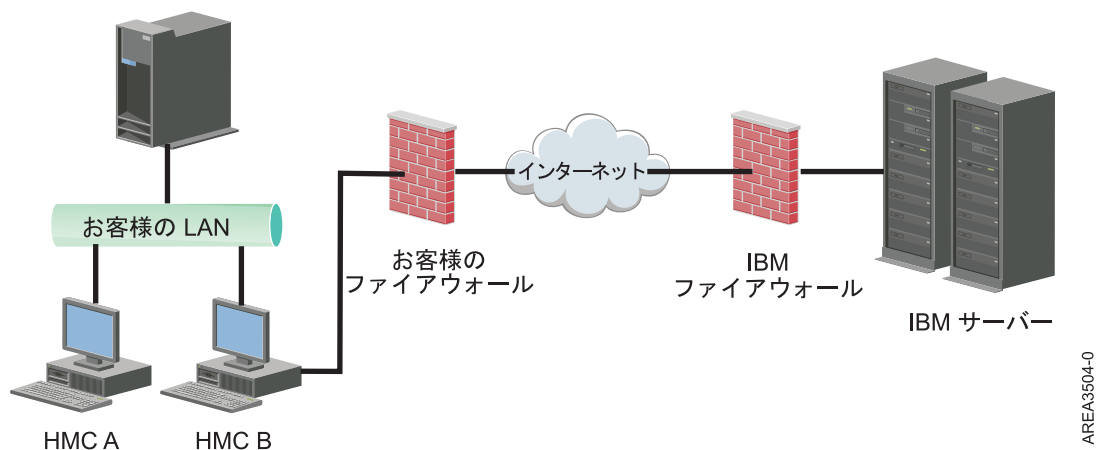
SSL ソケットをフォワードするには、そのプロキシ・サーバーは基本プロキシ・ヘッダー機能 (RFC 2616 に記載あり) と CONNECT メソッドをサポートする必要があります。オプションとして、基本プロキシ認証 (RFC 2617) を、プロキシ・サーバー経由でソケットを転送しようとする前に HMC が認証するように構成することができます。



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・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・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、86 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 86 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 (86 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・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、107 ページの『IPv4 アドレスの設定』および 108 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
- 129.42.42.224
- 129.42.50.224
- 129.42.56.216
- 129.42.58.216
- 129.42.60.216
- 170.225.15.41

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
- 207.25.252.197
- 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
- 207.25.252.197
- 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。

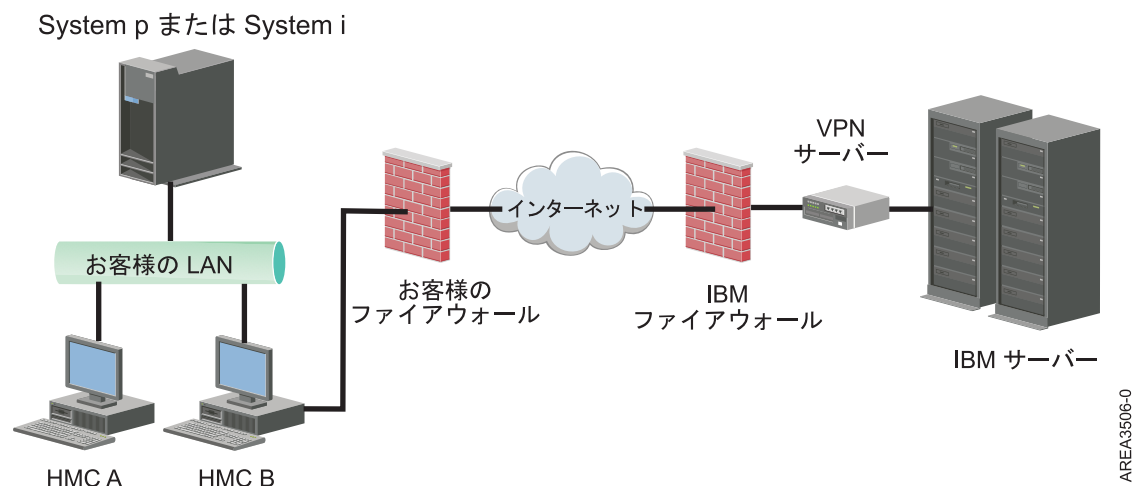
- 2620:0:6C0:1::1000
- 2620:0:6C2:1::1000
- 2620:0:6C4:1::1000

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。

注: この接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、88 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、102 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。

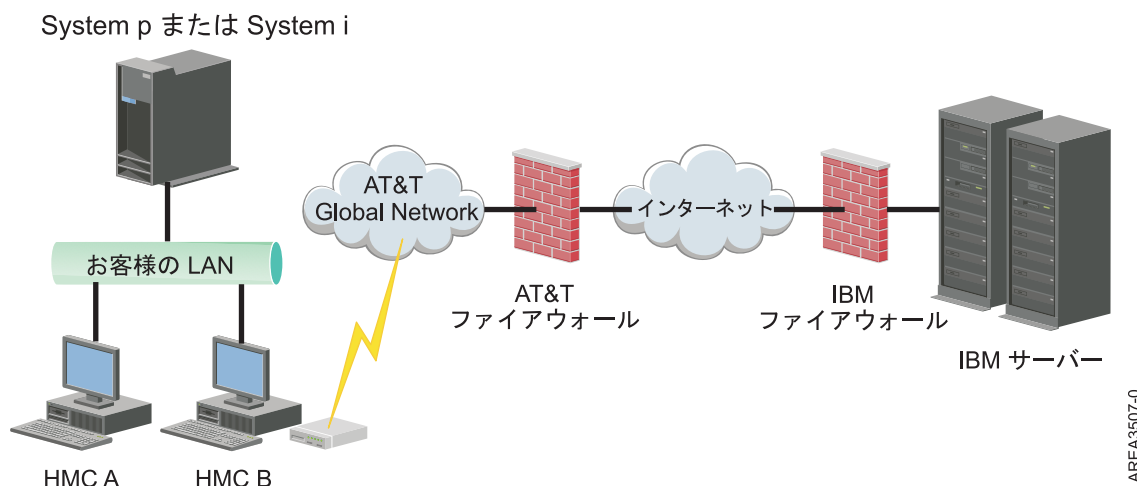
インターネット VPN 接続を使うように HMC を構成すると、HMC は以下のサーバーを使用します。ネットワーク・アドレス変換 (NAT) ファイアウォールを使うとする時に、すべての接続が ESP、およびポート 500 とポート 4500 上の UDP を使用します。

- 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。

注: この接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。



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、102 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。

HMC を構成するためには、関連する概念を理解し、決定し、情報を準備する必要があります。

このセクションでは、ご使用の HMC を以下のものに接続するために必要な情報について説明します。

- 管理対象システム内のサービス・プロセッサ
- 管理対象システム上の論理区画
- リモート・ワークステーション
- IBM Service (「コール・ホーム」機能をインプリメントする)

注: 追加の接続およびセキュリティ情報が使用可能です。詳しくは、「**ESA for HMC Connectivity Security for IBM POWER6, POWER7 and POWER8 Processor-Based Systems and IBM Storage Systems DS8000**」ホワイト・ペーパーを参照してください。これは、以下で入手できます。IBM Electronic Service Agent (<http://www-01.ibm.com/support/esa/security.htm>)。

HMC 構成を準備するには、以下の手順を実行します。

1. インストールする HMC コードの最新レベルのバージョンを取得してインストールします。
2. HMC が管理するサーバーとの関連で、HMC の物理的な位置を決定します。HMC とその管理対象システムとの間の距離が 7.62 m を超える場合は、サービス担当員が HMC にアクセスできるように、管理対象システムの位置から HMC に Web ブラウザーによるアクセスができる必要があります。
3. HMC が管理するサーバーを識別します。
4. サーバーの管理にプライベート・ネットワークまたはオープン・ネットワークを使用するかどうかを決定します。プライベート・ネットワークを使用することに決めた場合は、Cluster Systems Management (CSM) 構成を使用しない限り、DHCP を使用します。CSM は IPv6 をサポートしません。CSM にアクセスするには、2 つのネットワークを持つ必要があります。CSM の詳細については、該当のフィーチャーに付属の資料を参照してください。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、81 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。
5. オープン・ネットワークを使用して FSP を管理する場合は、Advanced System Management Interface メニューを使用して FSP のアドレスを手動で設定する必要があります。プライベートのルーティング不可能なネットワークをお勧めします。
6. 2 台の HMC がある場合は、プライマリー HMC とセカンダリー HMC を指定します。プライマリー HMC は、物理的にこのマシンに近くて、しかもコール・ホームに構成された HMC にする必要があります。
7. HMC をリモート・ワークステーション、論理区画、およびネットワーク・デバイスに接続するために必要なネットワーク設定を決定します。
8. HMC が「コール・ホーム」する方法を定義します。コール・ホーム・オプションには、アウトバウンドのみの Secure Sockets Layer (SSL) インターネット接続、モデム、または仮想プライベート・ネットワーク (VPN) 接続のいずれかの使用が含まれます。
9. 作成する HMC ユーザーおよびそのパスワード、ならびに付与するロールを決定します。hscroot および hscpe ユーザーにパスワードを割り当てる必要があります。
10. コール・ホームの構成時に必要となる以下の会社連絡先情報を記録します。
 - 会社名

- 管理者の連絡先
 - 電子メール・アドレス
 - 電話番号
 - FAX 番号
 - HMC の物理的な所在地住所
11. コール・ホームを介して IBM サービスに情報が送信された時の、オペレーターまたはシステム管理者への通知に電子メールを使用する計画がある場合は、Simple Mail Transfer Protocol (SMTP) サーバーおよび使用する電子メール・アドレスを確認します。
 12. 以下のパスワードを定義する必要があります。
 - FSP に対して HMC を認証するために使用されるアクセス・パスワード
 - 「管理者」ユーザーに使用される ASMI パスワード
 - 「一般」ユーザーに使用される ASMI パスワード

HMC から新規サーバーに最初に接続するときのパスワードを作成します。HMC が予備または 2 番目の HMC である場合は、HMC ユーザー・パスワードを取得して、管理対象サーバーの FSP に初めて接続するときにそのパスワードを入力する準備を整えます。

この準備ステップが完了したら、90 ページの『HMC 用のプリインストール構成ワークシート』に進みます。

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、79 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。

表 34. イーサネット・アダプターのスピードと二重モード

	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、81 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。

表 35. プライベート・ネットワークとオープン・ネットワーク

	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。

表 36. プライベート・ネットワーク

	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)		
「はい」の場合、使用する IP アドレスの範囲を記録します。		

7063-CR1 HMC を使用している場合、HMC 上のベースボード管理コントローラー (BMC) にアクセスするためにイーサネット IPMI ポートをネットワークに接続する必要があります。詳しくは、159 ページの『BMC 接続の構成』を参照してください。ご使用の BMC 接続について以下の表を記入します。

表 37. BMC 接続

	IPMI
この接続は DHCP モードを使用して構成しますか? (はい/いいえ)	
「いいえ」の場合、以下の指定された静的アドレスをリストしてください。	
IP アドレス:	
サブネット・マスク:	
ゲートウェイ:	

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、86 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。

表 38. IPv6 の使用

	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。				

表 39. IPv6 の使用

	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)				

表 40. IPv6 の使用

	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 108 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、108 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。

表 41. IPv4 の使用

	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:				
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。				

表 41. IPv4 の使用 (続き)

	eth0	eth1	eth2	eth3

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・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。

表 42. ローカル・ホスト情報

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)	
「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です。

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です。

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。

表 43. 電子メール通知

フィールド	
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

表 44. サービス連絡先情報

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 (セキュリティ特性と構成要件を含む) は、83 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。

表 45. 接続のタイプ

接続のタイプ	
	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 プロキシの使用 (Use SSL Proxy)**」を選択します。

表 46. インターネット経由の Secure Sockets Layer (SSL)

インターネット経由の Secure Sockets Layer (SSL)	
SSL プロキシの使用 ? (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、86 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。

表 47. ローカル HMC からのダイヤルアップ

フィールド	
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、88 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 48. 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

表 49. サポート上のさらなる利点

フィールド	
IBM ID のリスト	
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 エレクトロニック・サービス・エージェント 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の構成方法について説明します。

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、89 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、90 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 の始動、およびガイド付きセットアップ・ウィザードにある各ステップを完了:

HMC インターフェースにログインし、ガイド付きセットアップ・ウィザードを使用して HMC を構成します。

注: これが新規インストールの場合は、管理対象システムが電源に接続されていないことを確認します。ラック・マウント型 HMC では、主電源装置に接続する前に電源分配バス (PDB) に接続されている唯一のデバイスは HMC であることを意味します。これが同じ管理対象システムに接続された 2 番目の HMC である場合、この管理対象システムを電源に接続できます。

1. 電源ボタンを押して HMC をオンにします。
2. HMC が、30 秒後に自動的にデフォルトの言語とロケール設定を選択するのを待ちます。
3. ハードウェア管理コンソールのご使用条件に同意します。ハードウェア管理コンソールのご使用条件に同意しない場合は、HMC の構成を完了することはできません。
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. HMC に以下のようにしてログインします。

注: システム管理者 (**hmcadmin**) がパスワードを変更した場合は、そのパスワードをここで入力してください。

- ID: hscroot
- パスワード: abc123

ガイド付きセットアップ・ウィザードが開きます。

6. ガイド付きセットアップのエントリー・ウィンドウで、「了解」をクリックします。

注: HMC の始動時にガイド付きセットアップ・ウィザードが表示されなかった場合は、HMC ウェルカム・ページのナビゲーション領域の「ガイド付きセットアップ・ウィザード」をクリックします。

7. 記入済みのプリインストール構成ワークシートを使用して、ガイド付きセットアップ・ウィザードにある各ステップを完了します。「はい」をクリックして、「接続およびコール・ホーム・サーバー」ウィザードの各ステップを続行して完了します。
8. 「要約」ウィンドウで、「完了」をクリックします。
9. イーサネット・クロスケーブルを管理対象システムに接続していない場合は、この時点で接続します。
10. HMC ナビゲーション領域で、「サービス管理」をクリックします。
11. コンテンツ領域で、「ユーザーの許可」をクリックします。「ユーザーの許可」ウィンドウが開きます。
12. フィールドに IBM ID を入力し、「了解」をクリックします。

構成の確認:

「状況」ウィンドウで、選択したさまざまな構成設定の進行情況をモニターします。このウィンドウでは、いくつかのタスクについて数分間、保留の状況を表示することもあります。「ログの表示」をクリックして、各タスクに関連する状況メッセージを調べます。いつでも、「閉じる」をクリックすると、ガイド付きセットアップ・ウィザードが終了します。実行中のタスクは、そのまま実行を継続します。これで HMC が構成されました。

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。

この情報には、PDF に収録されていないタスクの参照も含まれています。HMC ウェルカム・ページの「**Additional Resources (追加のリソース)**」セクションを参照して、追加のサポート資料にアクセスできます。

前提条件

HMC メニューを使用した HMC の構成を始める前に、89 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。

表 50. 人手による HMC 構成タスクおよび関連情報の入手先

作業	関連情報の入手先
1. HMC を開始します。	101 ページの『HMC の始動』
2. 日時を設定します。	
3. 事前定義済みのパスワードを変更します。	
4. 追加のユーザーを作成して、そのステップを終了したら、このチェックリストに戻ります。	
5. ネットワーク接続を構成します。	102 ページの『HMC ネットワーク・タイプの構成』
6. オープン・ネットワークおよび固定 IP アドレスを使用する場合は、識別情報を設定します。	

表 50. 人手による HMC 構成タスクおよび関連情報の入手先 (続き)

作業	関連情報の入手先
7. オープン・ネットワークおよび固定 IP アドレスを使用する場合は、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します。	109 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』
8. オープン・ネットワークおよび固定 IP アドレスを使用する場合は、ドメイン名サービスを構成します。	110 ページの『ドメイン名サービスの構成』
9. 固定 IP アドレスを使用しており、DNS が使用可能である場合は、ドメイン・サフィックスを構成します。	110 ページの『ドメイン・サフィックスの構成』
10. ご使用のサーバーを IBM サービスおよびサポートに接続するように構成し、そのステップを終了したらこのチェックリストに戻ります。	112 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』
11. 「コール・ホーム用イベント・マネージャー」を構成します。	118 ページの『「コール・ホーム用イベント・マネージャー」の構成』
12. 管理対象システムに電源を接続します。	
13. 管理対象システムのパスワード、および各 ASMI パスワード (一般および管理者) を設定します。	119 ページの『管理対象システムに対するパスワードの設定』
14. 管理対象システムの日時を設定するために ASMI にアクセスします。	
15. 管理対象システムを始動して、そのステップを終了したら、このチェックリストに戻ります。	
16. 管理対象システムに論理区画が 1 つあることを確認します。	
17. オプション: 別の管理対象システムを追加して、そのステップを終了したら、このチェックリストに戻ります。	
18. オプション: 新しいサーバーを HMC とともに取り付ける場合は、論理区画を構成して、オペレーティング・システムをインストールします。	
19. この時点で新しいサーバーをインストールしない場合は、ご使用の構成をさらにカスタマイズするために、構成完了後のオプション・タスクを実行します。	120 ページの『構成完了後のステップ』

HMC の始動:

ハードウェア管理コンソール (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 を開始するには、以下の手順を実行します。

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. 以下のデフォルトのユーザー ID とパスワードを使用して、HMC にログインします。

ユーザー名: hscroot

パスワード: abc123

ログイン・ページで、システム、区画、および仮想入出力サーバーの状況を確認できます。また、アテンション LED およびサービス可能イベントの数も確認できます。ログイン・ページから、各種のソーシャル・メディアおよび IBM developerWorks® のリンクをクリックすることにより、HMC および使用可能なフィーチャーの詳細を知ることができます。

注: HMC バージョン 8.6.0.1 では、以下のログイン・オプションから選択できます。

ログイン: HMC Classicまたは HMC Enhanced+

HMC Enhanced+ インターフェースを選択して先へ進みます。HMC Classic インターフェースでは、HMC の従来の機能すべてにアクセスすることができ、HMC Enhanced+ インターフェースでは、システム、区画、および仮想入出力サーバーのグラフィカル・ビューと簡略ナビゲーションが提供されます。

HMC Classic

拡張 PowerVM 機能を備えていない、標準 GUI を表示します。

HMC Enhanced+

システム、区画、および仮想入出力サーバーのグラフィカル・ビューと簡略ナビゲーション付きの、直観的インターフェース作業環境を提供する完全に再設計された HMC 管理インターフェースの新しいビューを表示します。

注: HMC は、DHCP サーバーとして機能している場合、最初にサービス・プロセッサに接続する際に、デフォルトのパスワードを使用します。

5. 「サインイン」をクリックします。

日時の変更:

バッテリー作動時刻機構で 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、以下の手順を実行します。

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」アイコン をクリックしてから、「コンソール設定」を選択します。
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 51. 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。	90 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。	105 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。	106 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。	106 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。	107 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。	108 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。	109 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。	110 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。	120 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 52. 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。	90 ページの『HMC 用のプリインストール構成ワークシート』

表 52. 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。	105 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。	107 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。	120 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 53. 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。	90 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。	105 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。	106 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。	106 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。	107 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。	108 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。	109 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。	110 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。	120 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 54. 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。	90 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。	105 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。	106 ページの『メディア速度の設定』

表 54. 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。	106 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。	107 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。	108 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。	109 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。	110 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。	110 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、以下のようになります。

表 55. 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。	90 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。	113 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』 116 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。	117 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。	117 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。	117 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 56. 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 <code>eth0</code> 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 <code>eth1</code> として定義され、2 次内蔵イーサネット・ポートは <code>eth2</code> 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 <code>eth0</code> となります。Act/link B のラベルが付いたポートは <code>eth1</code> となります。この場合、1 次内蔵イーサネット・ポートは <code>eth2</code> として定義され、2 次内蔵イーサネット・ポートは <code>eth3</code> 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 <code>eth0</code> 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 <code>eth0</code> 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 <code>eth0</code> となります。Act/link B のラベルが付いたポートは <code>eth1</code> となります。この場合は、1 次内蔵イーサネット・ポートが <code>eth2</code> 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 <code>eth0</code> 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、106 ページの『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。

- 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。
- 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。

HMC アダプター設定のデフォルトは、「自動検出 (**Autodetection**)」です。このアダプターが LAN スイッチに接続されている場合は、スイッチのポート設定を一致させる必要があります。メディア速度および二重モードを設定するには、以下の手順を実行します。



1. ナビゲーション領域で、「**HMC 管理**」アイコンをクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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. 「了解」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**」アイコンをクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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. 「了解」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**」アイコンをクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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. 「了解」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、106 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、81 ページの『DHCP サーバーとしての HMC』を参照してください。

BMC 接続の構成:

管理コンソール用の BMC 上のネットワーク設定を構成したり表示したりすることができます。

注: このタスクは、7063-CR1 にのみ該当します。この接続は、HMC 上のベースボード管理コントローラー (BMC) にアクセスするために必要です。

BMC 接続を構成するには、以下の手順を実行します。



1. ナビゲーション領域で、「**HMC 管理**」アイコンをクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「**BMC/IPMI** ネットワーク設定の変更 (**Change BMC/IPMI network settings**)」をクリックします。

3. 接続モード（「**DHCP**」 または 「静的」）を選択します。

「静的」モードを選択した場合は、以下のアドレスを記入してください。

- **IP アドレス (IP address)**
- サブネット・マスク
- ゲートウェイ

4. 「了解」をクリックします。

BMC ネットワーク接続の構成は、Petitboot ブート・ローダー・インターフェースを使用して行うこともできます。詳しくは、ファームウェア IP アドレスの構成 (Configuring the firmware IP address)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**」アイコン をクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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. 「了解」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**」アイコン をクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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「了解」をクリックします。
8. 「了解」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**」アイコンをクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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、「了解」をクリックします。

「了解」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**」アイコンをクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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なります。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. 「了解」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「了解」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. ナビゲーション領域で、「**HMC 管理**」アイコン  をクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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. 「経路指定」タブをクリックします。
4. 「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。
5. 「了解」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。

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・サフィックスの検索順序の指定が含まれます。



1. ナビゲーション領域で、「**HMC 管理**」アイコン をクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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。
3. 「ネーム・サービス」タブをクリックします。
4. 「**DNS 使用可能**」を選択して DNS を使用可能にします。
5. DNS サーバーおよびドメイン・サフィックス・検索・オーダーを指定して、「追加」をクリックします。
6. 「了解」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**」アイコン をクリックしてから、「コンソール設定」を選択します。
2. 「コンテンツ」ペインで、「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:

ご使用のハードウェア管理コンソール (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、102 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 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、「ユーザーおよびセキュリティー」アイコンをクリックしてから、「システムおよびコンソール・セキュリティー」を選択します。
2. コンテンツ・ペインで、「LDAP の管理 (**Manage LDAP**)」を選択します。「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. 「了解」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、102 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、以下のようになります。

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、以下のようになります。
 - a. ナビゲーション領域で、「HMC 管理」アイコン  をクリックしてから、「コンソール設定」を選択します。
 - b. コンテンツ・ペインで、「日付と時刻の変更」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. 「了解」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、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「システムおよびコンソール・セキュリティ」を選択します。
- b. コンテンツ・ペインで、「**KDC の管理 (Manage KDC)**」を選択する。
- 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. 「了解」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、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「システムおよびコンソール・セキュリティ」を選択します。
- b. コンテンツ・ペインで、「**KDC の管理 (Manage KDC)**」を選択する。
- 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. 「了解」をクリックします。

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:

LAN 接続を使用してエラーをコール・ホーム機能で報告できるようにこの **HMC** を構成します。

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、89 ページの『**HMC** 構成の準備』を参照してください。

- プロキシ・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・サーバーの IP アドレスとポート
 - プロキシ認証情報
- **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、79 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、「保守容易」アイコン をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「コール・ホーム・セットアップ・ウィザード (**Call-Home Setup Wizard**)」をクリックします。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:

LAN 接続を使用してエラーをコール・ホーム機能で報告できるようにこの HMC を構成します。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、89 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、「保守容易性」 > 「サービス管理」 > 「カスタマー情報の管理」をクリックします。
- プロキシ・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・サーバーの IP アドレスとポート
 - プロキシ認証情報
- 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、81 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、「保守容易」アイコン をクリックしてから、「サービス管理」を選択します。
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**)」ページを選択します。
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 プロキシを使おうとしている場合、「**SSL プロキシの使用 (Use SSL proxy)**」ボックスにチェック・マークを付けます。
9. SSL プロキシを使おうとしている場合、プロキシ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**)」ページで、「テスト」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、「了解」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。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、89 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、「保守容易性」 > 「サービス管理」 > 「カスタマー情報の管理」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、「保守容易」アイコン  をクリックしてから、「サービス管理」を選択します。
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. 「了解」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」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、「了解」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。

注: インターネット仮想プライベート・ネットワーク (VPN) 接続タイプおよびダイヤルアップ接続タイプは、HMC バージョン 8.2.0 以前でのみ使用可能です。

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、89 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、79 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「保守容易性」 > 「サービス管理」 > 「カスタマー情報の管理」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、「保守容易」アイコン  をクリックしてから、「サービス管理」を選択します。
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」タブをクリックします。
7. 「インターネット VPN」ページで、「VPN および既存のインターネット接続でのサービスを許可する」を選択します。
8. 「インターネット VPN」ページで、「テスト」チェック・ボックスを選択します。
9. 「インターネット VPN のテスト」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」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、「了解」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、以下のようになります。



1. ナビゲーション領域で、「保守容易」アイコン をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「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. 「検出されたコール・ホーム・サーバーの使用 (**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. 「了解」をクリックします。

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、「了解」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、「保守容易」アイコン をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「イベントの作成 (**Create Event**)」をクリックします。
3. 「自動問題レポート機能のテスト」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て、「閉じる」をクリックします。
9. 「閉じる」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 90 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、以下のようになります。



1. ナビゲーション領域で、「保守容易」アイコン をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「ユーザーの許可」を選択します。
3. IBM ID を入力します。
4. 「了解」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、117 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 を取り付け、使用できるように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、以下のようになります。



1. ナビゲーション領域で、「保守容易」アイコン をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「サービス情報の送信」をクリックします。
3. 「サービス情報の送信」ウィンドウのタスクを完了し、「了解」をクリックします。

サービス情報のスケジュール:

サービス情報を問題判別に使用できるように送信する時期をスケジュールします。

注: サービス・プロバイダー情報は、ハードウェア管理コンソール (HMC) を取り付け、使用できるように構成したら直ちに送信する必要があります。

サービス情報をスケジュールするには、以下の手順を実行します。



1. ナビゲーション領域で、保守容易性アイコン  をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「サービス情報のスケジュール」をクリックします。
3. コンテンツ・ペインで、「データのスケジュールおよび送信」タブをクリックしてサービス情報をスケジュールします。

注: 以下のタブをクリックして、送信したいデータの選択および FTP 接続の構成を行うこともできます。

- データのスケジュールおよび送信: 情報をサービス・プロバイダーに即時に送信するか、またはその送信をスケジュールします。
 - 問題レポートの送信: 必要なデータ、およびそのデータの宛先を選択します。
 - **FTP 接続の構成:** FTP を使用したサービス情報のオフロードを可能にするための構成データを指定します。
4. 定期的送信を有効化したいか、または即時に送信したいサービス情報のタイプを選択します。
 - 操作テスト (ハートビート) 情報 -- 常時有効: 問題イベント・ログ・ファイルを送信します。
 - ハードウェア・サービス情報 (**VPD**): この HMC に接続されているすべての管理対象システムの重要プロダクト・データ (**VPD**) を送信します。
 - ソフトウェア・サービス情報: 各区画で実行されているすべてのソフトウェアの **VPD** を送信します。
 - パフォーマンス管理情報: パフォーマンス管理情報を収集し、送信します。
 - 更新アクセス・キー情報: アクセス・キー情報を検証し、更新します。
 5. 反復送信をスケジュールするために、間隔 (日単位) と時刻を選択します。情報を即時に送信するためには、「即時送信」をクリックします。
 6. 「了解」をクリックします。

サービス情報のスケジュールについて、詳しくはオンライン・ヘルプを参照してください。

「コール・ホーム用イベント・マネージャー」の構成:

「コール・ホーム用イベント・マネージャー」タスクの構成方法について説明します。このタスクにより、HMC から IBM に転送されるすべてのデータをモニターおよび承認することができます。

「コール・ホーム用イベント・マネージャー」モードの有効化または無効化は、HMC コマンド行インターフェースを使用して設定できます。「コール・ホーム用イベント・マネージャー」タスクが使用可能に設定されると、HMC は、イベントが発生したときに自動的にそれらをコール・ホームすることができません。承認なしでコール・ホームされるイベントを回避するには、この環境で稼働するすべての HMC で、「コール・ホーム用イベント・マネージャー」が使用可能に設定されている必要があります。

「コール・ホーム用イベント・マネージャー」タスクを使用可能または使用不可に設定するには、以下のコマンドを実行してください。

```
chhmc -c emch
```

```
-s {enable | disable}
```

[--callhome {enable | disable}]

[--help]

注: 「コール・ホーム用イベント・マネージャー」タスクが使用可能にされると、コール・ホーム・イベントは、コール・ホーム・タスクに対して承認されるまで保持されます。「コール・ホーム用イベント・マネージャー」タスクを使用不可にした場合、コール・ホーム機能が自動的に使用可能になることはありません。このセットアップにより、意図せずにデータが IBM にコール・ホームされることが回避されます。以下のコマンド・オプションから選択して、必要な構成をセットアップします。

- 「コール・ホーム用イベント・マネージャー」タスクを使用可能にする場合: **chhmc -c emch -s enable**
- 「コール・ホーム用イベント・マネージャー」タスクを使用不可にし、自動コール・ホームを再度使用可能にする場合: **chhmc -c emch -s disable --callhome enable**
- 「コール・ホーム用イベント・マネージャー」タスクを使用不可にし、自動的コール・ホームを再度使用可能にしない場合: **chhmc -c emch -s disable --callhome disable**

HMC が、この環境に配置されている他の HMC と通信できることを確認してください。「コール・ホーム用イベント・マネージャー」には、HMC の登録時のテスト接続機能が備わっています。

HMC を「コール・ホーム用イベント・マネージャー」に登録することができます。HMC を登録すると、イベント・マネージャーは、その登録された HMC に、IBM にコール・ホームされるのを待機しているイベントがないか照会します。イベント・マネージャーは、どのようなデータが IBM に送り戻されようとしているのかを示し、それらのイベントを承認します。イベント・マネージャーは、承認後、コール・ホーム操作を続行できることを、登録済み HMC に通知します。

「コール・ホーム用イベント・マネージャー」タスクは、いずれの HMC からでも、あるいは複数の HMC からでも実行することができます。管理コンソールを「コール・ホーム用イベント・マネージャー」タスクに登録するには、以下の手順を実行してください。



1. ナビゲーション領域で、「保守容易性」アイコン  をクリックしてから、「コール・ホーム用イベント・マネージャー」を選択します。
2. 「コール・ホーム用イベント・マネージャー」ペインから、「コンソールの管理」をクリックします。
3. 「登録済みコンソールの管理 (Manage Registered Consoles)」ウィンドウから、「コンソールの追加 (Add Console)」をクリックして、管理コンソールを「コール・ホーム用イベント・マネージャー」タスクに登録します。
4. 「了解」をクリックして、登録済み管理コンソールのリストへの変更をコミットします。

注: 「コール・ホーム用イベント・マネージャー」は、イベント・マネージャー・モードが使用不可に設定された状態で使用できます。引き続き、HMC を登録し、イベント・マネージャーでイベントを表示することはできますが、イベント・マネージャーは、イベントがいつコール・ホームされるかを制御しません。

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、「ユーザーおよびセキュリティー」アイコン



をクリックしてから、「ユーザーおよびロール」を選択します。

2. 「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。
3. 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 IP アドレスの選択 (Select a Service Processor IP Address)」を選択して、「了解」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」アイコン をクリックしてから、「コンソール設定」を選択します。

2. コンテンツ・ペインで、「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。詳しくは、論理区画化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、79 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、99 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) にマウントされたりリモート・システム
- FTP を介したりリモート・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**」 > 「コンソール管理」 > 「メディアのフォーマット」をクリックして、手順に従います。

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**」アイコン をクリックしてから、「コンソール管理」を選択します。
2. 「コンテンツ」ペインで、「管理コンソール・データのバックアップ (**Backup Managment Console Data**)」をクリックします。
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ます、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**」 > 「コンソール設定 (**Console Settings**)」 > 「ネットワーク設定の変更」 > 「**LAN** アダプター」をクリックします。
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、105 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、「**HMC 管理**」アイコンをクリックしてから、「コンソール管理」を選択します。
2. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (**Update the Hardware Management Console**)」をクリックします。
3. 新規ウィンドウの「現行 HMC ドライバー情報」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、「保守容易」アイコンをクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「アウトバウンド接続の管理 (**Manage Outbound Connectivity**)」をクリックします。
3. 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、「HMC 管理」アイコンをクリックしてから、「コンソール管理」を選択します。
2. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (Update the Hardware Management Console)」をクリックします。
3. 新規ウィンドウの「現行 HMC ドライバー情報」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。
4. 『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、120 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、次のステップを続行します。



2. ナビゲーション領域で、「HMC 管理」アイコンをクリックしてから、「コンソール管理」を選択します。
3. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (Update the Hardware Management Console)」をクリックします。「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、「HMC 管理」アイコン をクリックしてから、「コンソール管理」を選択します。
2. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (Update the Hardware Management Console)」をクリックします。
3. 新規ウィンドウの「現行 HMC ドライバー情報」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。
4. 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。
5. 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、以下のステップを実行します。
 - 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、「HMC 管理」アイコン をクリックしてから、「コンソール管理」を選択します。
2. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (Update the Hardware Management Console)」をクリックします。
3. 新規ウィンドウの「現行 HMC ドライバー情報」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。
4. 『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. 181 ページの『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、120 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・デバイスを手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. 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、120 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、次のステップを続行します。



4. ナビゲーション領域で、「HMC 管理」アイコン をクリックしてから、「コンソール管理」を選択します。
5. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (Update the Hardware Management Console)」をクリックします。「修正サービスのインストール」ウィザードが開きます。
6. ウィザードの指示に従って、更新をインストールする。
7. 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。

- 『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。



- ナビゲーション領域で、「HMC 管理」アイコンをクリックしてから、「コンソール管理」を選択します。
- コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (Update the Hardware Management Console)」をクリックします。
- 新規ウィンドウの「現行 HMC ドライバー情報」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。
- 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。
- 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、以下のステップを実行します。
 - 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。
 - 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。

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。

- 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。
- 「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。
- アップグレードする HMC バージョンへナビゲートする。
- 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。

- 表示されるプロンプトのとおり行って、注文を送信する。
- 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、「**HMC 管理**」アイコンをクリックしてから、「コンソール管理」を選択します。ナビゲーション領域で「更新」をクリックします。
2. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (**Update the Hardware Management Console**)」をクリックします。
3. 新規ウィンドウの「現行 HMC ドライバー情報」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。
4. 『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」を選択します。
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. 「了解」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、「保守容易」アイコンをクリックしてから、「サービス管理」を選択します。
- c. コンテンツ・ペインで、「メディアのフォーマット」をクリックします。
- 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. 「了解」をクリックします。



2. ナビゲーション領域で、「**HMC 管理**」アイコンをクリックしてから、「**コンソール管理**」を選択します。
3. 「コンテンツ」ペインで、「**管理コンソール・データのバックアップ (Backup Management Console Data)**」をクリックします。「**管理コンソール・データのバックアップ (Backup Management Console Data)**」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、「**マウントされたりリモート・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、「**HMC 管理**」 > 「**コンソール管理**」と開きます。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**」 > 「**コンソール管理**」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. 「**スケジュール操作**」ウィンドウを閉じる
 - d. スケジュール操作ごとに繰り返す。
6. 「**スケジュール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」アイコン をクリックしてから、「コンソール管理」を選択します。
2. コンテンツ・ペインで、「アップグレード・データの保管」をクリックします。「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. 「了解」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. ナビゲーション領域で、「HMC 管理」アイコン をクリックしてから、「コンソール管理」を選択します。
3. コンテンツ・ペインで、「管理コンソールのシャットダウンまたは再始動 (Shutdown or Restart the Management Console)」を選択する。
4. 必ず、「HMC の再始動 (Restart the HMC)」を選択する。

5. 「了解」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、「HMC 管理」アイコン をクリックしてから、「コンソール管理」を選択します。
2. コンテンツ・ペインで、「ハードウェア管理コンソールの更新 (**Update the Hardware Management Console**)」をクリックします。
3. 新規ウィンドウの「現行 HMC ドライバー情報」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。
4. 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。
5. 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。

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。

- `img2a`
- `img3a`
- `base.img`
- `disk1.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。

モデル 8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置

以下の図と表を使用して、8247-21L、8247-22L、8284-21A、または 8284-22A 上の HMC ポートを対応させます。

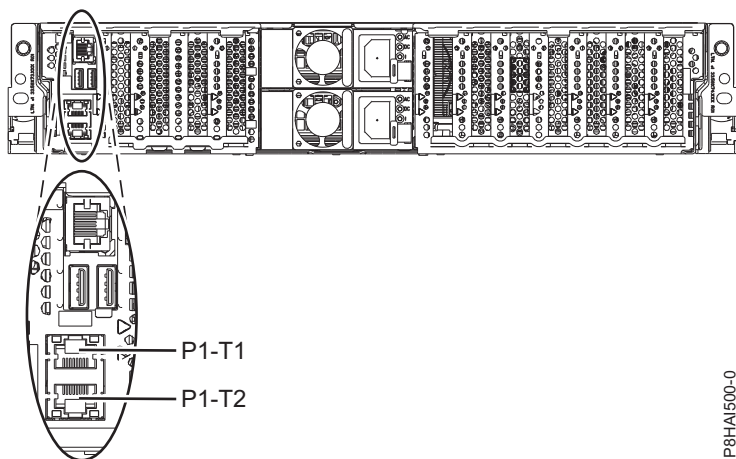


図 85. 8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置

表 57. 8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-T1	いいえ
HMC ポート 2	Un-P1-T2	いいえ

8247-21L、8247-22L、8284-21A、または 8284-22A の HMC ポート位置について詳しくは、n and location codes for 8247-21L、8247-22L、または 8284-22A の部品の位置およびロケーション・コードを参照してください。

モデル 8247-42L、8286-41A、または 8286-42A の HMC ポート位置

以下の図と表を使用して、8247-42L、8286-41A、または 8286-42A 上の HMC ポートの位置を対応させます。

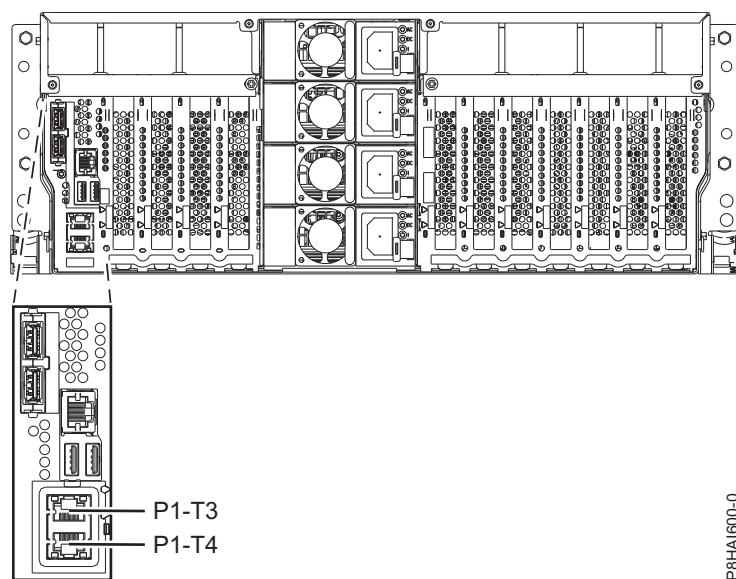


図 86. ラック図 - 8247-42L、8286-41A、または 8286-42A の HMC ポート位置

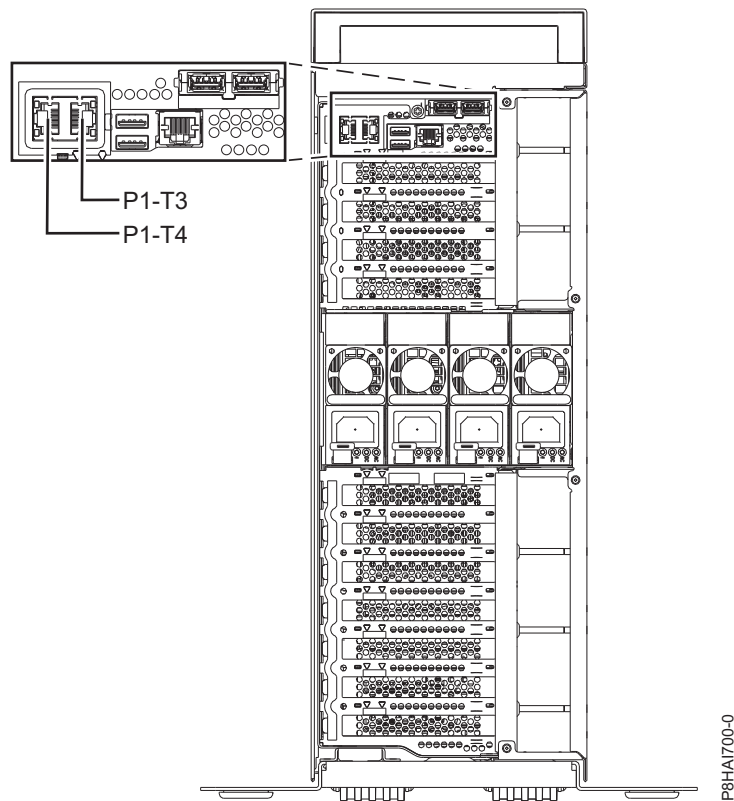


図 87. タワー図の 8286-41A HMC ポート位置

表 58. 8247-42L、8286-41A、または 8286-42A の HMC ポート位置

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
8247-42L、8286-41A、または 8286-42A 上の HMC ポート位置について詳しくは、『Part location and location codes for 8247-42L, 8286-41A, or 8286-42A』を参照してください。		

モデル 9080-MHE、9080-MME、9119-MHE、および 9119-MME の HMC ポート位置

以下の図と表を使用して、9080-MHE、9080-MME、9119-MHE、および 9119-MME 上に HMC ポートをマップします。

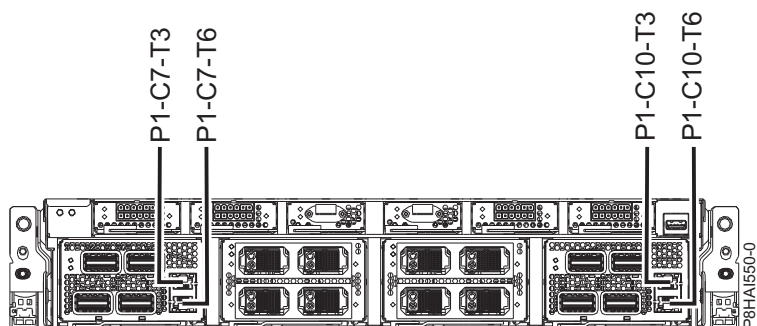


図 88. 9080-MHE、9080-MME、9119-MHE、および 9119-MME の HMC ポート位置

表 59. 9080-MHE、9080-MME、9119-MHE、および 9119-MME の HMC ポート位置

ポート	物理ロケーション・コード	識別 LED
サービス・プロセッサ・カード 1 - HMC ポート 1	Un-P1-C7-T3	いいえ
サービス・プロセッサ・カード 1 - HMC ポート 2	Un-P1-C7-T6	いいえ
サービス・プロセッサ・カード 2 - HMC ポート 1	Un-P1-C10-T3	いいえ
サービス・プロセッサ・カード 2 - HMC ポート 2	Un-P1-C10-T6	いいえ
9080-MHE、9080-MME、9119-MHE、および 9119-MME 上の HMC ポート位置について詳しくは、『部品の位置と、9080-MHE、9080-MME、9119-MHE、または 9119-MME の位置のロケーション・コード』を参照してください。		

モデル 8408-44E および 8408-E8E の HMC ポート位置

以下の図と表を使用して、8408-44E および 8408-E8E 上の HMC ポートを対応させます。

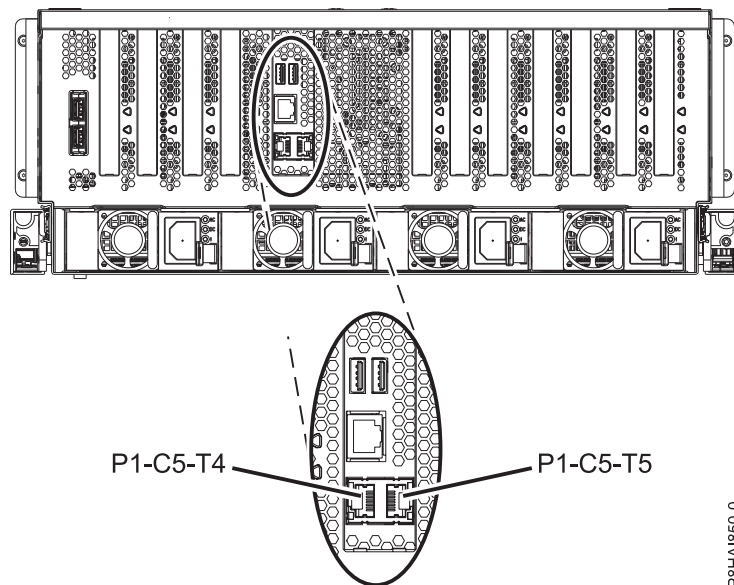


図 89. 8408-44E および 8408-E8E の HMC ポート位置

表 60. 8408-44E および 8408-E8E の HMC ポート位置

ポート	物理ロケーション・コード	識別 LED
HMC ポート 1	Un-P1-C5-T4	いいえ
HMC ポート 2	Un-P1-C5-T5	いいえ
8408-44E および 8408-E8E 上の HMC ポート位置について詳しくは、部品の位置と、8404-44E および 8408-E8E の位置のロケーション・コード (Part location and location codes for 8408-44E and 8408-E8E location)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、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

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

〒103-8510

東京都中央区日本橋箱崎町19番21号

日本アイ・ビー・エム株式会社

法務・知的財産

知的財産権ライセンス渉外

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

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

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

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

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

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

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

表示されている IBM の価格は IBM 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、類似する個人や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、IBM 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なりません。

IBM は、示されている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、IBM は何ら保証責任を負いません。

IBM 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、この危険性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 IBM の Web サイトをチェックする必要があります。

通信規制の注記

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

本製品は、電気通信事業者の通信回線との責任分界点への、直接的な接続を想定した認定取得作業を行っていません。そのような接続を行うには、電気通信事業者による事前検査等が必要となる場合があります。ご不明な点については、IBM 担当員または販売店にお問い合わせください。

IBM Power Systems サーバーのアクセシビリティ機能

アクセシビリティ機能は、運動障害または視覚障害など身体に障害を持つユーザーが情報技術コンテンツを快適に使用できるようにサポートします。

概説

IBM Power Systems サーバーには、次の主なアクセシビリティ機能が組み込まれています。

- キーボードのみによる操作
- スクリーン・リーダーを使用する操作

IBM Power Systems サーバーでは、最新の W3C 標準 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) が US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-

section-508-standards/section-508-standards) および Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) に準拠するように使用されています。アクセシビリティ機能を利用するためには、最新リリースのスクリーン・リーダーに加えて、IBM Power Systems サーバーでサポートされている最新の Web ブラウザーを使用してください。

IBM Knowledge Center に用意されている IBM Power Systems サーバーのオンライン製品資料は、アクセシビリティに対応しています。IBM Knowledge Center のアクセシビリティ機能は、IBM Knowledge Center のヘルプの『アクセシビリティ』セクション (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility)で説明されています。

キーボード・ナビゲーション

この製品では、標準ナビゲーション・キーが使用されています。

インターフェース情報

IBM Power Systems サーバーのユーザー・インターフェースには、1 秒当たり 2 回から 55 回明滅するコンテンツはありません。

IBM Power Systems サーバーの Web ユーザー・インターフェースは、コンテンツの適切なレンダリング、および使用可能なエクスペリエンスの提供を、カスケード・スタイル・シートに依存しています。アプリケーションは、視覚障害者が、ハイコントラスト・モードを含め、システム表示形式の設定を使用するために同等の仕組みを提供します。フォント・サイズの制御は、デバイスまたは Web ブラウザーの設定を使用して行うことができます。

IBM Power Systems サーバーの Web ユーザー・インターフェースには、アプリケーションの機能領域に迅速にナビゲートできる WAI-ARIA ナビゲーション・ランドマークが組み込まれています。

ベンダー・ソフトウェア

IBM Power Systems サーバーには、IBM の使用許諾契約書の適用外である特定のベンダー・ソフトウェアが組み込まれています。IBM では、それら製品のアクセシビリティ機能については、何ら保証責任を負いません。ベンダーの製品に関するアクセシビリティ情報については、該当のベンダーにお問い合わせください。

関連したアクセシビリティ情報

標準の IBM ヘルプ・デスクおよびサポートの各 Web サイトに加え、IBM では、聴覚障害を持つユーザーまたは聴覚機能が低下しているユーザーが販売サービスやサポート・サービスにアクセスするのに使用できる TTY 電話サービスを用意しています。

TTY サービス

800-IBM-3383 (800-426-3383)

(北アメリカ内)

アクセシビリティに対する IBM の取り組みについて詳しくは、IBM アクセシビリティ (www.ibm.com/able) を参照してください。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品（「ソフトウェア・オフアリング」）では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie をはじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オフアリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オフアリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オフアリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オフアリングは、展開される構成に応じて、セッション管理の目的のために、それぞれのお客様のユーザー名と IP アドレスを、セッション Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オフアリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』<http://www.ibm.com/privacy/details/jp/ja/> の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(<http://www.ibm.com/software/info/product-privacy>) を参照してください。

商標

IBM、IBM ロゴおよび [ibm.com](http://www.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。

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

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

電波障害規制特記事項

モニターを装置に取り付ける場合は、モニターと一緒に提供された指定のモニター・ケーブルおよび電波障害抑制装置を使用してください。

クラス A 表示

以下のクラス A 表示は、POWER8 プロセッサを搭載した IBM サーバーおよびそのフィーチャーに適用されます。ただし、フィーチャー情報で電磁適合性 (EMC) クラス B として指定されている場合は除きます。

Federal Communications Commission (FCC) Statement

Attention: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide

reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

CAN ICES-3 (A)/NMB-3(A)

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

European Community contact:

IBM Deutschland GmbH

Technical Regulations, Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

Tel: +49 800 225 5426

email: halloibm@de.ibm.com

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

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

以下は、上記枠内に示されている一般財団法人 VCCI 協会表示を要約したものです。

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

一般社団法人 電子情報技術産業協会 (JEITA) 表示

この表示は、日本工業規格 JIS C 61000-3-2 機器のワット数準拠について説明します。

**(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値: Knowledge Center の各製品の
仕様ページ参照**

この表示は、1 相当たり 20 A 以下の機器に関する一般社団法人 電子情報技術産業協会 (JEITA) 表示について説明します。

高調波電流規格 JIS C 61000-3-2 適合品

この表示は、20 A より大きい (単相) 機器に関する JEITA 表示について説明します。

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器 (高調波発生機器) です。

- ・回路分類: 6 (単相、PFC回路付)
- ・換算係数: 0

この表示は、20 A より大きい (3 相) 機器に関する JEITA 表示について説明します。

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器 (高調波発生機器) です。

- ・回路分類: 5 (3 相、PFC回路付)
- ・換算係数: 0

Electromagnetic Interference (EMI) Statement - People's Republic of China

声 明

此为 A 级产品,在生活环境中,
该产品可能会造成无线电干扰。
在这种情况下,可能需要用户对其
干扰采取切实可行的措施。

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

Electromagnetic Interference (EMI) Statement - Taiwan

警告使用者：

這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

The following is a summary of the EMI Taiwan statement above.

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

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서
가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur
Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55022 / EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
email: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

クラス B 表示

以下のクラス B 表示は、フィーチャー取り付け情報で電磁適合性 (EMC) クラス B として指定されているフィーチャーに適用されます。

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

CAN ICES-3 (B)/NMB-3(B)

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

European Community contact:

IBM Deutschland GmbH

Technical Regulations, Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

Tel: +49 800 225 5426

email: halloibm@de.ibm.com

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

一般社団法人 電子情報技術産業協会 (JEITA) 表示

この表示は、日本工業規格 JIS C 61000-3-2 機器のワット数準拠について説明します。

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値: Knowledge Center の各製品の
仕様ページ参照

この表示は、1 相当たり 20 A 以下の機器に関する一般社団法人 電子情報技術産業協会 (JEITA) 表示について説明します。

高調波電流規格 JIS C 61000-3-2 適合品

この表示は、20 A より大きい (单相) 機器に関する JEITA 表示について説明します。

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- ・回路分類：6（単相、PFC回路付）
- ・換算係数：0

この表示は、20 A より大きい (3 相) 機器に関する JEITA 表示について説明します。

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- ・回路分類：5（3 相、PFC回路付）
- ・換算係数：0

IBM Taiwan Contact Information

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.

New Orchard Road

Armonk, New York 10504

Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH

Technical Relations Europe, Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

Tel: +49 (0) 800 225 5426

email: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022/ EN 55032 Klasse 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を提供され、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